



User Guide for the Cisco Application Networking Manager 2.0

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Customer Order Number:
Text Part Number: OL-17628-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

User Guide for the Cisco Application Networking Manager 2.0
© 2008 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface ix

Audience ix

Organization ix

Conventions x

Open-Source Software Included in the Cisco Application Networking Manager xi

Obtaining Documentation and Submitting a Service Request xi

CHAPTER 1

Cisco Application Networking Manager Overview 1-1

Cisco Application Networking Manager New Features 1-1

Logging Into the Cisco Application Networking Manager 1-2

Changing Your Account Password 1-4

Understanding ANM Licenses 1-4

ANM Interface Overview 1-5

Understanding ANM Screens and Menus 1-6

Understanding ANM Buttons 1-9

Conventions in Tables 1-11

Customizing Tables 1-11

Using the Advanced Editing Option 1-13

ANM Screen Conventions 1-14

Understanding Cisco Application Networking Manager Terminology 1-15

CHAPTER 2

Adding and Managing Devices 2-1

Device Management Overview 2-2

Device Import Overview 2-3

Preparing Devices for Import 2-4

Enabling SSH or Telnet Access on Cisco Catalyst 6K and 7600 Chassis 2-5

Enabling SSH Access and HTTPS Interface on ACE Module and ACE Appliance 2-5

Enabling SNMP Polling from ANM 2-6

Adding Network Devices into ANM 2-7

Adding Devices to ANM 2-8

Adding ACE Modules to ANM 2-11

Importing Cisco Content Switching Module (CSM) Devices 2-13

Importing Cisco Global Site Selector (GSS) Devices 2-14

GSS Firewall Deployment Overview	2-15
Enabling Syslog Messages from the ACE	2-15
Discovering Large Numbers of Devices	2-16
Preparing Devices for IP Discovery	2-17
Configuring Device Access Credentials	2-17
Modifying Credential Pools	2-19
Running Discovery to Identify Devices	2-20
Monitoring Device Discovery Status	2-21
Configuring Devices	2-22
Configuring CSM Primary Attributes	2-23
Configuring CSS Primary Attributes	2-24
Configuring GSS Primary Attributes	2-25
Configuring Cisco Catalyst Chassis and 7600 Series Router Primary Attributes	2-26
Configuring Device Static Routes	2-27
Viewing and Configuring Device Interfaces	2-28
Configuring Access Ports	2-29
Configuring Trunk Ports	2-30
Configuring Switch Virtual Interfaces	2-32
Configuring Routed Ports	2-33
Viewing All Ports	2-34
Managing Device VLANs	2-35
Adding Device VLANs	2-35
Viewing All Device VLANs	2-36
Configuring Device Layer 2 VLANs	2-37
Configuring Device Layer 3 VLANs	2-38
Modifying Device VLANs	2-38
Creating VLAN Groups	2-39
Configuring Device Role-Based Access Controls	2-40
Configuring Device RBAC Users	2-40
Guidelines for Managing Users	2-40
Displaying a List of Device Users	2-41
Configuring Device User Accounts	2-41
Modifying Device User Accounts	2-42
Deleting Device User Accounts	2-43
Configuring Device RBAC Roles	2-43
Guidelines for Managing User Roles	2-44
Role Mapping in Device RBAC	2-44
Configuring Device User Roles	2-45
Modifying Device User Roles	2-46

Deleting Device User Roles	2-47
Adding, Editing, or Deleting Rules	2-47
Configuring Device RBAC Domains	2-48
Guidelines for Managing Domains	2-48
Displaying Domains for a Device	2-48
Configuring Device Domains	2-49
Modifying Device Domains	2-51
Deleting Device Domains	2-51
Managing Devices	2-52
Synchronizing Device Configurations	2-52
Synchronizing Chassis Configurations	2-52
Synchronizing Module Configurations	2-53
Configuring User-Defined Groups	2-54
Adding a User-Defined Group	2-54
Modifying a User-Defined Group	2-55
Duplicating a User-Defined Group	2-56
Deleting a User-Defined Group	2-56
Updating Chassis Passwords	2-57
Changing ACE Module Passwords	2-58
Restarting Device Polling	2-59
Viewing All Devices	2-60
Viewing Modules by Chassis	2-61
Removing Modules from the ANM Database	2-62

CHAPTER 3

Configuring Virtual Contexts 3-1

Using Virtual Contexts	3-1
Creating Virtual Contexts	3-2
Configuring Virtual Contexts	3-5
Configuring Virtual Context System Attributes	3-11
Configuring Virtual Context Primary Attributes	3-11
Configuring Virtual Context Syslog Settings	3-12
Configuring Syslog Log Hosts	3-16
Configuring Syslog Log Messages	3-17
Configuring Syslog Log Rate Limits	3-18
Configuring SNMP for Virtual Contexts	3-19
Configuring SNMP Version 2c Communities	3-20
Configuring SNMP Version 3 Users	3-21
Configuring SNMP Trap Destination Hosts	3-23
Configuring SNMP Notification	3-24

Configuring Virtual Context Global Traffic Policies	3-26
Managing ACE Licenses	3-27
Viewing ACE Licenses	3-27
Importing ACE Licenses	3-28
Installing ACE Licenses	3-29
Uninstalling ACE Licenses	3-30
Updating ACE Licenses	3-31
Displaying License Configuration and Statistics	3-32
Using Resource Classes	3-32
Global and Local Resource Classes	3-33
Resource Allocation Constraints	3-34
Using Global Resource Classes	3-35
Configuring Global Resource Classes	3-36
Deploying Global Resource Classes	3-37
Auditing Resource Classes	3-38
Modifying Global Resource Classes	3-39
Deleting Global Resource Classes	3-40
Using Local Resource Classes	3-41
Configuring Local Resource Classes	3-41
Deleting Local Resource Classes	3-42
Viewing Local Resource Class Use on Virtual Contexts	3-43
Configuring Security with ACLs	3-43
Creating ACLs	3-44
Setting Extended ACL Attributes	3-47
Resequencing Extended ACLs	3-50
Setting EtherType ACL Attributes	3-51
Configuring Object Groups	3-52
Configuring IP Addresses for Object Groups	3-53
Configuring Subnet Objects for Object Groups	3-54
Configuring Protocols for Object Groups	3-55
Configuring TCP/UDP Service Parameters for Object Groups	3-56
Configuring ICMP Service Parameters for an Object Group	3-58
Managing ACLs	3-60
Viewing All ACLs by Context	3-60
Editing or Deleting ACLs	3-61
Configuring Virtual Context Expert Options	3-62
Comparing Context and Building Block Configurations	3-62
Managing Virtual Contexts	3-63
Viewing All Virtual Contexts	3-64

Synchronizing Virtual Context Configurations	3-66
Managing Syslog Settings for Autosync	3-66
Editing Virtual Contexts	3-67
Deleting Virtual Contexts	3-68
Upgrading Virtual Contexts	3-68
Restarting Virtual Context Polling	3-69

CHAPTER 4

Configuring Virtual Servers 4-1

Load Balancing Overview	4-1
Configuring Virtual Servers	4-2
Understanding Virtual Server Configuration and ANM	4-2
Using ANM to Configure Virtual Servers	4-4
Virtual Server Configuration Procedure	4-4
Shared Objects and Virtual Servers	4-6
Virtual Server Protocols by Device Type	4-8
Configuring Virtual Server Properties	4-8
Configuring Virtual Server SSL Termination	4-12
Configuring Virtual Server Protocol Inspection	4-14
Configuring Virtual Server Layer 7 Load Balancing	4-25
Configuring Virtual Server Default Layer 7 Load Balancing	4-35
Configuring Application Acceleration and Optimization	4-37
Configuring Virtual Server NAT	4-47
Managing Virtual Servers	4-48
Deploying Virtual Servers	4-49
Viewing All Staged Virtual Servers	4-49
Modifying Deployed Virtual Servers	4-50
Modifying Staged Virtual Servers	4-50
Viewing Virtual Servers by Context	4-51
Activating Virtual Servers	4-51
Suspending Virtual Servers	4-52
Managing GSS VIP Answers	4-53
Activating and Suspending DNS Rules Governing GSS Load Balancing	4-54
Viewing Detailed Virtual Server Information	4-54
Viewing Virtual Servers	4-55
Understanding CLI Commands Sent from Virtual Server Table	4-56

CHAPTER 5

Configuring Real Servers and Server Farms 5-1

Server Load Balancing Overview	5-1
Load-Balancing Predictors	5-2

Real Servers	5-3
Server Farms	5-3
Configuring Real Servers	5-4
Managing Real Servers	5-6
Activating Real Servers	5-7
Suspending Real Servers	5-7
Modifying Real Servers	5-8
Viewing Real Servers	5-9
Understanding CLI Commands Sent from Real Server Table	5-10
Server Weight Ranges	5-12
Configuring Server Farms	5-12
Adding Real Servers to a Server Farm	5-14
Configuring the Predictor Method for Server Farms	5-16
Configuring Server Farm HTTP Return Error-Code Checking	5-21
Viewing All Server Farms	5-23
Health Monitoring	5-23
TCL Scripts	5-24
Configuring Health Monitoring for Real Servers	5-25
Configuring Probe Attributes	5-29
Configuring DNS Probe Expect Addresses	5-40
Configuring Headers for HTTP and HTTPS Probes	5-41
Configuring Health Monitoring Expect Status	5-42
Configuring an OID for SNMP Probes	5-43

CHAPTER 6

Configuring Stickiness 6-1

Stickiness Overview	6-1
Sticky Types	6-2
HTTP Content Stickiness	6-3
HTTP Cookie Stickiness	6-3
HTTP Header Stickiness	6-4
IP Netmask Stickiness	6-4
Layer 4 Payload Stickiness	6-4
RADIUS Stickiness	6-5
RTSP Header Stickiness	6-5
SIP Header Stickiness	6-5
Sticky Groups	6-6
Sticky Table	6-6
Configuring Sticky Groups	6-7

Sticky Group Attribute Tables	6-9
Viewing All Sticky Groups by Context	6-14
Configuring Sticky Statics	6-14

CHAPTER 7

Configuring Parameter Maps	7-1
Configuring Connection Parameter Maps	7-2
Configuring Generic Parameter Maps	7-7
Configuring HTTP Parameter Maps	7-8
Configuring Optimization Parameter Maps	7-10
Configuring RTSP Parameter Maps	7-17
Configuring SIP Parameter Maps	7-18
Configuring Skinny Parameter Maps	7-20
Supported MIME Types	7-21

CHAPTER 8

Configuring SSL	8-1
SSL Overview	8-1
SSL Configuration Prerequisites	8-2
Summary of SSL Configuration Steps	8-3
SSL Setup Sequence	8-4
Using SSL Certificates	8-5
Importing SSL Certificates	8-6
Using SSL Keys	8-8
Importing SSL Key Pairs	8-9
Generating SSL Key Pairs	8-11
Exporting SSL Certificates	8-12
Exporting SSL Key Pairs	8-14
Configuring SSL Parameter Maps	8-15
Configuring SSL Chain Group Parameters	8-18
Configuring SSL CSR Parameters	8-19
Generating CSRs	8-21
Configuring SSL Proxy Service	8-22
Enabling Client Authentication	8-23
Configuring SSL Authentication Groups	8-24
Configuring CRLs for Client Authentication	8-25

CHAPTER 9

Configuring Network Access 9-1

- VLAN Overview 9-1
 - ACE Module VLAN Overview 9-1
 - ACE Appliance VLAN Overview 9-2
- Configuring VLAN Interfaces 9-2
 - Viewing All VLAN Interfaces 9-6
- Configuring VLAN Interface Options 9-7
 - Configuring VLAN Interface Policy Map Use 9-7
 - Configuring VLAN Interface Access Control 9-8
 - Configuring VLAN Interface Static ARP Entries 9-9
 - Configuring VLAN Interface NAT Pools 9-10
 - Configuring VLAN Interface DHCP Relay 9-12
- Configuring Virtual Context BVI Interfaces 9-12
 - Viewing All BVI Interfaces by Context 9-14
- Configuring Virtual Context Static Routes 9-14
 - Viewing All Static Routes by Context 9-15
- Configuring Global IP DHCP 9-16
- Configuring Static VLANs for Over 8 K Static NAT Configurations 9-16
- Configuring Gigabit Ethernet Interfaces 9-17
- Configuring Port Channel Interfaces 9-21

CHAPTER 10

Configuring High Availability 10-1

- Understanding High Availability 10-1
 - Understanding High Availability Processes 10-2
 - CLI Commands for High Availability Processes 10-3
- Configuring High Availability Overview 10-4
- Configuring ACE High Availability 10-4
- Configuring ACE High Availability Peers 10-5
- Clearing High Availability Pairs 10-7
- Configuring High Availability Groups 10-8
 - Editing High Availability Groups 10-9
 - Taking a High Availability Group Out of Service 10-10
 - Enabling a High Availability Group 10-11
- Switching Over a High Availability Group 10-11
- Deleting High Availability Groups 10-12
- High Availability Tracking and Failure Detection Overview 10-13
- Tracking VLAN Interfaces for High Availability 10-13

Tracking Hosts for High Availability	10-14
Configuring Host Tracking Probes	10-15
Deleting Host Tracking Probes	10-16
Configuring Peer Host Tracking Probes	10-17
Deleting Peer Host Tracking Probes	10-18
Configuring ACE HSRP Groups	10-18
Synchronizing ACE High Availability Configurations	10-19
Synchronizing Virtual Context Configurations in High Availability Mode	10-19
Synchronizing SSL Certificate and Key Pairs on Both Peers	10-20
Understanding ACE Redundancy	10-20
ACE High Availability Polling	10-20
ACE Redundancy Protocol	10-21
ACE Stateful Failover	10-22
ACE Fault-Tolerant VLAN	10-23
ACE Configuration Synchronization	10-23
ACE Redundancy Configuration Requirements and Restrictions	10-24

CHAPTER 11

Configuring Traffic Policies 11-1

Traffic Policy Overview	11-1
Class Map and Policy Map Overview	11-2
Class Maps	11-3
Policy Maps	11-4
Parameter Maps and Their Use in Layer 3 and Layer 4 Policy Maps	11-5
Protocol Inspection Overview	11-5
Configuring Virtual Context Class Maps	11-6
Deleting Class Maps	11-8
Setting Match Conditions for Class Maps	11-8
Setting Match Conditions for Layer 3/Layer 4 Network Traffic Class Maps	11-9
Setting Match Conditions for Layer 3/Layer 4 Management Traffic Class Maps	11-12
Setting Match Conditions for Layer 7 Server Load Balancing Class Maps	11-13
Setting Match Conditions for Layer 7 HTTP Deep Packet Inspection Class Maps	11-15
Setting Match Conditions for Layer 7 FTP Command Inspection Class Maps	11-21
Setting Match Conditions for Generic Server Load Balancing Class Maps	11-22
Setting Match Conditions for RADIUS Server Load Balancing Class Maps	11-23
Setting Match Conditions for RTSP Server Load Balancing Class Maps	11-25
Setting Match Conditions for SIP Server Load Balancing Class Maps	11-27
Setting Match Conditions for Layer 7 SIP Deep Packet Inspection Class Maps	11-28
Configuring Virtual Context Policy Maps	11-30

Configuring Rules and Actions for Policy Maps	11-33
Setting Policy Map Rules and Actions for Generic Server Load Balancing	11-34
Setting Policy Map Rules and Actions for Layer 3/Layer 4 Management Traffic	11-37
Setting Policy Map Rules and Actions for Layer 3/Layer 4 Network Traffic	11-38
Setting Policy Map Rules and Actions for Layer 7 FTP Command Inspection	11-45
Setting Policy Map Rules and Actions for Layer 7 HTTP Deep Packet Inspection	11-47
Setting Policy Map Rules and Actions for Layer 7 HTTP Optimization	11-53
Setting Policy Map Rules and Actions for Layer 7 Server Load-Balancing Traffic	11-56
Setting Policy Map Rules and Actions for Layer 7 SIP Deep Packet Inspection	11-62
Setting Policy Map Rules and Actions for Layer 7 Skinny Deep Packet Inspection	11-64
Setting Policy Map Rules and Actions for RADIUS Server Load Balancing	11-66
Setting Policy Map Rules and Actions for RDP Server Load Balancing	11-68
Setting Policy Map Rules and Actions for RTSP Server Load Balancing	11-70
Setting Policy Map Rules and Actions for SIP Server Load Balancing	11-73
Special Characters for Matching String Expressions	11-76

CHAPTER 12

Configuring Application Acceleration and Optimization 12-1

Optimization Overview	12-1
Optimization Traffic Policies and Typical Configuration Flow	12-2
Configuring Action Lists for Application Acceleration and Optimization	12-3
Configuring Action Lists for ACE 2.0 Modules and ACE 4710 A3(1.0) Appliances	12-3
Configuring Action Lists for ACE Appliances	12-6
Configuring Pattern Replacements	12-10
Configuring Optimization Parameter Maps	12-12
Configuring Traffic Policies for HTTP Optimization	12-13
Enabling HTTP Optimization Using Virtual Servers	12-16
Configuring Global Application Acceleration and Optimization	12-16

CHAPTER 13

Using Configuration Building Blocks 13-1

Building Block Versions and Tagging	13-4
Creating Building Blocks	13-5
Extracting Building Blocks from Virtual Contexts	13-5
Configuring Building Blocks	13-6
Configuring Building Block Primary Attributes	13-7
Tagging Building Blocks	13-7
Applying Building Blocks	13-8
Applying a Building Block to a Single Virtual Context	13-8
Applying a Building Block to Multiple Virtual Contexts	13-9

Viewing Building Block Use 13-9

CHAPTER 14

Monitoring Your Network 14-1

Setting Up Devices for Monitoring 14-2

Device Monitoring Features 14-2

Monitoring Device Groups 14-3

Monitoring Devices 14-4

Monitoring the System 14-5

Monitoring Resource Usage 14-5

Monitoring Virtual Context Resource Usage 14-6

Monitoring System Traffic Resource Usage 14-7

Monitoring System Non-Connection Based Resource Usage 14-8

Monitoring Traffic 14-9

Viewing Device-Specific Traffic Data 14-11

Monitoring Load Balancing on Virtual Servers 14-12

Viewing Real Server Statistics 14-13

Viewing Probes Statistics 14-15

Monitoring Load Balancing Statistics 14-15

Monitoring Application Acceleration 14-17

Setting Polling Parameters 14-19

Enabling Polling on Specific Devices 14-19

Disabling Polling on Specific Devices 14-19

Enabling Polling on All Devices 14-20

Disabling Polling on All Devices 14-20

Monitoring Events 14-21

Device Audit Trail Logging 14-23

Configuring Alarm Notifications 14-25

Viewing Alarm Notifications 14-30

Viewing Alarms in ANM 14-30

Adding Notes to Alarms 14-31

Viewing E-mail Notifications 14-31

Viewing Traps 14-32

Configuring SMTP for E-mail Notifications 14-32

Testing Connectivity 14-33

CHAPTER 15

Administering the Cisco Application Networking Manager 15-1

Overview of the Admin Function 15-2

Controlling Access to the Cisco ANM	15-2
Types of Users	15-5
Understanding Roles	15-5
Understanding Operations Privileges	15-6
Understanding Domains	15-7
Understanding Organizations	15-7
How ANM Handles Role-Based Access Control	15-7
Configuring User Authentication	15-31
Guidelines for Managing Organizations	15-32
Changing Authentication Server Passwords	15-35
Changing the Admin Password	15-35
Modifying Organizations	15-35
Duplicating an Organization	15-36
Displaying Authentication Server Organizations	15-37
Deleting Organizations	15-37
Managing User Accounts	15-38
Guidelines for Managing User Accounts	15-38
Displaying a List of Users	15-38
Creating User Accounts	15-39
Duplicating a User Account	15-40
Modifying User Accounts	15-41
Deleting User Accounts	15-42
Displaying or Terminating Current User Sessions	15-42
Managing User Roles	15-43
Guidelines for Managing User Roles	15-43
Understanding Predefined Roles	15-44
Displaying User Role Relationships	15-45
Displaying User Roles	15-46
Creating User Roles	15-46
Duplicating a User Role	15-47
Modifying User Roles	15-48
Deleting User Roles	15-48
Managing Domains	15-49
Guidelines for Managing Domains	15-49
Displaying Network Domains	15-50
Creating a Domain	15-50
Duplicating a Domain	15-51
Modifying a Domain	15-52
Deleting a Domain	15-52

Managing ANM	15-54
Checking the Status of the ANM Server	15-54
Managing ANM Licenses	15-56
Understanding ANM License Information	15-57
Adding Licenses into License Management	15-58
Viewing Licenses in License Management	15-59
Checking on License Compliance	15-60
Ordering ANM Licenses	15-61
Removing Licenses Files	15-61
Viewing ANM Server Statistics	15-62
Configuring ANM Statistics Collection	15-63
Configuring Audit Log Settings	15-63
Viewing Change Audit Logs	15-64
Configuring Auto Sync Settings	15-65
Lifeline Management	15-65

CHAPTER 16
Troubleshooting Cisco Application Networking Manager Problems 16-1

Changing Configuration Property Values	16-1
Discovering and Adding a Device Does Not Work	16-3
Using Lifeline	16-3
Guidelines for Using Lifeline	16-4
Creating a Lifeline Package	16-4
Downloading a Lifeline Package	16-5
Adding a Lifeline Package	16-6
Deleting a Lifeline Package	16-7
Backing Up and Restoring Data	16-7
Backing Up Data	16-7
Restoring Data	16-8

APPENDIX A
ANM Ports Reference A-1

TCP Ports Used by ANM Processes	A-1
UDP Ports Used by ANM	A-2

GLOSSARY

INDEX



Draft - CISCO CONFIDENTIAL

Preface

Revised Date: 3/25/09

This guide describes the Cisco Application Networking Manager and explains how to use it to manage your network.

This preface provides information about using this guide. The topics include:

- [Audience, page ix](#)
- [Organization, page ix](#)
- [Conventions, page x](#)
- [Open-Source Software Included in the Cisco Application Networking Manager, page xi](#)
- [Obtaining Documentation and Submitting a Service Request, page xi](#)

Audience

This guide is intended for experienced system and network administrators. Depending on the configuration required, readers should have specific knowledge in the following areas:

- Networking and data communications
- Network security
- Router configuration

Organization

This documentation contains the following sections:

- [Chapter 1, “Cisco Application Networking Manager Overview”](#) summaries key features and provides an look into some general topics such as the interface.
- [Chapter 2, “Adding and Managing Devices”](#) describes how to add and manage your supported network devices.
- [Chapter 3, “Configuring Virtual Contexts”](#) describes how to configure virtual contexts on the ACE so that you can effectively and efficiently manage and allocate resources, users, and services.
- [Chapter 4, “Configuring Virtual Servers”](#) contains procedures for configuring virtual servers for load balancing on the ACE.

Draft - CISCO CONFIDENTIAL

- [Chapter 5, “Configuring Real Servers and Server Farms”](#) provides an overview of server load balancing and procedures for configuring real servers and server farms for load balancing on the ACE.
- [Chapter 6, “Configuring Stickiness”](#) provides information about sticky behavior and procedures for configuring stickiness with the ANM.
- [Chapter 7, “Configuring Parameter Maps”](#) describes how to configure parameter maps so that the ACE can perform actions on incoming traffic based on certain criteria, such as protocol or connection attributes.
- [Chapter 8, “Configuring SSL”](#) describes how to configure your ACE (both the ACE module and the ACE appliance) as a virtual Secure Sockets Layer (SSL) server for SSL initiation or termination.
- [Chapter 9, “Configuring Network Access”](#) describes how to configure network access using ANM.
- [Chapter 10, “Configuring High Availability”](#) describes how to configure redundancy to ensure that your network remains operational even if one of the ACE devices becomes unresponsive.
- [Chapter 11, “Configuring Traffic Policies”](#) describes how to configure class maps and policy maps to provide a global level of filtering traffic received by or passing through the ACE.
- [Chapter 12, “Configuring Application Acceleration and Optimization”](#) describes how to configure application acceleration and optimization options on the ACE.
- [Chapter 13, “Using Configuration Building Blocks”](#) provides an overview of configuration building blocks and describes how to configure them, tag them for version control, and apply them to virtual contexts.
- [Chapter 14, “Monitoring Your Network”](#) describes the ANM monitoring functions and explains how to configure thresholds and configure alarm notifications.
- [Chapter 15, “Administering the Cisco Application Networking Manager”](#) describes how to administer, maintain, and manage the ANM management system.
- [Chapter 16, “Troubleshooting Cisco Application Networking Manager Problems”](#) describes some procedures and tips on common troubleshooting scenarios.
- [Appendix A, “ANM Ports Reference”](#) identifies the TCP and UDP ports used by the ANM as well as well-known TCP and UDP port numbers and key words.
- [Glossary](#)

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	boldface font
Variables for which you supply values	<i>italic</i> font
Displayed session and system information	<code>screen</code> font
Information you enter	boldface screen font
Variables you enter	<i>italic screen</i> font
Menu items and button names	boldface font

Item	Convention
Selecting a menu item in paragraphs	Option > Network Preferences
Selecting a menu item in tables	Option > Network Preferences

**Note**

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

**Caution**

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Open-Source Software Included in the Cisco Application Networking Manager

- The Cisco Application Networking Manager includes the following open-source software, which is covered by the Apache 2.0 license (<http://www.apache.org/>): Ant, Avalon Logkit, Commons, Ehcache, Jetty, Log4J, Oro, Commons_Logging, Xmlrpc.
- The Cisco Application Networking Manager includes the following open-source software, which is covered by The Legion of the Bouncy Castle (<http://www.bouncycastle.org/licence.html>) license: BouncyCastle.
- The Cisco Application Networking Manager includes the following open-source software, which is covered by the GNU Lesser General Public License Version 2.1 (<http://www.gnu.org/licenses/lgpl.html>): c3p0-0.9.0.2.jar, Enterprise DT, Jasperreports 1.2, Jcommon 1.2, Jfreechart 1.0.1
- The Cisco Application Networking Manager includes the following open-source software, which is covered by the Mozilla Public License Version 1.1 (<http://www.mozilla.org/MPL/MPL-1.1.html>): Itext 1.4.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Draft - CISCO CONFIDENTIAL



Draft - CISCO CONFIDENTIAL

CHAPTER 1

Cisco Application Networking Manager Overview

Revised Date: 3/25/09

The Cisco Application Networking Manager (ANM) is a networking management application that manages Cisco Application Control Engine (ACE) modules or appliances in your networking environment.

The following topics introduce you to ANM:

- [Cisco Application Networking Manager New Features, page 1-1](#)
- [Logging Into the Cisco Application Networking Manager, page 1-2](#)
- [Changing Your Account Password, page 1-4](#)
- [Understanding ANM Licenses, page 1-4](#)
- [ANM Interface Overview, page 1-5](#)
- [Understanding Cisco Application Networking Manager Terminology, page 1-15](#)

Cisco Application Networking Manager New Features

ANM 2.0 provides the following new features and enhanced hardware support as noted:

- Support for Cisco ACE appliance software release version 3.1—Support for Cisco ACE 4710 device running software release 3.1.
- Support for Cisco ACE Global Site Selector (GSS) version 3.0 (2) including the following:
 - Support beginning with software release version 3.0 (2).
 - GSSM discovery for answers, answer groups, and DNS rules.
 - Activate/suspend answers and DNS rules.
 - On demand retrieval and display of answer operational status and hit information.
 - On demand retrieval and display of DNS hit information.
- SSL Enhancements including the following:
 - Provisioning workflow to set up keys, certificates, proxy, and generate certificate signing requests (CSRs).
 - Track and notification of SSL certificate expiration including threshold settings and alarm notification.

Draft - CISCO CONFIDENTIAL

- Certificate/Key association view across managed devices as permitted by ANM role based access control (RBAC).
- Option to import certificate/key on HA pair.
- Appropriate error messaging when imported certificate/key is invalid or certificate is imported as a key and vice versa.
- ACL Enhancements including the following:
 - Enhanced user-friendly view to manage ACLs or individual entries within ACL tables.
 - ACL/interface association view.
- Support for Cisco VFrame Data Center including the following:
 - Device management including chassis/ACE module discovery, and credential management.
 - Virtual context setup and administration.
 - Configuration support including server load balancing, SSL, security, NAT, and chassis features to set up ACE module.
 - Monitoring including ACE HA status, and real server statistics collected by ANM.
- Audit Trail Log Support—Event viewer and export capability to capture key ANM user activities including:
 - Device configuration, staging, deployment, and operational changes.
 - Device management and synchronization operations.
 - ANM RBAC, device group and threshold management.
 - User session management.
- Configuration Auto-Synchronization—Auto-synchronization from ACE to ANM for device configuration changes made out-of-band (by any means other than through the ANM user interface).
- Administrative enhancements including the following:
 - Expanded presentation of default values on configuration screens.
 - Visual and user interface enhancements for improved clarity and consistency.

Related Topics

- [Understanding Cisco Application Networking Manager Terminology, page 1-15](#)
- [ANM Interface Overview, page 1-5](#)
- [Using Lifeline, page 16-3](#)

Logging Into the Cisco Application Networking Manager

You access ANM features and functions through a web-based interface. The following sections describe logging in, the interface, and terms used in ANM.

The ANM login screen allows you to:

- Log into the ANM server
- Change the password for your account (See [Changing Your Account Password, page 1-4.](#))
- Obtain online help by clicking **Help**

Use this procedure to log into ANM.

Procedure

- Step 1** Select one the following:
- To log in after a new install (which uses the default web ports of 443 and 80 and therefore it is unnecessary to explicitly enter them), enter: **https://<host>**



Caution

If you want to log in using HTTP, you will need to change the properties file. See [Changing Configuration Property Values, page 16-1](#) for details. Remember, if you enable HTTP, you are making your connection to the ANM less secure.

- To log in after an upgrade (which uses the previously non-default web ports of 10443 and 10080 and therefore it is necessary to explicitly enter them), enter: **https://<host>:10443** or **https://<host>:10080**



Note

All browsers require that cookies, Javascript/scripting, and popup windows are enabled. If you reinstall a subsequent ANM release, delete the cookies and clear the browser cache.

For example, enter **https://192.168.10.10**. The login screen appears.

A new installation comes with predefined credentials; user name and password are both **admin**. Please use it for first time login.

- Step 2** In the User Name field, type **admin**.



Note

If you are logging in using ACS authentication (TACACS or RADIUS), you *must* add '@<organization>' to the username (initially admin as shown here) on the login page, or you will not be able to log in.

Once you are logged in using this account, you can create additional user accounts. For information on changing account passwords, see [Modifying User Accounts, page 15-41](#).

- Step 3** In the Password field, type **admin**.

This is the default password. We recommend you change the password after you install or upgrade. For information about changing the default password, see [Changing Your Account Password, page 1-4](#).

- Step 4** Click **Login**.

When you log in, the default window that appears is the **Config > Devices** screen. You can change your default window by editing your user profile. For a description of the user interface, see [Figure 1-1](#). The interface will not contain data until you add devices by one of the methods described in [Adding Network Devices into ANM, page 2-7](#).

Related Topics

- [Changing Your Account Password, page 1-4](#)
- [ANM Interface Overview, page 1-5](#)

Draft - CISCO CONFIDENTIAL

Changing Your Account Password

Use this procedure to change your account password.

Procedure

-
- Step 1** Using a web browser, navigate to the ANM login screen by typing the IP address or hostname where ANM is installed. For example, enter **https://192.168.10.10**. The login screen appears.
- Step 2** In the User Name field, enter your account user name.
- Step 3** Click **Change Password**. The Change Password configuration screen appears.
- Step 4** In the User Name field, enter the user name of the account you want to modify.
- Step 5** In the Old Password field, enter the current password for this account.
- Step 6** In the New Password field, enter the new password for this account.
- Password attributes such as minimum and maximum length or accepted characters are defined at the organizational level. For more information on configuring passwords, see [Configuring User Authentication, page 15-31](#).
- Step 7** In the Confirm New Password field, reenter the new password for this account.
- Step 8** Click:
- **OK** to save your entries and to return to the login screen.
 - **Cancel** to exit this procedure without saving your entries and to return to the login screen.
-

Related Topics

- [Logging Into the Cisco Application Networking Manager, page 1-2](#)
- [ANM Interface Overview, page 1-5](#)

Understanding ANM Licenses

In order for ANM to manage all your ACE devices, you must have the appropriate number of ANM licenses for your network devices. An ANM Server license comes with the software and must be uploaded to ANM after the installation in order for your software to work properly. ANM can manage up to two ACE devices with a default set of five virtual contexts each. You will need additional licenses for any devices you plan to manage beyond the standard configuration.

For detailed steps on adding new ANM licenses to expand the number of network devices you can manage, see [Managing ANM Licenses, page 15-56](#). For details on how to install ACE licenses to increase the number of virtual contexts that you can create and manage on a device, see [Managing ACE Licenses, page 3-27](#).

The ANM server also requires its own license (which you must install before ANM will work). For step-by-step instructions on uploading your ANM server license, see the *Installation Guide for the Cisco Application Networking Manager 1.2*.

Related Topics

- [Viewing ACE Licenses, page 3-27](#)

- [Installing ACE Licenses, page 3-29](#)
- [Understanding ANM License Information, page 15-57](#)
- [Checking on License Compliance, page 15-60](#)
- [Viewing Licenses in License Management, page 15-59](#)

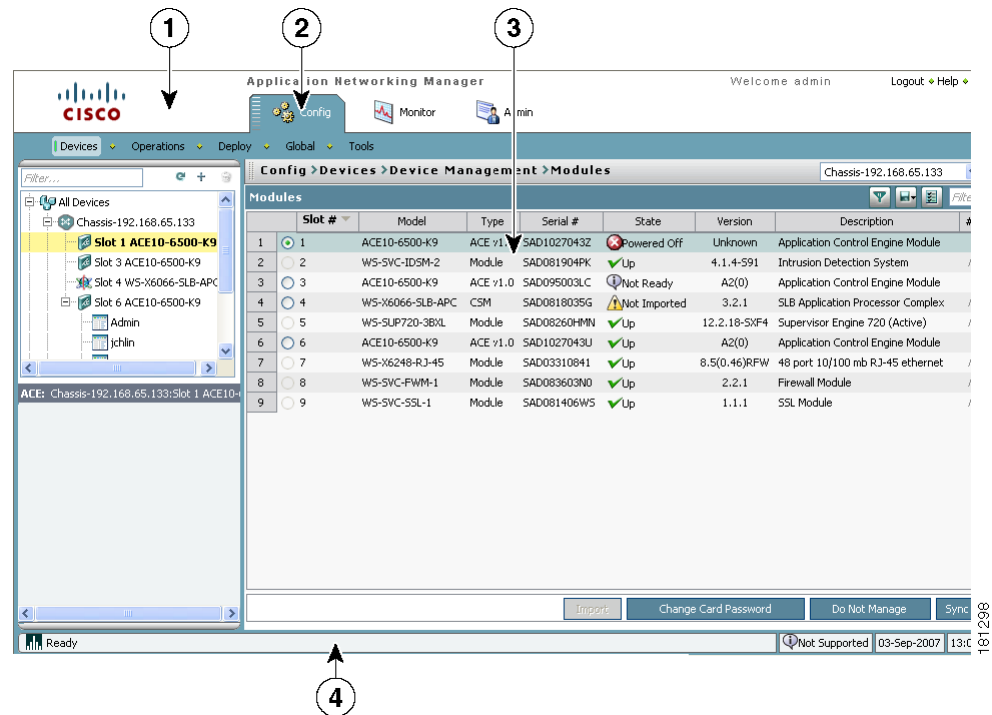
ANM Interface Overview

This section covers the following ANM interface components including:

- [Understanding ANM Screens and Menus, page 1-6](#)
- [Understanding ANM Buttons, page 1-9](#)
- [Conventions in Tables, page 1-11](#)
- [ANM Screen Conventions, page 1-14](#)

When you log into ANM, the default window that appears is the **Config > Devices** screen (similar to [Figure 1-1](#) except that a new installation will have no devices or modules). You will need to import devices in order for your data to display in ANM. [Table 1-1](#) describes the numbered fields.

Figure 1-1 ANM Interface Components



Draft - CISCO CONFIDENTIAL**Table 1-1 ANM Interface Components Descriptions**

Field	Description
1	Navigation pane, which contains: • The high-level navigation path within the ANM interface, which includes Config, Monitor, and Admin. You can click an item in the navigation path to view that screen. • The Logout button. • A Help button for providing context-sensitive help and a PDF version of the ANM user guide. • An About button that provides ANM version information.
2	Second-level Navigation pane, which contains another level of navigation. Clicking an option in this pane displays the associated screen in the content area.
3	Content area, which contains the display and input area of the window. It can include tables, configuration screens, buttons, or combinations of these items.
4	Status bar, which indicates the date and time of the ANM server machine and is updated frequently.

You can change the default window that appears when you log in by modifying user attributes under **Admin > Role-Based Access Control > Users** (see [Modifying User Accounts, page 15-41](#)).

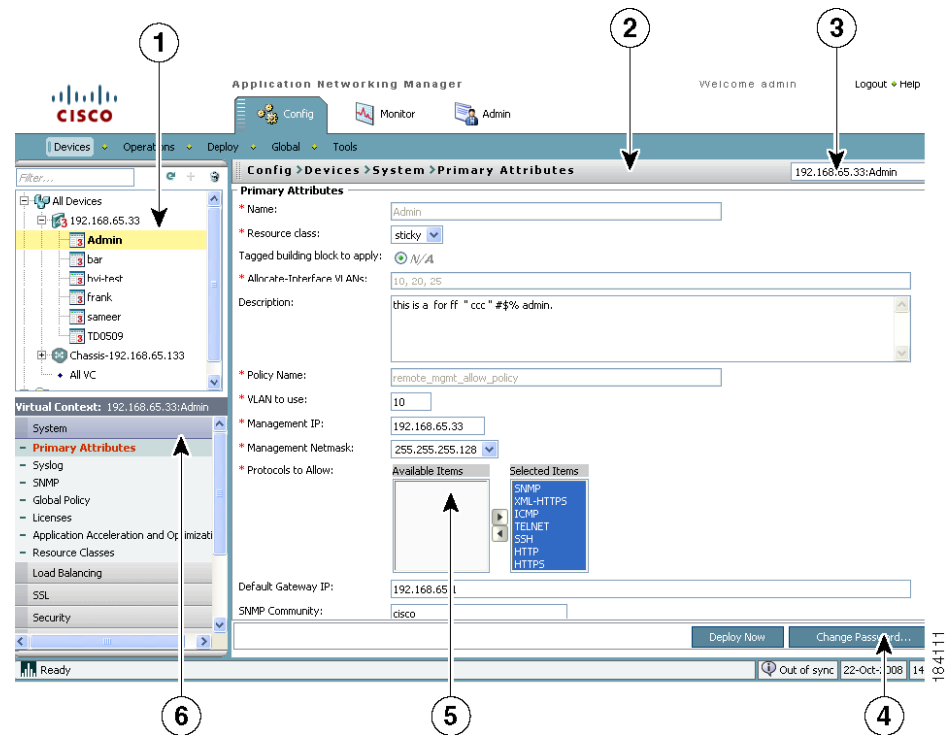
Related Topics

- [Understanding ANM Screens and Menus, page 1-6](#)
- [ANM Interface Overview, page 1-5](#)

Understanding ANM Screens and Menus

[Figure 1-2](#) contains many common screen elements found in ANM and described in [Table 1-2](#). Not all screens contain all buttons.

Figure 1-2 Example ANM Screen



Draft - CISCO CONFIDENTIAL**Table 1-2 Example ANM Screen Descriptions**

Number	Description
1	Device tree, which appears when you click Config or Monitor. The device tree includes All Devices and Groups: • The All Devices folder expands to show the names of imported Cisco devices and their associated modules or virtual contexts. When you click the plus sign (+) in front of a chassis icon, you can see a list of the modules in the chassis. When you expand an ACE appliance or ACE module, you can see the list of existing virtual contexts for that device. For more information about adding devices, see Adding Network Devices into ANM, page 2-7. • The Groups folder contains the list of user-defined groups. For more information about user-defined groups, see Configuring User-Defined Groups, page 2-54. The Organization tree displays when you click Admin > Role-Based Access Control. The organization tree includes all organizations in ANM. Selecting an organization name displays its details. To expand folders in the device tree, click the plus sign (+) to the right of an option. To collapse the structure, click the minus sign (-). Double-clicking on objects results in various actions; for example, displaying the object's configuration screen. At the top of the tree are the following buttons: • Refresh—Refreshes the device tree after you have imported devices or made changes to the User Groups. • Plus sign (+) —Allows you to add an item to the selected option in the device tree. • Garbage can—Deletes the selected entry. Note Menus are based on device types. Although menu labels are the same for different device types, the actual menu definition is different. For this reason, it is not possible to preserve the menu state while traversing from a module to a virtual context and vice-versa in the device tree.
2	Option menus, which appear in Config screens. Click the icon on the bar to show or hide the options.
3	Object selector. Use this field to select a device, context, building block, or other object that you want to view information on or configure. This filters what is displayed in the content area.
4	Command buttons. Use these buttons to perform the action identified by the button label.
5	Input fields. Use these fields to make selections and provide information. When there are more than three choices for any field, the field displays as a dropdown list. Otherwise, selections display with radio buttons.
6	Feature panel that contains functions that correspond to what is selected in the device or organization tree. Click on a command to expand the list of options that correspond to that command.

Related Topics

- [Understanding ANM Buttons, page 1-9](#)
- [ANM Screen Conventions, page 1-14](#)

Understanding ANM Buttons

Table 1-3 describes the buttons that appear in some of the Config, Monitor, and Admin screens.



Note

ANM documentation, including online help, uses the names of buttons in all procedures. For example, “Click **Next** to deploy the current entry and add another entry.”

Table 1-3 **Button Descriptions**

Button	Name	Description
	Add	Lets you add an entry to the displayed table.
	Add Another	Saves the current entries and refreshes the screen so you can add another entry.
	Advanced Editing Mode	Lets you view or enter advanced arguments for the selected display.
	Customize	Lets you customize the table to suit your needs. (See Customizing Tables, page 1-11 .)
	Delete	Deletes the selected entry in the table.
	Duplicate	Duplicates the selected entry in the table.
	Edit	Opens the configuration screen of a selected entry in the table.
	Filter	Filters the displayed list of items according to the criteria you specify. (See Filtering Entries, page 1-11 .) Also displays a filter text box where strings can be entered.
	Go	Appears when filtering is enabled; updates the table with the filtering criteria.
	Key	Indicates that the associated field is a foreign key field; that is, one that takes its values from another table.

Draft - CISCO CONFIDENTIAL**Table 1-3 Button Descriptions**

Button	Name	Description
	Plus	Displays a table with information related to the field where Plus appears. For example, if Plus appears next to the field label <i>VLAN Group</i> , clicking Plus displays a list of all VLAN groups in a separate window.
	Refresh	Refreshes the content area.
	Save	Displays the current information in a new window in either raw data or Excel format so you can save it to a file or print it.
	Sort	Sorts a column alphabetically up or down.
	Stop	Stops the current process. If a process is only partially complete, it will finish its current operation and exit. For example, when stop is used during the import of two modules, it will complete only the first of two module imports.
	Switch between Configure and Browse modes	Displays the subtables for those items that have additional sets of parameters that can be configured, such as Config > Devices > Network > VLAN Interfaces. Note This button is not available on single-row tables such as Config > Devices > System > Syslog or Config > Devices > System > SNMP. To switch between these modes, navigate to another screen where the button appears (for example, Config > Devices > Load Balancing > Server Farms), click the button to enter desired mode, then return to the screen on which the button was missing. You will remain in the mode you selected.
	View Excel	View the raw data in Excel format in a separate browser window.
	View Raw Data	View the raw data in table format.

Related Topics

- [Understanding ANM Screens and Menus, page 1-6](#)
- [ANM Screen Conventions, page 1-14](#)

Conventions in Tables

Filtering Entries

Click **Filter** to view table entries using criteria you select. When filtering is enabled, a filter row appears above the first table entry that allows you to filter entries in the following ways:

- In a drop-down list, select one of the ANM-identified categories (see [Figure 1-3](#)). The table refreshes automatically with the entries that match the selected criterion.
- In fields without drop-down lists, enter the string you want to match, then click **Go** above the first table entry. The table refreshes with the entries that match your input.
- Enter the string in the filter box. For example, by entering the string *gold* and clicking **Go**, only the gold Resource Class virtual contexts will be displayed (see [Figure 1-3](#)).

Figure 1-3 Example Table with Filtering Enabled

Virtual Contexts

Go

gold

All

	Name	Resource Class	Building Block	Config Status	Management IPs	Polling Status
1	x192.168.65.130:2:Admin	gold		OK	192.168.61.22, 192.168.65.131	Started
2	x192.168.65.130:2:jchlin	gold		OK	N/A	Not Polled
3	x192.168.65.130:2:mpc-test	gold		OK	N/A	Not Polled
4	x192.168.65.130:2:Sachin	gold		Out of sync	N/A	Not Polled
5	x192.168.65.130:2:sameer	gold		OK	10.10.10.10	Missing SNMP Credentials
6	x192.168.65.130:2:TD0607	gold		OK	N/A	Not Polled

184112

Related Topics

- [ANM Interface Overview, page 1-5](#)
- [Customizing Tables, page 1-11](#)
- [Using the Advanced Editing Option, page 1-13](#)

Customizing Tables

Click **Customize** in a table to configure the table to suit your needs.

When you place the cursor over **Customize**, the following items appear:

- **Default**—When selected with a check mark, this item indicates that the ANM default table format is being used by the current table.
- **Customized-Table-Name**—When the name of a customized table appears, it indicates that a customized table format has been configured. If a customized table name appears and is selected, it indicates that the current table is using this table format.
- **Configure**—When selected, this item opens a dialog box that allows you to create a new customized table format or to modify the table format currently in use.

Use this procedure to customize tables for your use.

Procedure

- Step 1** When viewing a table, select **Customize > Configure**. The List Configuration dialog box appears.
- Step 2** In the List Configuration dialog box, enter the information in [Table 1-4](#).

Draft - CISCO CONFIDENTIAL**Note**

Depending on the table you select, the available fields in the configuration table differ. [Table 1-4](#) includes sample fields that might appear.

**Note**

You can be as inclusive or as restrictive as you like when setting table configuration options. The criteria are cumulative and greater specificity results in fewer results.

Table 1-4 Table Configuration Attributes

Field	Description
List Customization Name	Enter a unique name for a new table configuration.
Fields	To include fields in the table, select the fields from the Available Items list, then click Add . To remove fields from the table, select the fields from the Selected Items list, then click Remove .
Up/Down	To change the location of a column in the table, select its name in the column on the right, then click Up or Down to place it in the desired location.
Group By	Select the field you want to group entries by. When you select a field for grouping, one or more entries appears in the table with + at the beginning of the entry, the name of the field, the grouping criteria, and the number of items in the group. Click + to view all entries in the group.
Descending	Select the Descending check box to sort the groups in reverse order. Clear the Descending check box to sort the groups in ascending order.
Sort By	Select field you want to sort entries by. When you select a field for sorting, all entries in the table are sorted according to the values in the selected field.
Name Filter	Where <i>Name</i> represents the name of each field in the table. Enter the string or value you want to filter the results by. You can enter complete or partial strings or values to be matched. Do not include wildcard characters.
Version Filter	Where <i>Version</i> represents the name of each field in the table. Enter the string or value you want to filter the results by. You can enter complete or partial strings or values to be matched. Do not include wildcard characters.

Step 3 Click:

- **Save** to save your entries under a new name and to close the List Configuration dialog box. If a table using this format is displayed, the table is updated automatically.
- **Cancel** to exit the procedure without saving your entries and to close the List Configuration dialog box.
- **Apply** to apply your current entries to the table you are viewing, save your entries, and to close the List Configuration dialog box.

- **Delete** to delete the currently selected customized table format. It no longer appears as an option when you click **Customize**.

Related Topics

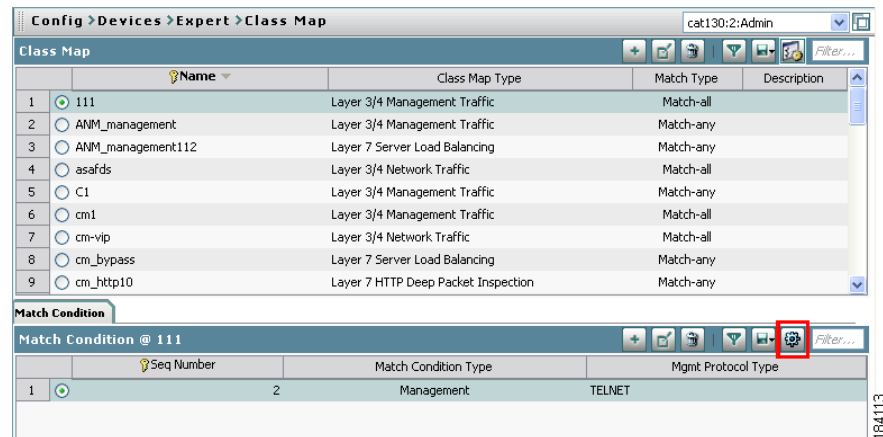
- [ANM Interface Overview, page 1-5](#)
- [Conventions in Tables, page 1-11](#)
- [Using the Advanced Editing Option, page 1-13](#)

Using the Advanced Editing Option

By default, tables include columns that contain configured attributes, or a subset of columns related to a key field.

To view all configurable attributes in table format, click **Advanced Editing Mode** (the highlighted button in [Figure 1-4](#)). When advanced editing mode is enabled, all columns appear for your review (see [Figure 1-4](#)).

Figure 1-4 Advanced Editing Enabled Screen



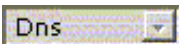
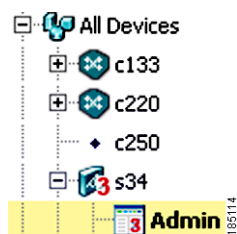
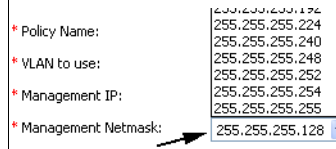
Related Topics

- [ANM Interface Overview, page 1-5](#)
- [Conventions in Tables, page 1-11](#)
- [Customizing Tables, page 1-11](#)

Draft - CISCO CONFIDENTIAL**ANM Screen Conventions**

Table 1-5 describes other conventions used in ANM screens.

Table 1-5 ANM Screen Conventions

Convention	Example	Description
Dimmed field		If no items are selected, buttons are dimmed. If an item is selected, only viable buttons appear.
Red asterisk	* Policy Name:	A red asterisk indicates a required field.
Yellow field with red font		Incorrect, invalid, or incomplete entries appear as red font against a yellow background along with the reason for that error. In the example, an IP address cannot begin with four digits, resulting in this display.
Highlighted text and red numerals on device icons		Selected text is highlighted in yellow in the Devices or Organizations pane. Menu path names are highlighted in green. Table text highlights are yellow until selected, then turn green. Note that device icons in the device tree may display red numerals indicating the device type: - No number = ACE 1.0 modules 2 = ACE 2.0 modules 3 = ACE appliances
Dropdown lists		When there are more than three choices for any field, the field displays as a dropdown list. Otherwise, selections display with radio buttons.

Related Topics

- Conventions in Tables, page 1-11
- ANM Interface Overview, page 1-5

Understanding Cisco Application Networking Manager Terminology

It is useful to understand the following terms when using the ANM:

- **ACE**
Cisco Application Control Engine, available as a module that resides in a Cisco Catalyst 6500 series chassis, Cisco 7600 series router, or as a standalone appliance. The ACE offers high-performance server load balancing (SLB), routing and bridging configuration, traffic policies, redundancy (high availability), virtualization for resource management, SSL, security features, and application acceleration and optimization.
- **Object**
A physical entity, service, or resource that can be managed using the ANM
- **Organizations**
An organization allows you to configure AAA server lookup for your users or set up users who work for a service provider customer. Organizations in the Cisco ANM system are defined by the system administrator.
- **Resource class**
A resource class is a defined set of resources and allocations available for use by a virtual context. Using resource classes prevents a single context from using all available resources.
- **User contexts**
There are two types of user contexts:
 - **Admin context**
The Admin context, which contains the basic settings for each virtual device or context, allows a user to configure and manage all contexts. When a user logs into the Admin context, he or she has full system administrator access to the entire ACE and all contexts and objects within it. The Admin context provides access to network-wide resources, for example, a syslog server or context configuration server. All global commands for ACE settings, contexts, resource classes, and so on, are available only in the Admin context.
 - **User context**
A user context has access to the resources in which the context was created. For example, a user context that was created by an administrator while in Admin context, by default, has access to all resources in an ACE device. Any user created by someone in a user-defined context, only has access to the resources within that context. In addition, roles are assigned to users, which determine the commands and resources that are available to that user.
- **Virtual context**
A virtual context is a concept that allows users to partition an ACE into multiple virtual devices. Each virtual context contains its own set of policies, interfaces, and resources, allowing administrators to more efficiently manage system resources and services.
- **Virtual server**
In a load-balancing environment, a virtual server is a construct that allows multiple physical servers to appear as one for load-balancing purposes. A virtual server is bound to physical services running on real servers in a server farm and uses IP address and port information to distribute incoming client requests to the servers in the server farm according to a specified load-balancing algorithm.

Draft - CISCO CONFIDENTIAL**Related Topics**

- [Cisco Application Networking Manager New Features, page 1-1](#)
- [ANM Interface Overview, page 1-5](#)
- [Conventions in Tables, page 1-11](#)
- [Glossary](#)



CHAPTER 2

Adding and Managing Devices

Revised: 3/25/09

After adding devices to ANM, you can configure them for use in your network. The following topics introduce you to adding and managing your supported network devices:

- [Device Management Overview, page 2-2](#)
- [Device Import Overview, page 2-3](#)
- [Preparing Devices for Import, page 2-4](#)
- [Adding Network Devices into ANM, page 2-7](#)
- [Discovering Large Numbers of Devices, page 2-16](#)
- [Configuring Devices, page 2-22](#)
- [Configuring Device Role-Based Access Controls, page 2-40](#)
- [Managing Devices, page 2-52](#)
- [Synchronizing Module Configurations, page 2-53](#)
- [Synchronizing Device Configurations, page 2-52](#)
- [Restarting Device Polling, page 2-59](#)
- [Configuring User-Defined Groups, page 2-54](#)

Device Management Overview

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

[Table 2-1](#) identifies common management categories and related topics.

Table 2-1 **Device Management Options**

Device Management Activities	Related Topics
Adding and importing devices	• Device Import Overview, page 2-3 • Preparing Devices for Import, page 2-4 • Adding Network Devices into ANM, page 2-7 • Adding Network Devices into ANM, page 2-7 • Adding ACE Modules to ANM, page 2-11 • Importing Cisco Content Switching Module (CSM) Devices, page 2-13 • Importing Cisco Global Site Selector (GSS) Devices, page 2-14 • Discovering Large Numbers of Devices, page 2-16
Configuring device attributes	• Configuring Devices, page 2-22 • Configuring CSM Primary Attributes, page 2-23 • Configuring CSS Primary Attributes, page 2-24 • Configuring GSS Primary Attributes, page 2-25 • Configuring Cisco Catalyst Chassis and 7600 Series Router Primary Attributes, page 2-26 • Configuring Device Static Routes, page 2-27 • Viewing and Configuring Device Interfaces, page 2-28 • Managing Device VLANs, page 2-35 • Creating VLAN Groups, page 2-39

Table 2-1 *Device Management Options (continued)*

Device Management Activities	Related Topics
Configuring device role-based access control (RBAC)	• Configuring Device RBAC Users, page 2-40 • Configuring Device RBAC Roles, page 2-43 • Configuring Device RBAC Domains, page 2-48
Managing devices	• Synchronizing Device Configurations, page 2-52 • Configuring User-Defined Groups, page 2-54 • Updating Chassis Passwords, page 2-57 • Changing ACE Module Passwords, page 2-58 • Restarting Device Polling, page 2-59 • Viewing All Devices, page 2-60 • Viewing Modules by Chassis, page 2-61 • Removing Modules from the ANM Database, page 2-62

Device Import Overview

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

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

Perform the following steps to prepare and import devices:

1. Enable SSH access (see [Preparing Devices for Import, page 2-4](#)).
2. Import devices (see [Adding Network Devices into ANM, page 2-7](#)).

To add large numbers of devices, you can use the IP Discovery before importing your devices. This is a multi-step process and not as efficient as using the Add function. IP discovery shows where devices are, but does not add the devices to ANM. We recommend you use the **Config > Devices > Add** function. For details on IP Discovery, see [Discovering Large Numbers of Devices, page 2-16](#).



Note

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

Preparing Devices for Import

ANM communicates with network devices through SSH and other protocols. You must set up your devices to allow ANM to collect data from them.

ANM uses the following protocols for communication:

- For communication to the ACE module and ACE appliance:
 - XML over HTTPS
 - Secure Shell (SSH) Protocol V2 (read and write)
 - SNMP V2C (read-only)
 - Syslog over User Datagram Protocol (UDP) (inbound notifications only)
- For communication to the chassis (Catalyst 6500/Cisco 7600) and CSM/CSM-S:
 - Secure Shell (SSH) Protocol V2 and Telnet (read and write)
 - SNMP V2C (read-only)
 - Syslog over UDP (inbound notifications only)
- For communication to the CSS:
 - Telnet (read and write)
 - SNMP V2C (read-only)
 - Syslog over UDP (inbound notifications only)
- For communication to the GSS:
 - Secure Shell (SSH) Protocol V2
 - RMI over SSL



Note

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

ANM communicates with network devices through SSH and other protocols. You must set up your devices to allow ANM to collect data from them. Perform the steps in the following sections to set up your devices.

- [Enabling SSH or Telnet Access on Cisco Catalyst 6K and 7600 Chassis, page 2-5](#)
- [Enabling SSH Access and HTTPS Interface on ACE Module and ACE Appliance, page 2-5](#)
- [Enabling SNMP Polling from ANM, page 2-6](#)



Note

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



Tip

Once you have added devices, please see the “[Enabling Syslog Messages from the ACE](#)” section on [page 2-15](#) to streamline ANM CLI synchronization process. For more information on supported devices, see the *Supported Devices Table for the Cisco Application Networking Manager 2.0*.

Enabling SSH or Telnet Access on Cisco Catalyst 6K and 7600 Chassis

You can choose to use Telnet or SSH to import a Catalyst 6K or 7600 device in ANM. Telnet is enabled by default on the Catalyst chassis. If you have disabled Telnet on the device, you will need to enable it, to perform "Initial Setup and import" of an ACE module. If you wish to directly import an ACE module into ANM, Telnet is not mandatory on a Catalyst 6K device.

If you use SSH to communicate with the device:

- SSH2 must be enabled on the chassis, as well as the ACE appliance, in order for the ANM to add device information about the chassis.
- The chassis must have a K9 (Triple Data Encryption Standard [3DES]) software image in order to enable the SSH server. The ANM requires SSH2 to be enabled on the chassis.

The following table identifies the commands needed to enable SSH2 on the chassis. Comments explain why entries are needed:

Command	Comment
<code>ip ssh version 2</code>	Enables SSH version 2
<code>ip domain-name abc.com</code>	
<code>crypto key generate rsa general-keys modulus 1024</code>	Generates the key
<code>username <username> password <password></code>	Enter the username and password.
<code>line vty 0 4</code>	
<code>session-timeout 60</code>	
<code>login local</code>	This is an example only. This commands works for Cisco IOS 12.2.18SXF(10), but not for 12.2.18SXF(8).
<code>transport input telnet ssh</code>	Allows SSH and Telnet to the chassis
<code>transport output telnet ssh</code>	Allows chassis to SSH and Telnet into the ACE module

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

ANM uses SSH and XML over HTTPS to communicate with the ACE devices (modules and ACE 4710 appliances). You need to enable both SSH access and HTTPS as explained in this section. These settings can be enabled during device import as described in [Adding Network Devices into ANM, page 2-7](#), or in CLI as shown below. If ANM does the initial ACE setup, then that is taken care of transparently.



Note

Make sure that the management policy applied on the management interface permits SSH.

The following example details how to set up SSH and HTTPS on the ACE to allow access by ANM. Comments explain why entries are needed. Issue the following commands in config mode in the Admin context.

**Tip**

If the ACE module or appliance is new and retains its factory settings, you do not need to issue these commands; SSH is enabled in bareblade configurations. If the ACE appliance does not have its factory settings, use the following commands in the Admin context.

Command**Comment**

```
ssh key rsa 1024 force
```

Configures SSH access on the ACE.

```
access-list acl line 10 extended permit ip any any
```

```
class-map type management match-any ANM_management
```

Needed by ANM for discovery.

```
  2 match protocol ssh any
  3 match protocol telnet any
  4 match protocol https any
  5 match protocol snmp any
  6 match protocol icmp any
  7 match protocol xml-https
```

The following comments apply to the line number specified before the command text in the left column:

- Line 2 classifies SSH traffic.
- Line 4 is needed by ANM for making configuration changes on the ACE.
- Line 5 is needed by ANM for periodic statistics.
- Line 6 is not mandatory but useful for network and route validation.
- Line 7 is needed only for ACE 4710 devices.

```
policy-map type management first-match
  ANM_management
    class ANM_management
      permit
```

Allows protocols matched in management class map

```
interface vlan 30
  ip address 192.168.65.131 255.255.255.0
  access-group input acl
  service-policy input ANM_management
  no shutdown
```

This is a management interface with the ACL, and defines the management service policy. This is not recommended as a client or server interface.

```
username admin password 5
$1$faXJEFBj$TJR1Nx7sLPTi5BZ97v08c/ role Admin
domain default-domain
```

Defined by the administrator.

```
ip route 0.0.0.0 0.0.0.0 192.168.0.1
```

Default route (or appropriate route) for traffic to reach ANM using the management interface, if ANM is not on the same subnet

For more information on configuring SSH access on ACE modules, see the *Cisco Application Control Engine Module Administration Guide* on Cisco.com.

Enabling SNMP Polling from ANM

In order for SNMP polling to be successfully performed by ANM:

- ACE 1.0 modules require a management IP with a suitable management policy that permits SNMP traffic on every context that needs to be polled.
- ACE 2.0 modules require the Admin context to be configured with a management IP with a suitable management policy that permits SNMP traffic. All other contexts can be polled using this Admin context management IP.

**Note**

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

Adding Network Devices into ANM

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

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

Adding devices using these procedures is a one-step way to see your devices in the ANM devices table. We recommend that you use this procedure to add your devices instead of running IP Discovery since it is faster and more efficient.

**Note**

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

- The ACE module or CMS has booted successfully and is in the OK/Pass state confirmed by a **show module** Supervisor IOS CLI command.
- The ACE 4710 or the CSS state is up and running. There is no command to validate whether these devices are up and running.

Use the following procedures to add devices to the ANM database:

- To add ACE appliances, Cisco Catalyst chassis, Cisco 7600 series routers, CSS devices, and GSS devices, see [Adding Network Devices into ANM, page 2-7](#).
- To add ACE modules, see [Adding ACE Modules to ANM, page 2-11](#).
- To add CSM devices, see [Importing Cisco Content Switching Module \(CSM\) Devices, page 2-13](#).
- To add GSS devices, see [Importing Cisco Global Site Selector \(GSS\) Devices, page 2-14](#).

**Tip**

Once devices have been added, to enhance the CLI synchronization process between ANM and managed devices, see [Enabling Syslog Messages from the ACE, page 2-15](#).

Adding Devices to ANM

ANM allows you to add ACE appliances, Cisco Catalyst chassis, 7600 series routers, CSS, and GSS devices individually to its database instead of or in addition to running discovery and importing them from the Discovery Jobs table. To import modules, see [Adding ACE Modules to ANM, page 2-11](#). To import CSM devices, see [Importing Cisco Content Switching Module \(CSM\) Devices, page 2-13](#).



Note

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

Use this procedure to add ACE appliances and other supported devices individually to the ANM database.

Procedure

- Step 1** Select **Config > Devices > All Devices**. The All Devices table appears.
- Step 2** Click **Add** in the device tree or in the All Devices table. The New Device screen appears.
- Step 3** Enter the information for the device using the information in [Table 2-2](#).

Table 2-2 **New Device Attributes**

Field	Description
Name	Enter a unique name for the device. Valid entries are unquoted text strings with no spaces and a maximum of 26 alphanumeric characters.
Model	From the pulldown menu, select the type of device to import: - ACE 4710—An ACE 4710 appliance. - CSS—A Cisco Content Services Switch. - Cisco IOS Device—A supported Cisco Catalyst chassis or 7600 series router. - GSS—A high end device that monitors the health and load of the SLBs in each of your data centers and then uses that information along with customer-controlled routing algorithms to select the best-suited and least-loaded data center in real time.
Primary IP	Enter the IP address for the device in dotted-decimal format.
Access Protocol	This field appears when GSS or IOS Device is selected for the model. Select Secure/SSH2 or Telnet as the protocol that ANM uses to access the device for IOS devices. GSS uses Secure/SSH2 (that is the only option that appears).
Username	Enter the account name for device access. Note If you did not configure an account on the chassis before starting this procedure, you can enter an alphanumeric string with no spaces to complete this procedure. We recommend, however, that you configure an account on the device to prevent unauthorized access.
Password	Enter the password for the account.
Enable Password	This field appears for Cisco Catalyst chassis, 7600 series routers and GSS devices for an extra level of security.

Table 2-2 **New Device Attributes (continued)**

Field	Description
SNMP V2C Enabled	This field appears for Cisco Catalyst chassis, 7600 series routers, and CSS. Select the check box to configure SNMP access.
Community	This field appears if you select the SNMP V2C check box. Enter the community string for the device. Note If you are adding a Cisco Catalyst chassis, in the Community field, enter the SNMP community string already configured on the Cisco Catalyst chassis. ANM uses this string to query device status information such as VLAN and interface status. This SNMP community string is also used for any CSM modules contained in the specified Cisco Catalyst. For Cisco Catalyst chassis, CSS, and CSM devices, the SNMP community string already configured on the device is used by ANM for polling. For ACE modules and ACE appliances, the SNMP community string entered into ANM is configured on the ACE module/appliance and is used for polling the devices.
Description	Enter a brief description of the device.

Step 4 Click:

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

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

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

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



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

You will see but cannot revise the *Module has been imported into ANM* field, confirm that the check box is selected to indicate that the module has already been imported or cleared to indicate that it has not been imported. This is a read-only field.

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

- Import—ANM is to import the ACE module configuration. Skip to [Step 9](#).
- Perform initial setup and import—Allows you to perform initial setup manually required for ANM to communicate with the ACE module and imports ACE module configuration. Skip to [Step 10](#).

**Note**

We recommend you select this option for ACE modules configured only with factory defaults.

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

- a. In the Admin Context IP field, enter the IP address to use for this module.
- b. In the Username field, enter the username for accessing this module.
- c. In the Password field, enter the password for accessing this module. Reenter the password in the Confirm field.
- d. Skip to [Step 11](#).

Step 10 If you select Perform initial setup and import, enter the following information:

- a. In the Hostname field, enter a unique name for this module. Valid entries are alphanumeric strings with no spaces and a maximum of 32 characters.
- b. In the Admin Context IP field, enter the IP address for this module.
- c. In the Netmask field, select from the pulldown menu the subnet mask to apply to this IP address from the pulldown menu.
- d. In the Gateway field, enter the IP address of the gateway router to use.
- e. In the VLAN field, select the VLAN to which this module belongs.

Step 11 Specify whether the ACE blade is configured with the factory default admin credentials (admin/admin):

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

**Note**

For security reasons, we recommend that you change the username and password on your ACE device (and modules) after you import them. Security on the ACE module can be compromised because the administrative username and password are configured to be the same for every ACE module shipped from Cisco Systems. See [“Changing ACE Module Passwords” procedure on page 2-58](#).

Step 12 Click:

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

**Note**

Clicking **Cancel** in this screen does not cancel the chassis importing process.

Step 13 To confirm that the virtual contexts on the ACE were successfully imported into ANM:

- a. Select **Config > Devices**. The device tree appears.
- b. In the device tree, select the ACE you just imported. The Virtual Contexts table appears, listing the contexts for that device.
- c. Confirm that the contexts imported successfully:

- If *OK* appears in the Config Status column, it means that the context imported successfully.
 - If *Import Failed* appears in the Config Status column, it means that the context did not import successfully.
- d. To synchronize the configurations for the context import that failed, select the context, then click **Sync**. ANM will synchronize the context by uploading it from the ACE device.

For more information on synchronizing virtual contexts, see [“Creating Virtual Contexts” procedure on page 3-2](#).

**Note**

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

Adding ACE Modules to ANM

You can import ACE modules into the ANM database at any time after chassis or routers have been imported.

Before You Begin

1. The time needed to import ACE modules depends on the number of modules and contexts that you are importing. For example, an ACE module with 20 virtual contexts takes longer than an ACE module with 5 contexts. While ANM imports the module, you cannot perform other activities in the same session. You can, however, establish a new session with the ANM server and perform activities on other devices, modules, or virtual contexts.
2. If you receive authentication errors or incorrect username/password errors when trying to import ACE devices, refer to the ACE documentation regarding username and password settings and limitations.
3. If you physically replace an ACE module in a chassis, you need to synchronize the chassis in ANM. We recommend you start by adjusting syslog settings to facilitate the ANM auto sync process as described in [Enabling Syslog Messages from the ACE, page 2-15](#).

Assumptions

- You have imported at least one device containing ACE modules into the ANM database.
- The module to be imported has booted successfully and is in *OK/Pass* state. To check the module state, run the **show module** Supervisor IOS CLI command.

Procedure

-
- Step 1** Select **Config > Devices > All Devices**. The All Devices table appears.
- Step 2** Select the device containing the ACE module you want to import, then click **Modules**. The Modules table appears.
- Step 3** Select the module you want to import, then click **Import**. The Modules configuration screen appears.
- Step 4** In the Card Slot field, confirm that the correct module appears.
- Step 5** In the Card Type field, confirm that the correct version appears.

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

- Import—ANM is to import the ACE module configuration. Skip to [Step 7](#).
- Perform initial setup and import—ANM is to provide the ACE module with a prediscovery configuration file and then import the ACE module configuration.

Select this option only if the ACE module has never been configured before. Specify whether the ACE blade is configured with the factory default admin credentials (admin/admin):

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

Skip to [Step 8](#).

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

- In the Admin Context IP field, enter the IP address to use for this module.
- In the Username field, enter the username for accessing this module.
- In the Password field, enter the password for accessing this module.



Note

For security reasons, we recommend that you change the username and password on your ACE modules after you import them. Security on the ACE module can be compromised because the administrative username and password are configured to be the same for every ACE module shipped from Cisco Systems. See the section [“Changing ACE Module Passwords” procedure on page 2-58](#).

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

- In the Hostname field, enter a unique name for the module. Valid entries are alphanumeric strings with no spaces and a maximum of 32 characters.
- In the Admin Context IP field, enter the IP address for the module.
- In the Netmask field, select from the pulldown menu the subnet mask to apply to the IP address.
- In the Gateway field, enter the IP address of the gateway router.
- In the VLAN field, select the VLAN to which the module belongs.

Step 9 Click:

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

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

- Select **Config > Devices**. The device tree appears.
- In the device tree, select the module you just imported. The Virtual Contexts table appears, listing the contexts for that module.
- Confirm that the contexts imported successfully:
 - If *OK* appears in the Config Status column, it means that the context imported successfully.
 - If *Import Failed* appears in the Config Status column, it means that the context did not import successfully.

- d. To synchronize the configurations for the context import that failed, select the context, then click **Sync**. ANM will synchronize the context by uploading it from the module.
For more information on synchronizing virtual contexts, see [““Creating Virtual Contexts” procedure on page 3-2.](#)
-

Importing Cisco Content Switching Module (CSM) Devices

You can import CSM devices into the ANM database at any time after chassis or routers have been imported.



Note

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

Use this procedure to import CSM devices into the ANM database independently of the discovery process.

Assumption

You have imported at least one device containing a CSM into the ANM database.

Procedure

- Step 1** Select **Config > Devices > All Devices**. The All Devices table appears.
 - Step 2** Select the device containing the CSM that you want to import, then click **Modules**. The Modules table appears.
 - Step 3** Select the CSM that you want to import, then click **Import**. The Modules configuration screen appears.
 - Step 4** Verify that the information is correct in the following read-only fields:
 - Card Slot—The slot in the chassis in which the module resides.
 - Card Type—The device type; in this instance, CSM.
 - Module has been imported into ANM—The check box is selected to indicate that the module has already been imported or cleared to indicate that it has not been imported.
 - Step 5** In the Operation to Perform field, select **Import**.
 - Step 6** Click:
 - **OK** to save your entries. A progress bar reports status and the Modules table refreshes with updated information.
 - **Cancel** to exit the procedure without importing the device and to return to the Modules table.
-

Importing Cisco Global Site Selector (GSS) Devices

Global Site Selectors work together in a GSS network to provide distributed and redundant GSLB DNS services. You accomplish the creation of GSLB DNS services by first performing a basic configuration of each individual device, and then accessing the primary Global Site Selector Manager (GSSM) to manage the centralized and shared GSLB configuration.

Please keep in mind the following operational notes as you import GSS devices into ANM:

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

Use this procedure to import GSS devices into the ANM database. Terminal length settings will be set to 0 during import, sync up, and background polling. The previous terminal length settings you had before import, sync up and background polling is performed will *not* be preserved.

Procedure

-
- Step 1** Select **Config > Devices > All Devices**. The All Devices table appears.
- Step 2** Select the **Add** button. The New Device page appears.
- Step 3** Configure the device using the information in [Table 2-3](#).

Table 2-3 *GSS Configuration Options*

Field	Description
Name	The name assigned to the device.
Model	Pull down menu from which you can select GSS.
Primary IP Address	This is a read-only field with the device IP address.
User Name	This field displays any other GSS devices that have been imported into the ANM database.
Password	Allows you to specify a password for this user account (configurable, based on minimum and maximum values defined).
Enable Password	This field appears for Cisco Catalyst chassis, 7600 series routers, CSS, and GSS devices to provide an extra level of security.
	 Note When a GSS is configured with remote authorization using the enable command in the user privilege, the enable password is not used.
Description	Enter a brief description for this device.

- Step 4** Click:
- **OK** to save your entries. A progress bar reports status and the Modules table refreshes with updated information.

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

Related Topic[GSS Firewall Deployment Overview](#)

GSS Firewall Deployment Overview

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

The GSS does not support deployment of devices behind a NAT for inter-GSS communication. The communication between the GSS devices cannot include an intermediate device behind a NAT because the actual IP address of the devices is embedded in the payload of the packets. For more information consult your GSS documentation.

[Table 2-4](#) lists the TCP ports that are used by ANM to communicate with GSS.

Table 2-4 TCP Ports Used by ANM for GSS

Port	Description
22	SSH
2001	Java RMI
3009	Secure RMI

Enabling Syslog Messages from the ACE

Setting auto sync to occur upon receipt of a syslog message from devices allows a faster, more streamlined synchronization process between ANM and any out-of-band configuration changes. Rather than wait the default polling period, ANM will sync when a syslog message is received if Setup Syslog for Autosync is enabled.

Use this procedure to have ANM receive syslog messages for a virtual context.

**Note**

GSS devices are not supported for Autosync.

Procedure

- Step 1** Select **Config > Devices > Setup Syslog for Autosync**. The Setup Syslog for Autosync screen appears.
- Step 2** Select either **All VC** or the ACE with the virtual context configuration for which you want to receive Autosync syslog messages. A progress bar window appears.

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

Step 3 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
```

Discovering Large Numbers of Devices

Discovering and importing chassis and ACEs into the ANM database involves:

1. Preparing devices for discovery. This involves enabling SSH and XML over HTTPS and adding device credentials. See [Preparing Devices for IP Discovery, page 2-17](#).
2. Discovering devices residing on your network. The ANM uses SSH, XML over HTTPS, and Telnet to discover its supported devices. When you run IP Discovery you locate IP addresses of ACE chassis and appliances. See [Running Discovery to Identify Devices, page 2-20](#).

After discovery, devices do not appear in the Devices table until device import is completed. To import a specific chassis into the ANM database, you need to enter IP and credentials information for the chassis and then import it and any associated modules. While this discovery method requires you to add more information initially, it provides more control over the discovery process.

3. Importing the device information into the ANM database to add the device into the Devices table. See [Adding Network Devices into ANM, page 2-7](#).
4. After importing devices, you can add ACE Modules into the ANM database. See [Adding ACE Modules to ANM, page 2-11](#) or [Importing Cisco Content Switching Module \(CSM\) Devices, page 2-13](#).
5. After you start a discovery job, you can monitor its status. See [Monitoring Device Discovery Status, page 2-21](#).

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

To add a chassis without running discovery, see [Adding Devices to ANM, page 2-8](#).

See the *Supported Devices Table for the Cisco Application Networking Manager 1.2* for device specifics.

Related Topics

- [Configuring Device Access Credentials, page 2-17](#)
- [Running Discovery to Identify Devices, page 2-20](#)
- [Monitoring Device Discovery Status, page 2-21](#)
- [Adding Network Devices into ANM, page 2-7](#)
- [Adding Network Devices into ANM, page 2-7](#)

Preparing Devices for IP Discovery

ANM communicates with network devices through SSH and Telnet during IP discovery. In order to use IP discovery, you must set up your devices to allow ANM to collect device data (for example, you need to enter network credentials before running discovery).

**Caution**

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

Perform all of the following steps to set up your devices for IP discovery:

- [Enabling SSH or Telnet Access on Cisco Catalyst 6K and 7600 Chassis, page 2-5](#)
- [Enabling SSH Access and HTTPS Interface on ACE Module and ACE Appliance, page 2-5](#)
- [Configuring Device Access Credentials, page 2-17](#)
- [Modifying Credential Pools, page 2-19](#)

Related Topics

- [Running Discovery to Identify Devices, page 2-20](#)
- [Adding Network Devices into ANM, page 2-7](#)
- [Discovering Large Numbers of Devices, page 2-16](#)

Configuring Device Access Credentials

Use this procedure to add device credentials to the ANM before running IP discovery.

Procedure

-
Step 1	Select Config > Tools > Credential Pool Management . The New Credential Pool screen appears.
Step 2	In the Name field, enter the name of the new credential pool.
Step 3	Click Save to save this entry and to proceed with credentials configuration. The configuration screen appears.

Step 4 Set Telnet credentials:

- a. Select **Configuration > Telnet Credentials**. The Telnet Credentials table appears.
- b. Click **Add** to add a set of credentials to this credential pool, or select an existing set of credentials, then click **Edit** to modify it.
- c. Enter the credentials (see [Table 2-5](#)).

Table 2-5 *Telnet Credentials*

Field	Description
IP Address	Enter a specific IP address in dotted-decimal notation or use an asterisk (*) as a wildcard character to identify a number of devices, such as 192.168.11.*.
Username	Enter the Telnet username for the specified devices.
Password	Enter the Telnet password for the specified devices.
Confirm	Reenter the Telnet password.
Enable Password	Enter the Telnet enable password for the specified devices. ANM uses this password during the Cisco Catalyst chassis import process.
Confirm	Reenter the Telnet enable password.

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

Step 5 Set SNMP credentials:

- a. Select **Configuration > SNMP Credentials**. The SNMP Credentials table appears.
- b. Click **Add** to add a set of credentials to this credential pool, or select an existing set of credentials, then click **Edit** to modify it.
- c. Enter the SNMP credentials (see [Table 2-6](#)).

Table 2-6 *SNMP Credentials*

Field	Description
IP Address	Enter either a specific IP address in dotted-decimal notation or use an asterisk (*) as a wildcard character to identify a number of devices, such as 192.168.11.*.
Model	Ensure that the default version of SNMP is selected for this credential pool. SNMPV2 indicates that SNMP version 2 is to be used for this credential pool for the specified devices.
RO Community	Enter the SNMP read-only string for the specified devices. This entry is case sensitive.

Table 2-6 *SNMP Credentials (continued)*

Field	Description
Timeout	Enter the time, in seconds, that the ANM is to wait for response from a device before performing the first retry.
Retries	Enter the number of times that the ANM is to attempt to communicate with a device before declaring that the device has timed out.

Step 6 Click:

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

After establishing the Telnet and SNMP credentials, you are ready to run discovery. See [Running Discovery to Identify Devices, page 2-20](#).

Related Topics

- [Running Discovery to Identify Devices, page 2-20](#)
- [Configuring Device Access Credentials, page 2-17](#)
- [Discovering Large Numbers of Devices, page 2-16](#)

Modifying Credential Pools

Use this procedure to modify existing Telnet or SNMP credentials.

Procedure

-
- Step 1** Select **Config > Tools > Credential Pool Management**. The Credential Pools configuration screen appears.
- Step 2** Select the credential pool you want to modify. The Edit Credential Pool configuration screen appears.
- Step 3** Click **Edit**.
- Step 4** To modify the existing Telnet credentials:
- Select **Configuration > Telnet Credentials**. The Telnet Credentials table appears.
 - Click **Add** to add a set of credentials to this credential pool, or select an existing set of credentials, then click **Edit** to modify it.
 - Enter the Telnet credentials (see [Table 2-5](#)).
 - Click:
 - **OK** to save your entries and to return to the Telnet Credentials table.
 - **Cancel** to exit this procedure without saving your entries and to return to the Telnet Credentials table.
 - **Next** to deploy your entries and to add another set of Telnet credentials.

- Step 5** To modify the existing SNMP credentials:
- Select **Configuration > SNMP Credentials**. The SNMP Credentials table appears.
 - Click **Add** to add a set of credentials to this credential pool, or select an existing set of credentials, then click **Edit** to modify it.
 - Enter the SNMP credentials (see [Table 2-6](#)).
 - Click:
 - OK** to save your entries and to return to the SNMP Credentials table.
 - Cancel** to exit without saving your entries and to return to the SNMP Credentials table.
 - Next** to deploy your entries and to configure another set of SNMP credentials.

Related Topics

- [Running Discovery to Identify Devices, page 2-20](#)
- [Configuring Device Access Credentials, page 2-17](#)
- [Discovering Large Numbers of Devices, page 2-16](#)

Running Discovery to Identify Devices

You can run IP discovery to locate IP addresses of ACE chassis and appliances.

After establishing Telnet and SNMP credentials (see [Configuring Device Access Credentials, page 2-17](#)), use this procedure to identify chassis and ACEs on your network.



Caution

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

Before You Begin

For this procedure you need:

- An IP address for the discovery process.
- The applicable subnet mask.
- Valid credentials for this discovery (see [Configuring Device Access Credentials, page 2-17](#)).
- To ensure devices have SSH enabled (see [Preparing Devices for IP Discovery, page 2-17](#)).

Procedure

- Step 1** Select **Config > Tools > IP Discovery**. The Discovery Jobs table appears.



Tip

If you already know the IP address of your devices, use the **Config > Devices > Add** function. See [Adding Network Devices into ANM, page 2-7](#).

- Step 2** To create a discovery job, click **Add**. The Discovery Jobs screen appears.

- Step 3** In the IP Address field, enter the IP address of a specific device in dotted-decimal notation such as 192.168.11.1.
- Step 4** In the Netmask field, select the subnet mask to be used. When you specify a subnet mask, the discovery process discovers all devices in the range of the IP address and its subnet mask. The default netmask is 255.255.255.0.



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

- Step 5** In the Credential Pool field, select the credential pool to be used for this discovery.
- Step 6** Click **Discover** to run discovery now or **Cancel** to exit this procedure without running discovery. When you run discovery, the Discovery Jobs table reflects the state of the discovery as it runs. The amount of time to finish a discovery job depends on the size of your network and network activity. If necessary, click **Stop** to stop the discovery process. When the process has stopped, the Discovery Jobs table appears with the discovery job in the table with the state *Aborted*.



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

- Step 7** Continue with either of the following:
- Viewing discovery status (see [Monitoring Device Discovery Status, page 2-21](#)).
 - Importing ACE appliance into the ANM (see [Adding Network Devices into ANM, page 2-7](#)).

Related Topics

- [Creating Virtual Contexts, page 3-2](#)
- [Adding and Managing Devices, page 2-1](#)
- [Using Configuration Building Blocks, page 13-1](#)

Monitoring Device Discovery Status

Use this procedure to view device discovery status after starting a discovery job.

Procedure

- Step 1** Click **Config > Tools > IP Discovery**. The Discovery Jobs table appears with the following information for each discovery job:
- IP address
 - Subnet mask
 - Start time in the format *hh:mm:ss.nnn*
 - End time, if available, in the format *hh:mm:ss.nnn*
 - Credential pool being used

- State of the discovery job, such as *Running* or *Completed*
- Number of devices found

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

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

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

You can now populate the ANM with chassis and ACEs. See [Adding Network Devices into ANM, page 2-7](#).

Related Topics

- [Adding Network Devices into ANM, page 2-7](#)
- [Running Discovery to Identify Devices, page 2-20](#)
- [Device Import Overview, page 2-3](#)

Configuring Devices

The Modules table (**Config > Devices > All Devices > chassis > Modules**) offers the following options:

- [Adding ACE Modules to ANM, page 2-11](#)
- [Changing ACE Module Passwords, page 2-58](#)
- [Removing Modules from the ANM Database, page 2-62](#)
- [Synchronizing Module Configurations, page 2-53](#)

After importing a device, you can configure it. The configuration options available depend on the type of device:

- For ACE appliances and modules, see [Configuring Virtual Contexts, page 3-1](#).
- For CSM devices, you can configure primary attributes. See [Configuring CSM Primary Attributes, page 2-23](#).
- For CSS devices, you can configure primary attributes. See [Configuring CSS Primary Attributes, page 2-24](#).
- For GSS devices, you can configure primary attributes. See [Configuring GSS Primary Attributes, page 2-25](#).
- For Cisco Catalyst chassis and 7600 series routers, you can configure a number of options, grouped by configuration subset, as described in [Table 2-7](#).

**Note**

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

Table 2-7 *Cisco Catalyst Chassis and 7600 Series Router Configuration Options*

Configuration Subset	Description	Related Topics
System	The System configuration subset allows you to configure primary attributes and static routes.	• Configuring Cisco Catalyst Chassis and 7600 Series Router Primary Attributes, page 2-26 • Configuring Device Static Routes, page 2-27
Interfaces	The Interfaces configuration subset lets you configure access ports, trunk ports, switch virtual interfaces, and routed ports for the device.	• Configuring Access Ports, page 2-29 • Configuring Trunk Ports, page 2-30 • Configuring Switch Virtual Interfaces, page 2-32 • Configuring Routed Ports, page 2-33
VLANs	The VLANs configuration subset lets you configure Layer 2 VLANs, Layer 3 VLANs, and VLAN groups. VLAN group attributes allow you to establish groups of VLANs on a Cisco Catalyst supervisor module so that the group can be assigned to an ACE which can then receive traffic from the supervisor module.	• Viewing All Device VLANs, page 2-36 • Configuring Device Layer 2 VLANs, page 2-37 • Configuring Device Layer 3 VLANs, page 2-38 • Creating VLAN Groups, page 2-39

Configuring CSM Primary Attributes

Use this procedure to configure primary attributes for CSM devices.

Procedure

- Step 1** Select **Config > Devices > All Devices**. The device tree appears.
- Step 2** Select the CSM you want to configure, then select **System > Primary Attributes**. The Primary Attributes screen appears with information about the device.
- Step 3** In the Description field, enter a brief description of the module.
- Step 4** The Redundant Device field displays any other CSM devices that have been imported into the ANM database.
Select another CSM for high availability pairing.
- Step 5** Click **Deploy Now** to deploy this configuration.
To exit this procedure without deploying your entries, select another device in the device tree or in the object selector above the configuration pane.

Related Topics

- [Configuring Devices, page 2-22](#)
- [Adding ACE Modules to ANM, page 2-11](#)

Configuring CSS Primary Attributes

Use this procedure to configure primary attributes for CSS devices.

Procedure

-
- Step 1** Select **Config > Devices > All Devices**. The All Devices table appears.
- Step 2** Select the CSS you want to configure, then select **System > Primary Attributes**. The Primary Attributes screen appears with information about the device.
- Step 3** Configure the device using the information in [Table 2-8](#).

Table 2-8 *CSS Primary Attributes Configuration Options*

Field	Description
Description	Enter a brief description for this device.
IP Address	This is a read-only field with the device IP address.
Redundant Device	This field displays any other CSS devices that have been imported into the ANM database. Select another CSS for high availability pairing.
SNMP V2C Enabled	Select this check box to enable SNMP version 2C access. Clear the check box to disable this feature. If you enable this feature, in the SNMP Trap Community string field, enter the SNMP community string.
SNMP V3 Enabled	Select this check box to enable SNMP Version 3 access. Clear the check box to disable this feature. If you enable this feature: 1. In the SNMP V3 Username field, enter the SNMP username. 2. In the SNMP V3 Mode field, select the level of security to be used when accessing the chassis: – NoAuthNoPriv—SNMP uses neither authentication nor encryption in its communications. – AuthNoPriv—SNMP uses authentication, but the data is not encrypted. 3. If you select AuthNoPriv: a. In the SNMP V3 Auth Proto field, select MD5 or DES to specify the authentication mechanism. b. In the SNMP V3 Auth Pass field, enter the user authentication password. Valid entries are unquoted text strings with no spaces and a maximum of 130 characters. c. In the Confirm field, reenter the user authentication password.

Step 4 Click **Deploy Now** to deploy this configuration.

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

Related Topics

- [Configuring Devices, page 2-22](#)
- [Adding Network Devices into ANM, page 2-7](#)

Configuring GSS Primary Attributes

Use this procedure to configure primary attributes for Cisco Global Site Selector devices.

Procedure

Step 1 Select **Config > Devices > All Devices**. The All Devices table appears.

Step 2 Select the GSS you want to configure, then select **System > Primary Attributes**. The Primary Attributes screen appears with information about the device.

Step 3 Configure the device using the information in [Table 2-9](#).

Table 2-9 GSS Primary Attributes Configuration Options

Field	Description
Description	Enter a brief description for this device.
Device Type	This is a read only field that has the device type, in this case GSS, in gray.
IP Address	Device IP address.

Step 4 Go to:

- [Step 5](#) to update IP address and/or password for the GSS on the ANM server *only*,
or
- [Step 6](#) to complete GSS Primary Attributes configuration.

Step 5 (Optional) To update IP address and/or password for the GSS on the ANM server *only*, click the Update IP Address/Password button.



Note

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

Step 6 Enter new credentials using the information in [Table 2-10](#).

Table 2-10 *GSS Change IP Address and Password Options*

Field	Description
Old Primary IP Address	Read only field displaying the device IP address.
New Primary IP Address	IP address you wish to have GSS associated with on the server.
Update	Radio buttons allowing you to choose to update either or both the password and enable passwords.
New Password	Enter the new password.
Confirm New Password	Reenter the new password.
Password	Enter the new enable password.
New Enable Password	Reenter the new enable password.

Step 7 Click:

- **OK** to save any changes made to GSS server IP address or password if changed and save to the ANM server

or

- **Cancel**

You will be returned to the Primary Attributes Page.

Step 8 Click one of the following:

- **Next** to save any changes made to device description or password if changed and save to the ANM server. You will be returned to the Primary Attributes Page.

or

- Another device in the device tree or in the object selector above the configuration pane.

Related Topics

- [Configuring Devices, page 2-22](#)
- [Adding Devices to ANM, page 2-8](#)
- [Adding Network Devices into ANM, page 2-7](#)

Configuring Cisco Catalyst Chassis and 7600 Series Router Primary Attributes

Use this procedure to configure primary attributes for Cisco Catalyst chassis and 7600 series routers.

Procedure

Step 1 Select **Config > Devices > All Devices**. The device tree appears.

Step 2 Select the device you want to configure, then select **System > Primary Attributes**. The Primary Attributes screen appears with information about the chassis.

Most of the information is read directly from the device during the import process and cannot be changed using the ANM interface. You can, however, add a description and configure the device for SNMP V2 or SNMP V3 access.

- Step 3** In the Description field, enter a brief description for the device.
- Step 4** To enable SNMP Version 2C access:
- Select the SNMP V2C Enabled check box.
 - In the SNMP Trap Community string field, enter the SNMP community string.
- Step 5** Click **Deploy Now** to save your entries and to return to the All Devices table.
-

Related Topics

- [Viewing and Configuring Device Interfaces, page 2-28](#)
- [Viewing Modules by Chassis, page 2-61](#)
- [Managing Device VLANs, page 2-35](#)

Configuring Device Static Routes

While interfaces can be shared across contexts, the ACE supports only static routes for virtual contexts. Use this procedure to configure static routes for Cisco Catalyst chassis and 7600 series routers.



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

Procedure

- Step 1** Select **Config > Devices > All Devices**. The device tree appears.
- Step 2** Select the device you want to configure, then select **System > Static Routes**. The Static Routes table appears.
- Step 3** Click **Add** to configure a new static route for the device, or select an existing static route, then click **Edit** to modify it. The Static Routes configuration screen appears.
- Step 4** In the Destination Prefix field, enter the IP address for the route. The address you specify for the static route is the address that is in the packet before entering the ACE and performing network address translation.
- Step 5** In the Destination Prefix Mask field, select the subnet for the static route.
- Step 6** In the Next Hop field, enter the IP address of the gateway router for the route. The gateway address must be on the same network as a VLAN interface for the device.
- Step 7** In the Admin Distance field, enter the administrative distance value of the route.

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

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

Table 2-11 lists default distance values of the protocols that Cisco supports.

Table 2-11 Cisco Default Distance Value Table

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

Step 8 Click:

- **Deploy Now** to implement this configuration and to return to the Static Route table.
- **Cancel** to exit the procedure without saving your entries and to return to the Static Route table.
- **Next** to deploy your entries and to add another static route.

Related Topics

- [Managing Device VLANs, page 2-35](#)
- [Viewing All Device VLANs, page 2-36](#)
- [Adding and Managing Devices, page 2-1](#)

Viewing and Configuring Device Interfaces

Use this procedure to view a list of interfaces on a selected Cisco Catalyst chassis or 7600 series router and to configure a few high-level attributes for an interface.

Procedure

- Step 1** Select **Config > Devices > All Devices**. The device tree appears.

- Step 2** To view all interfaces on a device, select the device in the device tree, then select **Interfaces > Summary**. The Interfaces table appears, listing all interfaces on the device and related information:
- Interface name
 - Description, if available
 - Configured state, such as Up or Down
 - Current state, if known
 - Mode of operation, such as Access, Routed, or Trunk
 - Interface hardware type
- Step 3** To configure the high level attributes of an interface, select the interface, then click **Edit**. The configuration screen appears.
- Step 4** Enter the following:
- a. In the Description field, enter a brief description of the interface.
 - b. In the Administrative State field, select Up or Down to indicate whether the port should be up or down.
 - c. In the Mode field, select the operational mode of the interface: Trunk, Access, or Routed.
 - d. Click **Apply** to save your changes or **Cancel** to exit the procedure without saving your changes. The Interfaces table appears.
-

Related Topics

- [Viewing and Configuring Device Interfaces, page 2-28](#)
- [Configuring Access Ports, page 2-29](#)
- [Configuring Trunk Ports, page 2-30](#)
- [Configuring Routed Ports, page 2-33](#)
- [Configuring Switch Virtual Interfaces, page 2-32](#)
- [Creating VLAN Groups, page 2-39](#)
- [Managing Device VLANs, page 2-35](#)

Configuring Access Ports

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

Use this procedure to configure access port attributes on the selected device.

Procedure

-
- Step 1** Select **Config > Devices > All Devices**. The device tree appears.
- Step 2** Select the device you want to configure an access port for, then select **Interfaces > Access Ports**. The Interfaces table appears.
- Step 3** Select the port you want to configure, then click **Edit**. The Access Ports configuration screen appears.

- Step 4** In the Description field, enter a description for the port. Valid entries are unquoted text strings with a maximum of 240 characters including spaces.
- Step 5** In the Administrative State field, select Up or Down to indicate whether the port should be up or down.
- Step 6** In the Speed field, either specify the speed at which the interface is to operate or that the interface is to automatically negotiate its speed:
- Auto—The interface is to automatically negotiate speed with the connected device.
 - 10 mbps—The interface is to operate at 10 Mbps.
 - 100 mbps—The interface is to operate at 100 Mbps.
 - 1000 mbps—The interface is to operate at 1000 Mbps.
- Step 7** In the Duplex Mode field, specify whether the interface is to automatically negotiate its duplex mode or use full- or half-duplex mode:
- Auto—The interface is to automatically negotiate duplex mode with the connected device.
 - Full—The interface is to operate in full-duplex mode. In this mode, two connected devices can send and receive traffic at the same time.
 - Half—The interface is to operate in half-duplex mode. In this mode, two connected devices can either send or receive traffic.
- Step 8** In the VLANs field, enter the comma-separated names of the VLANs to which the interface belongs (allowable range is 2-4094).
- Step 9** Click:
- **Apply** to save your entries and to return to the Interfaces table.
 - **Cancel** to exit the procedure without saving your entries and to return to the Interfaces table.
-

Related Topics

- [Configuring Trunk Ports, page 2-30](#)
- [Configuring Switch Virtual Interfaces, page 2-32](#)
- [Configuring Routed Ports, page 2-33](#)
- [Managing Device VLANs, page 2-35](#)

Configuring Trunk Ports

A trunk port carries the traffic of multiple VLANs and by default is a member of all VLANs in the VLAN database. Two types of trunk ports are:

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

Use this procedure to configure trunk ports for the selected device.

Procedure

- Step 1** Select **Config > Devices > All Devices**. The device tree appears.
- Step 2** Select the device you want to configure, then select **Interfaces > Trunk Ports**. The Interfaces table appears.
- Step 3** In the Interfaces table, select the port you want to configure, then click **Edit**. The Trunk Port configuration screen appears.
- Step 4** Configure the port using the information in [Table 2-12](#).

Table 2-12 *Trunk Port Configuration Attributes*

Field	Description
Description	Enter a description for the port. Valid entries are unquoted text strings with a maximum of 240 characters including spaces.
Administrative State	Select Up or Down to indicate whether the port should be up or down.
Speed	Specify the speed at which the interface is to operation or that the interface is to automatically negotiate its speed: • Auto—The interface is to automatically negotiate speed with the connected device. • 10 mbps—The interface is to operate at 10 Mbps. • 100 mbps—The interface is to operate at 100 Mbps. • 1000 mbps—The interface is to operate at 1000 Mbps.
Duplex Mode	Specify whether the interface is to automatically negotiate its duplex mode or use full- or half-duplex mode: • Auto—The interface is to automatically negotiate duplex mode with the connected device. • Full—The interface is to operate in full-duplex mode. In this mode, two connected devices can send and receive traffic at the same time. • Half—The interface is to operate in half-duplex mode. In this mode, two connected devices can either send or receive traffic.
Trunk Mode	Specify how the interface is to interact with neighboring interfaces: • Static—The interface is to enter permanent trunking mode and to negotiate converting a link into a trunk link. The interface becomes a trunk interface even if the neighboring interface does not change. • Dynamic—The interface is to convert a link to a trunk link if the neighboring interface is set to trunk or desirable mode. • Dynamic Desirable—The interface is to actively attempt to convert a link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to trunk, desirable, or auto mode.

Table 2-12 **Trunk Port Configuration Attributes**

Field	Description
Desired Encapsulation	Select the type of encapsulation to be used on the trunk port: • Dot1Q—The interface is to use 802.1Q encapsulation. • Negotiate—The interface is to negotiate with the neighboring interface to use ISL (Inter-Switch Link) (preferred) or 802.1Q encapsulation, depending on the configuration and capabilities of the neighboring interface. • ISL—The interface is to use ISL encapsulation.
Native VLAN	Select the VLAN to use as the native VLAN for the trunk in 802.1Q trunking mode. VLAN 1 (1) is the default native VLAN.
VLANs	Enter comma-separated names of the VLANs to which the interface belongs (allowable range is 2-4094). You can also enter ranges of VLANs, such as 101-120, 130 .
Prune VLANs	Enter comma-separated names of the VLANs that can be pruned (allowable range is 2-4094). VTP pruning blocks unneeded flooded traffic to VLANs on trunk ports that are included in this field. Only VLANs included in this field can be pruned. You can also specify ranges of VLANs that can be pruned, such as 75, 121-250, 351 .

Step 5 Click:

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

Related Topics

- [Configuring Access Ports, page 2-29](#)
- [Configuring Switch Virtual Interfaces, page 2-32](#)
- [Configuring Routed Ports, page 2-33](#)
- [Managing Device VLANs, page 2-35](#)

Configuring Switch Virtual Interfaces

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

Use this procedure to configure SVIs on an MSFC.

Procedure

-
- Step 1** Select **Config > Devices > All Devices**. The device tree appears.
- Step 2** Select the device you want to configure, then select **Interfaces > Switched Virtual Interfaces**. The Interfaces table appears.
- Step 3** In the Interfaces table, click **Add** to add a new SVI, or select the interface you want to configure, then click **Edit**. The Switched Virtual Interfaces configuration screen appears.

- Step 4** In the VLANs field, specify the VLAN to use in one of the following ways:
- To specify a new VLAN, select the first radio button, then enter a new VLAN.
 - To select an existing VLAN, select the second radio button, then select one of the existing VLANs.



Note You cannot modify a VLAN for an existing SVI.

- Step 5** In the Description field, enter a description for the SVI. Valid entries are unquoted text strings with a maximum of 240 characters including spaces.
- Step 6** In the Administrative State field, select Up or Down to indicate whether the SVI should be up or down.
- Step 7** In the IP Address field, enter the IP address to be used for the interface on the MSFC in dotted-decimal format.
- Step 8** In the Netmask field, select the subnet mask to be used for the IP address.
- Step 9** Click:
- **Apply** to save your entries and to return to the Interfaces table.
 - **Cancel** to exit the procedure without saving your entries and to return to the Interfaces table.
-

Related Topics

- [Configuring Access Ports, page 2-29](#)
- [Configuring Trunk Ports, page 2-30](#)
- [Configuring Routed Ports, page 2-33](#)
- [Managing Device VLANs, page 2-35](#)

Configuring Routed Ports

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

Use this procedure to configure routed ports.

Procedure

- Step 1** Select **Config > Devices > All Devices**. The device tree appears.
- Step 2** Select the device you want to configure, then select **Interfaces > Routed Ports**. The Interfaces table appears.
- Step 3** In the Interfaces table, select the interface you want to configure, then click **Edit**. The Routed Ports configuration screen appears.
- Step 4** In the Description field, enter a description for the interface. Valid entries are unquoted text strings with a maximum of 240 characters including spaces.
- Step 5** In the Administrative State field, select Up or Down to indicate whether the interface should be up or down.

- Step 6** In the Speed field, either specify the speed at which the interface is to operate or that the interface is to automatically negotiate its speed:
- Auto—The interface is to automatically negotiate speed with the connected device.
 - 10 mbps—The interface is to operate at 10 Mbps.
 - 100 mbps—The interface is to operate at 100 Mbps.
 - 1000 mbps—The interface is to operate at 1000 Mbps.
- Step 7** In the Duplex Mode field, specify whether the interface is to automatically negotiate its duplex mode, or use full- or half-duplex mode:
- Auto—The interface is to automatically negotiate duplex mode with the connected device.
 - Full—The interface is to operate in full-duplex mode. In this mode, two connected devices can send and receive traffic at the same time.
 - Half—The interface is to operate in half-duplex mode. In this mode, two connected devices can either send or receive traffic.
- Step 8** In the IP Address field, enter the IP address to be used for the interface in dotted-decimal format.
- Step 9** In the Netmask field, select the subnet mask to be used for the IP address.
- Step 10** Click:
- **Apply** to apply your entries and to return to the Interfaces table.
 - **Cancel** to exit the procedure without saving your entries and to return to the Interfaces table.
-

Related Topics

- [Configuring Trunk Ports, page 2-30](#)
- [Configuring Switch Virtual Interfaces, page 2-32](#)
- [Configuring Access Ports, page 2-29](#)
- [Managing Device VLANs, page 2-35](#)

Viewing All Ports

Use this procedure to view all configured interfaces on a chassis.

Procedure

-
- Step 1** Select **Config > Devices > All Devices**. The device tree appears.
- Step 2** Select the chassis with the interfaces you want to view, then select **Interfaces > Summary**. The Interfaces table appears, listing all interfaces on the device and related information:
- Interface name
 - Description, if available
 - Configured state, such as Up or Down
 - Current operational state, if known

- Mode of operation, such as Access, Routed, or Trunk
 - Interface hardware type
-

Related Topics

- [Configuring Trunk Ports, page 2-30](#)
- [Configuring Switch Virtual Interfaces, page 2-32](#)
- [Configuring Access Ports, page 2-29](#)
- [Managing Device VLANs, page 2-35](#)

Managing Device VLANs

ACE modules do not include any external physical interfaces. Instead, they use internal VLAN interfaces.

The related topics describe how to configure Layer 2 and Layer 3 VLANs on chassis, view all VLANs, and create VLAN groups.

For information about configuring VLANs for use with virtual contexts, see [Configuring VLAN Interfaces, page 9-2](#).

For more information about VLANs and their use with ACE modules, see the *Cisco Application Control Engine Module Routing and Bridging Configuration Guide*.

Related Topics

- [Adding Device VLANs, page 2-35](#)
- [Configuring Device Layer 3 VLANs, page 2-38](#)
- [Configuring Device Layer 2 VLANs, page 2-37](#)
- [Viewing All Device VLANs, page 2-36](#)
- [Creating VLAN Groups, page 2-39](#)

Adding Device VLANs

Use this procedure to add a VLAN to a device, such as a Cisco Catalyst chassis or 7600 series router.

Procedure

-
Step 1	Select Config > Devices > All Devices . The device tree appears.
Step 2	Select the device you want to configure, then select VLANs > Layer 2 or VLANs > Layer 3 . The VLANs table appears.
Step 3	Click Add . The VLAN configuration screen appears.
Step 4	Configure the VLAN using the information in Table 2-13 .

Table 2-13 **Device VLAN Configuration Attributes**

Field	Description
VLAN	Enter a unique identifier for the VLAN. Valid entries are integers from allowable range is 2-4094.
Name	Enter a name for the VLAN.
Description	Enter a description for the VLAN. Valid entries are unquoted text strings with a maximum of 240 characters including spaces.
Access Ports	Select the desired access ports from the Available Items list, then click Add . To remove a port that you do not want to use, select the port from the Selected Items list, then click Remove .
Trunk Ports	Select the desired trunk ports from the Available Items list, then click Add . To remove a port that you do not want to use, select the port from the Selected Items list, then click Remove .
VTP Domain	Enter the name of the VTP domain to which the VLAN belongs. A VTP domain is made up of one or more interconnected network devices that share the same VTP domain name. A network device can be configured to be in one and only one VTP domain.
IP Address	This field appears for Layer 3 VLANs only. Enter the IP address to be used for the VLAN interface. Enter the IP address in dotted-decimal notation, such as 192.168.1.1.
Mask	This field appears for Layer 3 VLANs only. Select the subnet mask to apply to the IP address.

Step 5 Click:

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

Related Topics

- [Configuring Device Layer 2 VLANs, page 2-37](#)
- [Configuring Device Layer 3 VLANs, page 2-38](#)
- [Viewing All Device VLANs, page 2-36](#)

Viewing All Device VLANs

Use this procedure to view all configured VLANs on a selected device, such as a Cisco Catalyst chassis.

Procedure

-
- Step 1** Select **Config > Devices > All Devices**. The device tree appears.
- Step 2** Select the device with VLANs you want to view, then select **VLANs > Summary**. The VLANs table appears, listing all VLANs on the selected chassis and related information:
- VLAN number
 - Name given to the VLAN

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

Related Topics

- [Configuring Device Layer 2 VLANs, page 2-37](#)
- [Configuring Device Layer 3 VLANs, page 2-38](#)
- [Viewing All Device VLANs, page 2-36](#)
- [Creating VLAN Groups, page 2-39](#)

Configuring Device Layer 2 VLANs

Use this procedure to add or modify a Layer 2 VLAN on a selected device, such as a Cisco Catalyst chassis.

Procedure

-
Step 1	Select Config > Devices > All Devices . The device tree appears.
Step 2	Select the device you want to configure a Layer 2 VLAN for, then select VLANs > Layer 2 . The VLANs table appears, listing all Layer 2 VLANs associated with the chassis.
Step 3	Click Add to add a new VLAN, or select an existing VLAN, then click Edit to modify it. The VLAN configuration screen appears.
Step 4	Configure the VLAN using the information in Table 2-13 .
Step 5	Click: • Apply to apply your entries and to return to the VLAN Management table. • Cancel to exit the procedure without saving your entries and to return to the VLAN Management table.
-

Related Topics

- [Managing Device VLANs, page 2-35](#)
- [Configuring Device Layer 3 VLANs, page 2-38](#)
- [Viewing All Device VLANs, page 2-36](#)
- [Creating VLAN Groups, page 2-39](#)

Configuring Device Layer 3 VLANs

Use this procedure to add or modify a Layer 3 VLAN on a selected device, such as a Cisco Catalyst chassis.

Procedure

-
- Step 1** Select **Config > Devices > All Devices**. The device tree appears.
 - Step 2** Select the device you want to configure a Layer 3 VLAN for, then select **VLANs > Layer 3**. The VLANs table appears, listing all Layer 3 VLANs associated with the chassis.
 - Step 3** Click **Add** to add a new VLAN, or select an existing VLAN, then click **Edit** to modify it. The VLAN configuration screen appears.
 - Step 4** Configure the VLAN using the information in [Table 2-13](#).
 - Step 5** Click:
 - **Apply** to apply your entries and to return to the VLAN Management table.
 - **Cancel** to exit the procedure without saving your entries and to return to the VLAN Management table.
-

Related Topics

- [Using Virtual Contexts, page 3-1](#)
- [Creating Virtual Contexts, page 3-2](#)
- [Deleting Virtual Contexts, page 3-68](#)

Modifying Device VLANs

Use this procedure to modify VLANs for a specific device.

Procedure

-
- Step 1** Select **Config > Devices > All Devices**. The device tree appears.
 - Step 2** Select the device with the VLAN you want to modify, then select **VLANs > Layer 2** or **VLANs > Layer 3**. The VLANs table appears.
 - Step 3** Select the VLAN you want to modify, then click **Edit**. The VLAN configuration screen appears.
 - Step 4** Modify the VLAN configuration, using the information in [Table 2-13](#).
 - Step 5** Click:
 - **Apply** to save your entries and to return to the VLANs table.
 - **Cancel** to exit the procedure without saving your entries and to return to the VLANs table.
-

Related Topics

- [Adding Device VLANs, page 2-35](#)
- [Creating VLAN Groups, page 2-39](#)

- [Managing Device VLANs, page 2-35](#)

Creating VLAN Groups

For an ACE module to receive traffic from the Cisco Catalyst supervisor module, you must create VLAN groups on the supervisor module, then assign the groups to the ACE module. When the VLANs are configured on the supervisor module to the ACE module, you can configure the VLANs on the ACE module.

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

Use this procedure to create VLAN groups and to assign each group to an ACE module.

Procedure

-
Step 1	Select Config > Devices > All Devices . The device tree appears.
Step 2	Select the device you want to create a VLAN group for, then select VLANs > Groups . The Groups table appears.
Step 3	Click Add to add a new VLAN group, or select an existing VLAN group, then click Edit to modify it. The Groups configuration screen appears.
Step 4	In the VLAN Group Id field, enter a unique identifier for the VLAN group. Valid entries are unquoted text strings with no spaces and a maximum of 256 alphanumeric characters.
Step 5	In the Module Slot Numbers field, enter the ACE module you want to associate with the VLAN group. For example, to add ACE module 3 on the chassis, you would enter 3 .
Step 6	In the VLANs field, enter the VLANs to be included in the VLAN group. Valid entries are comma-separated VLANs or ranges of VLANs (allowable range is 2-4094), such as 10, 50-110 .
Step 7	Click: • Deploy Now to implement the configuration and to return to the Groups table. • Cancel to exit the procedure without saving your entries and to return to the Groups table. • Next to deploy your entries and to add another VLAN group.
-

Related Topics

- [Configuring Device Layer 3 VLANs, page 2-38](#)
- [Configuring Device Layer 2 VLANs, page 2-37](#)
- [Viewing All Device VLANs, page 2-36](#)
- [Adding and Managing Devices, page 2-1](#)

Configuring Device Role-Based Access Controls

ANM provides an interface to allow you to configure device RBAC on the device only. This configuration is applicable only on the device and will not be enforced by ANM. If you want to set up authorization in ANM, go to **Admin > Role-Based Access Control**.

The following RBAC configurations can be set up on your device:

- [Configuring Device RBAC Users, page 2-40](#)
- [Configuring Device RBAC Roles, page 2-43](#)
- [Configuring Device RBAC Domains, page 2-48](#)

Related Topics

- [Controlling Access to the Cisco ANM, page 15-2](#)
- [How ANM Handles Role-Based Access Control, page 15-7](#)
- [Preparing Devices for Import, page 2-4](#)
- [Adding Network Devices into ANM, page 2-7](#)
- [Configuring Devices, page 2-22](#)

Configuring Device RBAC Users

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

Use the Role-Based Access Control feature to specify the people that are allowed to log onto a device. The following sections describe how to manage device user accounts:

- [Guidelines for Managing Users, page 2-40](#)
- [Displaying a List of Device Users, page 2-41](#)
- [Configuring Device User Accounts, page 2-41](#)
- [Modifying Device User Accounts, page 2-42](#)
- [Deleting Device User Accounts, page 2-43](#)

Related Topics

- [How ANM Handles Role-Based Access Control, page 15-7](#)
- [Configuring Device Role-Based Access Controls, page 2-40](#)

Guidelines for Managing Users

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

Related Topics

- [Configuring Device RBAC Users, page 2-40](#)
- [Configuring Device Role-Based Access Controls, page 2-40](#)

Displaying a List of Device Users

Use this procedure to display of list of users that can access this device.

Procedure

-
- Step 1** Select **Config > Devices > context > Role-Based Access Control > Users**. The Users table appears with the following fields:
- User Name
 - Expiration Date
 - Role
 - Domains
- Step 2** You can use the options in this screen to create a new user or modify or delete any existing user to which you have access (see [Table 2-14](#)).
-

Related Topics

- [Configuring Device RBAC Users, page 2-40](#)
- [Configuring Device Role-Based Access Controls, page 2-40](#)

Configuring Device User Accounts

Use this procedure to add or modify a user account on a selected device, such as a Cisco Catalyst chassis or ACE 4710.

**Note**

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

Procedure

-
- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > context > Device RBAC > Users**.
 - To configure a configuration building block, select **Config > Global > Building Blocks > building_block > Role-Based Access Control > Users**.
- A list of users appears.
- Step 2** In the Users table, click **Add** to add a new user, or select the user you want to configure, then click **Edit**. The Users configuration screen appears.

Step 3 Complete the following required fields:

Table 2-14 *User Attributes*

Field	Description
User Name	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.
Expiry Date	Date user account expires (optional).
Password	Allows you to specify a password for this user account (configurable, based on minimum and maximum values defined).
Confirm Password	Reenter the password for this account.
Encryption	Sets password to clear or encrypted text.
Role	Allows you to customize this user's role or accept any existing roles. To enter the Role for this user, see Configuring Device User Roles, page 2-45 . See Table 2-15 for details about setting up new roles.
Domains	Allows you to select domains to which this user belongs. Use the Add and Remove buttons.

Step 4 Click **Deploy Now**. The Users table is displayed.

Related Topics

- [Configuring Device RBAC Users, page 2-40](#)
- [Configuring Device Role-Based Access Controls, page 2-40](#)

Modifying Device User Accounts



Note

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

Procedure

Step 1 Select the item to configure:

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

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

Step 2 Select the user account you want to modify.

Step 3 Click **Edit**.

Step 4 Modify any of the attributes in the attributes table (see [Table 2-14](#)).

- Step 5** Click **Deploy Now**.
The Users table then appears.
-

Related Topics

- [Configuring Device RBAC Users, page 2-40](#)
- [Configuring Device Role-Based Access Controls, page 2-40](#)

Deleting Device User Accounts

Use this option to delete an existing device RBAC user account.



Note

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

Procedure

- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > context > Device RBAC > Users**.
 - To configure a configuration building block, select **Config > Global > Building Blocks > building_block > Role-Based Access Control > Users**.
- A table of users, their role and domain appears.
- Step 2** Select the user account to be deleted, then click **Delete**.
- Step 3** Confirm deletion of the user by clicking **OK** or **Cancel** to return to the Users table.
The user account is removed from the ANM database.
-

Related Topics

- [Configuring Device RBAC Users, page 2-40](#)
- [Configuring Device Role-Based Access Controls, page 2-40](#)

Configuring Device RBAC Roles

This topic contains the following device role sections:

- [Guidelines for Managing User Roles, page 2-44](#)
- [Role Mapping in Device RBAC, page 2-44](#)
- [Configuring Device User Roles, page 2-45](#)
- [Modifying Device User Roles, page 2-46](#)
- [Deleting Device User Roles, page 2-47](#)

Related Topics

- [How ANM Handles Role-Based Access Control, page 15-7](#)
- [Configuring Device Role-Based Access Controls, page 2-40](#)

Guidelines for Managing User Roles

Use these guidelines to manage roles:

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

Related Topics

- [Role Mapping in Device RBAC, page 2-44](#)
- [Controlling Access to the Cisco ANM, page 15-2](#)
- [Configuring Device RBAC Users, page 2-40](#)
- [Configuring Device RBAC Roles, page 2-43](#)
- [Configuring Device RBAC Domains, page 2-48](#)
- [How ANM Handles Role-Based Access Control, page 15-7](#)

Role Mapping in Device RBAC

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

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

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

**Note**

There are certain features in the ANM that do not have a corresponding feature mapping on the CLI. Examples of those are class maps and SNMP. To modify these features you need to select a predefined role that contains at least one feature with the Modify permission on it.

Related Topic

- [How ANM Handles Role-Based Access Control, page 15-7](#)
- [Understanding Roles, page 15-5](#)

Configuring Device User Roles

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

**Note**

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

Procedure

- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > context > Device RBAC > Roles**.
 - To configure a configuration building block, select **Config > Global > Building Blocks > building_block > Role-Based Access Control > Roles**.

A table of the defined roles and their settings appears.

- Step 2** Select the type of configuration you want to perform:
- To add a new role, click **Add**, enter the following attributes, then click **Deploy Now**.

Table 2-15 **Role Attributes**

Attribute	Description
Role Name	The name of the role.
Description	A brief description of the role.

The Roles configuration screen appears.

- To edit a role, select the role you want to configure, then click **Edit**. The Roles configuration screen appears.

- Step 3** Click **Edit** to open the Rules table.

- Step 4** In the Rules table, click **Add** to create rules for this role, or select the rule you want to configure, then click **Edit**. See [Table 2-16](#) for rule attribute descriptions.

Table 2-16 Rule Attributes

Attribute	Description
Rule Number	The number assigned to this rule.
Permission	Permit or deny the specified operation.
Operation	Create, debug, modify ¹ , and monitor the specified feature.
Feature	AAA, Access-list, Config-copy, Connection, DHCP, Fault-tolerant, Inspect, Interface, Loadbalance, NAT, PKI, Probe, Real-in-service, Routing, Rserver, Server Farm, SSL, Sticky, Syslog, and VIP.

1. Certain features are not available for certain operations. For **modify**, the following features cannot be used: config-copy, DHCP, NAT, real-in-service, routing, and syslog.

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

Step 6 Click **Deploy Now** to update this role.

Related Topics

- [Configuring Device RBAC Roles, page 2-43](#)
- [Configuring Device Role-Based Access Controls, page 2-40](#)

Modifying Device User Roles

You can modify any user-defined role.



Note

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

Procedure

Step 1 Select the item to configure:

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

A table of the defined roles and their settings appears.

Step 2 Select the role you want to modify.

Step 3 Click **Edit**. For details on updating role rules, see [Table 2-16](#).

Step 4 Make the changes. For details on updating role rules, see [Adding, Editing, or Deleting Rules, page 2-47](#).

Step 5 Click **Deploy Now** to update the rules for this role.

Related Topics

- [Configuring Device RBAC Roles, page 2-43](#)
- [Configuring Device Role-Based Access Controls, page 2-40](#)

Deleting Device User Roles

You can delete any user-defined roles.

**Note**

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

Procedure

-
- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > context > Device RBAC > Roles**.
 - To configure a configuration building block, select **Config > Global > Building Blocks > building_block > Role-Based Access Control > Roles**.
- Step 2** Select the role to be deleted.
- Step 3** Click **Delete**.
- Step 4** Click **OK** to confirm the deletion. Users that have the deleted role no longer have that access.
-

Related Topics

- [Configuring Device RBAC Roles, page 2-43](#)
- [Configuring Device Role-Based Access Controls, page 2-40](#)

Adding, Editing, or Deleting Rules

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

**Note**

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

Procedure

-
- Step 1** After selecting the user-defined role, click **Edit** to open the Rule window and perform any of the following tasks:
- Click **Add** to create a new rule. Enter the rule information (see [Table 2-16 on page 2-46](#)), then click **Deploy Now** to add the rule or **Next** to deploy this rule and add another rule.

- Select a rule and click **Edit** to change an existing rule. Click **Deploy Now** to save this rule.
- Select the rules to remove from this role, then click **Delete**. Click **OK** to confirm its deletion.

Step 2 Click **Deploy Now** to save these changes to the role.

Related Topic

- [Configuring Device RBAC Roles, page 2-43](#)
- [Configuring Device Role-Based Access Controls, page 2-40](#)

Configuring Device RBAC Domains

This section describes the following device domains tasks:

- [Guidelines for Managing Domains, page 2-48](#)
- [Configuring Device Domains, page 2-49](#)
- [Modifying Device Domains, page 2-51](#)
- [Deleting Device Domains, page 2-51](#)

Related Topics

- [Device Management Overview, page 2-2](#)
- [How ANM Handles Role-Based Access Control, page 15-7](#)
- [Configuring Device Role-Based Access Controls, page 2-40](#)

Guidelines for Managing Domains

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

Related Topics

- [Configuring Device RBAC Domains, page 2-48](#)
- [Configuring Device Role-Based Access Controls, page 2-40](#)

Displaying Domains for a Device



Note

Your user role determines whether you can use this option.

Procedure

-
- Step 1** Select the item to view:
- To view a domain for the device's virtual context, select **Config > Devices > context > Device RBAC > Domains**.
 - To view a domain for a configuration building block, select **Config > Global > Building Blocks > building_block > Role-Based Access Control > Domains**.
- The Domains table appears.
- Step 2** Expand the table until you can see all the network domains.
- Step 3** Select a domain from the Domains table to view the settings for that domain.
- Step 4** You can also perform these tasks from this pane:
- [Configuring Device Domains, page 2-49](#)
 - [Modifying Device Domains, page 2-51](#)
 - [Deleting Device Domains, page 2-51](#)
-

Related Topic

- [Configuring Device RBAC Domains, page 2-48](#)
- [Configuring Device Role-Based Access Controls, page 2-40](#)

Configuring Device Domains

Use this procedure to add or modify domains on a selected device, such as a Cisco Catalyst chassis.



Note

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

Procedure

-
- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > context > Device RBAC > Domains**.
 - To configure a configuration building block, select **Config > Global > Building Blocks > building_block > Role-Based Access Control > Domains**.
- The Domains table appears.
- Step 2** Select the type of configuration you want to perform:
- To add a new domain, click **Add**, enter the Domain Name, then click **Deploy Now**.
 - To edit a domain, select the domain you want to configure, then click **Edit**.
- The Domain Object field appears below the Domain Name in the content area.
- Step 3** Click **Edit** to enter the Domain Object table.

Step 4 Select the type of configuration you want to perform:

- Click **Add** to create domain objects for this domain. See [Table 2-17](#) for Domain Object attributes.
- To remove an object, select the object you want to remove, then click **Delete**.

Table 2-17 *Domain Attributes*

Field	Description
Object Type	The collection of objects which comprise this domain. The following options may be available depending on your virtual context: • All • Access list—Ethertype • Access list—Extended • Class-map • Interface VLAN • Interface BVI • Parameter map • Policy map • Probe • Real server • Script • Server farm • Sticky
Object Name	This field appears when any specific object type is selected. Name of an existing object defined.

Step 5 Click **Deploy Now**.

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

Related Topics

- [Configuring Device RBAC Domains, page 2-48](#)
- [Configuring Device Role-Based Access Controls, page 2-40](#)

Modifying Device Domains

Use this option to change the settings in a domain.

**Note**

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

Procedure

-
- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > context > Device RBAC > Domains**.
 - To configure a configuration building block, select **Config > Global > Building Blocks > building_block > Role-Based Access Control > Domains**.
- Step 2** Select the domain you want to change. Click **Edit**.
- Step 3** Click **Edit** to edit the domain object. For details on object fields, see [Table 2-17](#).
- Step 4** Make the changes.
- Step 5** Click **Deploy Now**.
-

Related Topics

- [Configuring Device RBAC Domains, page 2-48](#)
- [Configuring Device Role-Based Access Controls, page 2-40](#)

Deleting Device Domains

Use this option to delete a network domain from the system, as well as all the devices and subdomains it contains.

**Note**

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

Procedure

-
- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > context > Device RBAC > Domains**.
 - To configure a configuration building block, select **Config > Global > Building Blocks > building_block > Role-Based Access Control > Domains**.
- Step 2** Select the domain you want to delete.
- Step 3** Click **Delete**. A prompt asks if you to confirm this action.
- Step 4** Click **OK**. The domain is removed from the ANM database.
-

Related Topic

- [Configuring Device RBAC Domains, page 2-48](#)
- [Configuring Device Role-Based Access Controls, page 2-40](#)

Managing Devices

The following topics describe additional options for managing devices:

- [Synchronizing Device Configurations, page 2-52](#)
- [Configuring User-Defined Groups, page 2-54](#)
- [Updating Chassis Passwords, page 2-57](#)
- [Changing ACE Module Passwords, page 2-58](#)
- [Synchronizing Module Configurations, page 2-53](#)
- [Restarting Device Polling, page 2-59](#)
- [Viewing All Devices, page 2-60](#)
- [Viewing Modules by Chassis, page 2-61](#)
- [Removing Modules from the ANM Database, page 2-62](#)

Synchronizing Device Configurations

ANM provides three levels of synchronization. You can choose to “sync up” from the device to ANM:

- From the chassis level—Use this when you want to sync up Catalyst chassis and module updates. See [Synchronizing Chassis Configurations, page 2-52](#).
- From the ACE module level—Use this when you want to synchronize changes to your ACE or CSM modules, such as new virtual contexts. See [Synchronizing Module Configurations, page 2-53](#).
- From the virtual context level —Use this at the Admin level to synchronize all current and new VCs or at the individual level to synchronize a specific virtual context. See [Synchronizing Virtual Context Configurations, page 3-66](#).

**Caution**

It is important to note that if you see a difference between the ANM management system and your network device information, the management system contains the data that is least accurate. This is because of CLI access to network devices and the ability to change things outside of the ANM. We recommend that you synchronize the network devices up to the ANM using the Sync option, thus making the ANM data more accurate.

Synchronizing Chassis Configurations

ANM allows you to manually synchronize the configuration for Cisco Catalyst chassis, CSS devices, GSS devices and ACE appliances when there have been changes to a device that are not tracked in ANM.

**Note**

ANM does not support auto sync for Catalyst 6500/Cisco 7600) chassis, CSM, CSS and GSS devices. Be sure to synchronize configurations on these devices after import, and whenever their configurations have been modified via the CLI.

Changes that require synchronization include such items as:

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

Use this procedure to synchronize configurations for Cisco Catalyst chassis, CSS devices, and ACE appliances.

Procedure

-
- Step 1** Select **Config > Devices > All Devices**. The All Devices table appears.
- Step 2** Select the device with the configuration that you want to synchronize, then click **CLI Sync**. A window appears asking you to confirm the synchronization.
- Step 3** Click **OK** to synchronize the configuration or **Cancel** to cancel the synchronization.
- The ANM displays status while synchronization is in progress and returns to the All Devices table when synchronization is complete.
-

Related Topics

- [Configuring Devices, page 2-22](#)
- [Synchronizing Module Configurations, page 2-53](#)
- [Restarting Device Polling, page 2-59](#)

Synchronizing Module Configurations

The ANM allows you to synchronize the configuration for ACE or CSM modules or when there have been changes to the module that are not tracked in ANM. Changes that require synchronization for a module include such items as:

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

Use this procedure to synchronize configurations for ACE or CSM modules.

Procedure

-
- Step 1** Select **Config > Devices > All Devices**. The All Devices table appears.
- Step 2** Select the chassis containing the module with the configuration you want to synchronize, then click **Modules**. The Modules table appears.
- Step 3** Select the module with the configuration you want to synchronize, then click **Sync**. A window appears asking you to confirm the synchronization.
- Step 4** Click **OK** to synchronize the configuration or **Cancel** to cancel the synchronization.

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

Related Topics

- [Configuring Devices, page 2-22](#)
- [Managing Devices, page 2-52](#)
- [Synchronizing Device Configurations, page 2-52](#)

Configuring User-Defined Groups

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

Users can create their own groups, add and remove members, and assign group names that suit their environment and are meaningful to them. For information on managing user-defined groups, see:

- [Adding a User-Defined Group, page 2-54](#)
- [Modifying a User-Defined Group, page 2-55](#)
- [Duplicating a User-Defined Group, page 2-56](#)
- [Deleting a User-Defined Group, page 2-56](#)

**Note**

Device groups continue to display device information even after you remove that device from ANM. This allows the device group information to be easily reassociated if you reimport the device. The device name must remain the same for this to work properly.

Adding a User-Defined Group

Use this procedure to add a user-defined group.

Procedure

-
- Step 1** Select **Config > Devices > All Devices**. The device tree appears.
- Step 2** In the device tree, select **Groups**. The Groups table appears.
- Step 3** Click **Add** to add a new group, or select an existing group, then click **Edit** to modify it. The Group configuration screen appears.

- Step 4** In the Name field, enter a unique name for this group. Valid entries are unquoted text strings with no spaces and a maximum of 26 alphanumeric characters.
- The screen identifies the objects by type and provides a Search field for each:
- Virtual Context Members
 - Device Members
 - CSM Members
- Step 5** To add objects to the group, for each object type, select the object in the Available Items list, then click **Add**. The selected objects appear in the Selected Items list.
- To remove objects that you do not want to include, select the objects in the Selected Items list, then click **Remove**. The items then appear in the Available Items list.
- To search for specific objects, enter a search string containing the object name or part of the object name in the Search field, then click **Search**. The Available Items list refreshes with the objects that meet the search criteria.
- Step 6** In the Description field, enter a description for this group.
- Step 7** Click:
- **Save** to accept your entries and to return to the Groups table.
 - **Cancel** to exit this procedure without saving your entries and to return to the Groups table.
-

Related Topics

- [Configuring User-Defined Groups, page 2-54](#)
- [Modifying a User-Defined Group, page 2-55](#)
- [Duplicating a User-Defined Group, page 2-56](#)
- [Deleting a User-Defined Group, page 2-56](#)

Modifying a User-Defined Group

Use this procedure to change the members or the description of a user-defined group. You cannot change the name of an existing user-defined group.

Procedure

-
- Step 1** Select **Config > Devices > All Devices**. The device tree appears.
- Step 2** In the device tree, click **Groups**. The Groups table appears.
- Step 3** In the Groups table, select the group you want to modify, then click **Edit**. The Group configuration screen appears.
- Step 4** In the each Members field, add or remove group members:
- Select the items you want to add to this group in the Available Items list, then click **Add**.
 - Select the items you want to remove from this group in the Selected Items list, then click **Remove**.
- Step 5** In the Description field, modify the description as needed.

Step 6 Click:

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

Related Topics

- [Configuring User-Defined Groups, page 2-54](#)
- [Adding a User-Defined Group, page 2-54](#)
- [Duplicating a User-Defined Group, page 2-56](#)
- [Deleting a User-Defined Group, page 2-56](#)

Duplicating a User-Defined Group

Use this procedure to duplicate a user-defined group.

Procedure

-
- Step 1** Select **Config > Devices > All Devices**. The device tree appears.
- Step 2** In the device tree, click **Groups**. The Groups table appears.
- Step 3** Select the user-defined group that you want to remove, then click **Duplicate**. A window appears asking you to enter a new name.
- Step 4** Type the new group name, then click **OK**.
- The Groups table refreshes and the duplicated group name appears in the list.
-

Related Topics

- [Configuring User-Defined Groups, page 2-54](#)
- [Adding a User-Defined Group, page 2-54](#)
- [Modifying a User-Defined Group, page 2-55](#)
- [Deleting a User-Defined Group, page 2-56](#)

Deleting a User-Defined Group

Use this procedure to delete a user-defined group.

Procedure

-
- Step 1** Select **Config > Devices > All Devices**. The device tree appears.
- Step 2** In the device tree, click **Groups**. The Groups table appears.
- Step 3** Select the user-defined group that you want to remove, then click **Delete**. A window appears asking you to confirm the deletion.

Step 4 Click:

- **OK** to delete the selected user-defined group. The Groups table refreshes and the deleted group no longer appears.
 - **Cancel** to exit this procedure without deleting the group. The Groups table refreshes.
-

Related Topics

- [Configuring User-Defined Groups, page 2-54](#)
- [Adding a User-Defined Group, page 2-54](#)
- [Modifying a User-Defined Group, page 2-55](#)
- [Duplicating a User-Defined Group, page 2-56](#)

Updating Chassis Passwords

If you change chassis passwords using the CLI, you can update the chassis passwords in ANM without rediscovering or reimporting the chassis information.

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

**Note**

The password changes made in the UI apply to the ANM server *only*. Changing passwords in the Update Password window does not change the Password/Enable password on the device.

Procedure

-
- Step 1** Select **Config > Devices > All Devices**. The All Devices table appears.
- Step 2** Select the chassis with the passwords that you want to update in ANM, then click **Update Password**. The Update Password window appears.
- Step 3** Update the chassis passwords in ANM using the information in [Table 2-18](#).

Table 2-18 *Update Chassis Password Options*

Field	Description
Update	Specify the passwords that you want to update in the ANM: - Both—Update both the chassis password and the chassis enable password. - Password Only—Update the chassis password only. - Enable Password Only—Update the chassis enable password only.
New Password	Enter the updated chassis password.
Confirm New Password	Reenter the updated chassis password.
New Enable Password	Enter the updated enable password for the chassis.
Confirm New Enabled Password	Reenter the updated enable password for the chassis.

Related Topics

- [Changing ACE Module Passwords, page 2-58](#)
- [Managing Devices, page 2-52](#)
- [Configuring Devices, page 2-22](#)

Changing ACE Module Passwords

**Note**

This functionality is available only in Admin contexts.

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

Assumption

The ACE module has been imported into the ANM database and is in an operational state.

Procedure

- Step 1** Select **Config > Devices > All Devices**. The device tree appears.
- Step 2** Select the device containing the ACE module with the password you want to change. The Modules table appears.
- Step 3** Select the module whose password you want to change, then click **Change Card Password**. The Modules configuration screen appears.
- Step 4** In the Card Slot field, confirm that the correct module is selected.
- Step 5** In the Card Type field, confirm that the correct version appears.

- Step 6** In the *Module has been imported into ANM* field, confirm that the check box is selected to indicate that the module has been imported. This is a read-only field.
- Step 7** In the Operation to Perform field, select **Change card password**.
- Step 8** In the Username field, enter the username of the account whose password you want to change.
- Step 9** In the Password field, enter the existing password for the account.
- Step 10** In the New Password field, enter the new password for the account. Valid passwords are unquoted text strings with a maximum of 64 characters. Reenter the password in the Confirm field.
- Step 11** Click:
- **OK** to accept your entries and to return to the Modules table.
 - **Cancel** to exit the procedure without saving your entries and to return to the Modules table.
-

Related Topics

- [Configuring Devices, page 2-22](#)
- [Managing Devices, page 2-52](#)
- [Adding ACE Modules to ANM, page 2-11](#)
- [Updating Chassis Passwords, page 2-57](#)

Restarting Device Polling

Use this procedure to restart monitoring on a device that has stopped or failed to start.

Procedure

- Step 1** Select **Config > Devices > All Devices**. The All Devices table appears.
- Step 2** Select the device whose monitoring has stopped or failed, then click **Restart Polling**. The All Devices table refreshes with updated polling status. For a description of the various polling status variables see [Table 2-19 on page 2-60](#).

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

Related Topics

- [Configuring Devices, page 2-22](#)
- [Adding and Managing Devices, page 2-1](#)

Viewing All Devices

Use this procedure to view all devices that have been imported into the ANM database.

Procedure

-
- Step 1** Select **Config > Devices**. The device tree appears.
- Step 2** Select **All Devices**. The All Devices table displays information for the devices being managed by the ANM (see [Table 2-19](#)).

Table 2-19 All Devices Table Attributes

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

Related Topics

- [Adding and Managing Devices, page 2-1](#)
- [Configuring Cisco Catalyst Chassis and 7600 Series Router Primary Attributes, page 2-26](#)
- [Viewing and Configuring Device Interfaces, page 2-28](#)

Viewing Modules by Chassis

For devices that contain modules, such as Cisco Catalyst chassis, you can use this procedure to view all modules on a specific chassis.

Procedure

-
- Step 1** Select **Config > Devices > All Devices**. The All Devices table appears.
- Step 2** Select the chassis containing the modules that you want to view, then click **Modules**. The Modules table appears, listing all modules on that chassis with the following information:
- Slot number
 - Service module model
 - Module type, such as Cisco Content Switching Module (CSM), ACE module and version, or other modules, such as supervisor modules
 - Serial number
 - Module operational state, such as Up, Powered Off, or Not Imported
 - Version of software the module is running
 - Brief description
 - For ACE modules, the number of virtual contexts configured on the module
- Depending on the type of module selected, such as CSM or ACE modules, the following options are available from this screen:
- Import—Use this option to import an ACE module that resides in the selected chassis but that has not yet been imported into the ANM database. For more information, see [Adding ACE Modules to ANM, page 2-11](#) or [Importing Cisco Content Switching Module \(CSM\) Devices, page 2-13](#).
 - Change Card Password—Use this option to change the administrative password on an ACE module that has been imported into the ANM database. For more information, see [Changing ACE Module Passwords, page 2-58](#).
 - Do Not Manage—Use this option to remove a selected ACE module from the ANM database. For more information, see [Removing Modules from the ANM Database, page 2-62](#).
- Step 3** To view the modules of another chassis, select another chassis in the device tree or use the chassis selector field at the top of the screen.
-

Related Topics

- [Viewing and Configuring Device Interfaces, page 2-28](#)
- [Managing Device VLANs, page 2-35](#)
- [Adding ACE Modules to ANM, page 2-11](#)
- [Importing Cisco Content Switching Module \(CSM\) Devices, page 2-13](#)

Removing Modules from the ANM Database

Use this procedure to remove a module from the ANM database.

**Note**

If you physically replace an ACE module in a chassis, you need to synchronize the chassis in the ANM. See [Synchronizing Chassis Configurations, page 2-52](#) for more information.

Procedure

-
- Step 1** Select **Config > Devices > All Devices**. The All Devices table appears.
- Step 2** Select the device containing the module you want to remove, then click **Modules**. The Modules table appears.
- Step 3** Select the module you want to remove from ANM management, then click **Do Not Manage**. The Modules configuration screen appears.
- Step 4** Confirm the information in the following fields:
- Card Slot
 - Card Type
 - Module has been imported into ANM
- Step 5** In the Operation to Perform field, select **Do Not Manage**.
- Step 6** Click:
- **OK** to confirm removal of the module. The Modules table refreshes and the removed module appears with the state Not Imported.
You can import the module again when desired (see [Adding ACE Modules to ANM, page 2-11](#)).
 - **Cancel** to exit the procedure without removing the ACE module and to return to the Modules table.
-

Related Topics

- [Adding Network Devices into ANM, page 2-7](#)
- [Changing ACE Module Passwords, page 2-58](#)



CHAPTER 3

Configuring Virtual Contexts

Revised Date: 3/25/09

Cisco Application Networking Manager (ANM) provides a number of options for configuring Cisco Application Control Engine (ACE) hardware.

For information about these options, see:

- [Using Virtual Contexts, page 3-1](#)
- [Creating Virtual Contexts, page 3-2](#)
- [Configuring Virtual Contexts, page 3-5](#)
- [Configuring Virtual Context System Attributes, page 3-11](#)
- [Configuring Virtual Context Primary Attributes, page 3-11](#)
- [Configuring Virtual Context Syslog Settings, page 3-12](#)
- [Configuring SNMP for Virtual Contexts, page 3-19](#)
- [Configuring Virtual Context Global Traffic Policies, page 3-26](#)
- [Managing ACE Licenses, page 3-27](#)
- [Using Resource Classes, page 3-32](#)
- [Using Global Resource Classes, page 3-35](#)
- [Using Local Resource Classes, page 3-41](#)
- [Configuring Security with ACLs, page 3-43](#)
- [Configuring Object Groups, page 3-52](#)
- [Managing ACLs, page 3-60](#)
- [Configuring Virtual Context Expert Options, page 3-62](#)
- [Comparing Context and Building Block Configurations, page 3-62](#)
- [Managing Virtual Contexts, page 3-63](#)

Using 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.

The first time you configure a virtual context, you will see only the Admin context. In addition to the configurable attributes of other virtual contexts, the Admin context can configure:

- High Availability (HA or fault tolerance between ACE devices)
- Resource classes
- ACE licenses

**Note**

If you restore the ANM database from a backup repository and 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 3-2](#)
- [Configuring Virtual Contexts, page 3-5](#)
- [Deleting Virtual Contexts, page 3-68](#)
- [Comparing Context and Building Block Configurations, page 3-62](#)
- [Restarting Virtual Context Polling, page 3-69](#)
- [Managing Virtual Contexts, page 3-63](#)

Creating Virtual Contexts

Use this procedure to 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 [Managing User Roles, page 15-43](#) and [Managing Domains, page 15-49](#).

Assumption

The ANM is populated with ACE devices.

Procedure

- Step 1** Select **Config > Devices**, then select the ACE to which you want to add a virtual context. The Virtual Contexts table appears.

**Tip**

The ANM device tree indicates the type of ACE device by notation on the device:

- ACE devices with no red notation indicate ACE 1.0 modules.
- ACE devices with a red 2 indicate ACE 2.0 modules.
- ACE devices with a red 3 indicate ACE appliances.

- Step 2** Click **Add**. The New Virtual Context screen appears.
- Step 3** Configure the virtual context, using the information in [Table 3-1](#).

**Tip**

Fields that contain 3 or fewer choices use radio buttons. Fields that contain more than 3 choices use dropdown lists.

Table 3-1 **Virtual Context Configuration Attributes**

Field	Description
Name	Enter a 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	Select the device to associate with this context. This field appears for new contexts only.
Module	This field appears for chassis that contain multiple modules and for new contexts only. Select the module to associate with this context.
Resource Class	Select the resource class that this virtual context is to use.
Tagged Building Block to Apply ¹	Select the configuration building block to apply to this context.
Allocate-Interface VLANs	Enter the number of a VLAN or a range of VLANs so that the context can receive the associated traffic. You can specify VLANs in any of the following ways: - For a single VLAN, enter an integer from 2 to 4096. - For multiple, non-sequential VLANs, use comma-separated entries, such as 101, 201, 302. - For a range of VLANs, use the format <i><beginning-VLAN>-<ending-VLAN></i>, such as 101-150. Note VLANs cannot be modified in an Admin context.
Description	Enter a brief description of the virtual context.
Policy Name	This field is read-only for existing contexts and read/write if the virtual context was created using the CLI.
VLAN to use	Enter the VLAN that is to use for remote management of the context. Note For ACE 2.0 modules, you need to specify a management VLAN for the Admin context only; additional contexts will be polled using the same VLAN. For ACE 1.0 modules and ACE appliances, you need to specify a management VLAN for each context individually or the contexts will not be polled.
Management IP	Enter the 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 Interface Policy Map Use” section on page 9-7.
Management Netmask	Select the subnet mask to apply to this IP address.

Table 3-1 Virtual Context Configuration Attributes (continued)

Field	Description
Protocols to Allow	Select the protocols to allow on this VLAN. To specify protocols, select them in the Available Items list, then clicking Add. They then appear in the Selected Items list. To remove protocols, select them in the Selected Items list, then click Remove. They then appear in the Available Items lists. • HTTP—Specifies the Hypertext Transfer Protocol (HTTP). • HTTPS—Specifies the secure (SSL) Hypertext Transfer Protocol (HTTP) for connectivity with the ANM interface. • ICMP—Specifies the Internet Control Message Protocol (ICMP), commonly referred to as ping. • SNMP—Specifies the Simple Network Management Protocol (SNMP).  Note If SNMP is not selected, the 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. • KALAP UDP—Specifies the Keepalive Appliance Protocol over UDP. This option is available for ACE 2.0 modules and ACE 4710 A3(1.0) release only. • XML-HTTPS—Specifies HTTPS as the transfer protocol for sending and receiving XML documents between the ACE appliance and a Network Management System (NMS). This option is available for ACE appliances only. You can select multiple protocols by holding down the Shift key while selecting protocols or by holding down the mouse button while dragging it over the protocols.
Default Gateway IP	Enter the 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.
SNMP Community	If SNMP is one of the allowed protocols, enter the SNMP version 2c community string to be used. Note If SNMP is not an allowed protocol, the ANM will not be able to poll the context.

1. Building blocks were referred to as *configuration templates* in ANM 1.1.

Step 4 Click:

- **Deploy Now** to deploy this context. The screen refreshes and you can continue with virtual context configuration (see [Configuring Virtual Contexts, page 3-5](#)).
- **Cancel** to exit this procedure without saving your entries. The Virtual Contexts table appears.

Related Topics

- [Using Virtual Contexts, page 3-1](#)
- [Configuring Virtual Contexts, page 3-5](#)

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 select **Config > Devices > context** depend on the:

- Type of ACE device associated with the context: ACE 1.0 module, ACE 2.0 module, or ACE appliance.
- Role associated with your account, such as Admin, Network-Admin, or SSL-Admin.
- Context you are configuring: An Admin context or a user context.

Table 3-2 describes configuration options for Admin contexts for ACE modules and ACE appliances although not all options are available for both types of devices.

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

**Note**

You cannot modify a virtual context with the CLI Sync Status *Import Failed*. 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**).

Conventions

The ANM uses the following screen conventions:

- Fields with 1 to 3 choices use radio buttons. Fields with more than 3 choices use dropdown lists.
- The ANM device tree indicates the type of ACE device by red notation on the device:
 - No red notation indicates ACE 1.0 modules.
 - A red 2 indicates ACE 2.0 modules.

- A red 3 indicates ACE appliances.

Table 3-2 Virtual Context Configuration Options

Configuration Subset	Description	Related Topics
System	The System configuration subset includes: • 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 Note ACE licenses and resource classes can be configured in an Admin context only.	• Configuring Virtual Context Primary Attributes, page 3-11 • Configuring Virtual Context Syslog Settings, page 3-12 • Configuring SNMP for Virtual Contexts, page 3-19 • Configuring Virtual Context Global Traffic Policies, page 3-26 • Managing ACE Licenses, page 3-27 • Using Resource Classes, page 3-32
Load Balancing	Load-balancing attributes allow you to: • 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	• Load Balancing Overview, page 4-1 • Configuring Virtual Servers, page 4-2 • Configuring Server Farms, page 5-12 • Configuring Health Monitoring for Real Servers, page 5-25 • Configuring Sticky Groups, page 6-7 • Configuring Parameter Maps, page 7-1

Table 3-2 **Virtual Context Configuration Options (continued)**

Configuration Subset	Description	Related Topics
SSL	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 8-1 • Using SSL Certificates, page 8-5 • Using SSL Keys, page 8-8 • Generating CSRs, page 8-21 • Configuring SSL Parameter Maps, page 8-15 • Configuring SSL Chain Group Parameters, page 8-18 • Configuring SSL Proxy Service, page 8-22 • Configuring SSL Authentication Groups, page 8-24 • Configuring CRLs for Client Authentication, page 8-25
Security	Security configuration options enable you to create access control lists, set ACL attributes, resequence ACLs, delete ACLs, and configure object groups.	• Configuring Security with ACLs, page 3-43 • Creating ACLs, page 3-44 • Configuring Object Groups, page 3-52
Network	Network configuration options allow you to configure: • VLAN interfaces • BVI interfaces • Static routes • DHCP relay agents • Port channel interfaces • Gigabit Ethernet interfaces • Over 8,000 static NAT configurations	• Configuring VLAN Interfaces, page 9-2 • Configuring Virtual Context BVI Interfaces, page 9-12 • Configuring Virtual Context Static Routes, page 9-14 • Configuring VLAN Interface DHCP Relay, page 9-12 • Configuring Port Channel Interfaces, page 9-21 • Configuring Gigabit Ethernet Interfaces, page 9-17 • Configuring Static VLANs for Over 8 K Static NAT Configurations, page 9-16
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 High Availability Overview, page 10-4 • Configuring ACE High Availability Peers, page 10-5 • Configuring High Availability Groups, page 10-8

Table 3-2 Virtual Context Configuration Options (continued)

Configuration Subset	Description	Related Topics
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 10-13 • Tracking VLAN Interfaces for High Availability, page 10-13 • Tracking Hosts for High Availability, page 10-14 • Configuring ACE HSRP Groups, page 10-18
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 How ANM Handles Role-Based Access Control , page 15-7.	• Configuring Device RBAC Users, page 2-40 • Configuring Device RBAC Roles, page 2-43 • Configuring Device RBAC Domains, page 2-48
Expert	Expert attributes allow you to configure traffic policies, configure optimization action lists, and compare a context's configuration with the building block that is associated with it.	• Configuring Virtual Context Class Maps, page 11-6 • Configuring Virtual Context Policy Maps, page 11-30 • Configuring Action Lists for Application Acceleration and Optimization, page 12-3 • Comparing Context and Building Block Configurations, page 3-62

Table 3-3 Configuration Options by Device Type

Menu Option	ACE Device Type				Related Topic
	ACE 1.0	ACE 2.0	ACE 4710 Running Image A1(8)	ACE 4710 Running Image A3(1.0)	
System					
Primary Attributes	X	X	X	X	Configuring Virtual Context Primary Attributes, page 3-11
Syslog	X	X	X	X	Configuring Virtual Context Syslog Settings, page 3-12
SNMP	X	X	X	X	Configuring SNMP for Virtual Contexts, page 3-19
Global Policy	X	X	X	X	Configuring Virtual Context Global Traffic Policies, page 3-26
Licenses	X	X	X	X	Managing ACE Licenses, page 3-27
Application Acceleration and Optimization			X	X	Configuring Global Application Acceleration and Optimization, page 12-16

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

Menu Option	ACE Device Type				Related Topic
	ACE 1.0	ACE 2.0	ACE 4710 Running Image A1(8)	ACE 4710 Running Image A3(1.0)	
Resource Classes	X	X	X	X	Using Resource Classes, page 3-32
Load Balancing					
Virtual Servers	X	X	X	X	Configuring Virtual Servers, page 4-2
Real Servers	X	X	X	X	Configuring Real Servers, page 5-4
Server Farms	X	X	X	X	Configuring Server Farms, page 5-12
Health Monitoring	X	X	X	X	Configuring Health Monitoring for Real Servers, page 5-25
Stickiness	X	X	X	X	Configuring Sticky Groups, page 6-7
HTTP Parameter Map	X	X	X	X	Configuring HTTP Parameter Maps, page 7-8
Connection Parameter Map	X	X	X	X	Configuring Connection Parameter Maps, page 7-2
Optimization Parameter Map			X	X	Configuring Optimization Parameter Maps, page 7-10
Generic Parameter Map		X		X	Configuring Generic Parameter Maps, page 7-7
RTSP Parameter Map		X		X	Configuring RTSP Parameter Maps, page 7-17
SIP Parameter Map		X		X	Configuring SIP Parameter Maps, page 7-18
Skinny Parameter Map		X		X	Configuring Skinny Parameter Maps, page 7-20
SSL					
Certificates	X	X	X	X	Using SSL Certificates, page 8-5
Keys	X	X	X	X	Using SSL Keys, page 8-8
Parameter Map	X	X	X	X	Configuring SSL Parameter Maps, page 8-15
Chain Group Parameters	X	X	X	X	Configuring SSL Chain Group Parameters, page 8-18
CSR Parameters	X	X	X	X	Configuring SSL CSR Parameters, page 8-19
Proxy Service	X	X	X	X	Configuring SSL Proxy Service, page 8-22
Auth Group Parameters		X		X	Configuring SSL Authentication Groups, page 8-24
Certificate Revocation List		X		X	Configuring CRLs for Client Authentication, page 8-25
Security					
ACLs	X	X	X	X	Creating ACLs, page 3-44
Object Groups		X		X	Configuring Object Groups, page 3-52

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

Menu Option	ACE Device Type				Related Topic
	ACE 1.0	ACE 2.0	ACE 4710 Running Image A1(8)	ACE 4710 Running Image A3(1.0)	
Network					
Port Channel Interfaces			X	X	Configuring Port Channel Interfaces, page 9-21
Gigabit Ethernet Interfaces			X	X	Configuring Gigabit Ethernet Interfaces, page 9-17
VLAN Interfaces	X	X	X	X	Configuring VLAN Interfaces, page 9-2
BVI Interfaces	X	X	X	X	Configuring Virtual Context BVI Interfaces, page 9-12
Static Routes	X	X	X	X	Configuring Virtual Context Static Routes, page 9-14
Global IP DHCP	X	X	X	X	Configuring Global IP DHCP, page 9-16
Static NAT Overwrite		X			Configuring Static VLANs for Over 8 K Static NAT Configurations, page 9-16
High Availability					
Setup	X	X	X	X	Configuring ACE High Availability Peers, page 10-5
HA Tracking and Failure Detection					
Interfaces	X	X	X	X	Tracking VLAN Interfaces for High Availability, page 10-13
Hosts	X	X	X	X	Tracking Hosts for High Availability, page 10-14
HSRP Groups	X	X	X	X	Configuring ACE HSRP Groups, page 10-18
Role-Based Access Control					
Users	X	X	X	X	Configuring Device RBAC Users, page 2-40
Roles	X	X	X	X	Configuring Device RBAC Roles, page 2-43
Domains	X	X	X	X	Configuring Device RBAC Domains, page 2-48
Expert					
Class Map	X	X	X	X	Configuring Virtual Context Class Maps, page 11-6
Policy Map	X	X	X	X	Configuring Virtual Context Policy Maps, page 11-30
Action List		X	X	X	Configuring Action Lists for Application Acceleration and Optimization, page 12-3
Building Block Audit	X	X	X	X	Comparing Context and Building Block Configurations, page 3-62

Configuring Virtual Context System Attributes

Virtual context System configuration options for all ACE devices are:

- Virtual context primary attributes—See [Configuring Virtual Context Primary Attributes](#), page 3-11.
- Syslog
 - [Configuring Virtual Context Syslog Settings](#), page 3-12
 - [Configuring Syslog Log Hosts](#), page 3-16
 - [Configuring Syslog Log Messages](#), page 3-17
 - [Configuring Syslog Log Rate Limits](#), page 3-18
- SNMP
 - [Configuring SNMP for Virtual Contexts](#), page 3-19
 - [Configuring SNMP Version 2c Communities](#), page 3-20
 - [Configuring SNMP Version 3 Users](#), page 3-21
 - [Configuring SNMP Trap Destination Hosts](#), page 3-23
 - [Configuring SNMP Notification](#), page 3-24
- Global policy maps for all VLANs on a virtual context—See [Configuring Virtual Context Global Traffic Policies](#), page 3-26.
- ACE licenses—See [Managing ACE Licenses](#), page 3-27.
- ACE resource classes—See [Using Resource Classes](#), page 3-32.

For ACE appliances, you can also configure global application acceleration and optimization. See [Configuring Global Application Acceleration and Optimization](#), page 12-16.

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 [Configuring Virtual Contexts](#), page 3-5.

Procedure

-
Step 1	Select Config > Devices > context > System > Primary Attributes . The Primary Attributes configuration screen appears.
Step 2	Enter the primary attributes for this virtual context using the information in Table 3-1 .
Step 3	Click Deploy Now to save your entries and to return to the Virtual Contexts table.
-

Related Topics

- [Using Virtual Contexts](#), page 3-1
- [Configuring VLAN Interfaces](#), page 9-2
- [Configuring Virtual Context BVI Interfaces](#), page 9-12

- [Configuring Virtual Context Syslog Settings, page 3-12](#)
- [Configuring Traffic Policies, page 11-1](#)

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 Select the item to configure:

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

The Syslog configuration screen appears.

Step 2 Enter the syslog logging attributes in the displayed fields (see [Table 3-5](#)).

All fields that require you to select syslog severity levels use the values in [Table 3-4](#).

Table 3-4 Syslog Logging Levels

Severity	Description
Emergency	Unusable system
Alert	Immediate action required
Critical	Critical condition
Error	Error condition
Warning	Warning condition
Notification	Normal but significant condition
Information	Informational message only
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 3-5 *Virtual Context Syslog Configuration Attributes*

Field	Description	Action
Enable Syslog	This option indicates whether syslog logging should be enabled or disabled.	Select the check box to enable syslog logging or clear the check box to disable syslog logging.
Facility	The syslog daemon 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, refer to 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	This option enables system logging to a local buffer and limits the messages sent to the buffer based on severity.	Select 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	This option specifies the maximum level for system log messages sent to the console.	Select 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. Therefore, 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, as it can reduce ACE performance.
History Level	This option specifies the maximum level for system log messages sent as traps to an SNMP network management station.	Select 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	This option specifies the maximum level for system log messages sent to a remote connection using Secure Shell (SSH) or Telnet on the ACE.	Select 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 3-5 Virtual Context Syslog Configuration Attributes (continued)

Field	Description	Action
Persistence Level	This option specifies the maximum level for system log messages sent to Flash memory.	Select 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, since logging at a high rate to Flash memory on the ACE might impact performance.
Trap Level	This option specifies the maximum level for system log messages sent to a syslog server.	Select 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	This option specifies the maximum level for system log messages sent to the supervisor module on the Catalyst chassis. Note This option does not appear for ACE appliances or ACE 4710-type configuration building blocks.	Select the desired level for sending system log messages to the supervisor module on the Catalyst chassis. Note We recommend that you use a lower severity level, such as 3, since logging at a high rate to the supervisor module might impact performance of the Catalyst system.
Queue Size	This option 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	This option indicates whether syslog messages should include the date and time that the message was generated.	Select the check box to enable timestamps on syslog messages or clear the check box to disable timestamps on syslog messages. By default, timestamps are not included on syslog messages.
Enable Standby	This option indicates whether logging is enabled 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.	Select 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	This option indicates whether connection setup and teardown messages are logged.	Select 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 3-5 Virtual Context Syslog Configuration Attributes (continued)

Field	Description	Action
Reject New Connection when TCP Queue Full	This option indicates whether the ACE rejects new connections when the TCP queue is full.	Select 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	This option indicates whether the ACE rejects new connections when the syslog message rate is reached.	Select 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	This option indicates whether the ACE rejects new connections when the syslog daemon buffer is full.	Select the check box to reject new connections when the syslog daemon buffer is full. This option is disabled by default.
Device Id Type	This option 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.	Select the type of device identifier to use: • Undefined—No identifier is used. • Context Name—The name of the current virtual context is used to uniquely identify the syslog messages sent from the ACE. • Hostname—The hostname of the ACE is used to uniquely identify the syslog messages sent from the ACE. • Interface—The IP address of the interface is used to uniquely identify the syslog messages sent from the ACE. If you select this option, enter the name of the interface in the Device Interface Name field. • Any String—A text string that you specify is used to uniquely identify the syslog messages sent from the ACE. If you select this option, enter the text string to use in the Logging Device Id field.
Device Interface Name	This field appears if 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 the ACE uses to send the log data to the external server.
Logging Device Id	This field appears if 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 Finish this procedure:

- For virtual contexts, click **Deploy Now** to save your entries, or select 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.

See [Related Topics](#) for additional syslog configuration options.

Related Topics

- [Configuring Syslog Log Hosts, page 3-16](#)
- [Configuring Syslog Log Messages, page 3-17](#)
- [Configuring Syslog Log Rate Limits, page 3-18](#)

Configuring Syslog Log Hosts

After configuring basic syslog characteristics (see [Configuring Virtual Context Syslog Settings, page 3-12](#)), you can configure the log host, log messages, and log rate limits.

Use this procedure to configure Syslog log hosts.

Procedure

- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > *context* > System > Syslog**.
 - To configure a configuration building block, select **Config > Global > All Building Blocks > *building_block* > System > Syslog**.
- The Syslog configuration screen appears.
- Step 2** Click the Log Host tab. The Log Host table appears.
- Step 3** Click **Add** to add a new log host, or select an existing log host, then click **Edit** to modify it. The Log Host configuration screen appears.
- Step 4** In the IP Address field, enter the IP address of the host to use as the syslog server.
- Step 5** In the Protocol field, select 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 integers from 1-65535.
- Step 7** The Default UDP check box appears if TCP is selected in the Protocol field ([Step 5](#)). Select the Default UDP check box to specify that the ACE is to default to UDP if the TCP transport fails to communicate with the syslog server. Clear this check box to prevent the ACE from defaulting to UDP if the TCP transport fails.
- Step 8** In the Format field, select
- **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 Click:

- **Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts.
 - **OK** to save your entry. This option appears for configuration building blocks.
 - **Cancel** to exit 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 3-12](#)
- [Configuring Syslog Log Messages, page 3-17](#)
- [Configuring Syslog Log Rate Limits, page 3-18](#)

Configuring Syslog Log Messages

After configuring basic syslog characteristics (see [Configuring Virtual Context Syslog Settings, page 3-12](#)), you can configure the log host, log messages, and log rate limits.

Use this procedure to configure Syslog log messages.

Procedure**Step 1** Select the item to configure:

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

The Syslog configuration screen appears.

Step 2 Click the Log Message tab. The Log Message table appears.**Step 3** Click **Add** to add a new entry to this table, or select an existing entry, then click **Edit** to modify it. The Log Message configuration screen appears.**Step 4** In the Message Id field, select 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** Select the Enable State check box to indicate that logging is enabled for the specified message ID. Clear the check box to indicate that logging is not enabled for the specified message ID. If you select the Enable State check box, the Log Level field appears.**Step 6** In the Log Level field, select the desired level of syslog messages to be sent to the syslog server, using the levels identified in [Table 3-4](#).**Step 7** Click:

- **Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts.
- **OK** to save your entry. This option appears for configuration building blocks.
- **Cancel** to exit the procedure without saving your entries and to return to the Log Message table.

- **Next** to deploy your entries and to configure additional syslog message entries for this virtual context.
-

Related Topics

- [Configuring Virtual Contexts, page 3-5](#)
- [Configuring Virtual Context Syslog Settings, page 3-12](#)
- [Configuring Syslog Log Hosts, page 3-16](#)
- [Configuring Syslog Log Rate Limits, page 3-18](#)

Configuring Syslog Log Rate Limits

After configuring basic syslog characteristics (see [Configuring Virtual Context Syslog Settings, page 3-12](#)), you can configure the log host, log messages, and log rate limits.

Use this procedure to configure Syslog log rate limits.

Procedure

- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > *context* > System > Syslog**.
 - To configure a configuration building block, select **Config > Global > All Building Blocks > *building_block* > System > Syslog**.
- The Syslog configuration screen appears.
- Step 2** Click the Log Rate Limit tab. The Log Rate Limit table appears.
- Step 3** Click **Add** to add a new entry to this table, or select an existing entry, then click **Edit** to modify it. The Log Rate Limit configuration screen appears.
- Step 4** In the Type field, select the method by which syslog messages are to be limited:
- **Message**—Syslog messages are limited by message identification number. In the Message Id field, select the syslog message ID for those messages you want to suppress reporting.
 - **Level**—Syslog messages are limited by syslog level. In the Level field, select the level of syslog messages to be sent to the syslog server, using the levels identified in [Table 3-4](#).
- Step 5** Select the Unlimited check box to apply no limits to system message logging. Clear the Unlimited check box to apply limits to system message logging. If you clear the Unlimited check box, the Rate and Time Interval fields appear.
- Step 6** If you clear the Unlimited check box, specify the limits to apply to system message logging:
- a. In the Rate field, enter the number at which syslog is to be limited. When this limit is reached, the ACE rejects new syslog messages. Valid entries are integers from 0 to 2147483647.
 - b. In the Time Interval 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** Click:
- **Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts.

- **OK** to save your entry. This option appears for configuration building blocks.
- **Cancel** to exit the procedure without saving your entries and to return to the Log Rate Limit table.
- **Next** to deploy your entries and to add another entry to the Log Rate Limit table.

Related Topics

- [Configuring Virtual Contexts, page 3-5](#)
- [Configuring Virtual Context Syslog Settings, page 3-12](#)
- [Configuring Syslog Log Hosts, page 3-16](#)
- [Configuring Syslog Log Messages, page 3-17](#)

Configuring SNMP for Virtual Contexts

Use this procedure to configure SNMP for use with this virtual context.

Procedure

- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > context > System > SNMP**.
 - To configure a configuration building block, select **Config > Global > All Building Blocks > building_block > System > SNMP**.
- The SNMP configuration screen appears.
- Step 2** Configure SNMP using the information in [Table 3-6](#).

Table 3-6 *SNMP Attributes*

Field	Description
Contact Info	Enter 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	Enter the 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.
Trap Source Interface	Select the VLAN that identifies the interface from which SNMP traps originate.
IETF Trap	Select the check box to indicate that the ACE is to send linkUp and linkDown traps with the IETF standard IF-MIB (RFC 2863) variable bindings, consisting of ifIndex, ifAdminStatus, and ifOperStatus. Clear the check box to indicate that the ACE is not 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** Finish the procedure:

- For virtual contexts, click **Deploy Now** to save your entries or select another configuration option to exit the procedure without saving your entries.
- For configuration building blocks, click **OK** to save your entries or select another configuration option to exit the procedure without saving your entries.

See [Related Topics](#) for additional SNMP configuration options.

Related Topics

- [Configuring Virtual Contexts, page 3-5](#)
- [Configuring SNMP Version 2c Communities, page 3-20](#)
- [Configuring SNMP Version 3 Users, page 3-21](#)
- [Configuring SNMP Trap Destination Hosts, page 3-23](#)
- [Configuring SNMP Notification, page 3-24](#)

Configuring SNMP Version 2c Communities

After configuring basic SNMP information for a virtual context (see [Configuring SNMP for Virtual Contexts, page 3-19](#)), you can configure other SNMP attributes such as SNMP version 2c communities, SNMP version 3 users, trap destination hosts, and SNMP notification.



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

Use this procedure to configure SNMP communities for a virtual context or configuration building block.

Assumption

You have configured at least one SNMP contact (see [Configuring SNMP for Virtual Contexts, page 3-19](#)).

Procedure

Step 1 Select the item to configure:

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

The SNMP configuration screen appears.

Step 2 Click the SNMP v2c Community String tab. The SNMP v2c Community String table appears.

Step 3 Click **Add** to add an SNMP v2c community string. The SNMP v2c Community String configuration screen appears.



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

- Step 4** In the Community field, enter the SNMP community name. Valid entries are unquoted text strings with no spaces and a maximum of 32 characters.
- Step 5** Click:
- **Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts.
 - **OK** to save your entry. This option appears for configuration building blocks.
 - **Cancel** to exit this procedure without saving your entry and to return to the SNMP v2c Community String table.
 - **Next** to deploy your entry and to configure another SNMP community string. The screen refreshes and you can enter another community string.
-

Related Topics

- [Configuring Virtual Contexts, page 3-5](#)
- [Configuring SNMP Version 3 Users, page 3-21](#)
- [Configuring SNMP Trap Destination Hosts, page 3-23](#)
- [Configuring SNMP Notification, page 3-24](#)

Configuring SNMP Version 3 Users

After configuring basic SNMP information for a virtual context (see [Configuring SNMP for Virtual Contexts, page 3-19](#)), you can configure other SNMP attributes such as SNMP version 2c communities, SNMP version 3 users, trap destination hosts, and SNMP notification.

Use this procedure to configure SNMP version 3 users for a virtual context or configuration building block.

Assumption

You have configured at least one SNMP contact (see [Configuring SNMP for Virtual Contexts, page 3-19](#)).

Procedure

-
- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > context > System > SNMP**.
 - To configure a configuration building block, select **Config > Global > All Building Blocks > building_block > System > SNMP**.
- The SNMP configuration screen appears.
- Step 2** Click the SNMP v3 Configuration tab. The SNMP v3 Configuration table appears.
- Step 3** Click **Add** to add users, or select an existing entry in the SNMP v3 Configuration table, then **Edit** to modify it. The SNMP v3 Configuration screen appears.
- Step 4** Enter SNMP user attributes using the information in [Table 3-7](#).

Table 3-7 *SNMP User Configuration Attributes*

Field	Description
User Name	Enter the SNMP username. Valid entries are unquoted text strings with no spaces and a maximum of 24 characters.
Auth Algorithm	Select the authentication algorithm to be used for this user. - N/A—No authentication algorithm is used. - MD5—Message Digest 5 is used as the authentication mechanism. - SHA—Secure Hash Algorithm is used as the authentication mechanism.
Auth Password	Appears if you select an authentication algorithm. Enter the authentication password for this user. Valid entries are unquoted text strings with no spaces and a maximum of 130 characters. The ACE automatically updates the password for the CLI user with the SNMP authentication password.
Confirm	Appears if you select an authentication algorithm. Reenter the authentication password.
Localized	Appears if you select an authentication algorithm. Indicate whether 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	Appears if you select an authentication algorithm. Indicate whether 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.
AES 128	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. - N/A—This option is not configured. - False—AES 128 is not used for privacy. - True—AES 128 is used for privacy.
Privacy Password	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	Appears if you set Privacy to True. Reenter the privacy password.

Step 5 Click:

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

Related Topics

- [Configuring Virtual Contexts, page 3-5](#)
- [Configuring SNMP Version 2c Communities, page 3-20](#)
- [Configuring SNMP Trap Destination Hosts, page 3-23](#)
- [Configuring SNMP Notification, page 3-24](#)

Configuring SNMP Trap Destination Hosts

To receive SNMP notifications you must configure:

- At least one SNMP trap destination host. This section describes how to do this.
- At least one type of notification. See [Configuring SNMP Notification, page 3-24](#).

After configuring basic SNMP information for a virtual context (see [Configuring SNMP for Virtual Contexts, page 3-19](#)), you can configure other SNMP attributes such as SNMP version 2c communities, SNMP version 3 users, trap destination hosts, and SNMP notification.

Use this procedure to configure SNMP trap destination hosts for a virtual context.

Assumption

You have configured at least one SNMP contact (see [Configuring SNMP for Virtual Contexts, page 3-19](#)).

Procedure

Step 1 Select the item to configure:

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

The SNMP configuration screen appears.

Step 2 Click the Trap Destination Host tab. The Trap Destination Host table appears.**Step 3** Click **Add** to add a host, or select an existing entry in the table, then **Edit** to modify it. The Trap Destination Host configuration screen appears.**Step 4** In the IP Address field, 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, select the version of SNMP used to send traps:
- V1—SNMP version 1 is used to send traps. This option is not available for use with SNMP inform requests.
 - V2c—SNMP version 2c is used to send traps.
 - V3—SNMP version 3 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** Click:
- **Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts.
 - **OK** to save your entries. This option appears for configuration building blocks.
 - **Cancel** to exit this procedure without saving your entries and to return to the Trap Destination Host table.
 - **Next** to deploy your entries and to add another entry to the Trap Destination Host table. The screen refreshes and you can add another trap destination host.
-

Related Topics

- [Configuring Virtual Contexts, page 3-5](#)
- [Configuring SNMP Version 2c Communities, page 3-20](#)
- [Configuring SNMP Version 3 Users, page 3-21](#)
- [Configuring SNMP Notification, page 3-24](#)

Configuring SNMP Notification

After configuring basic SNMP information for a virtual context (see [Configuring SNMP for Virtual Contexts, page 3-19](#)), you can configure other SNMP attributes such as SNMP version 2c communities, SNMP version 3 users, trap destination hosts, and SNMP notification.

To receive SNMP notifications you must configure:

- At least one SNMP trap destination host. See [Configuring SNMP Trap Destination Hosts, page 3-23](#).
- At least one type of notification. This section describes how to do this.

Use this procedure to configure SNMP notification for a virtual context.

Assumptions

- You have configured at least one SNMP contact (see [Configuring SNMP for Virtual Contexts, page 3-19](#)).
- At least one SNMP server host has been configured (see [Configuring SNMP Trap Destination Hosts, page 3-23](#)).

Procedure

- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > context > System > SNMP**.
 - To configure a configuration building block, select **Config > Global > All Building Blocks > building_block > System > SNMP**.
- The SNMP configuration screen appears.
- Step 2** Click the SNMP Notification tab. The SNMP Notification table appears.
- Step 3** Click **Add** to add a new entry, or select an existing entry in the table, then click **Edit** to modify it. The SNMP Notification configuration screen appears.
- Step 4** In the Options field, select 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 select the more specific options. For example, select Slb real or Slb vserver instead of Slb. This ensures that the correct commands are issued on the ACE appliance.

- License—SNMP license notifications are to be sent. This option is available only in the Admin context.
- Virtual-context—Notifications are to be sent upon changes to a virtual context. This option is available only in the Admin context.
- Slb—Server load-balancing notifications are to be sent.
- Slb real—Notifications of real server state changes are to be sent.
- Slb vserver—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 coldstart—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 linkdown—Notifications are to be sent when a VLAN interface is down.
- Snmp linkup—Notifications are to be sent when a VLAN interface is up.
- Syslog—Error message notifications (Cisco Syslog MIB) are to be sent.

- Step 5** Click:
- **Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts.
 - **OK** to save your entries. This option appears for configuration building blocks.
 - **Cancel** to exit this procedure without saving your selection and to return to the SNMP Notification table.
 - **Next** to deploy your entries and to add another entry to the SNMP Notification table. The screen refreshes and you can select another SNMP notification option.

Related Topics

- [Configuring Virtual Contexts, page 3-5](#)
- [Configuring SNMP Version 2c Communities, page 3-20](#)
- [Configuring SNMP Version 3 Users, page 3-21](#)
- [Configuring SNMP Trap Destination Hosts, page 3-23](#)

Configuring Virtual Context Global Traffic Policies

With the ANM you can apply traffic policies to a specific VLAN interface or to all VLAN interfaces in the same virtual context or configuration building block.

Use this procedure to apply a policy to all VLAN interfaces in the selected context or configuration building block.

To apply a policy to a specific VLAN, see [Configuring Traffic Policies, page 11-1](#).



Note You cannot modify an existing policy. Instead, delete the existing global policy, then create a new one.

Assumption

A Layer 3/Layer 4 or Management policy map has been configured for the selected context or building block. For more information, see [Configuring Virtual Context Policy Maps, page 11-30](#).

Procedure

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

The Global Policy table appears.

- Step 2** Click **Add** to add a new global policy. The Global Policy configuration screen appears.



Note You cannot modify an existing policy. If you want to change the policy map used globally for a context or building block, first delete the existing global policy and then create a new one.

- Step 3** In the Policy Map field, select the policy map that you want to apply to all VLANs in this context.
- Step 4** In the Direction field, verify that the policy applies to incoming traffic.
- Step 5** Click:
- **Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts.
 - **OK** to save your entries. This option appears for configuration building blocks.
 - **Cancel** to exit the procedure without saving your entries and to return to the Global Policy table.
 - **Next** to deploy your entries and to configure another global policy.
-

Related Topics

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

Managing ACE Licenses

**Note**

This functionality is available for only Admin contexts.

Cisco Systems offers licenses for ACE devices that let you increase the number of default contexts, module bandwidth, and SSL TPS (transactions per second). For more information on these licenses, refer to 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 [Managing ANM Licenses, page 15-56](#).

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

Related Topics

- [Viewing ACE Licenses, page 3-27](#)
- [Installing ACE Licenses, page 3-29](#)
- [Updating ACE Licenses, page 3-31](#)
- [Adding Licenses into License Management, page 15-58](#)

Viewing ACE Licenses

**Note**

This functionality is available for only Admin contexts.

Use this procedure to view the licenses that are currently installed on an ACE.

Procedure

-
Step 1	Select Config > Devices . The device tree appears.
Step 2	Select the Admin context with ACE licenses you want to view, then click System > Licenses . The License table appears listing all installed licenses with their filename, vendor, and expiration date.
-

Related Topics

- [Managing ACE Licenses, page 3-27](#)
- [Installing ACE Licenses, page 3-29](#)
- [Uninstalling ACE Licenses, page 3-30](#)
- [Updating ACE Licenses, page 3-31](#)

Importing ACE Licenses

**Note**

This functionality is available for Admin contexts only.

Installing ACE licenses involves two steps:

1. Importing the license from the remote server to the ACE.
2. Installing the license on the ACE. See [Installing ACE Licenses, page 3-29](#).

Use this procedure to import new or upgrade ACE licenses from a remote server to the appropriate ACE.

Assumption

The ACE licenses are available on a remote server for importing to the ACE.

Procedure

-
- Step 1** Select **Config > Devices**. The device tree appears.
- Step 2** Select the Admin context with the license you want to update, then click **System > Licenses**. The License table appears listing all installed licenses.
- Step 3** Click **Install**. The Import License File dialog box appears.
- Step 4** In the Protocol field, select the protocol to use to copy the license file from the remote server to the ACE.
- If you select FTP, continue with [Step 5](#).
 - If you select TFTP, continue with [Step 6](#).
- Step 5** For FTP:
- In the User field, enter the username of the account on the network server.
 - In the Password field, enter the password for the user account. Reenter the password in the Confirm field.
- Step 6** In the Source File Name field, enter the host IP address, path, and filename of the license file on the remote server in the format *host-ip/path/filename* where:
- *host-ip* represents the IP address of the remote server.
 - *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 **192.168.11.2/usr/bin/ACE-VIRT-020.lic**.

**Note**

The license file will reside on disk:0. This option is not configurable from within ANM.

Step 7 Click:

- **OK** to accept your entries and to import the file from the remote server to the selected ACE. When the file has been imported, the License table appears, and you can continue with installing or upgrading licenses. See [Installing ACE Licenses, page 3-29](#).
- **Cancel** to exit this procedure without importing the file from the remote server and to return to the License table.

Related Topics

- [Managing ACE Licenses, page 3-27](#)
- [Installing ACE Licenses, page 3-29](#)
- [Viewing ACE Licenses, page 3-27](#)
- [Uninstalling ACE Licenses, page 3-30](#)
- [Updating ACE Licenses, page 3-31](#)

Installing ACE Licenses

**Note**

This functionality is available for Admin contexts only.

Installing ACE licenses involves two steps:

1. Importing the license from the remote server to the ACE. See [Importing ACE Licenses, page 3-28](#).
2. Installing the license on the ACE.

Use this procedure to install a license on an ACE.

Assumption

You have received the software license key for an ACE and have imported the license file onto that ACE.

Procedure

-
- Step 1** Select **Config > Devices**. The device tree appears.
- Step 2** Select the Admin context for the new license, then click **System > Licenses**. The License table appears listing all installed licenses.
- Step 3** Click **Install**. The Install License dialog box appears.
- Step 4** In the File field, specify the name of the license file:
- To specify a license that does not appear in the drop-down list, select the first radio button, then enter the name of the license file that you have imported and are now installing, such as **ACE-VIRT-020.lic**. You should rarely need to specify a license file with this option.
 - To specify an existing license, select the second radio button, then select the license file from the list of available license files.
- Step 5** In the License Name field, enter the name that you would like to use for this license, such as **myACE-VIRT-020.lic**.

Step 6 Click:

- **OK** to accept your entries and to install the license. When the license is installed, the License table refreshes with the new entry.
- **Cancel** to exit this procedure without installing the license and to return to the License table.

Related Topics

- [Managing ACE Licenses, page 3-27](#)
- [Viewing ACE Licenses, page 3-27](#)
- [Uninstalling ACE Licenses, page 3-30](#)
- [Updating ACE Licenses, page 3-31](#)

Uninstalling ACE Licenses

**Note**

This functionality is available for Admin contexts only.

**Caution**

Removing licenses can affect 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.

Use this procedure to remove ACE licenses.

Procedure

- Step 1** Select **Config > Devices**. The device tree appears.
- Step 2** Select the Admin context with the license you want to remove, then click **System > Licenses**. The License table appears listing all installed licenses.
- Step 3** Select the license to be removed.
- Step 4** Click **Uninstall**. A window 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.

Related Topics

- [Managing ACE Licenses, page 3-27](#)
- [Installing ACE Licenses, page 3-29](#)
- [Viewing ACE Licenses, page 3-27](#)
- [Updating ACE Licenses, page 3-31](#)

Updating ACE Licenses

**Note**

This functionality is available for Admin contexts only.

The ANM allows you to convert demonstration licenses to permanent licenses and to upgrade permanent licenses to increase the number of virtual contexts.

Updating ACE licenses involves two steps:

1. Importing the new license from the remote server onto the ACE. See [Importing ACE Licenses, page 3-28](#).
2. Installing the update license on the ACE. See [Installing ACE Licenses, page 3-29](#).

Use this procedure to install ACE update licenses.

Procedure

-
Step 1	Select Config > Devices . The device tree appears.
Step 2	Select the Admin context with the license you want to update, then click System > Licenses . The License table appears listing all installed licenses.
Step 3	Select the license to be updated, then click Update . The Update License window appears.
Step 4	In the License File Name field, enter the name that you gave the license file on the ACE when you installed it, such as <code>myACE-VIRT-020.lic</code> . (See Installing ACE Licenses, page 3-29 .)
Step 5	Click: • OK to update the license and to return to the License table. The License table displays the updated information. • Cancel to exit this procedure without updating the license and to return to the License table.
-

Related Topics

- [Managing ACE Licenses, page 3-27](#)
- [Installing ACE Licenses, page 3-29](#)
- [Viewing ACE Licenses, page 3-27](#)
- [Uninstalling ACE Licenses, page 3-30](#)

Displaying License Configuration and Statistics

**Note**

This functionality is available for only Admin contexts.

Use this procedure to view information about ACE licenses.

Procedure

-
- Step 1** Select **Config > Devices**. The device tree appears.
- Step 2** Select the Admin context with the license information you want to view, then select **System > Licenses**. The License table appears listing all installed licenses.
- Step 3** Select the license with the information you want to view, then click **Status**. The show license status window appears with the following information for all ACE devices:

- SSL transactions per second
- Number of supported virtual contexts
- ACE bandwidth in gigabits per second

For ACE appliances, it also displays:

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

**Note**

If no licenses are installed apart from the basic 5 context license shipped with the ACE device, you can click the Status button to view its details as described here.

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

Related Topics

- [Managing ACE Licenses, page 3-27](#)
- [Installing ACE Licenses, page 3-29](#)
- [Viewing ACE Licenses, page 3-27](#)
- [Uninstalling ACE Licenses, page 3-30](#)

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 than 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 (regex) 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 3-8](#) identifies and defines the resources that you can establish for resource classes.

Related Topics

- [Global and Local Resource Classes, page 3-33](#)
- [Resource Allocation Constraints, page 3-34](#)
- [Using Global Resource Classes, page 3-35](#)
- [Viewing Local Resource Class Use on Virtual Contexts, page 3-43](#)

Global and Local Resource Classes

The 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. Select **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, the 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, the ANM replaces the properties of the local resource class with those from the global resource class. Select **Config > Global > All Resource Classes** to add, view, modify, audit, or delete global resource classes.

Related Topics

- [Using Resource Classes, page 3-32](#)
- [Resource Allocation Constraints, page 3-34](#)
- [Using Global Resource Classes, page 3-35](#)
- [Using Local Resource Classes, page 3-41](#)
- [Auditing Resource Classes, page 3-38](#)

Resource Allocation Constraints

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

- rate bandwidth
- rate mgmt-traffic
- rate ssl-connections
- rate connections
- mgmt-connections
- conc-connections



Caution

If you allocate 100% 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 3-8 **Resource Class Attributes**

Resource	Definition
Default	The default percentage is used for any resource parameter not explicitly set.
acc-connections	This option is available ACE appliances only. Percentage of application acceleration connections.
acl-memory	Percentage of memory allocated for ACLs.
conc-connections	Percentage of simultaneous connections. Note If you consume all conc-connections by allocating 100% to virtual contexts, IP connectivity to the Admin context can be lost.
http-comp	Percentage of compression for HTTP data. Note This option appears for ACE appliances running OS versions A3(1.0).

Table 3-8 **Resource Class Attributes (continued)**

Resource	Definition
mgmt-connections	Percentage of management connections. Note If you consume all mgmt-connections by allocating 100% to virtual contexts, IP connectivity to the Admin context can be lost.
proxy-connections	Percentage of proxy connections.
regex	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-conn	Percentage of application protocol inspection connections.
rate bandwidth	Percentage of context throughput. Note If you consume all rate bandwidth by allocating 100% to virtual contexts, IP connectivity to the Admin context can be lost.
rate connections	Percentage of connections of any kind. Note If you consume all rate connections by allocating 100% to virtual contexts, IP connectivity to the Admin context can be lost.
rate mgmt-traffic	Percentage of management traffic connections. Note If you consume all rate mgmt-traffic by allocating 100% to virtual contexts, IP connectivity to the Admin context can be lost.
rate ssl-connections	Percentage of SSL connections. Note If you consume all rate ssl-connections by allocating 100% 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 3-35](#)
- [Configuring Global Resource Classes, page 3-36](#)
- [Configuring Local Resource Classes, page 3-41](#)
- [Auditing Resource Classes, page 3-38](#)
- [Deploying Global Resource Classes, page 3-37](#)

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.

The following options are available for global resource classes:

- [Configuring Global Resource Classes, page 3-36](#)
- [Deploying Global Resource Classes, page 3-37](#)
- [Auditing Resource Classes, page 3-38](#)
- [Modifying Global Resource Classes, page 3-39](#)
- [Deleting Global Resource Classes, page 3-40](#)

Configuring Global Resource Classes

Use this procedure to create a new global resource class and optionally to deploy it on an ACE by using the Admin virtual context.



Caution

If you allocate 100% 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, refer to [Resource Allocation Constraints, page 3-34](#).

Procedure

- Step 1** Select **Config > Global > All Resource Classes**. The Resource Classes table appears.
- Step 2** Click **Add** to create a new resource class. The New Resource Class configuration screen appears.
- Step 3** In the Name field, 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, enter the following information in the Default row: (See [Table 3-8](#) for a description of the resources.)
 - a. In the Min field, enter the minimum percentage of each resource you want to allocate to this resource class. Valid entries are numbers from 0 to 100 including those with decimals.
 - b. In the Max field, select the maximum percentage of each resource 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 6** To use different values for the resources, for each resource, select the method for allocating resources:
 - Select **Default** to use the values specified in [Step 5](#).
 - Select **Min** to enter a specific minimum value for the resource.

Step 7 If you select Min:

- 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% of the available ACL memory to this resource class.
- b. In the Max field, select the maximum percentage of the resource 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:

- a. Click **Admin VCs To Deploy To** to expand the configuration subset.
- b. Select the desired Admin context in the Available Items list, then click **Add**. The items appear in the Selected Items list.

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

Step 9 Click:

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

Related Topics

- [Using Resource Classes, page 3-32](#)
- [Modifying Global Resource Classes, page 3-39](#)
- [Deleting Global Resource Classes, page 3-40](#)
- [Auditing Resource Classes, page 3-38](#)

Deploying Global Resource Classes

After you create a global resource class, you can apply it to Admin contexts on selected ACE hardware. If you deploy a global resource class to an ACE that already has a resource class with the same name, the ANM replaces the properties of the local resource class with those 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, the ANM creates a new local resource class with the same name and properties as the global resource class.

Use this procedure to apply an existing global resource class to an ACE.

Assumptions

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

Procedure

-
- Step 1** Select **Config > Global > All Resource Classes**. The Resource Classes table appears.
- Step 2** Select the global resource class you want to apply to an ACE, then click **Edit**. The Edit Resource Class configuration screen appears.
- Step 3** In the Available Items list, select the context that you want to apply this global resource class to, then click **Add**. The item appear in the Selected Items list.
- To remove contexts, select them in the Selected Items list, then click **Remove**. The items appear in the Available Items list.
- Step 4** Click:
- **OK** to save your entries and to return to the Resource Classes table. The context is updated with the resource class configuration.
 - **Cancel** to exit this procedure without saving your entries and to return to the Resource Classes table.
-

Related Topics

- [Using Resource Classes, page 3-32](#)
- [Modifying Global Resource Classes, page 3-39](#)
- [Using Local Resource Classes, page 3-41](#)
- [Configuring Local Resource Classes, page 3-41](#)

Auditing Resource Classes

After a global resource class has been applied to an Admin context, you can view any discrepancies that exist between the global resource class and the local resource class on the 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.

Use this procedure to view discrepancies between global and local resource classes.

Procedure

-
- Step 1** Select **Config > Global > All Resource Classes**. The Resource Classes table appears.
- Step 2** Select the resource class you want to audit, then 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 Click:

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

Related Topics

- [Using Global Resource Classes, page 3-35](#)
- [Using Local Resource Classes, page 3-41](#)
- [Configuring Global Resource Classes, page 3-36](#)
- [Configuring Local Resource Classes, page 3-41](#)

Modifying Global Resource Classes

When you modify a global resource class, the changes are not applied to virtual contexts previously associated with the resource class. The ANM only applies updated resource class properties to virtual contexts that are associated with the resource class going forward.



Caution

If you allocate 100% 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, refer to [Resource Allocation Constraints, page 3-34](#).

Use this procedure to modify an existing global resource class.

Procedure

- Step 1** Select **Config > Global > All Resource Classes**. The Resource Classes table appears.
- Step 2** Select the resource class you want to modify, then click **Edit**. The Edit Resource Class configuration screen appears.
- Step 3** Modify the values as desired. For details on setting values, see [Configuring Global Resource Classes, page 3-36](#). For descriptions of the resources, see [Table 3-8](#).
- Step 4** To deploy the modified resource class to an Admin context:
 - a. Click **Admin VCs To Deploy To** to expand the configuration subset.
 - b. Select the desired context in the Available Items list, then click **Add**. The item appears in the Selected Items list.

**Note**

The ANM only applies the updated resource class to contexts that you select 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 Click:

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

Related Topics

- [Using Resource Classes, page 3-32](#)
- [Using Global Resource Classes, page 3-35](#)
- [Modifying Global Resource Classes, page 3-39](#)
- [Auditing Resource Classes, page 3-38](#)
- [Deleting Global Resource Classes, page 3-40](#)

Deleting Global Resource Classes

Use this procedure to 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** Select **Config > Global > All Resource Classes**. The Resource Classes table appears.
- Step 2** Select the resource class you want to remove, then click **Delete**. A 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 3-32](#)
- [Using Global Resource Classes, page 3-35](#)
- [Modifying Global Resource Classes, page 3-39](#)
- [Auditing Resource Classes, page 3-38](#)

Using Local Resource Classes

Local resource classes can be created in ANM in three ways:

- 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.

The following options are available for local resource classes:

- [Configuring Local Resource Classes, page 3-41](#)
- [Deleting Local Resource Classes, page 3-42](#)
- [Viewing Local Resource Class Use on Virtual Contexts, page 3-43](#)

Configuring Local Resource Classes



Note

This functionality is available in Admin contexts only.

Use this procedure to create or modify a local resource class for use within the selected Admin virtual context.

Procedure

- Step 1** Select **Config > Devices > Admin_context > System > Resource Classes**. The Resource Classes table appears.
- Step 2** Click **Add** to create a new local resource class or select an existing resource class, then click **Edit** to modify it. The Resource Class configuration screen appears.
- Step 3** In the Name field, 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, enter the following information in the Default row: (See [Table 3-8](#) for a description of the resources.)
 - In the Min field, enter the minimum percentage of each resource you want to allocate to this resource class. Valid entries are numbers from 0 to 100 including those with decimals.

- b. In the Max field, select the maximum percentage of each resource 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 6 To use different values for the resources, for each resource, select the method for allocating resources:

- Select **Default** to use the values specified in [Step 5](#).
- Select **Min** to enter a specific minimum value for the resource.

Step 7 If you select Min:

- 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% of the available ACL memory to this resource class.
- b. In the Max field, select the maximum percentage of the resource 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 When you finish allocating resources for this resource class, 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.
- **Cancel** to exit this procedure without saving your entries and to return to the Resource Classes table.

Related Topics

- [Using Resource Classes, page 3-32](#)
- [Using Local Resource Classes, page 3-41](#)
- [Viewing Local Resource Class Use on Virtual Contexts, page 3-43](#)
- [Deleting Local Resource Classes, page 3-42](#)

Deleting Local Resource Classes

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 view a resource class's current deployment, see [Viewing Local Resource Class Use on Virtual Contexts, page 3-43](#).

Use this procedure to delete a local resource class.

Procedure

- Step 1** Select **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 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 [Viewing Local Resource Class Use on Virtual Contexts, page 3-43](#).
- Step 3** Select the resource class you want to remove, then click **Delete**. A 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 3-32](#)
- [Configuring Local Resource Classes, page 3-41](#)
- [Viewing Local Resource Class Use on Virtual Contexts, page 3-43](#)

Viewing Local Resource Class Use on Virtual Contexts

Use this procedure to view local resource class usage on all virtual contexts on an ACE.

Procedure

-
- Step 1** Select **Config > Devices**.
- Step 2** In the device tree, select the ACE with the resource class usage that you want to view. The Virtual Contexts table appears, listing all contexts on the selected ACE and the resource class in use for each context.
- Step 3** Click the Resource Class column heading to sort the table by resource class.
-

Related Topics

- [Using Resource Classes, page 3-32](#)
- [Configuring Local Resource Classes, page 3-41](#)
- [Deleting Local Resource Classes, page 3-42](#)

Configuring Security with ACLs

An ACL (access control list) 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. Besides an action element (“permit” or “deny”), each entry also contains a filter element based on criteria such as source address, destination address, protocol, or 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.

For specific procedures, see:

- [Creating ACLs, page 3-44](#)
- [Setting EtherType ACL Attributes, page 3-51](#)
- [Setting Extended ACL Attributes, page 3-47](#)
- [Resequencing Extended ACLs, page 3-50](#)
- [Editing or Deleting ACLs, page 3-61](#)

Creating ACLs

**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.

Use this procedure to create, modify, or delete ACLs.

Procedure**Step 1**

Select the item to configure:

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

- Step 2** The ACL summary table appears, listing the existing ACLs. ACL summary fields are described in [Table 3-9](#).

Table 3-9 ACL Summary Table

Field	Description
Name	Enter a unique identifier for the ACL. Valid entries are unquoted text strings with a maximum of 64 alphanumeric characters.
Type	Specifies the type of ACL: - Extended—allows you to specify both the source and the destination IP addresses of traffic as well as the protocol and the action to be taken. For more information see “Setting Extended ACL Attributes”. - EtherType—This ACL controls network access for non-IP traffic based on its EtherType. An EtherType is a sub-protocol identifier. For more information see “Setting EtherType ACL Attributes”.
#	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	Indicates whether or not this ACL uses ICMP (Internet Control Message Protocol). For more information, see “Protocol Names and Numbers” .
Interface(s)	VLAN interface(s) that is/are associated with this ACL, for example <4,5:4> where, < denotes the input direction, > denotes the output direction.
Remark	Enter any comments 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.

- Step 3** From the summary table, perform 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 the **Add** icon.
 - To modify an ACL, select the radio button to the left of any table entry, then click the **Edit** icon.
 - To delete an ACL, select the radio button to the left of any table entry, then click the **Trash** icon.
- If you choose create or modify the New Access List screen appears.

Step 4 Add or edit required fields as described in [Table 3-10](#).

Table 3-10 ACL Configuration Attributes

Field	Description
ACL Properties	Includes name, type (Extended, Ether), remarks. For more information see “ACL Summary Table” .
ACL Entries	
Entry Attributes	Includes line number, action and protocol/service object group drop down descriptor menu.
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	New in ANM 2.0. Used to add multiple ACL entries, adding one at a time using this button, before clicking Deploy . In the past only one entry could be added at a time in a two-step process hopping between two different locations in the UI.
Remove from Table button	Used to remove multiple ACL entries, removing one at a time using this button, before clicking Deploy .
Interfaces	
- Input/Output Direction - Currently Assigned (ACL:Direction)	Allows you to associate the ACL with one or more interfaces allowing only one input and one output ACL for each interface. Check box allows you to select and apply to all interfaces "access-group input".
Deploy button	Allows deployment of newly created ACL entries along with VLAN interface assignments that were configured.
Cancel button	Exits without saving your entries.

Step 5 To add, modify, or delete Object Groups go to [“Configuring Object Groups” section on page 3-52](#).

Related Topics

- [Configuring Security with ACLs, page 3-43](#)
- [Setting EtherType ACL Attributes, page 3-51](#)
- [Setting Extended ACL Attributes, page 3-47](#)
- [Resequencing Extended ACLs, page 3-50](#)
- [Editing or Deleting ACLs, page 3-61](#)

Setting Extended ACL Attributes



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.

An extended ACL allows you to specify both the source and the destination IP addresses of traffic as well as 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

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** Select the item to configure:
- To configure a virtual context, select **Config > Devices > context > Security > ACLs**.
 - To configure a configuration building block, select **Config > Global > All Building Blocks > building_block > Security > ACLs**.
- The ACLs table appears, listing the existing ACLs.
- Step 2** Click **Add**. The New Access List configuration screen appears.
- Step 3** Click **Add to Table** to add an entry to the table, or select an existing entry and click **Edit** to modify it.
- Step 4** Configure extended ACL entries using the information in [Table 3-11](#).

Table 3-11 Extended ACL Configuration Options

Field	Description
Line No.	Enter a 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 Resequencing Extended ACLs, page 3-50 .
Action	Action to be taken (permit/deny).
Service Object Group	This option is not applicable to ACE modules running 3.0(0)A1(x) and ACE 4710 appliances Running image A1(x). Select a service object group to apply to this ACL.
Protocol	Select the protocol or protocol number to apply to this ACL entry. Table 3-12 lists common protocol names and numbers.
Source Network Object Group	This option is not applicable to ACE modules running 3.0(0)A1(x) and ACE 4710 appliances Running image A1(x). Select a source network object group to apply to this ACL.
Any Source	Select the Any Source radio button to indicate that network traffic from any source is allowed.
Source IP Address	Enter the source IP address that is allowed for this ACL. Use the value in the Source Netmask field to allow a range IP addresses.

Table 3-11 **Extended ACL Configuration Options (continued)**

Field	Description
Source Netmask	Use this field to limit access to a specific source IP address or a range of source IP addresses: - For a single source IP address, enter a specific IP address in the Source IP Address field and select its subnet mask in the Source Netmask field. - For a range of source IP addresses, select the appropriate subnet mask in the Source Netmask field.
Source Port Operator	This field appears if you select TCP or UDP in the Protocol field. Select the operand to use to compare source port numbers: - Eq—The source port must be the same as the number in the Source Port Number field. - Gt—The source port must be greater than the number in the Source Port Number field. - Lt—The source port must be less than the number in the Source Port Number field. - Neq—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	This field appears if you select <i>Eq</i> , <i>Gt</i> , <i>Lt</i> , or <i>Neq</i> 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 and keywords, see ANM Ports Reference, page A-1 .
Lower Source Port Number	This field appears if you select <i>Range</i> 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 integers 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	This field appears if you select <i>Range</i> 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 integers from 0 to 65535. The number in this field must be greater than the number entered in the Lower Source Port Number field.
Destination Network Object Group	This option is not applicable to ACE modules running 3.0(0)A1(x) and ACE 4710 appliances Running image A1(x). Select a destination network object group to apply to this ACL.
Any Destination	Select the Any Destination radio button to indicate that network traffic toward any destination is allowed.
Destination IP Address	Enter the destination IP address that is allowed for this ACL. Use the value in the Destination Netmask field to allow a range of IP addresses.
Destination Netmask	Use this field to limit access to a specific destination IP address or a range of destination IP addresses: - For a single destination IP address, enter the IP address in the Destination IP Address field and select its subnet mask in the Destination Netmask field. - For a range of destination IP addresses, select the appropriate subnet mask in the Destination Netmask field.

Table 3-11 **Extended ACL Configuration Options (continued)**

Field	Description
Destination Port Operator	This field appears if you select TCP or UPD in the Protocol field. Select the operand to use to compare destination port numbers: - Eq—The destination port must be the same as the number in the Destination Port Number field. - Gt—The destination port must be greater than the number in the Destination Port Number field. - Lt—The destination port must be less than the number in the Destination Port Number field. - Neq—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	This field appears if you select <i>Eq</i>, <i>Gt</i>, <i>Lt</i>, or <i>Neq</i> 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 ANM Ports Reference, page A-1.
Lower Destination Port Number	This field appears if you select <i>Range</i> 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 integers 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	This field appears if you select <i>Range</i> 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 integers from 0 to 65535. The number in this field must be greater than the number entered in the Lower Destination Port Number field.

Table 3-12 **Protocol Names and Numbers**

Protocol Name ¹	Protocol Number	Description
AH	51	Authentication Header
EIGRP	88	Enhanced IGRP
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.html.

Step 5 In the Extended configuration pane, click:

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

Step 6 Associate any VLAN interface to this ACL if required and click:

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

Related Topics

- [Configuring Security with ACLs, page 3-43](#)
- [Creating ACLs, page 3-44](#)
- [Setting EtherType ACL Attributes, page 3-51](#)
- [Resequencing Extended ACLs, page 3-50](#)
- [Editing or Deleting ACLs, page 3-61](#)

Resequencing Extended ACLs

Use this procedure to change the sequence of entries in an Extended ACL. EtherType ACL entries cannot be resequenced.

Procedure

Step 1 Select the item to configure:

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

The ACLs table appears, listing the existing ACLs.

Step 2 Select the Extended ACL you want to renumber, then click the **Resequence** icon appearing to the left of the filter field. The ACL Line Number Resequence window appears.

Step 3 In the Start field, enter the number that is to be assigned to the first entry in the ACL. Valid entries are 1-2147483647.

Step 4 In the Increment field, enter the number that is to be added to each entry in the ACL after the first entry. You can enter any integer. Valid entries are 1-2147483647.

Step 5 Click:

- **Resequence** to save your entries and to return to the ACLs table.

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

Related Topics

- [Configuring Security with ACLs, page 3-43](#)
- [Creating ACLs, page 3-44](#)
- [Setting EtherType ACL Attributes, page 3-51](#)
- [Setting Extended ACL Attributes, page 3-47](#)
- [Editing or Deleting ACLs, page 3-61](#)

Setting EtherType ACL Attributes



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.

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

Procedure

- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > context > Security > ACLs**.
 - To configure a configuration building block, select **Config > Global > All Building Blocks > building_block > Security > ACLs**.
- The ACLs table appears, listing the existing ACLs.
- Step 2** Click **Add**. The New Access List configuration screen appears.
- Step 3** Enter the ACL name in the ACL Properties pane and choose Ethertype.
- Step 4** Select one of the following radio buttons:
- **Permit** to indicate that the ACE is to allow connections.
 - **Deny** to indicate that the ACE is to block connections.
- Step 5** Select one of the following from the Protocol field pulldown menu for this ACL:
- **Any**—Specifies any EtherType.
 - **BPDUs**—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, refer to [Understanding ACE Redundancy, page 10-20](#).
 - **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 [Step 4](#) and [Step 5](#) as needed.

Step 7 Associate any VLAN interface to this acl if required and click:

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

Related Topics

- [Configuring Security with ACLs, page 3-43](#)
- [Creating ACLs, page 3-44](#)
- [Setting Extended ACL Attributes, page 3-47](#)
- [Resequencing Extended ACLs, page 3-50](#)
- [Editing or Deleting ACLs, page 3-61](#)

Configuring Object Groups



Note

Object groups are available for only ACE 2.0 modules. ACE 2.0 configuration building blocks, and the ACE 4710 A3(1.0) release.

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 select 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.

Use this procedure to configure object groups that you can associate with ACLs.

Procedure

Step 1 Select the item to configure:

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



Note

Object groups are available for only ACE 2.0 modules and ACE 2.0 configuration building blocks.

The Object Groups table appears, listing existing object groups.

- Step 2** Click **Add** to create a new object group, or select an existing object group, then click **Edit** to modify it. The Object Groups configuration screen appears.
- Step 3** In the Name field, 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, select the type of object group 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** Click:
- **Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts.
 - **OK** to save your entries. This option appears for configuration building blocks.
 - **Cancel** to exit without saving your entries and to return to the Object Groups table.
 - **Next** to deploy your entries and to add another entry to the Object Groups table.

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

- Step 7** Configure objects for the object group.

For network-type object groups, options include:

- [Configuring IP Addresses for Object Groups, page 3-53](#)
- [Configuring Subnet Objects for Object Groups, page 3-54](#)

For service-type object groups, options include:

- [Configuring Protocols for Object Groups, page 3-55](#)
- [Configuring TCP/UDP Service Parameters for Object Groups, page 3-56](#)
- [Configuring ICMP Service Parameters for an Object Group, page 3-58](#)

Related Topics

- [Configuring Security with ACLs, page 3-43](#)
- [Creating ACLs, page 3-44](#)
- [Setting Extended ACL Attributes, page 3-47](#)
- [Resequencing Extended ACLs, page 3-50](#)

Configuring IP Addresses for Object Groups



Note

Object groups are available for only ACE 2.0 modules and ACE 2.0 configuration building blocks.

Use this procedure to specify host IP addresses for network-type object groups.

Procedure

Step 1 Select the item to configure:

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

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

Step 2 Select the object group you want to configure host IP addresses for, then select the Host Setting for Object Group tab. The Host Setting for Object Group table appears.

Step 3 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 Click:

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

Related Topics

- [Configuring Object Groups, page 3-52](#)
- [Configuring Subnet Objects for Object Groups, page 3-54](#)
- [Configuring Protocols for Object Groups, page 3-55](#)
- [Configuring TCP/UDP Service Parameters for Object Groups, page 3-56](#)
- [Configuring ICMP Service Parameters for an Object Group, page 3-58](#)

Configuring Subnet Objects for Object Groups

**Note**

Object groups are available for only ACE 2.0 modules and ACE 2.0 configuration building blocks.

Use this procedure to specify subnet objects for a network-type object group.

Procedure

Step 1 Select the item to configure:

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

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

Step 2 Select the object group you want to configure subnet objects for, then select 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 N/w IP Address field, enter an IP address that, with the subnet mask, defines the subnet object.
- Step 5** In the N/w Mask field, select the subnet mask for this subnet object.
- Step 6** Click:
- **Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts.
 - **OK** to save your entries. This option appears for configuration building blocks.
 - **Cancel** to exit this procedure without saving your entries.
 - **Next** to deploy your entries and to add another entry to the Network Setting table.

Related Topics

- [Configuring Object Groups, page 3-52](#)
- [Configuring IP Addresses for Object Groups, page 3-53](#)
- [Configuring Protocols for Object Groups, page 3-55](#)
- [Configuring TCP/UDP Service Parameters for Object Groups, page 3-56](#)
- [Configuring ICMP Service Parameters for an Object Group, page 3-58](#)

Configuring Protocols for Object Groups



Note

Object groups are available for only ACE 2.0 modules and ACE 2.0 configuration building blocks.

Use this procedure to specify protocols for a service-type object group.

Procedure

- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > context > Security > Object Groups**.
 - To configure a configuration building block, select **Config > Global > All Building Blocks > building_block > Security > Object Groups**.
- The Object Groups table appears, listing the existing object groups.
- Step 2** Select an existing service-type object group, then select the Protocol Selection tab. The Protocol Selection table appears.
- Step 3** Click **Add** to add an entry to this table.
- Step 4** In the Protocol Number field, select the protocol or protocol number to add to this object group. See [Table 3-12](#) for common protocols and their numbers.
- Step 5** Click:
- **Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts.
 - **OK** to save your entries. This option appears for configuration building blocks.
 - **Cancel** to exit this procedure without saving your entries.

- **Next** to deploy your entries and to add another entry to the Protocol Selection table.
-

Related Topics

- [Configuring Object Groups, page 3-52](#)
- [Configuring IP Addresses for Object Groups, page 3-53](#)
- [Configuring Subnet Objects for Object Groups, page 3-54](#)
- [Configuring TCP/UDP Service Parameters for Object Groups, page 3-56](#)
- [Configuring ICMP Service Parameters for an Object Group, page 3-58](#)

Configuring TCP/UDP Service Parameters for Object Groups

**Note**

Object groups are available for only ACE 2.0 modules and ACE 2.0 configuration building blocks.

Use this procedure to add TCP or UDP service objects to a service-type object group.

Procedure

- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > *context* > Security > Object Groups**.
 - To configure a configuration building block, select **Config > Global > All Building Blocks > *building_block* > Security > Object Groups**.
- The Object Groups table appears, listing the existing object groups.
- Step 2** Select an existing service-type object group, then select 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 3-13](#).

Table 3-13 TCP and UDP Service Parameters

Field	Description
Protocol	Select the protocol for this service object: • TCP—TCP is the protocol for this service object. • UDP—UDP is the protocol for this service object. • TCP and UDP—Both TCP and UDP are the protocols for this service object.
Source Port Operator	Select the operand to use when comparing source port numbers for this service object: • Eq—The source port must be the same as the number in the Source Port field. • Gt—The source port must be greater than the number in the Source Port field. • Lt—The source port must be less than the number in the Source Port field. • Neq—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	This field appears if you select <i>Eq</i>, <i>Gt</i>, <i>Lt</i>, or <i>Neq</i> in the Source Port Operator field. Enter the source port name or number for this service object.
Lower Source Port	This field appears if you select <i>Range</i> 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 integers 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	This field appears if you select <i>Range</i> 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 integers from 0 to 65535. The number in this field must be greater than the number entered in the Lower Source Port field.
Destination Port Operator	Select the operand to use when comparing destination port numbers: • Eq—The destination port must be the same as the number in the Destination Port field. • Gt—The destination port must be greater than the number in the Destination Port field. • Lt—The destination port must be less than the number in the Destination Port field. • Neq—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	This field appears if you select <i>Eq</i>, <i>Gt</i>, <i>Lt</i>, or <i>Neq</i> in the Destination Port Operator field. Enter the destination port name or number for this service object.
Lower Destination Port	This field appears if you select <i>Range</i> 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 integers 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	This field appears if you select <i>Range</i> 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 integers from 0 to 65535. The number in this field must be greater than the number entered in the Lower Destination Port field.

Step 5 Click:

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

Related Topics

- [Configuring Object Groups, page 3-52](#)
- [Configuring IP Addresses for Object Groups, page 3-53](#)
- [Configuring Subnet Objects for Object Groups, page 3-54](#)
- [Configuring Protocols for Object Groups, page 3-55](#)
- [Configuring ICMP Service Parameters for an Object Group, page 3-58](#)

Configuring ICMP Service Parameters for an Object Group

**Note**

Object groups are available for only ACE 2.0 modules and ACE 2.0 configuration building blocks.

Use this procedure to add ICMP service parameters to a service-type object group.

Procedure**Step 1** Select the item to configure:

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

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

Step 2 Select an existing service-type object group, then select 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 3-14](#).

Table 3-14 ICMP Type Service Parameters

Field	Description
ICMP Type	Select the ICMP type or number for this service object. Table 3-15 lists common ICMP types and numbers.
Message Code Operator	Select the operand to use when comparing message codes for this service object: - Eq—The message code must be the same as the number in the Message Code field. - Gt—The message code must be greater than the number in the Message Code field. - Lt—The message code must be less than the number in the Message Code field. - Neq—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	This field appears if you select <i>Eq</i> , <i>Gt</i> , <i>Lt</i> , or <i>Neq</i> in the Message Code Operator field. Enter the ICMP message code for this service object.
Min Message Code	This field appears if you select <i>Range</i> 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 integers 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	This field appears if you select <i>Range</i> 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 integers from 0 to 255. The number in this field must be greater than the number entered in the Min Message Code field.

Table 3-15 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

Table 3-15 *ICMP Type Numbers and Names (continued)*

Number	ICMP Type Name
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 Click:

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

Related Topics

- [Configuring Object Groups, page 3-52](#)
- [Configuring IP Addresses for Object Groups, page 3-53](#)
- [Configuring Subnet Objects for Object Groups, page 3-54](#)
- [Configuring Protocols for Object Groups, page 3-55](#)
- [Configuring TCP/UDP Service Parameters for Object Groups, page 3-56](#)

Managing ACLs

In addition to creating and configuring ACLs, you can:

- Viewing All ACLs by Context—See [Viewing All ACLs by Context, page 3-60](#).
- Delete ACLs—See [Editing or Deleting ACLs, page 3-61](#).

Viewing All ACLs by Context

Use this procedure to view all access control lists that have been configured.

Procedure

-
- Step 1** Select **Config > Devices**. The device tree appears.

- Step 2** Select the virtual context with the ACLs you want to view, then select **Security > ACLs**. The ACLs table appears, listing the existing ACLs in that context with their name, their type (Extended or EtherType), and all relevant details (such as Action, Protocol, Interface information).
- Step 3** To view all the ACLs for a given table entry, click the plus sign to the left of that entry.
- Step 4** To view all the of ACLs for all of the entries click the **Expand All** icon on the Add/Edit/Delete row.
- Step 5** To collapse all the of ACLs for all of the entries click the **Collapse All** icon on the Add/Edit/Delete row.
-

Related Topics

- [Configuring Security with ACLs, page 3-43](#)
- [Creating ACLs, page 3-44](#)
- [Setting EtherType ACL Attributes, page 3-51](#)
- [Setting Extended ACL Attributes, page 3-47](#)
- [Editing or Deleting ACLs, page 3-61](#)

Editing or Deleting ACLs

Use this procedure to delete or edit an ACL or any of its subentries.

Procedure

- Step 1** Select the ACL to edit or delete:
- Select **Config > Devices > *context* > Security > ACLs**.
- or
- Select **Config > Global > All Building Blocks > *building_block* > Security > ACLs**.
- The ACLs table appears, listing the existing ACLs.
- Step 2** Select the radio button to the left of the ACL 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** Perform one of the following steps:
- Click **Edit** if you are editing an ACL or one of its entries and go to [Step 4](#).
- or
- Click **Delete** if you are deleting an ACL or one of its entries and go to [Step 5](#).
- Step 4** Edit the entry using the summary information listed in [Table 3-10](#) if needed, and click **Deploy** when done.
- Step 5** Click **Delete**. A 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 3-44](#)

- [Setting EtherType ACL Attributes, page 3-51](#)
- [Setting Extended ACL Attributes, page 3-47](#)
- [Resequencing Extended ACLs, page 3-50](#)

Configuring Virtual Context Expert Options

The ANM virtual context Expert configuration options allow you to:

- 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 [Configuring Traffic Policies, page 11-1](#).
- Compare a virtual context configuration with a tagged configuration building block that has been applied to the context. See [Comparing Context and Building Block Configurations, page 3-62](#).
- For ACE 2.0 modules and ACE appliances, configure optimization action lists. See [Configuring Action Lists for Application Acceleration and Optimization, page 12-3](#).

Comparing Context and Building Block Configurations

The 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.

Use this procedure to 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** Select **Config > Devices > context > Expert > Building Block Audit**. The Building Block Audit screen appears with the Comparison Results table, listing any discrepancies between the configurations.
- Step 2** Identify the discrepancies in any of the following ways:
- 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:
 - *nc* (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 in the applied building block. That is, two settings have been changed in the context.

- *nd* (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. That is, five items in the applied building block have been deleted from the context configuration.
- *na* (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. That is, compared to the applied building block, three items 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 When viewing results in the Comparison Results table, you can:

- 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 3-5](#)
- [Managing Virtual Contexts, page 3-63](#)
- [Using Configuration Building Blocks, page 13-1](#)

Managing Virtual Contexts

You can perform the following administrative actions on virtual contexts:

- [Viewing All Virtual Contexts, page 3-64](#)
- [Synchronizing Virtual Context Configurations, page 3-66](#)
- [Managing Syslog Settings for Autosync, page 3-66](#)
- [Editing Virtual Contexts, page 3-67](#)
- [Upgrading Virtual Contexts, page 3-68](#)
- [Restarting Virtual Context Polling, page 3-69](#)
- [Comparing Context and Building Block Configurations, page 3-62](#)

Viewing All Virtual Contexts

Use this procedure to view some or all virtual contexts being managed by the ANM.

Procedure

- Step 1** Select **Config > Devices > All VC**. The All Virtual Contexts table appears with the information described in [Table 3-16](#).

Table 3-16 *All Virtual Contexts Table*

Field	Description
Name	The context name including chassis and slot.
Resource Class	The resource class applied to the context.
Building Block	The configuration building block applied to the context.
CLI Sync Status	The administrative configuration status of the context: • Import Failed—The context did not import successfully. This 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 being 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 Synchronizing Virtual Context Configurations, page 3-66. • Unprovisioned—The context has been removed from the ACE using the CLI but has not been removed from the ANM. To remove unprovisioned contexts, synchronize the associated Admin context.
Management IPs	A list of IP addresses used for remote management of the context.

Table 3-16 All Virtual Contexts Table (continued)

Field	Description
Polling Status	The current polling status of the context: • Missing SNMP Credentials—SNMP credentials are not configured for this virtual context; therefore, statistics are not collected. Add SNMP v2c credentials to fix this error. • Not Polled—SNMP polling has not started. This happens when the virtual context is first created from the ANM and the SNMP credentials are not configured. Add SNMP v2c credentials to fix this error. • Not Supported—This status appears at the device level only and applies to Cisco Catalyst chassis, 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 required. Everything is working properly. Polling states will display activity. • Polling Timed Out—SNMP polling has timed out. This might occur if the wrong credentials were configured or might be caused by an internal error (such as SNMP protocol configured incorrectly or 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 SNMP v2c credential configuration.
ACE HA State	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 it needs to statefully assume the active state if a switchover occurs.
ACE HA Autosync	Indicates whether high availability automatic synchronization is enabled on the context.

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 3-69](#)
- [Enabling Polling on All Devices, page 14-20](#)
- [Synchronizing Virtual Context Configurations, page 3-66](#)

Synchronizing Virtual Context Configurations

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 your role-based permission level, the ANM Status bar displays the number of virtual contexts out of sync with the ACE CLI against the total number of virtual contexts as well as the number of failed synchronization attempts.

It is important to synchronize contexts when:

- You configure the ACE directly via the CLI instead of using the ANM interface:
 - For ACE 2.0 modules and ACE appliances, the CLI Sync Status is *Out of Sync* in the Virtual Contexts table (**Config > Devices > ACE**) if the configurations for a virtual context differ.
 - For ACE 1.0 modules running software version 3.0(0)A1.x, the CLI Sync Status is always *OK* in the Virtual Contexts table even if the configurations for a virtual context differ. If any changes are made to virtual context configurations using the CLI on ACE 1.0 modules, you need to remember to synchronize them.
- 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 the 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.

Use this procedure to synchronize the configurations for a virtual context.

Procedure

-
Step 1	Select Config > Devices . The device tree appears.
Step 2	Select either All VC or the ACE with the virtual context configuration you want to synchronize. The Virtual Contexts table appears.
Step 3	Select the virtual context with the configuration you want to synchronize, then click CLI Sync . The Virtual Contexts table refreshes when synchronization is complete.
-

Related Topics

- [Configuring Auto Sync Settings, page 15-65](#)
- [Editing Virtual Contexts, page 3-67](#)
- [Restarting Virtual Context Polling, page 3-69](#)
- [Comparing Context and Building Block Configurations, page 3-62](#)

Managing Syslog Settings for Autosync

Setting auto sync to occur upon receipt of a syslog message from devices allows a faster, more streamlined synchronization process between ANM and any out-of-band configuration changes. Rather than wait the default polling period, ANM will sync when a syslog message is received if Setup Syslog for Autosync is enabled.

Use this procedure to have ANM receive syslog messages for a virtual context.

Procedure

-
- Step 1** Select **Config > Devices > Virtual Context Management > Setup Syslog for Autosync**. The Setup Syslog for Autosync screen appears.
- Step 2** Select either **All VC** or the ACE with the virtual context configuration for which you want to receive Autosync syslog messages. Click **Setup Syslog**. A progress bar window appears.
- A checkbox with checkmark will appear in the **Setup Syslog for Autosync?** column for each virtual context and ACE device you checked.
- Step 3** 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 3-66](#)
- [Restarting Virtual Context Polling, page 3-69](#)

Editing Virtual Contexts

Use this procedure to modify the configuration of an existing virtual context.

Procedure

-
- Step 1** Select **Config > Devices**. The device tree appears.
- Step 2** Select the virtual context, then select the configuration attributes you want to modify. For information on configuration options, see [Configuring Virtual Contexts, page 3-5](#).
- Step 3** Click:
- **OK** to save your entries.
 - **Cancel** to exit the procedure without saving your entries.
-

Related Topics

- [Using Virtual Contexts, page 3-1](#)
- [Configuring Virtual Contexts, page 3-5](#)

Deleting Virtual Contexts

Use this procedure to 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 [Synchronizing Virtual Context Configurations, page 3-66](#)) or delete the virtual context by selecting the virtual context, then clicking **Delete**.

Procedure

-
- Step 1** Select **Config > Devices**. The device tree appears.
- Step 2** In the device tree, select the virtual context you want to configure, then click **Delete** in either the device pane or the configuration pane.
- A window appears, asking you to confirm the deletion.
- Step 3** Click:
- **OK** to delete the selected context. The device tree refreshes and the deleted context no longer appears.
 - **Cancel** to exit this procedure and to retain the selected context.
-

Related Topics

- [Configuring Virtual Contexts, page 3-5](#)
- [Comparing Context and Building Block Configurations, page 3-62](#)

Upgrading Virtual Contexts

Use this procedure to apply a different resource class, configuration building block, or VLAN to a virtual context.

Procedure

-
- Step 1** Select **Config > Devices**. The device tree appears.
- Step 2** Select the virtual context you want to upgrade, then select **System > Primary Attributes**. The Edit Virtual Context screen appears.
- Step 3** In the Resource Class field, select the resource class 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 [Resource Allocation Constraints, page 3-34](#).

- Step 4** In the Tagged Building Block to Apply field, select 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 in any of the following ways:
- For a single VLAN, enter an integer from 2 to 4096.
 - For multiple, non-sequential 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 save your entries. The screen refreshes with updated information.
- To exit this procedure without saving your entries, select another item in the menu bar or device tree. A popup window appears, confirming that you have not saved your entries.
-

Related Topics

- [Using Virtual Contexts, page 3-1](#)
- [Configuring Virtual Contexts, page 3-5](#)

Restarting Virtual Context Polling

Use this procedure to restart monitoring and enable SNMP collection on a single context that has stopped or failed to start.

To restart polling and enable SNMP collection on all virtual contexts, select **Monitor > Settings > Global Polling Configuration**, and configure global polling attributes using the information in [Enabling Polling on All Devices, page 14-20](#).

Procedure

- Step 1** Select **Config > Devices**. The device tree appears.
- Step 2** Select the ACE associated with the virtual context with stopped or failed polling. The Virtual Contexts table appears.
- Step 3** Select the context with the stopped or failed polling, then click **Restart Polling**.
- If the ANM cannot monitor the selected context, it displays an error message stating the reason.
-

Related Topics

- [Using Virtual Contexts, page 3-1](#)
- [Configuring Virtual Contexts, page 3-5](#)
- [Enabling Polling on All Devices, page 14-20](#)



CHAPTER 4

Configuring Virtual Servers

Revised Date: 3/25/09

This section provides an overview of server load balancing and procedures for configuring virtual servers for load balancing on an ACE.

Topics include:

- [Load Balancing Overview, page 4-1](#)
- [Configuring Virtual Servers, page 4-2](#)
- [Managing Virtual Servers, page 4-48](#)

Load Balancing Overview

Server load balancing (SLB) is the process of deciding to which server a load balancer should send a client request for service. For example, a client request can consist of an HTTP GET for a Web page or an FTP GET to download a file. The job of the load balancer is to select the server that can successfully fulfill the client request and do so in the shortest amount of time without overloading either the server or the server farm as a whole.

Depending on the load-balancing algorithm or predictor that you configure, the ACE performs a series of checks and calculations to determine the server that can best service each client request. The ACE bases server selection on several factors, including the server with the fewest connections with respect to load, source or destination address, cookies, URLs, or HTTP headers.

The ANM allows you to configure load balancing using:

- Virtual servers—See [Configuring Virtual Servers, page 4-2](#).
- Real servers—See [Configuring Real Servers, page 5-4](#).
- Server farms—See [Configuring Server Farms, page 5-12](#).
- Sticky groups—See [Configuring Sticky Groups, page 6-7](#).
- Parameter maps—See [Configuring Parameter Maps, page 7-1](#).

For information about SLB as configured and performed by the ACE, see:

- [Configuring Virtual Servers, page 4-2](#)
- [Load-Balancing Predictors, page 5-2](#)
- [Real Servers, page 5-3](#)
- [Server Farms, page 5-3](#)
- [Health Monitoring, page 5-23](#)

- [TCL Scripts, page 5-24](#)
- [Configuring Stickiness, page 6-1](#)

Configuring Virtual Servers

In a load-balancing environment, a virtual server is a construct that allows multiple physical servers to appear as one for load-balancing purposes. A virtual server is bound to physical services running on real servers in a server farm and uses IP address and port information to distribute incoming client requests to the servers in the server farm according to a specified load-balancing algorithm.

You use class maps to configure a virtual server address and definition. The load-balancing predictor algorithms (for example, roundrobin, least connections, and so on) determine the servers to which the ACE sends connection requests.

For more information about virtual servers and ANM, see:

- [Understanding Virtual Server Configuration and ANM, page 4-2](#)
- [Using ANM to Configure Virtual Servers, page 4-4](#)
- [Virtual Server Configuration Procedure, page 4-4](#)

Understanding Virtual Server Configuration and ANM

The ANM Virtual Server configuration interface, an abstraction of the Modular Policy CLI, simplifies, reorders, and makes more atomic the configuration and deployment of a functional load-balancing environment. With simplification or abstraction, some constraints or limitations are necessarily introduced. This section identifies the constraints and framework used by the ANM for virtual server configuration.

In the ANM, a viable virtual server has the following attributes:

- A single Layer 3/Layer 4 match condition
This means that you can specify only a single IP address (or single IP address range if a netmask is used), with only a single port (or port range). Having a single match condition greatly simplifies and aids virtual server configuration.
- A default Layer 7 action
- A Layer 7 policy map
- A Layer 3/Layer 4 class map
- A multi-match policy map, a class-map match, and an action

In addition:

- The virtual server multi-match policy map is associated with an interface or is global.
- The name of the virtual server is derived from the name of the Layer 3/Layer 4 class map.

[Example 4-1](#) shows the minimum configuration statements required for a virtual server.

Example 4-1 Minimum Configuration Required for a Virtual Server

```
class-map match-all Example_VIP
  2 match virtual-address 10.10.10.10 tcp eq www
policy-map type loadbalance first-match Example_VIP-l7slb
  class class-default
    forward
policy-map multi-match int10
  class Example_VIP
    loadbalance policy Example_VIP-l7slb

interface vlan 10
  ip address 192.168.65.37 255.255.255.0
  service-policy input int10
  no shutdown
```

Note also the following items regarding the ANM and virtual servers:

- **Additional configuration options**

The Virtual Server configuration screen allows you to configure additional items for a functional VIP. These items include server farms, sticky groups, real servers, probes, parameter maps, inspection, class maps, and inline match conditions. Because too many items on a screen can be overwhelming, not all configuration options appear on Virtual Server configuration screen, such as sticky statics or backup real servers. These options are available elsewhere in the ANM interface instead of on the Virtual Server configuration screen.

- **Configuration options and roles**

To support and maintain the separation of roles, some objects cannot be configured using the Virtual Server configuration screen. These objects include SSL certificates, SSL keys, NAT pools, interface IP addresses, and ACLs. Providing these options as separate configuration options in the ANM interface ensures that a user who can view or modify virtual servers or aspects of virtual servers cannot create or delete virtual servers.

- **Changes to virtual servers using the CLI or Expert options can prevent further modifications in the Virtual Server configuration screen**

If you create a virtual server using the Virtual Server configuration screen, modify it using the CLI or Expert options (**Config > Devices > Expert**), and then attempt to modify it again using the Virtual Server configuration screen, error messages will be displayed and you will not be able to modify the virtual server.

Related Topics

- [Configuring Virtual Servers, page 4-2](#)
- [Using ANM to Configure Virtual Servers, page 4-4](#)
- [Virtual Server Configuration Procedure, page 4-4](#)

Using ANM to Configure Virtual Servers

It is important to understand the following concepts when using the ANM to configure virtual servers:

- **Virtual server configuration screens**

The ANM virtual server configuration screens are designed to aid you in configuring virtual servers by presenting configuration options that are relevant to your choices. For example, the protocols that you select in the Properties configuration subset determine the other configuration subsets that appear.

- **Use the virtual server configuration method that suits you**

The ANM Virtual Server configuration screens simplify the process of creating, modifying, and deploying virtual servers by displaying those options that you are most likely to use. In addition, as you specify attributes for a virtual server, such as protocols, the interface refreshes with related configuration options, such as Protocol Inspection or Application Acceleration and Optimization, thereby speeding virtual server configuration and deployment.

While Virtual Server configuration screens remove some configuration complexities, they have a few constraints that the Expert configuration options do not. If you are comfortable using the CLI, you can use the Expert options (such as **Config > Devices > context > Expert > Class Map or Policy** or **Config > Devices > context > Load Balancing > Parameter Maps** to configure more complex attributes of virtual servers, traffic policies, and parameter maps.

- **Synchronizing virtual server configurations**

If you configure a virtual server using the CLI and then use the Sync option (**Config > Devices > ACE > Sync**) to synchronize configurations, the configuration that appears in ANM for the virtual server might not display all configuration options for that virtual server. The configuration that appears in the ANM depends on a number of items, such as the protocols configured in class maps or the rules defined for policy maps.

For example, if you configure a virtual server on the CLI that includes a class map that can match any protocol, you will not see the virtual server Application Acceleration and Optimization configuration subset in the ANM.

- **Modifying shared objects**

Modifying an object that is used by multiple virtual servers, such as a server farm, real server, or parameter map, could impact the other virtual servers. See [Shared Objects and Virtual Servers, page 4-6](#) for more information about modifying objects used by multiple virtual servers.

Related Topics

- [Configuring Virtual Servers, page 4-2](#)
- [Understanding Virtual Server Configuration and ANM, page 4-2](#)
- [Virtual Server Configuration Procedure, page 4-4](#)

Virtual Server Configuration Procedure

Use this procedure to add virtual servers to the ANM for load-balancing purposes.

Assumptions

- Depending on the protocol to be used for the virtual server, parameter maps need to be defined.

- For SSL service, SSL certificates, keys, chain groups, and parameter maps must be configured.

Procedure

- Step 1** Select **Config > Devices > context > Load Balancing > Virtual Servers**. The Virtual Servers table appears.
- Step 2** Click **Add** to add a new virtual server, or select an existing virtual server, then click **Edit** to modify it. The Virtual Server configuration screen appears with a number of configuration subsets. The subsets that you see depend on whether you use the Basic View or the Advanced View and entries you make in the Properties subset. Change views by using the View object selector at the top of the configuration pane.

[Table 4-1](#) identifies and describes virtual server configuration subsets with links to related topics for configuration information.



Note The protocols that are available depend on the ACE device that you are configuring. For a list of the protocols available for each ACE device type, see [Table 4-2](#).

Table 4-1 Virtual Server Configuration Subsets

Configuration Subset	Description	Related Topics
Properties	This subset allows you to specify basic virtual server characteristics, such as the virtual server name, IP address, protocol, port, and VLANs.	Configuring Virtual Server Properties, page 4-8
SSL Termination	This subset appears when TCP is the selected protocol and Other or HTTPS is the application protocol. This subset allows you to configure the virtual server to act as an SSL proxy server and terminate SSL sessions between it and its clients.	Configuring Virtual Server SSL Termination, page 4-12
Protocol Inspection	This subset appears in the Advanced View for: • TCP with FTP, HTTP, HTTPS, RTSP, or SIP • UDP with DNS or SIP This subset appears in the Basic view for TCP with FTP. This subset allows you to configure the virtual server so that it can verify protocol behavior and identify unwanted or malicious traffic passing through the ACE on selected application protocols.	Configuring Virtual Server Protocol Inspection, page 4-14
Application Acceleration and Optimization	This subset appears only for ACE appliances. It appears in the Advanced View when HTTP or HTTPS is the selected application protocol. This subset allows you to configure application acceleration and optimization options for HTTP or HTTPS traffic.	Configuring Application Acceleration and Optimization, page 4-37

Table 4-1 Virtual Server Configuration Subsets (continued)

Configuration Subset	Description	Related Topics
L7 Load-Balancing	This subset appears only in the Advanced View for: - TCP with Generic, HTTP, HTTPS, RTSP, or SIP - UDP with Generic, RADIUS, or SIP This subset allows you to configure Layer 7 load-balancing options, including SSL initiation.	Configuring Virtual Server Layer 7 Load Balancing, page 4-25
Default L7 Load-Balancing Action	This subset allows you to establish the default Layer 7 load-balancing actions for all network traffic that does not meet previously specified match conditions including the SSL initiation configuration.	Configuring Virtual Server Default Layer 7 Load Balancing, page 4-35
NAT	This subset appears in the Advanced View only. This subset allows you to set up Name Address Translation (NAT) for the virtual server.	Configuring Virtual Server NAT, page 4-47

- Step 3** When you finish configuring virtual server properties, click:
- **Deploy Now** to deploy the configuration on the ACE.
 - **Cancel** to exit the procedure without saving your entries and to return to the Virtual Servers table.
 - **Deploy Later** to save your entries and apply them at a later time.

Related Topics

- [Configuring Virtual Servers, page 4-2](#)
- [Understanding Virtual Server Configuration and ANM, page 4-2](#)
- [Using ANM to Configure Virtual Servers, page 4-4](#)
- [Shared Objects and Virtual Servers, page 4-6](#)
- [Understanding Roles, page 15-5](#)

Shared Objects and Virtual Servers

A shared object is one that is used by multiple virtual servers. Examples of shared objects are:

- Action lists
- Class maps
- Parameter maps
- Real servers
- Server farms
- SSL services
- Sticky groups

Because these objects are shared, modifying an object's configuration in one virtual server can impact other virtual servers that use the same object.

Configuring Shared Objects

ANM offers the following options for shared objects in virtual server configuration screens (**Config > Devices > context > Load Balancing > Virtual Servers**):

- **View**—Click **View** to review the object's configuration. The screen refreshes with read-only fields and the following three buttons.
- **Cancel**—Click **Cancel** to close the read-only view and to return to the previous screen.
- **Edit**—Click **Edit** to modify the selected object's configuration. The screen refreshes with fields that can be modified, except for the Name field which remains read-only.



Note Before changing a shared object's configuration, make sure you understand the effect of the changes on other virtual servers using the same object. As an alternative, consider using the Duplicate option instead.

- **Duplicate**—Click **Duplicate** to create a new object with the same configuration as the selected object. The screen refreshes with configurable fields. In the Name field, enter a unique name for the new object, then modify the configuration as desired. This option allows you to create a new object without impacting other virtual servers using the same object.

Deleting Virtual Servers with Shared Objects

If you create a virtual server and include shared objects in its configuration, deleting the virtual server does not delete the associated shared objects. This ensures that other virtual servers using the same shared objects are not impacted.

Related Topics

- [Managing Virtual Servers, page 4-48](#)
- [Virtual Server Protocols by Device Type, page 4-8](#)
- [Configuring Virtual Server Properties, page 4-8](#)
- [Configuring Virtual Server SSL Termination, page 4-12](#)
- [Configuring Virtual Server Protocol Inspection, page 4-14](#)
- [Configuring Virtual Server Layer 7 Load Balancing, page 4-25](#)
- [Configuring Virtual Server Default Layer 7 Load Balancing, page 4-35](#)
- [Configuring Application Acceleration and Optimization, page 4-37](#)

Virtual Server Protocols by Device Type

The protocols that are available for a virtual server depend on the ACE device you are configuring. [Table 4-2](#) lists the protocols available for each device type.

Table 4-2 Virtual Server Protocols for ACE Modules and Devices

Protocol	ACE 1.0 Modules	ACE 2.0 Modules	ACE 4710 Appliance Running Image A1(8)	ACE 4710 Appliance Running Image A3(1.0)
Any	X	X	X	X
TCP				
Other	X	X	X	X
HTTP	X	X	X	X
HTTPS	X	X	X	X
FTP	X	X	X	X
RTSP		X		X
RDP		X		X
Generic		X		X
SIP		X		X
UDP				
Other	X	X	X	X
DNS	X	X	X	X
RADIUS		X		X
Generic		X		
SIP		X		

Related Topics

- [Configuring Virtual Servers, page 4-2](#)
- [Configuring Virtual Server Properties, page 4-8](#)

Configuring Virtual Server Properties

Use this procedure to configure virtual server properties.

Procedure

-
- Step 1** Select **Config > Devices > context > Load Balancing > Virtual Servers**. The Virtual Servers table appears.
- Step 2** Click **Add** to add a new virtual server, or select an existing virtual server, then click **Edit** to modify it. The Virtual Server configuration screen appears. The Properties configuration subset is open by default.

The fields that you see in the Properties configuration subset depend on whether you are using Advanced View or Basic View:

- To configure Advanced View properties, continue with [Step 3](#).
- To configure Basic View properties, continue with [Step 4](#).

Step 3 To configure virtual server properties in the Advanced View, enter the information in [Table 4-3](#).

Table 4-3 Virtual Server Properties – Advanced View

Field	Description
VIP Name	Enter the name for the virtual server.
VIP IP	Enter the IP address for the virtual server.
Netmask	Select the subnet mask to apply to the virtual server IP address.
Protocol	Select the protocol the virtual server supports: • Any—The virtual server is to accept connections using any IP protocol. • TCP—The virtual server is to accept connections that use TCP. • UDP—The virtual server is to accept connections that use UDP.
Application Protocol	This field appears if TCP or UDP is selected. The application protocols that are available depend on the type of ACE being configured. Select the application protocol to be supported by the virtual server. Table 4-2 identifies the available protocols for each ACE device type.
Port	This field appears for any TCP or UDP protocol. Enter the port to be used for the specified protocol. Valid entries are integers from 0 to 65535 or a range of integers, such as 10-20. Enter 0 (zero) to indicate all ports. For a complete list of protocols and ports, see the Internet Assigned Numbers Authority available at www.iana.org/numbers.html.
All VLANs	Select the check box to support incoming traffic from all VLANs. Clear the check box to support incoming traffic from specific VLANs only.
VLAN	This field appears if the All VLANs check box is cleared. In the Available Items list, select the VLANs to use for incoming traffic, then click Add. The items appear in the Selected Items list. To remove VLANs, select them in the Selected Items lists, then click Remove. The items appear in the Available Items list. Note You cannot change the VLAN for a virtual server once it is specified. Instead, delete the virtual server and create a new one with the desired VLAN.
Connection Parameter Map	This field appears if TCP is the selected protocol. Select an existing connection parameter map or click *New* to create a new one: • If you select an existing parameter map, you can view, modify, or duplicate the existing configuration. See Shared Objects and Virtual Servers, page 4-6 for more information about modifying shared objects. • If you click *New*, the Connection Parameter Map configuration pane appears. Configure the connection parameter map as described in Table 7-2.

Table 4-3 **Virtual Server Properties – Advanced View (continued)**

Field	Description
HTTP Parameter Map	This field appears if HTTP or HTTPS is the selected application protocol. Select an existing HTTP parameter map or click *New* to create a new one: • If you select an existing parameter map, you can view, modify, or duplicate the existing configuration. See Shared Objects and Virtual Servers, page 4-6 for more information about modifying shared objects. • If you click *New*, the HTTP Parameter Map configuration pane appears. Configure the HTTP parameter map as described in Table 7-5.
RTSP Parameter Map	This field appears if RTSP is the selected application protocol over TCP. Select an existing RTSP parameter map or click *New* to create a new one: • If you select an existing parameter map, you can view, modify, or duplicate the existing configuration. See Shared Objects and Virtual Servers, page 4-6 for more information about modifying shared objects. • If you click *New*, the RTSP Parameter Map configuration pane appears. Configure the RTSP parameter map as described in Table 7-7.
Generic Parameter Map	This field appears if Generic is the selected application protocol over TCP or UDP. Select an existing Generic parameter map or click *New* to create a new one. • If you select an existing parameter map, you can view, modify, or duplicate the existing configuration. See Shared Objects and Virtual Servers, page 4-6 for more information about modifying shared objects. • If you click *New*, the Generic Parameter Map configuration pane appears. Configure the Generic parameter map as described in Table 7-4.
ICMP Reply	Indicate how the virtual server is to respond to ICMP ECHO requests: • None—The virtual server is not to send ICMP ECHO-REPLY responses to ICMP requests. • Active—The virtual server is to send ICMP ECHO-REPLY responses only if the configured VIP is active. • Always—The virtual server is always to send ICMP ECHO-REPLY responses to ICMP requests.

Table 4-3 **Virtual Server Properties – Advanced View (continued)**

Field	Description
VIP Advertise	This field appears for ACE 1.0 and 2.0 modules only. This option allows the ACE to advertise the IP address of the virtual server as the host route. Select the desired VIP advertise option: • None—The ACE is not to advertise the IP address of the virtual server as the host route. • Active—The ACE is to advertise the IP address of the virtual server as the host route only if there is at least one active real server in the server farm. • Always—The ACE is always to advertise the IP address of the virtual server as the host route. • Active-metric—The ACE is to advertise the IP address of the virtual server as the host route if: – There is at least one active real server in the server farm. – A distance metric is specified for the route in the Distance field. • Always-metric—The ACE is to advertise the IP address of the virtual server as the host route, using the distance metric in the Distance field.
Distance	This field appears if you select Active-metric or Always-metric in the VIP Advertise field. Enter the administrative distance to be included in the routing table. Valid entries are integers from 1 to 254.
Status	Indicate whether the virtual server is to be in service or out of service: • In Service—Enables the virtual server for load-balancing operations. • Out of Service—Disables the virtual server for load-balancing operations.

Step 4 To configure virtual server properties in the Basic View, enter the information in [Table 4-4](#).

Table 4-4 **Virtual Server Properties – Basic View**

Field	Description
VIP Name	Enter the name for the virtual server.
VIP IP	Enter the IP address for the virtual server.
Protocol	Select the protocol that the virtual server supports: • Any—The virtual server is to accept connections using any IP protocol. • TCP—The virtual server is to accept connections that use TCP. • UDP—The virtual server is to accept connections that use UDP.
Application Protocol	This field appears if TCP or UDP is selected. The application protocols that are available depend on the type of ACE being configured. Select the application protocol to be supported by the virtual server. Table 4-2 identifies the available protocols for each ACE device type.

Table 4-4 Virtual Server Properties – Basic View (continued)

Field	Description
Port	This field appears for any specific TCP or UDP protocol. Enter the port to be used for the specified protocol. Valid entries are integers from 0 to 65535 or a range of integers, such as 10-20. Enter 0 (zero) to indicate all ports. For a complete list of all protocols and ports, see the Internet Assigned Numbers Authority available at www.iana.org/numbers.html.
All VLANs	Select the check box to support incoming traffic from all VLANs. Clear the check box to support incoming traffic from specific VLANs only.
VLAN	This field appears if the All VLANs check box is cleared. In the Available Items list, select the VLANs to use for incoming traffic, then click Add. The items appear in the Selected Items list. To remove VLANs, select them in the Selected Items lists, then click Remove. The items appear in the Available Items list. Note You cannot change the VLAN for a virtual server once it is specified. Instead, delete the virtual server and create a new one with the desired VLAN.

- Step 5** When you finish configuring virtual server properties, click:
- **Deploy Now** to deploy the configuration on the ACE.
 - **Cancel** to exit the procedure without saving your entries.
 - **Deploy Later** to save your entries and apply them at a later time.

Related Topics

- [Configuring Virtual Servers, page 4-2](#)
- [Configuring Virtual Server SSL Termination, page 4-12](#)

Configuring Virtual Server SSL Termination

SSL termination service allows the virtual server to act as an SSL proxy server and terminate SSL sessions between it and its clients.

Use this procedure to configure virtual server SSL termination service.

Assumption

A virtual server has been configured for HTTPS over TCP or Other over TCP in the Properties configuration subset. For more information, see [Configuring Virtual Server Properties, page 4-8](#).

Procedure

- Step 1** Select **Config > Devices > context > Load Balancing > Virtual Servers**. The Virtual Servers table appears.
- Step 2** Select the virtual server you want to configure for SSL termination, then click **Edit**. The Virtual Server configuration screen appears.

- Step 3** Click **SSL Termination**. The Proxy Service Name field appears.
- Step 4** In the Proxy Service Name field, select an existing SSL termination service, or select ***New*** to create a new SSL proxy service:
- If you select an existing SSL service, the screen refreshes and allows you to view, modify, or duplicate the existing configuration. See [Shared Objects and Virtual Servers, page 4-6](#) for more information about modifying shared objects.
 - If you select ***New***, the Proxy Service configuration subset appears.
- Step 5** Configure the SSL service using the in [Table 4-5](#).
For more information about SSL, see [Configuring SSL, page 8-1](#).

Table 4-5 Virtual Server SSL Attributes

Field	Description
Name	Enter a name for this SSL proxy service. Valid entries are alphanumeric strings with a maximum of 26 characters.
Key List	Select the SSL key pair to use during the SSL handshake for data encryption.
Certificate List	Select the SSL certificate to use during the SSL handshake.
Chain Group Name	Select the chain group to use during the SSL handshake.
Auth Group Name	Select the SSL authentication group to associate with this proxy server service.
	 Note This option appears for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.
CRL Best-Effort	This option appears if you select an authentication group in the Auth Group Name field. Select the check box to allow the ANM to search client certificates for the service to determine if it contains a CRL in the extension and retrieve the value, if it exists. Clear the check box to disable this feature.
CRL Name	This option appears if the CRL Best-Effort check box is clear. Select the Certificate Revocation List the ANM is to use for this proxy service.
Parameter Map Name	Select the SSL parameter map to associate with this proxy server service.

- Step 6** When you finish configuring virtual server properties, click:
- **Deploy Now** to deploy this configuration on the ACE.
 - **Cancel** to exit this procedure without saving your entries.
 - **Deploy Later** to save your entries and apply them at a later time.

Related Topics

- [Configuring Virtual Servers, page 4-2](#)

- [Configuring Virtual Server Properties, page 4-8](#)

Configuring Virtual Server Protocol Inspection

Configuring protocol inspection allows the virtual server to verify protocol behavior and identify unwanted or malicious traffic passing through the ACE.

In the Advanced View, protocol inspection configuration is available for the following virtual server protocol configurations:

- TCP with FTP, HTTP, HTTPS, RTSP, or SIP
- UDP with DNS or SIP

In the Basic View, protocol inspection configuration is available for TCP with FTP.

See [Table 4-2](#) for a list of protocols by ACE device type.

Use this procedure to configure protocol inspection on a virtual server.

Assumption

A virtual server has been configured to use one of the protocols that supports protocol inspection in the Properties configuration subset. See [Configuring Virtual Server Properties, page 4-8](#) for information on configuring these protocols.

Procedure

-
- Step 1** Select the item to configure:
- To configure a virtual server, select **Config > Devices > context > Load Balancing > Virtual Servers**.
 - To configure a configuration building block, select **Config > Global > All Building Blocks > building_block > Load Balancing > Virtual Servers**.
- The Virtual Servers table appears.
- Step 2** Select the virtual server that you want to configure for protocol inspection, then click **Edit**. The Virtual Server configuration screen appears.
- Step 3** Click **Protocol Inspection**. The Enable Inspect check box appears.
- Step 4** Select the Enable Inspect check box to enable inspection on the specified traffic. Clear this check box to disable inspection on this traffic. By default, the ACE allows all request methods.
- Step 5** If you select the Enable Inspect check box, configure additional inspection options using the information in [Table 4-6](#).

Table 4-6 Protocol Inspection Configuration Options

Protocol	Description
DNS	In the Length field enter the maximum length of the DNS packet in bytes. If you do not enter a value in this field, the DNS packet size is not checked.
FTP	1. Select the Use Strict check box to indicate that the virtual server is to perform enhanced inspection of FTP traffic and enforce compliance with RFC standards. Clear this check box to indicate that the virtual server is not to perform enhanced FTP inspection. 2. If you select the Use Strict check box, in the Blocked FTP Commands field, identify the commands that are to be denied by the virtual server. See Table 11-9 for more information about the FTP commands. – Select the commands that are to be blocked by the virtual server in the Available Items list, then click Add. The commands appear in the Selected Items list. – To remove commands that you do not want to be blocked, select them in the Selected Items list, then click Remove. The commands appear in the Available Items list.
HTTP or HTTPS	1. Select the Logging Enabled check box to enable monitoring of Layer 3 and Layer 4 traffic. When enabled, this feature logs every URL request that is sent in the specified class of traffic, including the source or destination IP address and the URL that is accessed. Clear this check box to disable monitoring of Layer 3 and Layer 4 traffic. 2. In the Policy subset, click Add to add a new match condition and action, or select an existing match condition and action, then click Edit to modify it. The Policy configuration pane appears. 3. In the Matches field, select an existing class map or *New* or *Inline Match* to configure new match criteria for protocol inspection. If you select an existing class map, the screen refreshes and allows you to view, modify, or duplicate the selected class map. See Shared Objects and Virtual Servers, page 4-6 for more information about modifying shared objects. 4. Configure match criteria and related actions using the information in Table 4-7. 5. Click: – OK to save your entries. The Conditions table refreshes with the new entry. – Cancel to exit the Policy subset without saving your entries. 6. In the Default Action field, select the default action that the virtual server is to take when specified match conditions for protocol inspection are not met: – Permit—The specified HTTP traffic is to be received by the virtual server. – Reset—The specified HTTP traffic is to be denied by the virtual server.

Table 4-6 Protocol Inspection Configuration Options (continued)

Protocol	Description
SIP	1. In the Actions subset, click Add to add a new match condition and action, or select an existing match condition and action, then click Edit to modify it. The Actions configuration pane appears. 2. In the Matches field, select an existing class map or *New* or *Inline Match* to configure new match criteria for protocol inspection. If you select an existing class map, the screen refreshes and allows you to view, modify, or duplicate the selected class map. See Shared Objects and Virtual Servers, page 4-6 for more information about modifying shared objects. 3. Configure match criteria and related actions using the information in Table 4-9. 4. In the Action field, select the action that the virtual server is to take when the specified match conditions are met: – Permit—The specified SIP traffic is to be received by the virtual server. – Drop—The specified SIP traffic is to be discarded by the virtual server. – Reset—The specified SIP traffic is to be denied by the virtual server. 5. Click: – OK to save your entries. The Conditions table refreshes with the new entry. – Cancel to exit the Conditions subset without saving your entries and to return to the Conditions table. 6. In the SIP Parameter Map field, select an existing parameter map or select *New* to configure a new one. If you select an existing parameter map, the screen refreshes and allows you to view, modify, or delete the selected parameter map. See Shared Objects and Virtual Servers, page 4-6 for more information about modifying shared objects. 7. Configure SIP parameter map options using the information in Table 7-8. 8. In the Secondary Connection Parameter Map field, select an existing parameter map or select *New* to configure a new one. If you select an existing parameter map, the screen refreshes and allows you to view, modify, or delete the selected parameter map. See Shared Objects and Virtual Servers, page 4-6 for more information about modifying shared objects. 9. Configure secondary connection parameter map options using the information in Table 7-2. 10. In the Default Action field, select the default action that the virtual server is to take when specified match conditions for SIP protocol inspection are not met: – Permit—The specified SIP traffic is to be received by the virtual server. – Drop—The specified SIP traffic is to be discarded by the virtual server. – Reset—The specified SIP traffic is to be denied by the virtual server. 11. Select the Logging Enabled check box to enable monitoring of Layer 3 and Layer 4 traffic. When enabled, this feature logs every URL request that is sent in the specified class of traffic, including the source or destination IP address and the URL that is accessed. Clear this check box to disable monitoring of Layer 3 and Layer 4 traffic.
RTSP	There are no protocol-specific inspection options for RTSP.

Table 4-7 HTTP and HTTPS Protocol Inspection Match Criteria Configuration

Selection	Action
Existing class map	- Click View to review the match condition information for the selected class map. - Click: Cancel to continue without making changes and to return to the previous screen. Edit to modify the existing configuration. Duplicate to create a new class map with the same attributes without affecting other virtual servers using the same classmap. See Shared Objects and Virtual Servers, page 4-6 for information about modifying shared objects. - In the Action field, indicate the action that the virtual server is to perform on the traffic if it matches the specified match criteria: Permit—The specified traffic is to be received by the virtual server if it meets the specified deep inspection match criteria. Reset—The specified traffic is to be denied by the virtual server, which then sends a TCP reset message to the client or server to close the connection.
New	- In the Name field, specify a unique name for this class map. - In the Match field, select the method to be used to evaluate multiple match statements when multiple match conditions exist: Any—A match exists if at least one of the match conditions is satisfied. All—A match exists only if all match conditions are satisfied. - In the Conditions table, click Add to add a new set of conditions, or select an existing entry, then click Edit to modify it. The Type field appears. - In the Type field, select the type of condition that is to be met for protocol inspection. - Provide condition-specific criteria using the information in Table 4-8. - In the Action field, indicate the action that the virtual server is to perform on the traffic if it matches the specified match criteria: Permit—The specified traffic is to be received by the virtual server if it meets the specified deep inspection match criteria. Reset—The specified traffic is to be denied by the virtual server, which then sends a TCP reset message to the client or server to close the connection.
Inline Match	- In the Conditions Type field, select the type of inline match condition that is to be met for protocol inspection. - Provide condition-specific criteria using the information in Table 4-8. - In the Action field, indicate the action that the virtual server is to perform on the traffic if it matches the specified match criteria: Permit—The specified traffic is to be received by the virtual server if it meets the specified deep inspection match criteria. Reset—The specified traffic is to be denied by the virtual server, which then sends a TCP reset message to the client or server to close the connection.

Table 4-8 HTTP and HTTPS Protocol Inspection Conditions and Options

Condition	Description
None	No conditions are defined for application inspection decisions.
URL	URL names are to be used for application inspection decisions. In the URL field, enter a URL or a portion of a URL to match. Valid entries are URL strings from 1 to 255 alphanumeric characters and include only the portion of the URL following <code>www.hostname.domain</code>. For example, in the URL <code>www.anydomain.com/latest/whatsnew.html</code>, include only <code>/latest/whatsnew.html</code>.
URL Length	URL length is to be used for application inspection decisions. - In the URL Length Operator field, select the operand to use to compare URL length: - Equal—The URL length must equal the number in the URL Length Value field. - Greater Than—The URL length must be greater than the number in the URL Length Value field. - Less Than—The URL length must be less than the number in the URL Length Value field. - Range—The URL length must be within the range specified in the URL Length Lower Value field and the URL Length Higher Value field. - Enter values to apply for URL length comparison: - If you select Equal, Greater Than, or Less Than in the URL Length Operator field, the URL Length Value field appears. In the URL Length Value field, enter the value for comparison. Valid entries are from 1 to 65535 bytes. - If you select Range in the URL Length Operator field, the URL Length Lower Value and the URL Length Higher Value fields appear: - In the URL Length Lower Value field, enter the lowest number of bytes to be used for this match condition. Valid entries are integers from 1 to 65535. The number in this field must be less than the number entered in the URL Length Higher Value field. - In the URL Length Higher Value field, enter the highest number of bytes to be used for this match condition. Valid entries are integers from 1 to 65535. The number in this field must be greater than the number entered in the URL Length Lower Value field.
Content	Specific content contained within the HTTP entity-body is to be used for application inspection decisions. - In the Content Expression field, enter the content that is to be matched. Valid entries are alphanumeric strings from 1 to 255 characters. - In the Content Offset field, enter the number of bytes to be ignored starting with the first byte of the Message body, after the empty line (CR,LF,CR,LF) between the headers and the body of the message. Valid entries are from 1 to 255 bytes.

Table 4-8 HTTP and HTTPS Protocol Inspection Conditions and Options (continued)

Condition	Description
Content Length	The content parse length is used for application inspection decisions. - In the Content Length Operator field, select the operand to use to compare content length: - Equal—The content length must equal the number in the Content Length Value field. - Greater than—The content length must be greater than the number in the Content Length Value field. - Less than—The content length must be less than the number in the Content Length Value field. - Range—The content length must be within the range specified in the Content Length Lower Value field and the Content Length Higher Value field. - Enter values to apply for content length comparison: - If you select Equal, Greater than, or Less than in the Content Length Operator field, the Content Length Value field appears. In the Content Length Value field, enter the number of bytes for comparison. Valid entries are integers from 0 to 4294967295. - If you select Range in the Content Length Operator field, the Content Length Lower Value and the Content Length Higher Value fields appear: - In the Content Length Lower Value field, enter the lowest number of bytes to be used for this match condition. Valid entries are integers from 0 to 4294967295. The number in this field must be less than the number entered in the Content Length Higher Value field. - In the Content Length Higher Value field, enter the highest number of bytes to be used for this match condition. Valid entries are integers from 0 to 4294967295. The number in this field must be greater than the number entered in the Content Length Lower Value field.
Header	The name and value in an HTTP header are used for application inspection decisions. - In the Header field, select one of the predefined HTTP headers to match, or select HTTP Header to specify a different HTTP header. - If you select HTTP Header, in the Header Name field, enter the name of the HTTP header to match. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. - In the Header Value field, enter the header-value expression string to compare against the value in the specified field in the HTTP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. Header expressions allow spaces, provided that the spaces are escaped or quoted. All headers in the header map must be matched. See Table 11-35 for a list of the supported characters that you can use in regular expressions.

Table 4-8 HTTP and HTTPS Protocol Inspection Conditions and Options (continued)

Condition	Description
Header Length	The length of the header in the HTTP message is used for application inspection decisions. - In the Header Length Type field, specify whether HTTP header request or response messages are to be used for application inspection decisions: - Request—HTTP header request messages are to be checked for header length. - Response—HTTP header response messages are to be checked for header length. - In the Header Length Operator field, select the operand to be used to compare header length: - Equal—The header length must equal the number in the Header Length Value field. - Greater Than—The header length must be greater than the number in the Header Length Value field. - Less Than—The header length must be less than the number in the Header Length Value field. - Range—The header length must be within the range specified in the Header Length Lower Value field and the Header Length Higher Value field. - Enter values to apply for header length comparison: - If you select Equal, Greater Than, or Less Than in the Header Length Operator field, the Header Length Value field appears. In the Header Length Value field, enter the number of bytes for comparison. Valid entries are integers from 0 to 255. - If you select Range in the Header Length Operator field, the Header Length Lower Value and the Header Length Higher Value fields appear: - In the Header Length Lower Value field, enter the lowest number of bytes to be used for this match condition. Valid entries are integers from 0 to 255. The number in this field must be less than the number entered in the Header Length Higher Value field. - In the Header Length Higher Value field, enter the highest number of bytes to be used for this match condition. Valid entries are integers from 1 to 255. The number in this field must be greater than the number entered in the Header Length Lower Value field.
Header MIME Type	Multipurpose Internet Mail Extension (MIME) message types are used for application inspection decisions. In the Header MIME Type field, select the MIME message type to use for this match condition.
Port Misuse	The misuse of port 80 (or any other port running HTTP) is to be used for application inspection decisions. Indicate the application category to use for this match condition: - IM—Instant messaging applications are to be checked. - P2P—Peer-to-peer applications are to be checked. - Tunneling—Tunneling applications are to be checked.
Request Method	A request method is to be used for application inspection decisions. - Select the type of request method to use for this match condition: - EXT—An HTTP extension method is to be used. - RFC—The request method defined in RFC 2616 is to be used. - In the Request Method field, select the request method that is to be inspected.

Table 4-8 HTTP and HTTPS Protocol Inspection Conditions and Options (continued)

Condition	Description
Transfer Encoding	An HTTP transfer-encoding type is to be used for application inspection decisions. The transfer-encoding general-header field indicates the type of transformation, if any, that has been applied to the HTTP message body to safely transfer it between the sender and the recipient. In the Transfer Encoding field, select the type of encoding that is to be checked: • Chunked—The message body is transferred as a series of chunks. • Compress—The encoding format that is produced by the UNIX file compression program <i>compress</i>. • Deflate—The .zlib format that is defined in RFC 1950 in combination with the DEFLATE compression mechanism described in RFC 1951. • Gzip—The encoding format that is produced by the file compression program GZIP (GNU zip) as described in RFC 1952. • Identity—The default (identity) encoding which does not require the use of transformation.
Strict HTTP	Compliance with HTTP RFC 2616 is to be used for application inspection decisions.
Content Type Verification	Verification of MIME-type messages with the header MIME-type is to be used for application inspection decisions. This option verifies that the header MIME-type value is in the internal list of supported MIME-types and that the header MIME-type matches the content in the data or body portion of the message.

Table 4-9 SIP Protocol Inspection Match Criteria Configuration

Selection	Action
Existing class map	- Click View to review the match condition information for the selected class map. - Click: Cancel to continue without making changes and to return to the previous screen. Edit to modify the existing configuration. Duplicate to create a new class map with the same attributes without affecting other virtual servers using the same classmap. See Shared Objects and Virtual Servers, page 4-6 for more information about modifying shared objects. - In the Action field, indicate the action that the virtual server is to perform on the traffic if it matches the specified match criteria: Permit—The specified traffic is to be received by the virtual server. Drop—The specified traffic is to be dropped by the virtual server. Reset—The specified traffic is to be denied by the virtual server, which then sends a TCP reset message to the client or server to close the connection.
New	- In the Name field, specify a unique name for this class map. - In the Conditions table, click Add to add a new set of conditions, or select an existing entry, then click Edit to modify it. The Type field appears. - In the Type field, select the type of condition that is to be met for protocol inspection. - Provide condition-specific criteria using the information in Table 4-10. - In the Action field, indicate the action that the virtual server is to perform on the traffic if it matches the specified match criteria: Permit—The specified traffic is to be received by the virtual server. Drop—The specified traffic is to be dropped by the virtual server. Reset—The specified traffic is to be denied by the virtual server, which then sends a TCP reset message to the client or server to close the connection.
Inline Match	- In the Conditions Type field, select the type of inline match condition that is to be met for protocol inspection. Table 4-10 describes the types of conditions and their related configuration options. - Provide condition-specific criteria using the information in Table 4-10. - In the Action field, indicate the action that the virtual server is to perform on the traffic if it matches the specified match criteria: Permit—The specified traffic is to be received by the virtual server. Drop—The specified traffic is to be dropped by the virtual server. Reset—The specified traffic is to be denied by the virtual server, which then sends a TCP reset message to the client or server to close the connection.

Table 4-10 **SIP Protocol Inspection Conditions and Options**

Condition	Description
None	No conditions are defined for application inspection decisions.
Message Path	SIP inspection allows you to filter messages coming from or transiting through certain SIP proxy servers. The ACE maintains a list of the unauthorized SIP proxy IP addresses or URLs in the form of regular expressions and checks this list against the VIA header field in each SIP packet. In the Message Path field, enter a regular expression that identifies the SIP proxy server for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions.
SIP Request Method	A SIP request method is used for application inspection decisions. In the Request Method field, select the request method that is to be inspected.
IM Subscriber	An IM (instant messaging) subscriber is used for application inspection decisions. In the IP Subscriber field, enter a regular expression that identifies the IM subscriber for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions.
Third Party	SIP allows users to register other users on their behalf by sending REGISTER messages with different values in the From and To header fields. This process can pose a security threat if the REGISTER message is actually a Deregister message. A malicious user could cause a DoS (denial-of-service) attack by deregistering all users on their behalf. To prevent this security threat, you can specify a list of privileged users who can register or unregister someone else on their behalf. The ACE maintains the list as a regex table. If you configure this policy, the ACE drops REGISTER messages with mismatched From and To headers and a From header value that does not match any of the privileged user IDs. In the Third Party Registration Entities field, enter a regular expression that identifies a privileged user who is authorized for third-party registrations. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions.
URI Length	The ACE can validate the length of SIP URIs or Tel URIs. A SIP URI is a user identifier that a calling party (source) uses to contact the called party (destination). A Tel URI is a telephone number that identifies the endpoint of a SIP connection. For more information about SIP URIs and Tel URIs, see RFC 2534 and RFC 3966, respectively. To filter SIP traffic based on URIs: - In the URI Type field, indicate the type of URI to be used: - SIP URI—The calling party URI is to be used for this match condition. - Tel URI—A telephone number is to be used for this match condition. - In the URI Operator field, confirm that Greater Than is selected. - In the URI Length field, enter the maximum length of the SIP URI or Tel URI in bytes. Valid entries are integers from 0 to 254 bytes.

Table 4-10 *SIP Protocol Inspection Conditions and Options (continued)*

Condition	Description
Called Party	The destination or called party specified in the URI of the SIP To header is used for SIP protocol inspection decisions. In the Called Party field, enter a regular expression that identifies the called party in the URI of the SIP To header for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions.
Calling Party	The source or caller specified in the URI of the SIP From header is used for SIP protocol inspection decisions. In the Calling Party field, enter a regular expression that identifies the calling party in the URI of the SIP From header for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions.
SIP Content Type	The content type in the SIP message body is used for SIP protocol inspection decisions. In the Content Type field, enter a regular expression that identifies the content type in the SIP message body to use for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions.
SIP Content Length	The SIP message body content length is used for SIP protocol inspection decisions. To specify SIP traffic based on SIP message body length: 1. In the Content Operator field, confirm that Greater Than is selected. 2. In the Content Length field, enter the maximum size of a SIP message body in bytes that the ACE is to allow without performing SIP protocol inspection. If a SIP message exceeds the specified value, the ACE performs SIP protocol inspection as defined in an associated policy map. Valid entries are integers from 0 to 65534 bytes.

Step 6 When you finish configuring virtual server properties, click:

- **Deploy Now** to deploy this configuration on the ACE.
- **Cancel** to exit this procedure without saving your entries.
- **Deploy Later** to save your entries and deploy the configuration at a later time.

Related Topics

- [Configuring Virtual Server Properties, page 4-8](#)
- [Configuring Virtual Server SSL Termination, page 4-12](#)
- [Configuring Virtual Server Layer 7 Load Balancing, page 4-25](#)

Configuring Virtual Server Layer 7 Load Balancing

In the Advanced View, Layer 7 load balancing is available for virtual servers configured with one of the following protocol combinations:

- TCP with Generic, HTTP, HTTPS, RTSP, or SIP
- UDP with Generic, RADIUS, or SIP

See [Configuring Virtual Server Properties, page 4-8](#) for information on configuring these protocols.

[Table 4-2](#) identifies the protocols that are available for each type of ACE device.

Use this procedure to configure Layer 7 load balancing on a virtual server.

Assumption

A virtual server has been configured with one of the following protocol combinations:

- TCP with Generic, HTTP, HTTPS, RTSP, or SIP
- UDP with Generic, RADIUS, or SIP

Procedure

-
Step 1	Select Config > Devices > context > Load Balancing > Virtual Servers . The Virtual Servers table appears.
Step 2	Select the virtual server you want to configure for Layer 7 load balancing, then click Edit . The Virtual Server configuration screen appears.
Step 3	Click L7 Load-Balancing . The Layer 7 Load-Balancing Rule Match table appears.
Step 4	In the Rule Match table, click Add to add a new match condition and action, or select an existing match condition and action, then click Edit to modify it. The Rule Match configuration pane appears.
Step 5	In the Rule Match field, select an existing class map or *New* or *Inline Match* to configure new match criteria for Layer 7 load balancing: • If you select an existing class map, click View to review, modify, or duplicate the existing configuration. See Shared Objects and Virtual Servers, page 4-6 for more information about modifying shared objects. • If you click *New* or *Inline Match*, the Rule Match configuration pane appears.

Step 6 Configure match criteria using the information in [Table 4-11](#).

Table 4-11 Layer 7 Load-Balancing Match Criteria Configuration

Selection	Action
Existing class map	1. Click View to review the match condition information for the selected class map. 2. Click: – Cancel to continue without making changes and to return to the previous screen. – Edit to modify the existing configuration. – Duplicate to create a new class map with the same attributes without affecting other virtual servers using the same classmap. See Shared Objects and Virtual Servers, page 4-6 for more information about modifying shared objects.
New	1. In the Name field, enter a unique name for this class map. 2. In the Match field, select the method to be used to evaluate multiple match statements when multiple match conditions exist: – Match Any—Aa match exists if at least one of the match conditions is satisfied. – Match All—A match exists only if all match conditions are satisfied. 3. In the Conditions table, click Add to add a new set of conditions or select an existing entry, then click Edit to modify it. 4. In the Type field, select the match condition and configure any protocol-specific options: – For Generic protocol options, see Table 11-10. – For HTTP and HTTPS protocol options, see Table 4-12. – For RADIUS protocol options, see Table 11-11. – For RTSP protocol options, see Table 11-12. – For SIP protocol options, see Table 11-13. 5. Click: – OK to accept your entries and to return to the Conditions table. – Cancel to exit this procedure without saving your entries and to return to the Conditions table.
Inline Match	In the Conditions Type field, select the type of inline match condition and configure any protocol-specific options: • For Generic protocol options, see Table 11-10. • For HTTP and HTTPS protocol options, see Table 4-12. • For RADIUS protocol options, see Table 11-11. • For RTSP protocol options, see Table 11-12. • For SIP protocol options, see Table 11-13.

Table 4-12 **Layer 7 HTTP/HTTPS Load-Balancing Conditions and Options**

Match Condition	Description
Http-cookie	HTTP cookies are used for the match condition. 1. In the Cookie Name field, enter a unique cookie name. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. 2. In the Cookie Value field, enter a unique cookie value expression. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions. 3. Select the Secondary Cookie Matching check box to indicate that the ACE is to use both the cookie name and the cookie value to satisfy this match condition. Clear this check box to indicate that the ACE is to use either the cookie name or the cookie value to satisfy this match condition. This field does not appear for inline match conditions.
Http-header	An HTTP header and corresponding value are used to establish match conditions. 1. In the Header Name field, specify the header in one of the following ways: – To specify an HTTP header that is not one of the standard HTTP headers, select the first radio button and enter the HTTP header name in the Header Name field. Enter an unquoted text string with no spaces and a maximum of 64 characters. – To specify one of the standard HTTP headers, select the second radio button and select the desired HTTP header from the list. 2. In the Header Value field, enter the header-value expression string to compare against the value in the specified field in the HTTP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. Header expressions allow spaces, provided that the spaces are escaped or quoted. All headers in the header map must be matched. Table 11-35 lists the supported characters that you can use in regular expressions.
Http-url	The ACE performs regular expression matching against the received packet data from a particular connection based on the HTTP URL string. 1. In the URL Expr field, enter a URL, or portion of a URL, to match. Valid entries are URL strings from 1 to 255 alphanumeric characters. Include only the portion of the URL following <code>www.hostname.domain</code> in the match statement. For example, in the URL <code>www.anydomain.com/latest/whatsnew.html</code>, include only <code>/latest/whatsnew.html</code>. To match the <code>www.anydomain.com</code> portion, the URL string can take the form of a URL regular expression. The ACE supports regular expressions for matching URL strings. Table 11-35 lists the supported characters that you can use in regular expressions. 2. In the Method field, enter the HTTP method to match. Valid entries are unquoted text strings with no spaces and a maximum of 15 alphanumeric characters. The method can either be one of the standard HTTP 1.1 method names (OPTIONS, GET, HEAD, POST, PUT, DELETE, TRACE, or CONNECT) or a text string that must be matched exactly (for example, CORVETTE).
Source-address	A client source IP address is used for the match condition. 1. In the Source Address field, enter the source IP address of the client. Enter the IP address in dotted-decimal notation (for example, 192.168.11.2). 2. In the Source Netmask field, select the subnet mask to apply to the source IP address.

Table 4-12 Layer 7 HTTP/HTTPS Load-Balancing Conditions and Options (continued)

Match Condition	Description
Class-map	An existing class map is used for the match condition. In the Class Map field, select the class map to be used.
Http-content	 Note This option appears for ACE 2.0 modules and the ACE 4710 A3(1.0) release only. Specific content contained within the HTTP entity-body is used to establish a match condition. 1. In the Content Expression field, enter the content that is to be matched. Valid entries are alphanumeric strings from 1 to 255 characters. 2. In the Content Offset field, enter the number of bytes to be ignored starting with the first byte of the Message body, after the empty line (CR,LF,CR,LF) between the headers and the body of the message. Valid entries are integers from 1 to 255.

- Step 7** In the Primary Action field, indicate the action that the virtual server is to perform on the traffic if it matches the specified match criteria:
- Drop—Client requests for content are to be discarded when match conditions are met. Continue with [Step 11](#).
 - Forward—Client requests for content are to be forwarded without performing load balancing on the requests when match conditions are met. Continue with [Step 11](#).
 - Load Balance—Client requests for content are to be directed to a server farm when match conditions are met. Continue with [Step 8](#).
 - Sticky—Client requests for content are to be handled by a sticky group when match conditions are met. Continue with [Step 9](#).

- Step 8** If you select Load Balance as the primary action:
- a. In the Server Farm field, select the primary server farm to use for load balancing, or select ***New*** to configure a new server farm (see [Table 4-13](#)).
 - b. In the Backup Server Farm field, select the server farm to act as the backup server farm for load balancing if the primary server farm is unavailable, or select ***New*** to configure a new backup server farm (see [Table 4-13](#)).



Note If you select an existing object in either of these fields, you can view, modify, or duplicate the selected object's existing configuration. See [Shared Objects and Virtual Servers, page 4-6](#) for more information about modifying shared objects in virtual servers.

Table 4-13 ***New Server Farm Attributes***

Field	Description
Name	Enter a unique name for the server farm. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters.
Type	Select the type of server farm: • Host—A typical server farm that consists of real servers that provide content and services to clients. By default, if you configure a backup server farm and all real servers in the primary server farm go down, the primary server farm fails over to the backup server farm. Use the following options to specify thresholds for failover and returning to service. a. In the Partial Threshold Percentage field, enter the minimum percentage of real servers in the primary server farm that must remain active for the server farm to stay up. If the percentage of active real servers falls below this threshold, the ACE takes the server farm out of service. Valid entries are integers from 0 to 99. b. In the Back Inservice field, enter the percentage of real servers in the primary server farm that must be active again for the ACE to place the server farm back into service. Valid entries are integers from 0 to 99. The value in this field should be larger than the value in the Partial Threshold Percentage field. • Redirect—A server farm that consists only of real servers that redirect client requests to alternate locations specified in the real server configuration.

Table 4-13 **New Server Farm Attributes (continued)**

Field	Description
Predictor	Specify the method for selecting the next server in the server farm to respond to client requests. You can configure additional predictor attributes under Config > Devices > context > Load Balancing > Server Farm as explained in Table 5-7. - Roundrobin—Server selection is based on server weight. - Leastconns—Server selection is based on the number of connections; the server with the fewest connections is selected next. In the Slowstart Duration field, enter the slow-start value to apply. Valid entries are integers from 1 to 65535, where 1 is the slowest ramp-up time. The slow-start mechanism is used to avoid sending a high number of new connections to servers that have just been put into service. - Least Loaded—Server selection is based on the lowest load based on information obtained from SNMP probes. In the SNMP Probe Name field, enter the name of the SNMP probe to use. - Least Bandwidth—Server selection is based on the least amount of network traffic over a specified sampling period. a. In the Assess Time field, enter the number of seconds for which the ACE is to collect traffic information. Valid entries are integers from 1 to 10 seconds. b. In the Least Bandwidth Samples field, enter the number of samples over which you want to weight and average the results of the probe query to calculate the final load value. Valid entries are 1, 2, 4, 8, and 16 (integers from 1 to 16 that are also a power of 2). - Response—Server selection is based on the lowest response time for the requested response-time measurement. a. In the Response Type field, select the type of measurement to use: - App-req-to-resp—Measures the response time from when the ACE sends an HTTP request to a server to the time that the ACE receives a response from the server for that request. - Syn-to-close—Measures the response time from when the ACE sends a TCP SYN to a server to the time that the ACE receives a CLOSE from the server. - Syn-to-synack—Measures the response time from when the ACE sends a TCP SYN to a server to the time that the ACE receives a SYN-ACK from the server. b. In the Response Samples field, enter the number of samples over which you want to average the results of the response-time measurement. Valid entries are 1, 2, 4, 8, and 16 (integers from 1 to 16 that are also a power of 2).

Table 4-13 ***New Server Farm Attributes (continued)***

Field	Description
Probes	Specify the health monitoring probes to use: - To include a probe that you want to use for health monitoring, select it in the Available Items list, then click Add. The probe appears in the Selected Items list. - To remove a probe that you do not want to use for health monitoring, select it in the Selected Items list, then click Remove. The probe appears in the Available Items list. - To specify a sequence for probe use, select probes in the Selected Items list, then click Up or Down until you have the desired sequence. - To add a new probe, click Create. See Configuring Health Monitoring for Real Servers, page 5-25. - To view an existing probe's configuration, select a probe, then click View.
Real Servers	The Real Servers table allows you to add, modify, remove, or change the order of real servers. - Select an existing server, or click Add to add a server to the server farm: - If you select an existing server, you can view, modify, or duplicate the server's existing configuration. See Shared Objects and Virtual Servers, page 4-6 for more information about modifying shared objects. - If you click Add, the screen refreshes so you can enter server information. - In the Name field, specify the name of the real server in one of the following ways: - To identify a new real server, select the first radio button, then enter the name of the real server in the adjoining field. - To specify an existing real server, select the second radio button, then select one of the real servers listed. - In the IP Address field, enter the IP address of the real server in dotted-decimal format. - In the Port field, enter the port number to be used for server port address translation (PAT). Valid entries are integers from 1 to 65535. - In the Weight field, enter the weight to assign to this server in the server farm. Valid entries are integers from 1 to 100, and the default is 8. - In the Rate Bandwidth field, enter the real server bandwidth limit in bytes per second. Valid entries are integers from 1 to 300000000 bytes. - In the Rate Connection field, enter the limit for connections per second. Valid entries are integers from 1 to 350000. - In the State field, select the administrative state of this server: - Inservice—The server is to be placed in use as a destination for server load balancing - Out of Service—The server is not to be placed in use by a server load balancer as a destination for client connections. - Click: OK to accept your entries and add this real server to the server farm. The table refreshes with updated information. Cancel to exit this procedure without saving your entries and to return to the Real Servers table.

- Step 9** If you select Sticky as the primary action, in the Sticky Group field, select an existing sticky group or click ***New*** to add a new sticky group (see [Table 4-14](#)).



Note If you select an existing sticky group, you can view, modify, or duplicate the selected object's existing configuration. See [Shared Objects and Virtual Servers, page 4-6](#) for more information about modifying shared objects in virtual servers.

Table 4-14 *Sticky Group Attributes*

Field	Description
Group Name	Enter a unique identifier for the sticky group. You can either accept the automatically incremented entry given or you can enter your own. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
Type	Select the method to be used when establishing sticky connections and configure any type-specific attributes: • HTTP Cookie—The virtual server is either to learn a cookie from the HTTP header of a client request or to insert a cookie in the Set-Cookie header of the response from the server to the client, and then use the learned cookie to provide stickiness between the client and server for the duration of the transaction. See Table 6-3 for additional configuration options. • HTTP Header—The virtual server is to stick client connections to the same real server based on HTTP headers. See Table 6-4 for additional configuration options. • IP Netmask—The virtual server is to stick a client to the same server for multiple subsequent connections as needed to complete a transaction using the client source IP address, the destination IP address, or both. See Table 6-5 for additional configuration options. Note If an organization uses a megaproxy to load balance client requests across multiple proxy servers when a client connects to the Internet, the source IP address is no longer a reliable indicator of the true source of the request. In this situation, you can use cookies or another sticky method to ensure session persistence. • HTTP Content—The virtual server is to stick client connections to the same real server based on a string in the data portion of the HTTP packet. See Table 6-2 for additional configuration options. • Layer 4 Payload—The virtual server is to stick client connections to the same real server based on a string in the payload portion of the Layer 4 protocol packet. See Table 6-6 for additional configuration options. • RADIUS—The virtual server is to stick client connections to the same real server based on a RADIUS attribute. • RTSP Header—The virtual server is to stick client connections to the same real server based on the RTSP Session header field. Table 6-8 for additional configuration options. • SIP Header—The virtual server is to stick client connections to the same real server based on the SIP Call-ID header field.
Aggregate State	Select the check box to indicate that the state of the primary server farm is to be tied to the state of all real servers in the server farm and in the backup server farm, if configured. The ACE declares the primary server farm down if all real servers in the primary server farm and all real servers in the backup server farm are down. Clear the check box if the state of the primary server farm is not to be tied to all real servers in the server farm and in the backup server farm.

Table 4-14 **Sticky Group Attributes (continued)**

Field	Description
Sticky Enabled on Backup Server Farm	Select the check box to indicate that the backup server farm is sticky. Clear the check box if the backup server farm is not sticky.
Replicate	Select the check box to indicate that the virtual server is to replicate sticky table entries on the backup server farm. If a failover occurs and this option is selected, the new active server farm can maintain the existing sticky connections. Clear the check box to indicate that the virtual server is not to replicate sticky table entries on the backup server farm.
Timeout	Enter the number of minutes that the virtual server keeps the sticky information for a client connection in the sticky table after the latest client connection terminates. Valid entries are integers from 1 to 65535; the default is 1440 minutes (24 hours).
Timeout Active Connections	Select the check box to specify that the virtual server is to time out sticky table entries even if active connections exist after the sticky timer expires. Clear the check box to specify that the virtual is not to time out sticky table entries even if active connections exist after the sticky timer expires. This is the default behavior.
Server Farm	Select an existing server farm to act as the primary server farm for this sticky group, or select *New* to create a new server farm. If you select *New* , configure the server farm using the information in Table 4-13 .
Backup Server Farm	Select an existing server farm to act as the backup server farm this sticky group, or select *New* to create a new server farm. If you select *New* , configure the server farm using the information in Table 4-13 .

- Step 10** In the Compression Method field, select the HTTP compression method to indicate how the ACE appliance is to compress packets when a client request indicates that the client browser is capable of packet compression. By default, HTTP compression is disabled in the ACE. When you configure HTTP compression using the ACE, the appliance compresses data in the HTTP GET responses from the real servers. The ACE does not compress HTTP requests from clients or the HTTP headers in the server responses.

**Note**

By default, the ACE supports HTTP compression at rates of 100 megabits per second (Mbps). Installing an optional HTTP compression license allows you to increase this value to a maximum of 2 Gbps. See the *Cisco 4700 Series Application Control Engine Appliance Administration Guide* for information on ACE licensing options.

Options include:

- deflate—Specifies the deflate compression format as the method to use when the client browser supports both the deflate and gzip compression methods. deflate, the data format for compression described in RFC1951
- gzip—Specifies the gzip compression format as the method to use when the client browser supports both the deflate and gzip compression methods. Gzip is the file format for compression described in RFC1952.
- N/A—HTTP compression is disabled.

When you enable HTTP compression, the ACE compresses the packets using the following default compression parameter values:

- Mime type—All text formats (text/*).
- Minimum size—512 bytes.
- User agent—None.

Step 11 In the SSL Initiation field, select an existing service, or select ***New*** to create a new service:

- If you select an existing SSL service, you can view, modify, or duplicate the existing configuration. See [Shared Objects and Virtual Servers, page 4-6](#) for more information about modifying shared objects.
- If you select ***New***, configure the service using the information in [Table 4-5](#). For more information about SSL, see [Configuring SSL, page 8-1](#).

Step 12 In the Insert HTTP Headers field, enter the name of the HTTP header and the value to be matched using the format *header_name=header_value* where:

- *header_name* represents the name of the HTTP header to insert in the client HTTP request. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. You can specify predefined header or any custom header name provided that it does not exceed the maximum length limit.
- *header_value* represents the expression string to compare against the value in the specified field in the HTTP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. Header expressions allow spaces, provided that the spaces are escaped or quoted. All headers in the header map must be matched. [Table 11-35](#) lists the supported characters that you can use in regular expressions.

For example, you might enter `Host=www.cisco.com`.

Step 13 Click:

- **OK** to save your entries and to return to the Rule Match table.
- **Cancel** to exit this procedure without saving your entries and to return to the Rule Match table.

Step 14 When you finish configuring virtual server properties, click:

- **Deploy Now** to deploy this configuration on the ACE.
- **Cancel** to exit this procedure without saving your entries.
- **Deploy Later** to save your entries and apply them at a later time.

Related Topics

- [Configuring Virtual Servers, page 4-2](#)
- [Configuring Virtual Server Properties, page 4-8](#)
- [Configuring Virtual Server SSL Termination, page 4-12](#)
- [Configuring Virtual Server Protocol Inspection, page 4-14](#)

Configuring Virtual Server Default Layer 7 Load Balancing

Use this procedure configure default Layer 7 load-balancing actions for all network traffic that does not meet previously specified match conditions.

Assumption

A virtual server has been configured. See [Configuring Virtual Servers, page 4-2](#) for information on configuring a virtual server.

Procedure

-
- Step 1** Select **Config > Devices > context > Load Balancing > Virtual Servers**. The Virtual Servers table appears.
- Step 2** Select the virtual server you want to configure for default Layer 7 load balancing, then click **Edit**. The Virtual Server configuration screen appears.
- Step 3** Click **Default L7 Load-Balancing Action**. The Default L7 Load-Balancing Action configuration pane appears.
- Step 4** In the Primary Action field, indicate the default action the virtual server is to take in response to client requests for content when specified match conditions are not met:
- Drop—Client requests that do not meet specified match conditions are to be discarded. Continue with [Step 8](#).
 - Forward—Client requests that do not meet specified match conditions are to be forwarded without performing load balancing on the requests. Continue with [Step 8](#).
 - Load Balance—Client requests for content are to be directed to a server farm. Continue with [Step 5](#).
 - Sticky—Client requests for content are to be handled by a sticky group when match conditions are met. Continue with [Step 6](#).
- Step 5** If you select Load Balance as the primary action:
- a. In the Server Farm field, select the primary server farm to use for load balancing, or select ***New*** to configure a new server farm (see [Table 4-13](#)).
 - b. In the Backup Server Farm field, select the server farm to act as the backup server farm for load balancing if the primary server farm is unavailable, or select ***New*** to configure a new backup server farm (see [Table 4-13](#)).



Note If you select an existing object in either field, you can view, modify, or duplicate the selected object's existing configuration. See [Shared Objects and Virtual Servers, page 4-6](#) for more information about modifying shared objects in virtual servers.

- Step 6** If you select Sticky as the primary action, in the Sticky Group field, select an existing sticky group or click ***New*** to add a new sticky group (see [Table 4-14](#)).



Note If you select an existing sticky group, you can view, modify, or duplicate the selected object's existing configuration. See [Shared Objects and Virtual Servers, page 4-6](#) for more information about modifying shared objects in virtual servers.

- Step 7** In the Compression Method field, select the HTTP compression method to indicate how the ACE appliance is to compress packets when a client request indicates that the client browser is capable of packet compression. By default, HTTP compression is disabled in the ACE. When you configure HTTP compression using the ACE, the appliance compresses data in the HTTP GET responses from the real servers. The ACE does not compress HTTP requests from clients or the HTTP headers in the server responses.



Note By default, the ACE supports HTTP compression at rates of 100 megabits per second (Mbps). Installing an optional HTTP compression license allows you to increase this value to a maximum of 2 Gbps. See the *Cisco 4700 Series Application Control Engine Appliance Administration Guide* for information on ACE licensing options.

Options include:

- deflate—Specifies the deflate compression format as the method to use when the client browser supports both the deflate and gzip compression methods. deflate, the data format for compression described in RFC1951
- gzip—Specifies the gzip compression format as the method to use when the client browser supports both the deflate and gzip compression methods. Gzip is the file format for compression described in RFC1952.
- N/A—HTTP compression is disabled.

When you enable HTTP compression, the ACE compresses the packets using the following default compression parameter values:

- Mime type—All text formats (text/*).
- Minimum size—512 bytes.
- User agent—None.

- Step 8** In the SSL Initiation field, select an existing service, or select ***New*** to create a new service:
- If you select an existing SSL service, you can view, modify, or duplicate the existing configuration. See [Shared Objects and Virtual Servers, page 4-6](#) for more information about modifying shared objects.
 - If you select ***New***, configure the service using the information in [Table 4-5](#). For more information about SSL, see [Configuring SSL, page 8-1](#).
- Step 9** In the Insert HTTP Headers field, enter the name of the HTTP header and the value to be matched using the format *header_name=header_value* where:
- *header_name* represents the name of the HTTP header to insert in the client HTTP request. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. You can specify predefined header or any custom header name provided that it does not exceed the maximum length limit.
 - *header_value* represents the expression string to compare against the value in the specified field in the HTTP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. Header expressions allow spaces, provided that the spaces are escaped or quoted. All headers in the header map must be matched. [Table 11-35](#) lists the supported characters that you can use in regular expressions.

For example, you might enter `Host=www.cisco.com`.

- Step 10** When you finish configuring virtual server properties, click:
- **Deploy Now** to deploy this configuration on the ACE.

- **Cancel** to exit this procedure without saving your entries and to return to the Virtual Servers table.
 - **Deploy Later** to save your entries and apply the configuration at a later time.
-

Related Topics

- [Configuring Virtual Server Properties, page 4-8](#)
- [Configuring Virtual Server SSL Termination, page 4-12](#)
- [Configuring Virtual Server Protocol Inspection, page 4-14](#)
- [Configuring Virtual Server Layer 7 Load Balancing, page 4-25](#)

Configuring Application Acceleration and Optimization

The ACE appliance includes configuration options that allow you to accelerate enterprise applications, resulting in increased employee productivity, enhanced customer retention, and increased online revenues. The application acceleration functions of the ACE appliance apply several optimization technologies to accelerate Web application performance. This application acceleration functionality enables enterprises to optimize network performance and improve access to critical business information. It also accelerates the performance of Web applications, including customer relationship management (CRM), portals, and online collaboration by up to 10 times.

Refer to [Configuring Application Acceleration and Optimization, page 12-1](#) or the *Cisco 4700 Series Application Control Engine Appliance Application Acceleration and Optimization Configuration Guide* for more information about application acceleration and optimization.

Use this procedure to configure acceleration and optimization on virtual servers that are configured on ACE appliances.

This option is available only for ACE appliances and only in the Advanced View.

Assumption

A virtual server has been configured on an ACE appliance with HTTP or HTTPS as the application protocol. See [Configuring Virtual Servers, page 4-2](#) for information on configuring a virtual server.

Procedure

-
Step 1	Select Config > Devices > context > Load Balancing > Virtual Servers . The Virtual Servers table appears.
Step 2	Select the virtual server you want to configure for optimization, then click Edit . The Virtual Server configuration screen appears.
Step 3	Click Application Acceleration and Optimization . The Application Acceleration and Optimization configuration pane appears.
Step 4	In the Configuration field, indicate the method you want to use to configure application acceleration and optimization: • EZ—Use standard acceleration and optimization options. Continue with Step 5. • Custom—Associate specific match criteria, actions, and parameter maps for application acceleration and optimization for the virtual server. If you choose this option, continue with Step 6 through Step 14.

- Step 5** If you select EZ, the Latency Optimization (FlashForward) and Bandwidth Optimization (Delta) fields appear.
- Select the Latency Optimization (FlashForward) check box to indicate that the ACE appliance is to use bandwidth reduction and download acceleration techniques to objects embedded within HTML pages. Clear the check box to indicate that the ACE appliance is not to employ these techniques to objects embedded within HTML pages. Latency optimization corresponds to FlashForward functionality. For more information about FlashForward functionality, see [Optimization Overview, page 12-1](#).
 - Select the Bandwidth Optimization (Delta) check box to indicate that the ACE appliance is to dynamically update client browser caches with content differences, or deltas. Clear the check box to indicate that the ACE appliance is not to dynamically update client browser caches. Bandwidth optimization corresponds to action list Delta optimization. For more information about configuring Delta optimization, see [Optimization Overview, page 12-1](#) and [Configuring Action Lists for Application Acceleration and Optimization, page 12-3](#).
 - Continue with [Step 14](#).
- Step 6** If you select Custom, the Actions configuration pane appears with a table listing match criteria and actions. Click **Add** to add an entry to this table, or select an existing entry, then click **Edit** to modify it. The configuration pane refreshes with the available configuration options.
- Step 7** In the Apply Building Block field, select one of the configuration building blocks for the type of optimization you want to configure, or leave blank to configure optimization without a building block:
- Bandwidth Optimization—Maximizes bandwidth for Web-based traffic.
 - Latency Optimization for Embedded Objects—Reduces the latency associated with embedded objects in Web-based traffic.
 - Latency Optimization for Embedded Images—Reduces the latency associated with embedded images in Web-based traffic.
 - Latency Optimization for Containers—Reduces the latency associated with Web containers.
- If you select one of the building blocks, the Rule Match configuration subset displays the configuration options with selections based on the building block chosen. You can accept the entries as they are or modify them.
- If you do not select a building block, additional configuration options appear depending on the features you enable.
- Step 8** In the Rule Match field, select an existing class map or click ***New*** to specify new match criteria:
- If you select an existing class map, you can view, modify, or duplicate the existing configuration. See [Shared Objects and Virtual Servers, page 4-6](#) for more information about modifying shared objects.
 - If you click ***New***, the screen refreshes so that you can enter new match criteria.
- Step 9** Configure match criteria using the information in [Table 4-15](#).

Table 4-15 Optimization Match Criteria Configuration

Field	Description
Name	Enter a unique name for this match criteria rule.
Match	Select the method to be used to evaluate multiple match statements when multiple match conditions exist: - Match Any—A match exists if at least one of the match conditions is satisfied. - Match All—A match exists only if all match conditions are satisfied.
Conditions	Click Add to add a new set of conditions or select an existing entry, then click Edit to modify it: - In the Type field, select the match condition to be used, then configure any condition-specific options using the information in Table 4-12. - Click OK to save your entries, or Cancel to exit this procedure without saving your entries.

Step 10 In the Actions field, select an existing action list to use for optimization or click ***New*** to create a new action list:

- If you select an existing action list, you can view, modify, or duplicate the existing configuration. See [Shared Objects and Virtual Servers, page 4-6](#) for more information about modifying shared objects.
- If you click ***New***, the screen refreshes so you can configure an action list.

Step 11 Configure the action list using the information in [Table 4-16](#).

Table 4-16 Optimization Action List Configuration Options

Field	Description
Action List Name	Enter a unique name for the action list. Valid entries are unquoted text strings with a maximum of 64 alphanumeric characters.
Enable Delta	Delta optimization dynamically updates client browser caches directly with content differences, or deltas, resulting in faster page downloads. Select this check box to enable delta optimization for the specified URLs. Clear this check box to disable this feature. If you are configuring optimization without a building block, additional options appear. Configure these options using the information in Table 4-17 .
Enable AppScope	AppScope runs on the Management Console of the optional Cisco AVS 3180A Management Station and measures end-to-end application performance. Select this check box to enable AppScope performance monitoring for use with the ACE appliance. Clear this check box to disable this feature. If you are configuring optimization without a building block, additional options appear. Configure these options using the information in Table 4-17 .
Fast Redirect	The Fast Redirect feature specifies that the ACE appliance is to intercept 302 responses from the origin server and make a second request on behalf of the client for the redirect URL, fetch it, and send it to the client. This feature applies only to redirects within the same domain. Select this check box to enable the fast redirect feature. Clear this check box to disable the fast redirect feature.

Table 4-16 Optimization Action List Configuration Options (continued)

Field	Description
FlashForward	The FlashForward feature reduces bandwidth usage and accelerates embedded object downloading by combining local object storage with dynamic renaming of embedded objects, thereby enforcing object freshness within the parent HTML page. Specify how the ACE appliance is to implement FlashForward: • N/A—This feature is not enabled. • FlashForward—FlashForward is to be enabled for the specified URLs and embedded objects are to be transformed. • FlashForward Object—FlashForward static caching is to be enabled for the objects that the corresponding URLs refer to, such as Cascading Style Sheets (CSS), JPEG, and GIF files. If you are configuring without a building block and select either FlashForward or FlashForward Object, an addition option appears. Configure this option using the information in Table 4-17.
FlashConnect	The FlashConnect feature reduces bandwidth usage and accelerates the downloading of objects that are embedded within HTML pages. FlashConnect dynamically renames embedded objects by adding a prefix and changing the hostname so that the objects appear to reside on different hosts. FlashConnect then has the browser open a separate connection to the origin server for each object and retrieve the objects in parallel instead of sequentially. Note If you enable this feature, you must configure DNS so that all requests for the rewritten object URLs are resolved back to the ACE appliance that rewrote them initially. Specify how the ACE appliance is to implement FlashConnect: • N/A—This feature is not enabled. • FlashConnect—FlashConnect is to be enabled for the specified URLs. • FlashConnect Object—FlashConnect is to be enabled for corresponding embedded object URLs.
Cache Dynamic	Select this check box to enable Adaptive Dynamic Caching for the specified URLs even if the expiration settings in the response indicate that the content is dynamic. The expiration of cache objects is controlled by the cache expiration settings based on time or server load. Clear this check box to disable this feature.
Cache Forward	Specify how the ACE appliance is to implement cache forwarding: • N/A—This feature is not enabled. • With Wait—Cache forwarding is enabled with the wait option for the specified URLs. If the object has expired but the maximum cache TTL time period has not yet expired, the ACE appliance sends a request to the origin server for the object. Users requesting this page continue to receive content from the cache during this time but must wait for the object to be updated before their request is satisfied. When the fresh object is returned, it is sent to the requesting user and the cache is updated. • Without Wait—Cache forwarding is enabled without the wait option.
Dynamic Etag	This feature enables the acceleration of embedded objects not able to be cached, which results in improved application response time. When enabled, this feature eliminates the need for users to download objects not able to be cached on each request. Select this check box to indicate that the ACE appliance is to implement just-in-time object acceleration for embedded objects not able to be cached. Clear this check box to disable this feature.

Table 4-16 Optimization Action List Configuration Options (continued)

Field	Description
Meta Refresh	The Meta Refresh feature enables the ACE appliance to automatically and transparently convert HTML META tag redirections into more efficient HTTP header-based redirections. When enabled, this feature eliminates the need for unnecessary freshness validation requests and results in significantly faster page response time. Select this check box to enable the smart URL redirection on the ACE appliance. Clear this check box to disable this feature.
XSLT Merge	Select this check box to indicate that the ACE appliance is to apply XSL style sheet transformations to an XML source document and return the resulting HTML document to the requestor. The ACE appliance applies other optimizations after the XML is transformed, but before the result is returned to the requestor. Clear this check box to disable this feature. If you are configuring optimization without a building block, additional options appear. Configure these options using the information in Table 4-17.
Image Type	Image optimization controls how the ACE appliance compresses how JPEG and PNG images. Image optimization is not applied to small images, such as thumbnails, or when optimization reduces the file size by less than 10 percent. Image optimization is not intended for images with many high-frequency components that do not compress well. Specify how the ACE appliance is to handle image optimization: • N/A—This feature is not enabled. • Standard—The ACE appliance is to perform standard image optimization and smooth the image, if needed, to reduce noise. • Advanced—The ACE is to override standard settings and control individual optimization options. If you select this option and are configuring optimization without a building block, additional options appear. Configure these options using the information in Table 4-17.

Table 4-16 Optimization Action List Configuration Options (continued)

Field	Description
URL Maps	URL mapping enables the ACE appliance to alter URLs and other content in the data stream between an origin server and a client browser. - In the URL Maps table, click Add to add a new URL mapping, or select an existing mapping, then click Edit to modify it. The table refreshes with editable fields for your entries. - In the URL scope field, select the portion of the URL that is to be remapped: - All—URLs are to be altered, regardless of their locations. - Content—The content is to be altered, not just that which appears in URLs. - Cookie—The domain section of cookies are to be altered. - Header—URLs only within the Location response-header field are to be altered. - HTML—URLs only within the URL attribute of META HTTP-EQUIV tags and within the SRC attribute of the HTML tags BASE, HREF, IMG, LINK, SCRIPT, and STYLE are to be altered. - In the Replacement Directive field, indicate how the URL is to be altered: - Host—The host portion of the URL that is specified in the Source field is to be replaced with the string specified in the Destination field. - Pattern—The portion of the input stream specified in the Source field is to be replaced with the string specified in the Destination field. - Port—The port of the URL that is specified in the Source field is to be replaced with the port specified in the Destination field. Valid entries are integers from 0 to 65535. - Protocol—The URL protocol HTTP is to be replaced with HTTPS or HTTPS is to be replaced with HTTP. - In the Source field, enter the string or value that is to be replaced: - For Host replacements, enter the host portion that is to be replaced. - For Pattern replacements, enter a regular expression that defines subexpressions within the input stream that are to be replaced. - For Port replacements, enter the port number that is to be replaced. - For Protocol replacement, enter either HTTP or HTTPS as the protocol to be replaced. - In the Destination field, enter the string or value that is to replace the entry in the Source field: - For Host replacements, enter the new host string. Valid entries include a maximum of 64 alphanumeric characters. - For Pattern replacements, enter the pattern that is to replace the existing pattern. Valid entries include a maximum of 64 alphanumeric characters. For more information on Pattern replacements, see Configuring Pattern Replacements, page 12-10. - For Port replacements, enter the port number that is to replace the existing port number. Valid entries are integers from 0 to 65535. - For Protocol replacements, enter HTTP or HTTPS as the protocol to replace the existing protocol. - Click OK to save your entries and to return to the URL Maps table. Click Cancel to exit this procedure without saving your entries and to return to the URL Maps table.

- Step 12** If you are configuring optimization without a building block, additional options appear when you enable specific features. Configure the additional options using the information in [Table 4-17](#).

Table 4-17 Application Acceleration and Optimization Additional Configuration Options

Field	Description
Response Codes to Ignore	Enter a comma-separated list of HTTP response codes for which the response body must not be read. For example, an entry of 302 indicates that the ACE is to ignore the response body of a 302 (redirect) response from the origin server. Valid entries are unquoted text strings with a maximum of 64 alphanumeric characters.
Enable Delta Options	
Max for POST Data to Scan for Logging (kBytes)	Enter the maximum number of kilobytes of POST data the ACE is to scan for parameters for the purpose of logging transaction parameters in the statistics log. Valid entries are 0 to 1000 KB.
Specify Base File Anonymous Level	Information that is common to a large set of users is generally not confidential or user-specific. Conversely, information that is unique to a specific user or a small set of users is generally confidential or user-specific. The anonymous base file feature enables the ACE to create and deliver condensed base files that contain only information that is common to a large set of users. No information unique to a particular user, or across a very small subset of users, is included in anonymous base files. Enter the value for base file anonymity for the all-user condensation method. Valid entries are integers from 0 to 50; the default value of 0 disables the base file anonymity feature.
Canonical URL Expressions	The ACE uses the canonical URL feature to eliminate the “?” and any characters that follow to identify the general part of the URL. This general URL is then used to create the base file. In this way, the ACE maps multiple URLs to a single canonical URL. Enter a comma-separated list of parameter expander functions as defined in Table 12-4 to identify the URLs to associate with this parameter map. Valid entries are unquoted text strings with a maximum of 255 alphanumeric characters.
Enable Cacheable Content Optimization	This feature allows the ACE to detect content that can be cached and perform delta optimization on it. Select the check box to enable delta optimization of content that can be cached. Clear the check box to disable this feature.
Enable Delta Optimization on First Visit to Web Page	Select the check box to enable condensation on the first visit to a Web page. Clear the check box to disable this feature.
Minimum page size for Delta Optimization (bytes)	Enter the minimum page size, in bytes, that can be condensed. Valid entries are integers from 1 to 250000 bytes.
Maximum page size for Delta Optimization (bytes)	Enter the maximum page size, in bytes, that can be condensed. Valid entries are integers from 1 to 250000 bytes.
Set Default Client Script	Indicate the scripting language that the ACE is to recognize on condensed content pages: • N/A—Indicates that this option is not configured. • Javascript—Indicates that the default scripting language is JavaScript. • Visual Basic Script—Indicates that the default scripting language is Visual Basic.

Table 4-17 Application Acceleration and Optimization Additional Configuration Options (continued)

Field	Description
Exclude Iframes from Delta Optimization	Select the check box to indicate that delta optimization is not to be applied to IFrames (inline frames). Clear the check box to indicate that delta optimization is to be applied to IFrames.
Exclude Non-ASCII Data from Delta Optimization	Select the check box to indicate that delta optimization is not to be applied to non-ASCII data. Clear the check box to indicate that delta optimization is to be applied to non-ASCII data.
Exclude JavaScripts from Delta Optimization	Select the check box to indicate that delta optimization is not to be applied to JavaScript. Clear the check box to indicate that delta optimization is to be applied to JavaScript.
MIME Types to Exclude from Delta Optimization	1. In the first field, enter a comma-separated list of the MIME (Multipurpose Internet Mail Extension) type messages that are not to have delta optimization applied, such as image/Jpeg, text/html, application/msword, or audio/mpeg. See Supported MIME Types, page 7-21 for a list of supported MIME types. 2. Click Add to add the entry to the list box on the right. You can position the entries in the list box by using the Up and Down buttons.
Remove HTML META Elements from Documents	Select the check box to indicate that HTML META elements are to be removed from documents to prevent them from being condensed. Clear the check box to indicate that HTML META elements are not to be removed from documents.
Rebase Delta Optimization Threshold (%)	Enter the delta threshold, expressed as a percent, when rebasing is to be triggered. This entry represents the size of a page delta relative to total page size, expressed as a percent. This entry triggers rebasing when the delta response size exceeds the threshold as a percentage of base file size. Valid entries are 0 to 10000 percent.
Rebase FlashForward Threshold (%)	Enter the threshold, expressed as a percent, when rebasing is to be triggered based on the percent of FlashForwarded URLs in the response. This entry triggers rebasing when the difference between the percentages of FlashForwarded URLs in the delta response and the base file exceeds the threshold. Valid entries are 0 to 10000 percent.
Rebase History Size (pages)	Enter the number of pages to be stored before the ACE resets all rebase control parameters to zero and starts over. This option prevents the base file from becoming too rigid. Valid entries are 10 to 2147483647.
Rebase Modify Cool-off Period (seconds)	Enter the number of seconds after the last modification before performing a rebase. Valid entries are 1 to 14400 seconds (4 hours).
Rebase Reset Period (seconds)	Enter the period of time, in seconds, for performing a meta data refresh. Valid entries are 1 to 900 seconds (15 minutes).
UTF-8 Character Set Threshold	The UTF-8 (8-bit Unicode Transformation Format) character set is an international standard that allows Web pages to display non-ASCII or non-English multibyte characters. It can represent any universal character in the Unicode standard and is backwards compatible with ASCII. Enter the number of UTF-8 characters that need to appear on a page to constitute a UTF-8 character set page. Valid entries are integers from 1 to 1,000,000.

Table 4-17 Application Acceleration and Optimization Additional Configuration Options (continued)

Field	Description
Specify Delta Optimization Mode	Select the method by which delta optimization is to be implemented: • N/A—Indicates that a delta optimization mode is not configured. • Enable all-user mode for delta optimization—Indicates that the ACE is to generate the delta against a single base file that is shared by all users of the URL. This option is usable in most cases if the structure of a page is common across all users, and the disk space overhead is minimal. • Enable the per-user mode for delta optimization—Indicates that the ACE is to generate the delta against a base file that is created specifically for that user. This option is useful when page contents, including layout elements, are different for each user, and delivers the highest level of condensation. However, this increases disk space requirements because a copy of the base page that is delivered to each user is cached. This option is useful when privacy is required because base pages are not shared among users.
Enable Appscope Options	
Appscope Optimize Rate (%)	Enter the percentage of all requests or sessions to be sampled for performance with acceleration (or optimization) applied. All applicable optimizations for the class will be performed. Valid entries are from 0 to 100 percent, with a default of 10 percent. The sum of this value and the value entered in the Passthru Rate Percent field must not exceed 100.
Appscope Passthrough Rate (%)	Enter the percentage of all requests or sessions to be sampled for performance without optimization. No optimizations for the class will be performed. Valid entries are from 0 to 100, with a default of 10 percent. The sum of this value and the value entered in the Optimize Rate Percent field must not exceed 100.
Max Number for Parameter Summary Log (bytes)	Enter the maximum number of bytes that are to be logged for each parameter value in the parameter summary of a transaction log entry in the statistics log. If a parameter value exceeds this limit, it is truncated at the specified limit. Valid entries are 0 to 10,000 bytes.
Specify String for Grouping Requests	Enter the string the ACE is to use to sort requests for AppScope reporting. The string can contain a URL regular expression that defines a set of URLs in which URLs that differ only by their query parameters are to be treated as separate URLs in AppScope reports. For example, to define a string that is used to identify the URLs <code>http://server/catalog.asp?region=asia</code> and <code>http://server/catalog.asp?region=america</code> as two separate reporting categories, you would enter <code>http_query_param(region)</code>. Valid entries contain 1 to 255 characters and can contain the parameter expander functions listed in Table 12-4.
FlashConnect Enabled Option	
Hosts Limit for FlashConnect	FlashConnect dynamically renames embedded objects by adding a prefix and changing the hostname so that the objects appear to reside on different hosts. FlashConnect then has the browser open a separate connection to the origin server for each object and retrieve the objects in parallel instead of sequentially. Enter the maximum number of artificial hosts that FlashConnect can create for retrieving embedded objects. Valid entries are integers from 0 to 99.
XSLT Merge Options	
Enable XSLT Merge Debug	Select the check box to enable the XSLT merge debug function. Clear the check box to disable the XSLT merge debug function.

Table 4-17 **Application Acceleration and Optimization Additional Configuration Options (continued)**

Field	Description
Specify XSLT Stylesheet for PreTransform	Enter the URL of an XSLT style sheet to indicate that the ACE is to perform a pretransformation of the style sheet.
Specify XSLT Stylesheet for XSLT Merge	Enter the URL of an XSLT style sheet to force the use of this style sheet, regardless of any XSL specified in the XML source file.
Image Type - Advanced Options	
Smooth Transform of Image	Select the check box to indicate that the ACE is to apply a smoothing transformation to images, if needed. Clear the check box to indicate that the ACE is not to apply a smoothing transformation to images.
Ignore Thumbnail Images	Select the check box to indicate that the ACE is to ignore small thumbnail images without transforming them in any way. Clear the check box to indicate that the ACE is not to ignore thumbnail images.
Progressive Rendering of Image	Select the check box to indicate that the ACE is to transform images so that they are rendered progressively by the browser. When enabled, this feature results in slightly larger image sizes. Because images render progressively, this feature might not be useful in fast networking environments, such as LANs. Clear the check box to indicate that the ACE is not to transform images so that they are rendered progressively by the browser.
High Quality Transform of Image	Select the check box to indicate that the ACE is to apply higher quality transformation with less compression to images. When enabled, this option results in images that are larger than those compressed without this option, but they have less visual deterioration. Image size is smaller with this option than for uncompressed images. Clear the check box to indicate that the ACE is not to apply higher quality transformation to images.
Grayscale Transform of Image	Select the check box to indicate that the ACE is to optimize images by transforming JPEG and PNG images to grayscale images. Clear the check box to indicate that the ACE is not to optimize images by transforming JPEG and PNG images to grayscale images.

Step 13 When you finish configuring match criteria and actions, click:

- **OK** to save your entries and to return to the Rule Match and Actions table.
- **Cancel** to exit this procedure without saving your entries and to return to the Rule Match and Actions table.

Step 14 When you finish configuring virtual server properties, click:

- **Deploy Now** to save your entries. The ACE appliance validates the action list configuration and deploys it.
- **Cancel** to exit this procedure without saving your entries and to return to the Virtual Servers table.
- **Deploy Later** to save your entries and apply the configuration at a later time.

Related Topics

- [Optimization Traffic Policies and Typical Configuration Flow, page 12-2](#)
- [Configuring Traffic Policies for HTTP Optimization, page 12-13](#)
- [Configuring Virtual Server Protocol Inspection, page 4-14](#)
- [Configuring Virtual Server Layer 7 Load Balancing, page 4-25](#)
- [Configuring Virtual Server Default Layer 7 Load Balancing, page 4-35](#)

Configuring Virtual Server NAT

Use this procedure to configure Name Address Translation (NAT) for virtual servers. The NAT configuration subset appears in the Advanced View only.

Assumptions

- A virtual server has been configured. See [Configuring Virtual Servers, page 4-2](#) for information on configuring a virtual server.
- A VLAN has been configured. See [Configuring VLAN Interfaces, page 9-2](#) for information on configuring a VLAN interface.
- At least one NAT pool has been configured on a VLAN interface. See [Configuring VLAN Interface NAT Pools, page 9-10](#) for information on configuring a NAT pool.

Procedure

-
Step 1	Select Config > Devices > context > Load Balancing > Virtual Servers . The Virtual Servers table appears.
Step 2	Select the virtual server you want to configure for NAT, then click Edit . The Virtual Server configuration screen appears.
Step 3	Click NAT . The NAT table appears.
Step 4	Click Add to add an entry, or select an existing entry, then click Edit to modify it.
Step 5	In the VLAN field, select the VLAN you want to use NAT. For more information about NAT, see Configuring VLAN Interface NAT Pools, page 9-10 .
Step 6	In the NAT Pool ID field, select the NAT pool that you want to associate with the selected VLAN.
Step 7	Click: • OK to save your entries and to return to the NAT table. The NAT table refreshes with the new entry. • Cancel to exit the procedure without saving your entries and to return to the NAT table.
Step 8	When you finish configuring virtual server properties, click: • Deploy Now to deploy this configuration on the ACE. • Cancel to exit this procedure without saving your entries and to return to the Virtual Servers table. • Deploy Later to save your entries and apply the configuration at a later time.
-

Related Topics

- [Configuring Virtual Servers, page 4-2](#)

- [Configuring Virtual Server Properties, page 4-8](#)
- [Configuring Virtual Server SSL Termination, page 4-12](#)
- [Configuring Virtual Server Protocol Inspection, page 4-14](#)
- [Configuring Virtual Server Layer 7 Load Balancing, page 4-25](#)
- [Configuring Virtual Server Default Layer 7 Load Balancing, page 4-35](#)

Managing Virtual Servers

The Virtual Servers table (**Config > Operations > Virtual Servers**) provides the following information by default for each virtual server:

- Server name, sorted by virtual context
- Admin state
- Operational state



Note

This column is populated for ACE 4710 appliances running image A3(1.0) and later. Clicking on the value in this column (irrespective of ACE version) will display detailed information about the Virtual Server in a popup.

- Number of active connections



Note

This column is populated for ACE 4710 appliances running image A3(1.0) and later. For ACE devices, the Active Connections column will display N/A for older versions of the ACE appliance and module.

- VIP address
- Configured port
- VLANs
- Associated server farms
- Device
- High availability

You can activate or suspend virtual servers from this table and obtain additional information about the state of the virtual server.

The following options are available from the Virtual Servers table:

- [Deploying Virtual Servers, page 4-49](#)
- [Viewing All Staged Virtual Servers, page 4-49](#)
- [Modifying Deployed Virtual Servers, page 4-50](#)
- [Modifying Staged Virtual Servers, page 4-50](#)
- [Viewing Virtual Servers by Context, page 4-51](#)
- [Activating Virtual Servers, page 4-51](#)
- [Suspending Virtual Servers, page 4-52](#)

- [Managing GSS VIP Answers, page 4-53](#)
- [Activating and Suspending DNS Rules Governing GSS Load Balancing, page 4-54](#)
- [Viewing Detailed Virtual Server Information, page 4-54](#)
- [Viewing Virtual Servers, page 4-55](#)
- [Understanding CLI Commands Sent from Virtual Server Table, page 4-56](#)

Deploying Virtual Servers

You can deploy virtual servers on your network at times that are convenient and appropriate for your environment. For example, if your site prefers to make changes to the network during a specific time each night, you can modify and save virtual server configurations during the day and then deploy them when appropriate.

Use this procedure to deploy staged virtual servers on your network.

Procedure

-
Step 1	Select Config > Deploy . The Staged Objects table appears.
Step 2	Select the virtual server you want to deploy on your network, then click Deploy . The virtual server is deployed and the table refreshes with updated information.
-

Related Topics

- [Configuring Virtual Servers, page 4-2](#)
- [Viewing All Staged Virtual Servers, page 4-49](#)
- [Modifying Staged Virtual Servers, page 4-50](#)

Viewing All Staged Virtual Servers

The ANM allows you to deploy configured virtual servers when it is appropriate for your environment. To view all objects that have been configured but have not yet been deployed on your network, select **Config > Deploy**. The Staged Objects table appears listing the:

- Virtual server name
- Device ID and virtual context
- Time the virtual server was created
- User who last modified the object
- Time the object was last updated

Deployment status is also available in the Virtual Servers table (**Config > Devices > context > Load Balancing > Virtual Servers**). Virtual servers with configurations that have not been deployed appear with the status Not Deployed in the Configured State column.

Related Topics

- [Configuring Virtual Servers, page 4-2](#)

- [Deploying Virtual Servers, page 4-49](#)
- [Modifying Staged Virtual Servers, page 4-50](#)
- [Modifying Deployed Virtual Servers, page 4-50](#)

Modifying Deployed Virtual Servers

Use this procedure to modify the configuration of a deployed virtual server.

Procedure

-
Step 1	Select Config > Devices > context > Load Balancing > Virtual Servers . The Virtual Servers table appears.
Step 2	Select the virtual server you want to modify, then click Edit . The Virtual Server configuration screen appears.
Step 3	Modify the virtual server's configuration as desired. See Table 4-1 for virtual server configuration options.
Step 4	When you are done modifying the configuration, click: • Deploy Now to immediately deploy this configuration. • Cancel to exit this procedure without saving your entries and to return to the Virtual Servers table.
-

Related Topics

- [Managing Virtual Servers, page 4-48](#)
- [Viewing All Staged Virtual Servers, page 4-49](#)
- [Activating Virtual Servers, page 4-51](#)
- [Suspending Virtual Servers, page 4-52](#)

Modifying Staged Virtual Servers

Use this procedure to modify the configuration of a staged virtual server.

Procedure

-
Step 1	Select Config > Deploy . The Staged Objects table appears, listing those virtual servers that have not yet been deployed in the network.
Step 2	Select the virtual server you want to modify, then click Edit . The virtual server configuration screen appears.
Step 3	Modify the virtual server's configuration as desired. See Table 4-1 for virtual server configuration options.
Step 4	When you are done modifying the configuration, click: • Deploy Now to immediately deploy this configuration. • Cancel to exit this procedure without saving your entries and to return to the Virtual Servers table.

- **Deploy Later** to save your entries and apply this configuration at a later time.
-

Related Topics

- [Deploying Virtual Servers, page 4-49](#)
- [Viewing All Staged Virtual Servers, page 4-49](#)
- [Viewing Virtual Servers by Context, page 4-51](#)

Viewing Virtual Servers by Context

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

Procedure

-
- Step 1** Select **Config > Devices**. The device tree appears.
- Step 2** Select the context associated with the virtual servers you want to view, then select **Load Balancing > Virtual Servers**. The Virtual Servers table appears with the following information:
- Virtual server name
 - Configured state, such as Inservice or Out of service
 - VIP address
 - Port
 - Associated VLANs
 - Associated server farms
 - The owner, and context in which the virtual server was created
-

Related Topics

- [Configuring Virtual Servers, page 4-2](#)
- [Managing Virtual Servers, page 4-48](#)

Activating Virtual Servers

Use this procedure to activate a virtual server.

**Note**

A missing operation or Admin state on a CSM or CSS device most likely means that the community string was not enabled on those devices. If the community string is not enabled on a CSM or CSS device, and any kind of operation is performed on those devices, it will not succeed, and ANM will not provide any kind of indication.

- For CSM devices, you must enable the community string of the Catalyst 6K chassis.
- For CSS devices, you must enable the community string of the CSS device itself.

Procedure

-
- Step 1** Select **Config > Operations > Virtual Servers**. The Virtual Servers table appears.
- Step 2** Select the virtual server that you want to activate, then click **Activate**. The server is activated and the screen refreshes with updated information in the Configured State column.
-

Related Topics

- [Managing Virtual Servers, page 4-48](#)
- [Viewing Virtual Servers, page 4-55](#)
- [Suspending Virtual Servers, page 4-52](#)

Suspending Virtual Servers

Use this procedure to suspend a virtual server.



Note

A missing operation or Admin state on a CSM or CSS device most likely means that the community string was not enabled on those devices. If the community string is not enabled on a CSM or CSS device, and any kind of operation is performed on those devices, it will not succeed, and ANM will not provide any kind of indication.

- For CSM devices, you must enable the community string of the Catalyst 6K chassis.
- For CSS devices, you must enable the community string of the CSS device itself.

Procedure

-
- Step 1** Select **Config > Operations > Virtual Servers**. The Virtual Servers table appears.
- Step 2** Select the virtual server that you want to suspend, then click **Suspend**. The server is taken out of service and the screen refreshes with updated information in the Configured State column.
-

Related Topics

- [Managing Virtual Servers, page 4-48](#)
- [Viewing Virtual Servers, page 4-55](#)
- [Activating Virtual Servers, page 4-51](#)

Managing GSS VIP Answers

In a GSS network, the term answers refers to resources that respond to content queries. When you create an answer using the primary Global Site Selector Manager (PGSSM), you are simply identifying a resource on your GSS network to which queries can be directed and that can provide your user's D-proxy with the address of a valid host to serve their request.

Virtual IP (VIP) addresses associated with an SLB such as the Cisco CSS, Cisco CSM, Cisco IOS-compliant SLB, LocalDirector, or a Web server are types of answers that are specified in the ANM UI in the GSS VIP Answers table found in ANM under **Configuration > Operations**. Use this procedure to poll, activate or suspend GSS VIP answers.

Assumption

You have established GSS VIP answers using the PGSSM.

Procedure

-
- Step 1** Select **Config > Operations > GSS VIP Answers**. The GSS Answers table appears.
- Step 2** Click the checkbox(es) to the left of the servers you want to poll, activate or suspend.
- Step 3** Click:
- **Active/Suspended** hyperlink to view the VIP answer details across the GSS node(s). A popup window appears listing all nodes associated with the VIP, operational state, hit count, and timestamp for each node.
 - **Poll Now** to query the chosen resource to verify it is still active.



Note

If you click **Poll Now** immediately after you click **Activate** or **Suspend**, you might not get the VIP answer operational status on the PGSSM that reflects your most recent configuration. It might be necessary to click Poll Now 2 or 3 times in succession to get an accurate result.

Apart from this, the ability of ANM to update the VIP answer operational status and statistics accurately in detailed GSS statistics window might depend on the polling interval that has been configured on the GSS. The polling interval can be configured directly on the GSS device. (The default is 5 minutes.) Therefore, it can take 5 minutes or more, depending on the interval, for the ANM server to show an accurate result.

- **Activate** to reactivate a GSS answer.
- **Suspend** to temporarily stop the GSS from using an associated answer.

If you clicked **Activate** or **Suspend**, a dialog box prompts for a Reason. Acceptable text consists of any characters or nothing at all.

- Step 4** Click:
- **Deploy Now** to complete Activation or Suspension.
 - **Cancel** to cancel the Activation or Suspension operation.
-

Related Topics

- [Load Balancing Overview, page 4-1](#)

- [Activating and Suspending DNS Rules Governing GSS Load Balancing, page 4-54](#)

Activating and Suspending DNS Rules Governing GSS Load Balancing

The DNS rules table in **Configuration > Operations** navigation tree specifies actions for the GSS to take when it receives a request from a known source (a member of a source address list) for a known hosted domain (a member of a domain list).

The DNS rule specifies which response (answer) is given to the requesting user's local DNS host (D-proxy) and how that answer is chosen. One of a variety of balance methods is used to determine the best response to the request, based on the status and load of the GSS host devices.

Use this procedure to activate or suspend DNS rules associated with your GSS VIP answers table.

Assumption

You have established GSS VIP answers and DNS rules using the PGSSM.

Procedure

-
- Step 1** Select **Config > Operations > DNS Rules**. The DNS Rules table appears.
 - Step 2** Click the checkbox(es) to the left of the servers you want to activate or suspend.
 - Step 3** Click the **Activate** or **Suspend** button. A dialog box prompts for a Reason. Acceptable text consists of any characters or none at all.
 - Step 4** Click:
 - **Deploy Now** to complete Activation or Suspension.
 - **Cancel** to cancel the Activation or Suspension operation.
-

Related Topics

- [Load Balancing Overview, page 4-1](#)
- [Managing GSS VIP Answers, page 4-53](#)

Viewing Detailed Virtual Server Information

Use this procedure to view detailed information about the state of a virtual server.

Procedure

-
- Step 1** Select **Config > Operations > Virtual Servers**. The Virtual Servers table appears.
 - Step 2** Select the virtual server whose configuration details you want to view. Click the hyperlinked entry for that virtual server that appears in the Operational State column. The Details window appears with the following information:
 - Current operational status
 - Description, if one was entered
 - Configured interfaces, such as VLANs

- Configured service policies including:
 - Configured class maps, detailed by type (such as load balancing or inspection)
 - States of configured options, indicated by word (**ACTIVE**, **DISABLED**, **OUTOFSERVICE**) and color (green, orange/yellow, and red)
 - Associated policy maps with details on their type and action (L7 loadbalance, serverfarm)
 - Statistics regarding connections and counts

Step 3 Click **Refresh** to view updated information or **Cancel** to return to the Virtual Servers table.

Related Topics

- [Configuring Virtual Servers, page 4-2](#)
- [Managing Virtual Servers, page 4-48](#)

Viewing Virtual Servers

To view all virtual servers, select **Config > Operations > Virtual Servers**. The Virtual Servers table appears with the following information for each server:

- Server name, sorted by virtual context
- Admin state
- Operational state



Note This column is populated for ACE 4710 appliances running image A3(1.0) and later. Clicking on the value in this column (irrespective of ACE version) will display detailed information about the Virtual Server in a popup.

- Number of active connections



Note This column is populated for ACE 4710 appliances running image A3(1.0) and later. For ACE devices, the Active Connections column will display N/A for older versions of the ACE appliance and module.

- VIP address
- Configured port
- VLANs
- Associated server farms
- Device
- High availability

You can activate or suspend virtual servers from this table and obtain additional information about the state of the virtual server.

Related Topics

- [Activating Virtual Servers, page 4-51](#)
- [Suspending Virtual Servers, page 4-52](#)
- [Viewing Detailed Virtual Server Information, page 4-54](#)

Understanding CLI Commands Sent from Virtual Server Table

Table 4-18 displays the CLI commands dispatched to the device for a given Virtual Servers table option, and is sorted by device.

Table 4-18 CLI Commands Deployed from Real Servers Table

Command	Sample CLI Sent
ACE Modules and Appliances	
Virtual Server Activate	<pre>policy-map multi-match int25 class VIP3 loadbalance vip inservice</pre>
Virtual Server Suspend	<pre>policy-map multi-match int25 class VIP3 no loadbalance vip inservice</pre>
CSMs	
Virtual Server Activate	<pre>vserver APP1 inservice</pre>
Virtual Server Suspend	<pre>vserver APP1 no inservice</pre>
CSS Devices	
Virtual Server Activate	<pre>owner hm content LB active</pre>
Virtual Server Suspend	<pre>owner hm content LB suspend</pre>



Draft - CISCO CONFIDENTIAL

CHAPTER 5

Configuring Real Servers and Server Farms

Revised Date: 3/25/09

This section provides an overview of server load balancing and procedures for configuring real servers and server farms for load balancing on an ACE.

Topics include:

- [Server Load Balancing Overview, page 5-1](#)
- [Configuring Real Servers, page 5-4](#)
- [Configuring Server Farms, page 5-12](#)
- [Health Monitoring, page 5-23](#)
- [Configuring Health Monitoring for Real Servers, page 5-25](#)
- [Managing Real Servers, page 5-6](#)

Server Load Balancing Overview

Server load balancing (SLB) is the process of deciding to which server a load-balancing device should send a client request for service. For example, a client request can consist of an HTTP GET for a Web page or an FTP GET to download a file. The job of the load balancer is to select the server that can successfully fulfill the client request and do so in the shortest amount of time without overloading either the server or the server farm as a whole.

Depending on the load-balancing algorithm or predictor that you configure, the ACE performs a series of checks and calculations to determine the server that can best service each client request. The ACE bases server selection on several factors, including the server with the fewest connections with respect to load, source or destination address, cookies, URLs, or HTTP headers.

to load, source or destination address, cookies, URLs, or HTTP headers.

The ANM allows you to configure load balancing using:

- Virtual servers—See [Configuring Virtual Servers, page 4-2](#).
- Real servers—See [Configuring Real Servers, page 5-4](#).
- Server farms—See [Configuring Server Farms, page 5-12](#).
- Sticky groups—See [Configuring Sticky Groups, page 6-7](#).
- Parameter maps—See [Configuring Parameter Maps, page 7-1](#).

Draft - CISCO CONFIDENTIAL

For information about SLB as configured and performed by the ACE, see:

- [Configuring Virtual Servers, page 4-2](#)
- [Load-Balancing Predictors, page 5-2](#)
- [Real Servers, page 5-3](#)
- [Server Farms, page 5-3](#)
- [Health Monitoring, page 5-23](#)
- [TCL Scripts, page 5-24](#)
- [Configuring Stickiness, page 6-1](#)

Load-Balancing Predictors

The ACE uses the following predictors to select the best server to satisfy a client request:

- **Roundrobin**—Selects the next server in the list of real servers based on server weight (weighted roundrobin). Servers with a higher weight value receive a higher percentage of the connections. This is the default predictor.
- **Leastconns**—Selects the server with the fewest number of active connections based on server weight. For the least connection predictor, you can configure a slow-start mechanism to avoid sending a high rate of new connections to servers that you have just put into service.
- **Hash_url**—Selects the server using a hash value based on the requested URL. You can specify a beginning pattern and an ending pattern to match in the URL. Use this predictor method to load-balance cache servers. Cache servers perform better with the URL hash method because you can divide the contents of the caches evenly if the traffic is random enough. In a redundant configuration, the cache servers continue to work even if the active ACE switches over to the standby ACE. For information about configuring redundancy, see [Configuring High Availability, page 10-1](#).
- **Hash_address**—Selects the server using a hash value based on either the source or destination IP address, or both. Use these predictors for firewall load balancing (FWLB).



Note FWLB allows you to scale firewall protection by distributing traffic across multiple firewalls on a per-connection basis. All packets belonging to a particular connection must go through the same firewall. The firewall then allows or denies transmission of individual packets across its interfaces. For more information about configuring FWLB on the ACE, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

- **Hash_cookie**—Selects the server using a hash value based on a cookie name.
- **Hash_header**—Selects the server using a hash value based on the HTTP header name.
- **Least Loaded**—Selects the server with the lowest load as determined by information from SNMP probes.
- **Least Bandwidth**—Selects the server with the least amount of network traffic or a specified sampling period. Use this type for server farms with heavy traffic, such as downloading video clips.
- **Response**—Selects the server with the lowest response time for a specific response-time measurement.

**Note**

The different hash predictor methods do not recognize the weight value that you configure for real servers. The ACE uses the weight that you assign to real servers only in the round-robin and least-connections predictor methods.

Related Topic

[Configuring the Predictor Method for Server Farms, page 5-16](#)

Real Servers

To provide services to clients, you configure real servers on the ACE. Real servers are dedicated physical servers that you typically configure in groups called server farms. These servers provide client services such as HTTP or XML content, Web site hosting, FTP file uploads or downloads, redirection for Web pages that have moved to another location, and so on. You identify real servers with names and characterize them with IP addresses, connection limits, and weight values. The ACE also allows you to configure backup servers in case a server is taken out of service for any reason.

After you create and name a real server on the ACE, you can configure several parameters, including connection limits, health probes, and weight. You can assign a weight to each real server based on its relative importance to other servers in the server farm. The ACE uses the server weight value for the weighted round-robin and the least-connections load-balancing predictors. The load-balancing predictor algorithms (for example, roundrobin, least connections, and so on) determine the servers to which the ACE sends connection requests. For a listing and brief description of the load-balancing predictors, see [Load-Balancing Predictors, page 5-2](#).

The ACE uses traffic classification maps (class maps) within policy maps to identify traffic that meets defined criteria and to apply specific actions to that traffic based on the SLB configuration.

If a primary real server fails, the ACE takes that server out of service and no longer includes it in load-balancing decisions. If you configured a backup server for the real server that failed, the ACE redirects the primary real server connections to the backup server. For information about configuring a backup server, see the [Configuring Virtual Server Layer 7 Load Balancing, page 4-25](#).

The ACE can take a real server out of service for the following reasons:

- Probe failure
- ARP timeout
- Specifying Out of Service as the administrative state of a real server
- Specifying Inservice Standby as the administrative state of a real server

The Out of Service and Inservice Standby selections both provide the graceful shutdown of a server.

Related Topics

- [Configuring Real Servers, page 5-4](#)
- [Configuring Health Monitoring for Real Servers, page 5-25](#)

Server Farms

Typically, in data centers, servers are organized into related groups called *server farms*. Servers within server farms often contain identical content (referred to as mirrored content) so that if one server becomes inoperative, another server can take its place immediately. Also, having mirrored content

Draft - CISCO CONFIDENTIAL

allows several servers to share the load of increased demand during important local or international events, such as the Olympic Games. This phenomenon of a sudden large demand for content is called a *flash crowd*.

After you create and name a server farm, you can add existing real servers to it and configure other server farm parameters, such as the load-balancing predictor, server weight, backup server, health probe, and so on. For a listing and brief description of load-balancing predictors, see [Load-Balancing Predictors](#), page 5-2.

Related Topic

[Configuring Server Farms](#), page 5-12

Configuring Real Servers

Real servers are dedicated physical servers that are typically configured in groups called server farms. These servers provide services to clients, such as HTTP or XML content, streaming media (video or audio), TFTP or FTP services, and so on. When configuring real servers, you assign names to them and specify IP addresses, connection limits, and weight values.

The ACE uses traffic classification maps (class maps) within policy maps to filter specified traffic and to apply specific actions to that traffic based on the load-balancing configuration. A load-balancing predictor algorithm (such as round-robin or least connections) determines the servers to which the ACE sends connection requests. For information about configuring class maps, see [Configuring Virtual Context Class Maps](#), page 11-6.

Use this procedure to configure load balancing on real servers.

Procedure

-
- Step 1** Select **Config > Devices > context > Load Balancing > Real Servers**. The Real Servers table appears.
- Step 2** Click **Add** to add a new real server, or select a real server you want to modify, then click **Edit**. The Real Servers configuration screen appears.
- Step 3** Configure the server using the information in [Table 5-1](#).

Table 5-1 Real Server Attributes

Field	Description
Name	Either accept the automatically incremented value in this field, or enter a unique name for this server. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters.
Type	Select the type of server: - Host—The real server provides content and services to clients. - Redirect—The server redirects traffic to a new location.
Description	Enter a brief description for this real server. Valid entries are strings of up to 240 characters. Spaces and special characters are allowed.
IP Address	This field appears for only real servers specified as hosts. Enter a unique IP address in dotted-decimal format (such as 192.168.11.1). The IP address cannot be an existing virtual IP address (VIP).

Table 5-1 *Real Server Attributes (continued)*

Field	Description
Max Connections	Enter the maximum number of active connections allowed on this server. When the number of connections exceeds this value, the ACE appliance stops sending connections to this server until the number of connections falls below the Min Connections value. Valid entries are integers from 2 to 4000000, and the default is 4000000.
Min Connections	Enter the minimum number of connections to be allowed on this server before the ACE appliance starts sending connections again after it has exceeded the Max Connections limit. This value must be less than or equal to the Max Connections value. By default, this value is equal to the Max Connections value. Valid entries are integers from 2 to 4000000.
Weight	This field appears only for real servers identified as hosts. Enter the weight to be assigned to this real server in a server farm. Valid entries are integers from 1 to 100, and the default is 8.
State	Select the state of this real server: • In Service—The real server is in service. • Out of Service—The real server is out of service.
Probes	This field appears only for real servers identified as hosts. In the Probes field, select the probes to use for health monitoring in the Available Items list, then click Add . The probes appear in the Selected Items list. To remove probes that you do not want to use for health monitoring, select them in the Selected Items list, then click Remove . The probes appear in the Available Items list.
Webhost Redirection	URL string used to redirect requests to another server. This field appears only for real servers identified as redirect servers. Enter the URL and port used to redirect requests to another server. Valid entries are in the form http://host.com:port where host is the name of the server and port is the port to be used. Valid host entries are unquoted text strings with no spaces and a maximum of 255 characters. Valid port numbers are from 1 to 65535. The relocation string supports the following special characters: • %h—Inserts the hostname from the request Host header • %p—Inserts the URL path string from the request
Redirection Code	This field appears only for real servers identified as redirect servers. Select the appropriate redirection code: • N/A—The webhost redirection code is not defined. • 301—The requested resource has been moved permanently. For future references to this resource, the client should use one of the returned URIs. • 302—The requested resource has been found, but has been moved temporarily to another location. For future references to this resource, the client should use the request URI because the resource may be moved to other locations from time to time.

Draft - CISCO CONFIDENTIAL**Table 5-1** **Real Server Attributes (continued)**

Field	Description
Rate Bandwidth	The bandwidth rate is the number of bytes per second and applies to the network traffic exchanged between the ACE and the real server in both directions. Specify the real server bandwidth limit in bytes per second. Valid entries are integers from 2 to 300000000. The default is 300000000.
Rate Connection	The connection rate is the number of connections per second received by the ACE and applies only to new connections destined to a real server. Specify the limit for connections per second. Valid entries are integers from 2 to 350000. The default is 350000.

Step 4 Click:

- **Deploy Now** to deploy this configuration.
- **Cancel** to exit the procedure without saving your entries and to return to the Real Servers table.
- **Next** to deploy your entries and to configure another real server.

Related Topics

- [Configuring Health Monitoring for Real Servers, page 5-25](#)
- [Configuring Server Farms, page 5-12](#)
- [Configuring Sticky Groups, page 6-7](#)

Managing Real Servers

The Real Servers table (**Config > Operations > Real Servers**) provides the following information by default for each server:

- Server name
- IP address
- Port
- Admin State (In Service, Out of Service, or In Service Standby)
- Operational state (See [Table 5-2](#) for descriptions of real server operational states.)
- Number of current connections
- Current server weight
- Associated server farm
- Associated virtual servers
- Device details
- Whether the server is part of a high availability pair

In the table, N/A indicates that either the information is not available from the database or that it is not being collected via SNMP. To identify any SNMP-related issues, select the real server's virtual context in the object selector. If there are problems with SNMP, SNMP status will appear in the upper right above the content pane.

The following options are available from the Real Servers table:

- [Activating Real Servers, page 5-7](#)
- [Suspending Real Servers, page 5-7](#)
- [Modifying Real Servers, page 5-8](#)
- [Viewing Real Servers, page 5-9](#)
- [Understanding CLI Commands Sent from Real Server Table, page 5-10](#)
- [Server Weight Ranges, page 5-12](#)

Activating Real Servers

Use this procedure to activate a real server.

Procedure

-
Step 1	Select Config > Operations > Real Servers . The Real Servers table appears.
Step 2	Select the servers that you want to activate, then click Activate . The Activate Server screen appears.
Step 3	In the Reason field, enter a reason for this action. You might enter a trouble ticket, an order ticket, or a user message. Do not enter a password in this field.
Step 4	Click: • OK to activate the server and to return to the Real Servers table. The server appears in the table with the status Inservice. • Cancel to exit this procedure without activating the server and to return to the Real Servers table.
-

Related Topics

- [Managing Real Servers, page 5-6](#)
- [Suspending Real Servers, page 5-7](#)
- [Viewing Real Servers, page 5-9](#)

Suspending Real Servers

Use this procedure to suspend a real server.

Procedure

-
Step 1	Select Config > Operations > Real Servers . The Real Servers table appears.
Step 2	Select the server that you want to suspend, then click Suspend . The Suspend Real Servers window appears.

Draft - CISCO CONFIDENTIAL

Step 3 In the Reason field, enter the reason for this action. You might enter a trouble ticket, an order ticket, or a user message. **Do not enter a password in this field.**

Step 4 Select one of the following from the **Suspend Real Servers Type** pulldown menu:

- Graceful
- Suspend
- Suspend and Clear Connections to clear the existing connections to this server as part of the shutdown process.

**Note**

Graceful suspend and suspend options vary by device type. For exact commands deployed by device type when these options are selected, see the [“Understanding CLI Commands Sent from Real Server Table”](#) section on page 5-10.

Step 5 Click:

- **Deploy Now** to suspend the server and to return to the Real Servers table. The server appears in the table with the status Out of Service.
- **Cancel** to exit this procedure without suspending the server and to return to the Real Servers table.

Related Topics

- [Managing Real Servers, page 5-6](#)
- [Activating Real Servers, page 5-7](#)
- [Viewing Real Servers, page 5-9](#)

Modifying Real Servers

Use this procedure to modify server weight and connection limits for real servers.

Procedure

Step 1 Select **Config > Operations > Real Servers**. The Real Servers table appears.

Step 2 Select the servers whose configuration you want to modify, then click **Change Weight** below the table to the right of **Activate** and **Suspend**. The **Change Weight Real Servers** window appears.

Step 3 Enter the following information for the selected server:

- Reason for change such as trouble ticket, order ticket or user message. **Do not enter a password in this field.**
- Weight (For allowable ranges for each device type, see [Table 5-4](#).)

Step 4 Click:

- **Deploy Now** to accept your entries and to return to the Real Servers table. The server appears in the table with the updated information.
- **Cancel** to exit this procedure without saving your entries and to return to the Real Servers table.

Related Topics

- [Managing Real Servers, page 5-6](#)
- [Activating Real Servers, page 5-7](#)
- [Viewing Real Servers, page 5-9](#)

Viewing Real Servers

To view all real servers, select **Config > Operations > Real Servers**. The Real Servers table displays the following information by default:

- Server name
- IP address
- Port
- Admin State (In Service, Out of Service, or In Service Standby)
- Operational state (See [Table 5-2](#) for descriptions of real server operational states.)
- Number of current connections
- Current server weight
- Associated server farm
- Associated virtual servers
- Device details
- Whether the server is part of a high availability pair

In the table, N/A indicates that either the information is not available from the database or that it is not being collected via SNMP. To identify any SNMP-related issues, select the real server's virtual context in the object selector. If there are problems with SNMP, SNMP status will appear in the upper right above the content pane.

Table 5-2 *Real Server Operational States*

State	Description
Failed	The server has failed and will not be retried for the amount of time specified by its retry timer.
Inband probe failed	The server has failed the inband Health Probe agent.
In service	The server is in use as a destination for server load balancing client connections.
Operation wait	The server is ready to become operational but is waiting for the associated redirect virtual server to be in service.
Out of service	The server is not in use by a server load balancer as a destination for client connections.
Probe failed	The server load-balancing probe to this server has failed. No new connections will be assigned to this server until a probe to this server succeeds.
Probe testing	The server has received a test probe from the server load balancer.
Ready to test	The server has failed and its retry timer has expired; test connections will begin flowing to it soon.

Draft - CISCO CONFIDENTIAL**Table 5-2 Real Server Operational States (continued)**

State	Description
Return code failed	The server has been disabled because it returned an HTTP code that matched a configured value.
Test wait	The server is ready to be tested. This state is applicable only when the server is used for HTTP redirect load balancing.
Testing	The server has failed and has been given another test connection. The success of this connection is not known.
Throttle: DFP	DFP has lowered the weight of the server to throttle level; no new connections will be assigned to the server until DFP raises its weight.
Throttle: max clients	The server has reached its maximum number of allowed clients.
Throttle: max connections	The server has reached its maximum number of connections and is no longer being given connections.
Unknown	The state of the server is not known.

Related Topics

- [Activating Real Servers, page 5-7](#)
- [Suspending Real Servers, page 5-7](#)
- [Modifying Real Servers, page 5-8](#)

Understanding CLI Commands Sent from Real Server Table

Table 5-3 displays the CLI commands dispatched to the device for a given Real Servers table option, and is sorted by device.

Table 5-3 CLI Commands Deployed from Real Servers Table

Command	Sample CLI Sent
ACE Modules and Appliances	
Real Server Activation	<pre>serverfarm host sf1 rserver rs1 80 inservice</pre>
Real Server Graceful Suspend	<pre>serverfarm host sf1 rserver rs1 80 inservice standby</pre>
Real Server Suspend	<pre>serverfarm host sf1 rserver rs1 80 no inservice</pre>
Real Server Suspend and Clear Connections	<pre>serverfarm host sf1 rserver rs1 80 no inservice clear conn rserver rs1 80 serverfarm sf1</pre>

Table 5-3 CLI Commands Deployed from Real Servers Table

Command	Sample CLI Sent
Real Server Change Weight	serverfarm host sf1 rserver rs1 80 weight 2
CSMs	
Real Server Activation	serverfarm host sf1 real 10.10.10.10 80 inservice
Real Server Graceful Suspend	serverfarm host sf1 real 10.10.10.10 80 weight 0
Real Server Suspend	serverfarm host sf1 real 10.10.10.10 80 no inservice
Real Server Suspend and Clear Connections	serverfarm host sf1 real 10.10.10.10 80 no inservice clear module contentSwitchingModule 3 connections real 10.10.10.10
Real Server Change Weight	serverfarm host sf1 rserver 10.10.10.10 80 weight 2
CSM Named Real Commands Sent	
Real Server Activation	serverfarm host sf1 real name rs1 80 inservice
Real Server Graceful Suspend	serverfarm host sf1 real name rs1 80 weight 0
Real Server Suspend	serverfarm host sf1 real name rs1 80 no inservice
Real Server Suspend and Clear Connections	serverfarm host sf1 real name rs1 80 no inservice clear module contentSwitchingModule 3 connections real 10.10.10.10
Real Server Change Weight	serverfarm host sf1 real name rs1 80 weight 2

Draft - CISCO CONFIDENTIAL

Table 5-3 *CLI Commands Deployed from Real Servers Table*

Command	Sample CLI Sent
CSS Devices	
Real Server Activation	service myReal7 active
Real Server Graceful Suspend	service myReal7 weight 0
Real Server Suspend	service myReal7 suspend
Real Server Suspend and Clear Connections	service myReal7 suspend
Real Server Change Weight	service myReal7 weight 2

Server Weight Ranges

Table 5-4 displays the allowable server weight ranges by device type.

Table 5-4 *Real Servers Table Server Weight Ranges*

Device Type	Valid Weight Configurations
ACE Appliances and Modules	1-100
CSMs	0-100
CSS Devices	0-10

Configuring Server Farms

Server farms are groups of networked real servers that contain the same content and that typically reside in the same physical location in a data center. Web sites often comprise groups of servers configured in a server farm. Load-balancing software distributes client requests for content or services among the real servers based on the configured policy and traffic classification, server availability and load, and other factors. If one server goes down, another server can take its place and continue to provide the same content to the clients who requested it.

Use this procedure to configure load balancing using server farms.

Procedure

- Step 1** Select **Config > Devices > context > Load Balancing > Server Farms**. The Server Farms table appears.
- Step 2** Click **Add** to add a new server farm, or select an existing server farm, then click **Edit**. The Server Farms configuration screen appears.
- Step 3** Configure the server farm using the information in [Table 5-5](#).

Table 5-5 **Server Farm Attributes**

Field	Description
Name	Either accept the automatically incremented value in this field, or enter a unique name for this server farm. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters.
Type	Select the type of server farm: • Host—The server farm consists of real servers that provide content and services to clients. • Redirect—The server farm consists only of real servers that redirect client requests to alternate locations specified in the real server configuration. (See Configuring Real Servers, page 5-4.)
Description	Enter a brief description for this server farm. Valid entries are unquoted alphanumeric text strings with no spaces and a maximum of 240 characters.
Fail Action	Select the action the ACE is to take with respect to connections if any real server in the server farm fails: • N/A—The ACE is to take no action if any server in the server farm fails. • Purge—The ACE is to remove connections to a real server if that real server in the server farm fails. The ACE sends a reset command to both the client and the server that failed.
Transparent	This field appears only for host server farms. Specify whether network address translation from VIP address to server IP is to occur: • N/A—The default value is to be used; the default value is False. • False—Network address translation from VIP address to server IP address is not to occur. • True—Network address translation from VIP address to server IP address is to occur.
Partial Threshold Percentage	This field appears only for host server farms. Enter the minimum percentage of real servers in the primary server farm that must remain active for the server farm to stay up. If the percentage of active real servers falls below this threshold, the ACE takes the server farm out of service. Valid entries are integers from 0 to 99. The default is 0.
Back In Service	This field appears only for host server farms. Enter the percentage of real servers in the primary server farm that must be active again for the ACE to place the server farm back into service. Valid entries are integers from 0 to 99. The value in this field should be larger than the value in the Partial Threshold Percentage field. The default is 0.
Probes	This field appears only for host server farms. In the Available Items list, select the probes to use for health monitoring, then click Add. The selected probes appear in the Selected Items list. To remove probes that you do not want to use for health monitoring, select them in the Selected Items list, then click Remove. The selected probes appear in the Available Items list.

Draft - CISCO CONFIDENTIAL**Step 4** Click:

- **Deploy Now** to deploy this configuration on the ACE.

The screen refreshes with additional configuration options:

- To add real servers to the server farm, see [Adding Real Servers to a Server Farm, page 5-14](#).
 - To specify a predictor method for the server farm, see [Configuring the Predictor Method for Server Farms, page 5-16](#).
 - To configure return code checking, see [Configuring Server Farm HTTP Return Error-Code Checking, page 5-21](#).
 - **Cancel** to exit the procedure without saving your entries and to return to the Server Farms table.
 - **Next** to deploy your entries and to configure another server farm.
-

Related Topics

- [Configuring Health Monitoring for Real Servers, page 5-25](#)
- [Configuring Real Servers, page 5-4](#)
- [Configuring Sticky Groups, page 6-7](#)
- [Configuring the Predictor Method for Server Farms, page 5-16](#)
- [Configuring Server Farm HTTP Return Error-Code Checking, page 5-21](#)

Adding Real Servers to a Server Farm

After adding a server farm, (see [Configuring Server Farms, page 5-12](#)), you can associate real servers with it and configure predictors and retcode maps. The options for these attributes appear after you have successfully added a new server farm.

Use this procedure to add real servers to a server farm.

Assumptions

- A server farm has been added to the ANM. (See [Configuring Server Farms, page 5-12](#).)
- At least one real server exists.

Procedure

-
- Step 1** Select **Config > Devices > context > Load Balancing > Server Farms**. The Server Farms table appears.
- Step 2** Select the server farm you want to associate with real servers. The Real Servers table appears.
- Step 3** Click **Add** to add a new entry to the Real Servers table, or select an existing server, then click **Edit** to modify it. The Real Servers configuration pane appears.

Step 4 Configure the real server using the information in [Table 5-6](#).

Table 5-6 Real Server Configuration Attributes

Field	Description
Name	Select the server that you want to associate with the server farm.
Port	Enter the port number to be used for server port address translation (PAT). Valid entries are integers from 1 to 65535.
Backup Server Name	Select the server that is to act as the backup server for the server farm. Leave this field blank to indicate that there is no designated backup server for the server farm.
Backup Server Port	If you select a backup server, enter the backup server port number. Valid entries are integers from 1 to 65535.
Max Connections	Enter the maximum number of active connections that can be sent to the server. When the number of connections exceeds this number, the ACE stops sending connections to the server until the number of connections falls below the number specified in the Min Connections field. For ACE 1.0 modules and ACE appliances, valid entries are integers from 2 to 4294967295. For ACE 2.0 modules, valid entries are integers from 2 to 4000000.
Min Connections	Enter the minimum number of connections that the number of connections must fall below before the ACE resumes sending connections to the server after it has exceeded the number in the Max Connections field. The number in this field must be less than or equal to the number in the Max Connections field. For ACE 1.0 modules and ACE appliances, valid entries are integers from 2 to 4294967295. For ACE 2.0 modules, valid entries are integers from 2 to 4000000.
Weight	Enter the weight to assign to the server. Valid entries are integers from 1 to 100, and the default is 8.
State	Select the state of this server: • In Service—The server is in service. • Out of Service—The server is out of service. • In Service Standby—The server is a backup server and remains inactive unless the primary server fails. If the primary server fails, the backup server becomes active and starts accepting connections.
Probes	Select the probes in the Available Items list that you want to apply to this server, then click Add . The selected probes appear in the Selected Items list. To remove probes you do not want to use, select the probes in the Selected Items list, then click Remove . The selected probes appear in the Available Items list.
Rate Bandwidth	The bandwidth rate is the number of bytes per second and applies to the network traffic exchanged between the ACE and the real server in both directions. Specify the bandwidth limit in bytes per second. Valid entries are integers from 2 to 300000000. The default is 300000000.
Rate Connection	The connection rate is the number of connections per second received by the ACE and applies only to new connections destined to a real server. Specify the limit for connections per second. Valid entries are integers from 2 to 350000. The default is 350000.

Draft - CISCO CONFIDENTIAL

- Step 5** When you finish configuring this server for this server farm, click:
- **Deploy Now** to deploy this configuration and to return to the Real Servers table.
 - **Cancel** to exit this procedure without saving your entries and to return to the Real Servers table.
 - **Next** to deploy your entries and to add another real server for this server farm.
-

Related Topics

- [Configuring Health Monitoring for Real Servers, page 5-25](#)
- [Configuring Real Servers, page 5-4](#)
- [Configuring Sticky Groups, page 6-7](#)
- [Configuring the Predictor Method for Server Farms, page 5-16](#)
- [Configuring Server Farm HTTP Return Error-Code Checking, page 5-21](#)

Configuring the Predictor Method for Server Farms

After adding a server farm, ([Configuring Server Farms, page 5-12](#)), you can associate real servers with it and configure the predictor method and retcode maps. The options for these attributes appear after you have successfully added a new server farm.

Use this procedure to configure the predictor method for a server farm. The predictor method specifies how the ACE is to select a server in the server farm when it receives a client request for a service.



Note You can configure only one predictor method per server farm.

Assumptions

- A server farm has been added to the ANM. (See [Configuring Server Farms, page 5-12](#).)
- At least one real server exists.

Procedure

-
- Step 1** Select **Config > Devices > context > Load Balancing > Server Farms**. The Server Farms table appears.
- Step 2** Select the server farm you want to configure the predictor method for, then click the Predictor tab. The Predictor configuration pane appears.
- Step 3** In the Type field, select the method that the ACE is to use to select a server in this server farm when it receives a client request. [Table 5-7](#) lists the available options and describes them.

Step 4 Enter the required information for the selected predictor method. See [Table 5-7](#).

Table 5-7 Predictor Method Attributes

Predictor Method	Description / Action
Round_Robin	The ACE selects the next server in the list of servers based on server weight. This is the default predictor method.
Least_Connections	The ACE selects the server with the fewest number of connections. In the Slowstart Duration field, enter the slow-start value to be applied to this predictor method. Valid entries are integers from 1 to 65535, where 1 is the slowest ramp-up value. The slow-start mechanism is used to avoid sending a high rate of new connections to servers that you have just put into service.
Hash_URL	The ACE selects the server using a hash value based on the URL. Use this method to load balance firewalls. Enter values in one or both of the pattern fields: - In the URL Begin Pattern field, enter the beginning pattern of the URL and the pattern string to parse. - In the URL End Pattern field, enter the ending pattern of the URL and the pattern string to parse. Valid entries for these fields are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters for each pattern you configure.
Hash_Address	The ACE selects the server using a hash value based on the source or destination IP address. To configure the hash address predictor method: - In the Mask Type field, indicate whether server selection is based on source IP address or the destination IP address: - N/A—This option is not defined. - Source—The server is selected based on the source IP address. - Destination—The server is selected based on the destination IP address. - In the IP Netmask field, select the subnet mask to apply to the address. If none is specified, the default is 255.255.255.255.
Hash_Cookie	The ACE selects the server by using a hash value based on the cookie name. In the Cookie Name field, enter a cookie name in the form of an unquoted text string with no spaces and a maximum of 64 characters.
Hash_Header	The ACE selects the server by using a hash value based on the header name. In the Header Name field, select the HTTP header to be used for server selection: - To specify an HTTP header that is not one of the standard HTTP headers, select the first radio button and enter the HTTP header name in the Header Name field. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters. - To specify one of the standard HTTP headers, select the second radio button, then select one of the HTTP headers from the list.

Draft - CISCO CONFIDENTIAL**Table 5-7 Predictor Method Attributes (continued)**

Predictor Method	Description / Action
Hash_Content	The ACE selects the server by using a hash value based on the specified content string of the HTTP packet body. 1. In the Begin Pattern field, enter the beginning pattern of the content string and the pattern string to match before hashing. If you do not specify a beginning pattern, the ACE starts parsing the HTTP body immediate following the offset byte. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions. 2. In the End Pattern field, enter the pattern that marks the end of hashing. If you do not specify either a length or an end pattern, the ACE continues to parse the data until it reaches the end of the field or the end of the packet, or until it reaches the maximum body parse length. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions. 3. In the Length field, enter the length in bytes of the portion of the content (starting with the byte after the offset value) that the ACE uses for sticking the client to the server. Valid entries are integers from 1 to 1000 bytes. The offset and length can vary from 0 to 1000 bytes. If the payload is longer than the offset but shorter than the offset plus the length of the payload, the ACE sticks the connection based on that portion of the payload starting with the byte after the offset value and ending with the byte specified by the offset plus the length. The total of the offset and the length cannot exceed 1000. Note You cannot specify both the length and the end-pattern options for a Hash Content predictor. 4. In the HTTP Content Offset field, enter the portion of the content that the ACE uses to stick the client on a particular server by indicating the bytes to ignore starting with the first byte of the payload. Valid entries are integers from 0 to 999 bytes. The default is 0, which indicates that the ACE does not exclude any portion of the content.

Table 5-7 **Predictor Method Attributes (continued)**

Predictor Method	Description / Action
Hash_Layer4	The ACE selects the server by using a Layer 4 generic protocol load-balancing method. Use this predictor to load balance packets from protocols that are not explicitly supported by the ACE. 1. In the Begin Pattern field, enter the beginning pattern of the Layer 4 payload and the pattern string to match before hashing. If you do not specify a beginning pattern, the ACE starts parsing the HTTP body immediate following the offset byte. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions. 2. In the End Pattern field, enter the pattern that marks the end of hashing. If you do not specify either a length or an end pattern, the ACE continues to parse the data until it reaches the end of the field or the end of the packet, or until it reaches the maximum body parse length. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions. 3. In the Length field, enter the length in bytes of the portion of the payload (starting with the byte after the offset value) that the ACE uses for sticking the client to the server. Valid entries are integers from 1 to 1000 bytes. The offset and length can vary from 0 to 1000 bytes. If the payload is longer than the offset but shorter than the offset plus the length of the payload, the ACE sticks the connection based on that portion of the payload starting with the byte after the offset value and ending with the byte specified by the offset plus the length. The total of the offset and the length cannot exceed 1000. Note You cannot specify both the length and end-pattern options for a Hash Layer 4 predictor. 4. In the HTTP Content Offset field, enter the portion of the content that the ACE uses to stick the client on a particular server by indicating the bytes to ignore starting with the first byte of the payload. Valid entries are integers from 0 to 999 bytes. The default is 0, which indicates that the ACE does not exclude any portion of the content.
Least_Bandwidth	The ACE selects the server with the least amount of network traffic over a specified sampling period. 1. In the Assess Time field, enter the number of seconds for which the ACE is to collect traffic information. Valid entries are integers from 1 to 10 seconds. 2. In the Least Bandwidth Samples field, enter the number of samples over which you want to weight and average the results of the probe query to calculate the final load value. Valid entries are 1, 2, 4, 8, and 16 (integers from 1 to 16 that are also a power of 2).

Draft - CISCO CONFIDENTIAL**Table 5-7 Predictor Method Attributes (continued)**

Predictor Method	Description / Action
Least Loaded	The ACE selects the server with the lowest load based on information from SNMP probes. 1. In the SNMP Probe Name field, select the name of the SNMP probe to use. 2. In the Auto Adjust field, configure the autoadjust feature to assign a maximum load value of 16000 to that server to prevent it from being flooded with new incoming connections. The ACE periodically adjusts this load value based on feedback from the server's SNMP probe and other configured options. Options include: – N/A—Indicates that this option is not defined. – Average—Instructs the ACE to apply the average load of the server farm to a real server whose load reaches zero. The average load is the running average of the load values across all real servers in the server farm. – Off—Overrides the default behavior of the ACE of setting the load value for a server with a load of zero to 16000. When you configure this parameter, the ACE sends all new connections to the server that has a load of zero until the next load update arrives from the SNMP probe for this server. There may be times when you want the ACE to send all new connections to a real server whose load is zero. 3. In the Weight Connection field, check the check box to instruct the ACE to use the current connection count in the final load calculation for a real server. When you configure this option, the ACE includes the current connection count in the total load calculation for each real server in a server farm. Clear the check box to reset the behavior of the ACE to the default of excluding the current connection count from the load calculation. To instruct the ACE to select the server with the lowest load, use the predictor least-loaded command in server farm host or redirect configuration mode. With this predictor, the ACE uses SNMP probes to query the real servers for load parameter values (for example, CPU utilization or memory utilization). This predictor is considered adaptive because the ACE continuously provides feedback to the load-balancing algorithm based on the behavior of the real server. To use this predictor, you must associate an SNMP probe with it. The ACE queries user-specified OIDs periodically based on a configurable time interval. The ACE uses the retrieved SNMP load value to determine the server with the lowest load. The syntax of this predictor command is as follows: predictor least-loaded probe <i>name</i> The name argument specifies the identifier of the existing SNMP probe that you want the ACE to use to query the server. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters. For example, to configure the ACE to select the real server with the lowest load based on feedback from an SNMP probe called PROBE_SNMP, enter: <pre>host1/Admin(config)# serverfarm SF1 host1/Admin(config-sfarm-host)# predictor least-loaded probe PROBE_SNMP host1/Admin(config-sfarm-host-predictor)#</pre> To reset the predictor method to the default of round-robin, enter: <pre>host1/Admin(config-sfarm-host)# no predictor</pre>

Table 5-7 Predictor Method Attributes (continued)

Predictor Method	Description / Action
Response	The ACE selects the server with the lowest response time for a requested response-time measurement. - In the Response Type field, select the type of measurement to use: - App-req-to-resp—The response time from when the ACE sends an HTTP request to a server to the time that the ACE receives a response from the server for that request. - Syn-to-close—The response time from when the ACE sends a TCP SYN to a server to the time that the ACE receives a CLOSE from the server. - Syn-to-synack—The response time from when the ACE sends a TCP SYN to a server to the time that the ACE receives a SYN-ACK from the server. - In the Response Samples field, enter the number of samples over which you want to average the results of the response-time measurement. Valid entries are 1, 2, 4, 8, and 16 (integers from 1 to 16 that are also a power of 2).

Step 5 Click **Deploy Now** to deploy this configuration.

Related Topics

- [Configuring Health Monitoring for Real Servers, page 5-25](#)
- [Configuring Real Servers, page 5-4](#)
- [Configuring Sticky Groups, page 6-7](#)
- [Adding Real Servers to a Server Farm, page 5-14](#)
- [Configuring Server Farm HTTP Return Error-Code Checking, page 5-21](#)

Configuring Server Farm HTTP Return Error-Code Checking

After adding a server farm, ([Configuring Server Farms, page 5-12](#)), you can associate real servers with it and configure the predictor method and retcode maps. These options appear after you have successfully added a server farm.

Use this procedure to configure HTTP return error-code checking (retcode map) for a server farm.



Note

This feature is available only for server farms configured as hosts. It is not available for server farms configured with the type Redirect.

Assumption

A host type server farm has been added to the ANM. (See [Configuring Server Farms, page 5-12](#).)

Procedure

Step 1 Select **Config > Devices > context > Load Balancing > Server Farms**. The Server Farms table appears.

Draft - CISCO CONFIDENTIAL

Step 2 Select the server farm you want to configure for return error-code checking, then click the Retcode Map tab. The Retcode Map table appears.

Step 3 Click **Add** to add a new entry to the table. The Retcode Map configuration pane appears.



Note You cannot modify an entry in the Retcode Map table. Instead, delete the existing entry, then add a new one.

Step 4 In the Lowest Retcode field, enter the minimum value for an HTTP return error code. Valid entries are integers from 100 to 599. This number must be less than or equal to the number in the Highest Retcode field.

Step 5 In the Highest Retcode field, enter the maximum number for an HTTP return error code. Valid entries are integers from 100 to 599. This number must be greater than or equal to the number in the Lowest Retcode field.

Step 6 In the Type field, specify the action to be taken and related options using the information in [Table 5-8](#).



Note For ACE 1.0 modules and ACE appliances, the only available option is Count.

Table 5-8 Return-Code Type Configuration Options

Option	Description
Count	The ACE tracks the total number of return codes received for each return code number that you specify.
Log	The ACE generates a syslog error message when the number of events reaches a specified threshold. 1. In the Threshold field, enter the number of events that the ACE is to receive before generating a syslog error message. Valid entries are integers from 1 to 4294967295. 2. In the Reset field, enter the time interval in seconds for which the ACE checks for the return code. Valid entries are integers from 1 to 4294967295 seconds.
Remove	The ACE generates a syslog error message when the number of events reaches a specified threshold and then removes the server from service. 1. In the Threshold field, enter the number of events that the ACE is to receive before generating a syslog error message and removing the server from service. Valid entries are integers from 1 to 4294967295. 2. In the Reset field, enter the time interval in seconds for which the ACE checks for the return code. Valid entries are integers from 1 to 4294967295 seconds. 3. In the Resume Service field, enter the number of seconds that the ACE waits before it resumes service for the real server automatically after taking the real server out of service. Valid entries are 30 to 3600 seconds with a default of 300 seconds.

Step 7 Click:

- **Deploy Now** to deploy this configuration.
- **Cancel** to exit this procedure without saving your entries and to return to the Retcode Map table.
- **Next** to deploy your entries and to add another retcode map.

Related Topics

- [Using Virtual Contexts, page 3-1](#)
- [Configuring Virtual Context Class Maps, page 11-6](#)
- [Configuring Virtual Context Policy Maps, page 11-30](#)
- [Configuring Real Servers, page 5-4](#)
- [Configuring Sticky Groups, page 6-7](#)

Viewing All Server Farms

Use this procedure to view all server farms associated with a virtual context.

Procedure

-
- Step 1** Select **Config > Devices**. The Virtual Contexts table appears.
- Step 2** Select the virtual context with the server farms you want to view, then click **Load Balancing > Server Farms**. The Server Farms table appears with the following information:
- Server farm name
 - Server farm type (either host or redirect)
 - Description
 - Number of real servers associated with the server farm
 - Number of predictor methods for the server farm
 - Number of entries in the HTTP retcode map table

You can click on any of the entries in the last three columns to view specific information about those entries.

Related Topics

- [Configuring Server Farms, page 5-12](#)
- [Adding Real Servers to a Server Farm, page 5-14](#)
- [Configuring the Predictor Method for Server Farms, page 5-16](#)
- [Configuring Server Farm HTTP Return Error-Code Checking, page 5-21](#)

Health Monitoring

You can instruct the ACE to check the health of servers and server farms by configuring health probes (sometimes referred to as *keepalives*). After you create a probe, you assign it to a real server or a server farm. A probe can be one of many types, including TCP, ICMP, Telnet, HTTP, and so on. You can also configure scripted probes using the TCL scripting language (see [TCL Scripts, page 5-24](#)).

The ACE sends out probes periodically to determine the status of a server, verifies the server response, and checks for other network problems that may prevent a client from reaching a server. Based on the server response, the ACE can place the server in or out of service, and, based on the status of the servers in the server farm, can make reliable load-balancing decisions.

Draft - CISCO CONFIDENTIAL

Health monitoring on the ACE tracks the state of a server by sending out probes. Also referred to as out-of-band health monitoring, the ACE verifies the server response or checks for any network problems that can prevent a client to reach a server. Based on the server response, the ACE can place the server in or out of service, and can make reliable load balancing decisions.

The ACE identifies the health of a server in the following categories:

- Passed—The server returns a valid response.
- Failed—The server fails to provide a valid response to the ACE is unable to reach a server for a specified number of retries.

By configuring the ACE for health monitoring, the ACE sends active probes periodically to determine the server state.

The ACE supports 4000 unique probe configurations which includes ICMP, TCP, HTTP, and other predefined health probes. The ACE also allows the opening of 1000 sockets simultaneously.

Related Topics

- [Configuring Health Monitoring for Real Servers, page 5-25](#)
- [TCL Scripts, page 5-24](#)

TCL Scripts

The ACE supports several specific types of health probes (for example HTTP, TCP, or ICMP health probes) when you need to use a diverse set of applications and health probes to administer your network. The basic health probe types supported in the current ACE software release may not support the specific probing behavior that your network requires. To support a more flexible health-probing functionality, the ACE allows you to upload and execute TCL scripts on the ACE.

The TCL interpreter code in the ACE is based on Release 8.44 of the standard TCL distribution. You can create a script to configure health probes. Script probes operate similar to other health probes available in the ACE software. As part of a script probe, the ACE executes the script periodically, and the exit code that is returned by the executing script indicates the relative health and availability of specific real servers. For information on health probes, see [Configuring Health Monitoring for Real Servers, page 5-25](#).

For your convenience, the following sample scripts for the ACE are available to support the TCL feature and are supported by Cisco TAC:

- CHECKPORT_STD_SCRIPT
- ECHO_PROBE_SCRIPT
- FINGER_PROBE_SCRIPT
- FTP_PROBE_SCRIPT
- HTTP_PROBE_SCRIPT
- HTTPCONTENT_PROBE
- HTTPHEADER_PROBE
- HTTPPROXY_PROBE
- IMAP_PROBE
- LDAP_PROBE
- MAIL_PROBE

- POP3_PROBE
- PROBENOTICE_PROBE
- RTSP_PROBE
- SSL_PROBE_SCRIPT
- TFTP_PROBE

The ace_scripts.tgz zip file contains these scripts and is located at the URL:

<http://www.cisco.com/cgi-bin/tablebuild.pl/cat6000-intellother>

To load a script into memory on the ACE and enable it for use, use the **script file** command. For detailed information on uploading and executing Toolkit Command Language (TCL) scripts on the ACE, refer to the *Cisco 4700 Series Application Control Engine Appliance Routing and Bridging Configuration Guide*.

Configuring Health Monitoring for Real Servers

To check the health and availability of a real server, the ACE periodically sends a probe to the real server. Depending on the server response, the ACE determines whether to include the server in its load-balancing decision.

Use this procedure to establish monitoring of real servers to determine their viability in load-balancing decisions.

Procedure

-
Step 1	Select Config > Devices > context > Load Balancing > Health Monitoring . The Health Monitoring table appears.
Step 2	Click Add to add a new health monitoring probe, or select an existing entry, then click Edit to modify it. The Health Monitoring screen appears.
Step 3	In the Name field, enter a name that identifies the probe and that associates the probe with the real server. Valid entries are text strings with a maximum of 64 characters.

Draft - CISCO CONFIDENTIAL

- Step 4** In the Type field, select the type of probe you want to use. The probe type determines what the probe sends to the real server. See [Table 5-9](#) for the types of probes and their descriptions.

Table 5-9 Probe Types

Probe Type	Description
DNS	Sends a request to a DNS server giving it a configured domain. To determine if the server is up, the ACE must receive the configured IP address for that domain.
ECHO-TCP	Sends a string to the server and compares the response with the original string. If the response string matches the original, the server is marked as passed. If not, the ACE retries as configured before the server is marked as failed.
ECHO-UDP	Sends a string to the server and compares the response with the original string. If the response string matches the original, the server is marked as passed. If not, the ACE retries as configured before the server is marked as failed.
FINGER	Sends a probe to the server to verify that a defined username is a username on the server.
FTP	Initiates an FTP session. By default, this probe is for an anonymous login with the option of configuring a user ID and password. The ACE performs an FTP GET or LS to determine the outcome of the problem. This probe supports only active connections.
HTTP	Sets up a TCP connection and issues an HTTP request. Any valid HTTP response causes the probe to mark the real server as passed.
HTTPS	Similar to an HTTP probe, but this probe uses SSL to generate encrypted data.
ICMP	Sends an ICMP request and listens for a response. If the server returns a response, the ACE marks the real server as passed. If there is no response and times out, or an ICMP standard error occurs, such as <code>DESTINATION_UNREACHABLE</code> , the ACE marks the real server as failed.
IMAP	Initiates an IMAP session, using a configured user ID and password. Then, the probe attempts to retrieve e-mail from the server and validates the result of the probe based on the return codes received from the server.
POP	Initiates a POP session, using a configured user ID and password. Then, the probe attempts to retrieve e-mail from the server and validates the result of the probe based on the return codes received from the server.
RADIUS	Connects to a RADIUS server and logs into it to determine if the server is up.
RTSP	Establishes a TCP connection and sends a request packet to the server. The ACE compares the response with the configured response code to determine whether the probe succeeded.
Scripted	Executes probes from a configured script to perform health probing. This method allows you to author specific scripts with features not present in standard probes. For ACE appliances, the script probe file name must first be established on the device.

Table 5-9 *Probe Types (continued)*

Probe Type	Description
SIP-TCP	Establishes a TCP connection and sends an OPTIONS request packet to the user agent on the server. The ACE compares the response with the configured response code or expected string, or both, to determine whether the probe has succeeded. If you do not configure an expected status code, any response from the server is marked as failed.
SIP-UDP	Establishes a UDP connection and sends an OPTIONS request packet to the user agent on the server. The ACE compares the response with the configured response code or expected string, or both, to determine whether the probe has succeeded. If you do not configure an expected status code, any response from the server is marked as failed.
SMTP	Initiates an SMTP session by logging into the server.
SNMP	Establishes a UDP connection and sends a maximum of eight SNMP OID queries to probe the server. The ACE weighs and averages the load information that is retrieved and uses it as input to the least-loaded algorithm for load-balancing decisions. If the retrieved value is within the configured threshold, the server is marked as passed. If the threshold is exceeded, the server is marked as failed.
TCP	Initiates a TCP handshake and expects a response. By default, a successful response causes the probe to mark the server as passed. The probe then sends a FIN to end the session. If the response is not valid, or if there is no response, the probe marks the real server as failed.
TELNET	Establishes a connection to the real server and verifies that a greeting from the application was received.
UDP	Sends a UDP packet to a real server. The probe marks the server as failed only if an ICMP Port Unreachable messages is returned.

Step 5 Enter health monitoring general attributes (see [Table 5-10](#)).

Table 5-10 *Health Monitoring General Attributes*

Field	Action
Description	Enter a description for this probe. Valid entries are unquoted alphanumeric text strings with no spaces and a maximum of 240 characters.
Probe Interval	Enter the number of seconds that the ACE is to wait before sending another probe to a server marked as passed. Valid entries are from 2 to 65535 with a default of 120.
Pass Detect Count	Enter the number of successful probe responses from the server before the server is marked as passed. Valid entries are integers from 1 to 65535 with a default of 3.
Pass Detect Interval	Enter the number of seconds that the ACE is to wait before sending another probe to a server marked as failed. Valid entries are integers from 2 to 65535 with a default of 300.
Receive Timeout	Enter the number of seconds the ACE is to wait for a response from a server that has been probed before marking the server as failed. Valid entries are integers from 1 to 65535 with a default of 10.

Draft - CISCO CONFIDENTIAL**Table 5-10 Health Monitoring General Attributes (continued)**

Field	Action
Fail Detect	Enter the consecutive number of times that an ACE must detect that probes have failed to contact a server before marking the server as failed. Valid entries are integers from 1 to 65535 with a default of 3.
Dest IP Address ¹	By default, the probe uses the IP address from the real or virtual server configuration for the destination IP address. To override the destination address that the probe uses, enter the preferred destination IP address in this field using dotted-decimal notation, such as 192.168.11.1.
Is Routed ²	Select the check box to indicate that the destination IP address is routed according to the ACE internal routing table. Clear the check box to indicate that the destination IP address is not routed according to the ACE internal routing table.

1. The Dest IP Address field does not appear for the Scripted and SNMP probe types.

2. The Is Routed field does not appear for the RTSP, Scripted, SIP-TCP, SIP-UDP, and SNMP probe types.

Step 6 Enter the attributes for the specific probe type selected:

- For DNS probes, see [Table 5-11](#).
- For Echo-TCP probes, see [Table 5-12](#).
- For Echo-UDP probes, see [Table 5-13](#).
- For Finger probes, see [Table 5-14](#).
- For FTP probes, see [Table 5-15](#).
- For HTTP probes, see [Table 5-16](#).
- For HTTPS probes, see [Table 5-17](#).
- There are no specific attributes for ICMP probes.
- For IMAP probes, see [Table 5-18](#).
- For POP probes, see [Table 5-19](#).
- For RADIUS probes, see [Table 5-20](#).
- For RTSP probes, see [Table 5-21](#).
- For Scripted probes, see [Table 5-22](#).
- For SIP-TCP probes, see [Table 5-23](#).
- For SIP-UDP probes, see [Table 5-24](#).
- For SMTP probes, see [Table 5-25](#).
- For SNMP probes, see [Table 5-26](#).
- For TCP probes, see [Table 5-27](#).
- For Telnet probes, see [Table 5-28](#).
- For UDP probes, see [Table 5-29](#).

Step 7 Click:

- **Deploy Now** to deploy this configuration on the ACE.
 - **Cancel** to exit this procedure without saving your entries and to return to the Health Monitoring table.
 - **Next** to deploy your entries and to configure another probe.
-

Related Topics

- [Configuring DNS Probe Expect Addresses, page 5-40](#)
- [Configuring Headers for HTTP and HTTPS Probes, page 5-41](#)
- [Configuring Health Monitoring Expect Status, page 5-42](#)
- [Configuring Real Servers, page 5-4](#)
- [Configuring Server Farms, page 5-12](#)
- [Configuring Sticky Groups, page 6-7](#)

Configuring Probe Attributes

Refer to the following topics to configure health monitoring probe-specific attributes:

- [DNS Probe Attributes, page 5-30](#)
- [Echo-TCP Probe Attributes, page 5-30](#)
- [Echo-UDP Probe Attributes, page 5-30](#)
- [Finger Probe Attributes, page 5-31](#)
- [FTP Probe Attributes, page 5-31](#)
- [HTTP Probe Attributes, page 5-31](#)
- [HTTPS Probe Attributes, page 5-33](#)
- [IMAP Probe Attributes, page 5-35](#)
- [POP Probe Attributes, page 5-35](#)
- [RADIUS Probe Attributes, page 5-36](#)
- [RTSP Probe Attributes, page 5-36](#)
- [Scripted Probe Attributes, page 5-37](#)
- [SIP-TCP Probe Attributes, page 5-38](#)
- [SIP-UDP Probe Attributes, page 5-38](#)
- [SMTP Probe Attributes, page 5-39](#)
- [SNMP Probe Attributes, page 5-39](#)
- [TCP Probe Attributes, page 5-39](#)
- [Telnet Probe Attributes, page 5-40](#)
- [UDP Probe Attributes, page 5-40](#)

Refer to the following topics for additional configuration options for health monitoring probes:

- [Configuring DNS Probe Expect Addresses, page 5-40](#)

Draft - CISCO CONFIDENTIAL

- [Configuring Headers for HTTP and HTTPS Probes, page 5-41](#)
- [Configuring Health Monitoring Expect Status, page 5-42](#)
- [Configuring an OID for SNMP Probes, page 5-43](#)

DNS Probe Attributes**Table 5-11 DNS Probe Attributes**

Field	Action
Domain Name	Enter the domain name that the probe is to send to the DNS server. Valid entries are unquoted text strings with a maximum of 255 characters.
Port	Enter the port number that the probe is to use. By default, the probe uses the port number based on its type.

To configure expect addresses for DNS probes, see [Configuring DNS Probe Expect Addresses, page 5-40](#).

Echo-TCP Probe Attributes**Table 5-12 Echo-TCP Probe Attributes**

Field	Action
Port	Enter the port number that the probe is to use. By default, the probe uses the port number based on its type.
Is Connection	Select the check box to indicate that connection parameters are configured. Clear the check box to indicate that connection parameters are not configured.
Open Timeout	Enter the number of seconds to wait when opening a connection with a real server. Valid entries are integers from 1 to 65535, and the default value is 10.
Send Data	Enter the ASCII data that the probe is to send to the server. Valid entries are unquoted text strings with no spaces and a maximum of 255 characters.

Echo-UDP Probe Attributes**Table 5-13 Echo-UDP Probe Attributes**

Field	Action
Port	Enter the port number that the probe is to use. By default, the probe uses the port number based on its type.
Send Data	Enter the ASCII data that the probe is to send to the server. Valid entries are unquoted text strings with no spaces and a maximum of 255 characters.

Finger Probe Attributes

Table 5-14 *Finger Probe Attributes*

Field	Action
Port	Enter the port number that the probe is to use. By default, the probe uses the port number based on its type.
Is Connection	Select the check box to indicate that connection parameters are configured. Clear the check box to indicate that connection parameters are not configured.
Open Timeout	Enter the number of seconds to wait when opening a connection with a real server. Valid entries are integers from 1 to 65535, and the default value is 10.
Send Data	Enter the ASCII data that the probe is to send to the server. Valid entries are unquoted text strings with no spaces and a maximum of 255 characters.

FTP Probe Attributes

Table 5-15 *FTP Probe Attributes*

Field	Action
Port	Enter the port number that the probe is to use. By default, the probe uses the port number based on its type.
Is Connection	Select the check box to indicate that connection parameters are configured. Clear the check box to indicate that connection parameters are not configured.
Open Timeout	Enter the number of seconds to wait when opening a connection with a real server. Valid entries are integers from 1 to 65535, and the default value is 10.

To configure probe expect statuses for FTP probes, see [Configuring Health Monitoring Expect Status](#), page 5-42.

HTTP Probe Attributes

Table 5-16 *HTTP Probe Attributes*

Field	Action
Port	Enter the port number that the probe is to use. By default, the probe uses the port number based on its type.
Is Connection	Select the check box to indicate that connection parameters are configured. Clear the check box to indicate that connection parameters are not configured.
Open Timeout	Enter the number of seconds to wait when opening a connection with a real server. Valid entries are integers from 1 to 65535, and the default value is 10.
User Name	Enter the user identifier to be used for authentication on the real server. Valid entries are unquoted text strings with a maximum of 64 characters.

Draft - CISCO CONFIDENTIAL**Table 5-16 HTTP Probe Attributes (continued)**

Field	Action
Password	Enter the password to be used for authentication on the real server. Valid entries are unquoted text strings with a maximum of 64 characters. Reenter the password in the Confirm field.
Expect Regex	Enter the expected response data from the probe destination. Valid entries are text strings (quotes allowed) with a maximum of 255 characters.
Expect Regex Offset	Enter the number of characters into the received message or buffer where the ACE is to begin looking for the string specified in the Expect Regex field. Valid entries are integers from 1 to 4000.
Hash	Select the Hash check box to indicate that the ACE is to use an MD5 hash for an HTTP GET probe. Clear the Hash check box to indicate that the ACE should not use an MD5 hash for an HTTP GET probe.
Hash String	This field appears if the Hash check box is selected. Enter the 32-bit hash value that the ACE is to compare with the hash that is generated from the HTTP page sent by the server. If you do not provide this value, the ACE generates a value the first time it queries the server, stores this value, and matches this value with other responses from the server. A successful comparison causes the probe to maintain an Alive state. Enter the MD5 hash value as a quoted or unquoted hexadecimal string with 16 characters.
Request Method Type	Select the type of HTTP request method that is to be used for this probe: • N/A—This option is not defined. • Head—The server is to only get the header for the page. Using this method can prevent the ACE from assuming that the service is down due to changed content and therefore changed hash values. • Get—The HTTP request method is a GET with a URL of “/”. This request method directs the server to get the page, and the ACE calculates a hash value for the content of the page. If the page content information changes, the hash value no longer matches the original hash value and the ACE assumes the service is down. This is the default request method.
Request HTTP URL	This field appears if you select Head or Get in the Request Method Type field. Enter the URL path on the remote server. Valid entries are strings of up to 255 characters specifying the URL path. The default path is “/”.

To configure probe headers and expect statuses for HTTP probes, see:

- [Configuring Headers for HTTP and HTTPS Probes, page 5-41](#)
- [Configuring Health Monitoring Expect Status, page 5-42](#)

HTTPS Probe Attributes

Table 5-17 *HTTPS Probe Attributes*

Field	Action
Port	Enter the port number that the probe is to use. By default, the probe uses the port number based on its type.
Is Connection	Select the check box to indicate that connection parameters are configured. Clear the check box to indicate that connection parameters are not configured.
Open Timeout	Enter the number of seconds to wait when opening a connection with a real server. Valid entries are integers from 1 to 65535, and the default value is 10.
User Name	Enter the user identifier to be used for authentication on the real server. Valid entries are unquoted text strings with a maximum of 64 characters.
Password	Enter the password to be used for authentication on the real server. Valid entries are unquoted text strings with a maximum of 64 characters. Reenter the password in the Confirm field.
Expect Regex	Enter the expected response data from the probe destination. Valid entries are text strings (quotes allowed) with a maximum of 255 characters.
Expect Regex Offset	Enter the number of characters into the received message or buffer where the ACE is to begin looking for the string specified in the Expect Regex field. Value entries are integers from 1 to 4000.
Hash	Select the Hash check box to indicate that the ACE is to use an MD5 hash for an HTTP GET probe. Clear this check box to indicate that the ACE is not to use an MD5 hash for an HTTP GET probe.
Hash String	This field appears if the Hash check box is selected. Enter the 32-bit hash value that the ACE is to compare with the hash that is generated from the HTTP page sent by the server. If you do not provide this value, the ACE generates a value the first time it queries the server, stores this value, and matches this value with other responses from the server. A successful comparison causes the probe to maintain an Alive state. Enter the MD5 hash value as a quoted or unquoted hexadecimal string with 16 characters.
Request Method Type	Select the type of HTTP request method that is to be used for this probe: • N/A—This option is not defined. • Head—The server is to only get the header for the page. Using this method can prevent the ACE from assuming that the service is down due to changed content and therefore changed hash values. • Get—The HTTP request method is a GET with a URL of “/”. This request method directs the server to get the page, and the ACE calculates a hash value for the content of the page. If the page content information changes, the hash value no longer matches the original hash value and the ACE assumes the service is down. This is the default request method.

Draft - CISCO CONFIDENTIAL**Table 5-17 HTTPS Probe Attributes (continued)**

Field	Action
Request HTTP URL	This field appears if you select Head or Get in the Request Method Type field. Enter the URL path on the remote server. Valid entries are strings of up to 255 characters specifying the URL path. The default path is “/”.
Cipher	Select the cipher suite to be used with this HTTPS probe: • RSA_ANY—The HTTPS probe accepts all RSA-configured cipher suites and that no specific suite is configured. This is the default action. • RSA_EXPORT1024_WITH_DES_CBC_SHA • RSA_EXPORT1024_WITH_RC4_56_MD5 • RSA_EXPORT1024_WITH_RC4_56_SHA • RSA_EXPORT_WITH_DES40_CBC_SHA • RSA_EXPORT_WITH_RC4_40_MD5 • RSA_WITH_3DES_EDE_CBC_SHA • RSA_WITH_AES_128_CBC_SHA • RSA_WITH_AES_256_CBC_SHA • RSA_WITH_DES_CBC_SHA • RSA_WITH_RC4_128_MD5 • RSA_WITH_RC4_128_SHA
SSL Version	Select the version of SSL or TLS to be used in ClientHello messages sent to the server: • SSLv2—The probe is to use SSL version 2. • SSLv3—The probe is to use SSL version 3. • TLSv1—The probe is to use TLS version 1. By default, the probe sends ClientHello messages with an SSL version 3 header and a TLS version 1 message.

To configure probe headers and expect statuses for HTTPS probes, see:

- [Configuring Headers for HTTP and HTTPS Probes, page 5-41](#)
- [Configuring Health Monitoring Expect Status, page 5-42](#)

IMAP Probe Attributes

Table 5-18 *IMAP Probe Attributes*

Field	Action
Port	Enter the port number that the probe is to use. By default, the probe uses the port number based on its type.
Is Connection	Select the check box to indicate that connection parameters are configured. Clear the check box to indicate that connection parameters are not configured.
Open Timeout	Enter the number of seconds to wait when opening a connection with a real server. Valid entries are integers from 1 to 65535, and the default value is 10.
User Name	Enter the user identifier to be used for authentication on the real server. Valid entries are unquoted text strings with a maximum of 24 characters.
Password	Enter the password to be used for authentication on the real server. Valid entries are unquoted text strings with a maximum of 24 characters. Reenter the password in the Confirm field.
Mailbox Name	Enter the user mailbox name from which to retrieve e-mail for this IMAP probe. Valid entries are unquoted text strings with a maximum of 64 characters.
Request Method	Enter the request method command for this probe. Valid entries are text strings with a maximum of 32 characters and no spaces.

POP Probe Attributes

Table 5-19 *POP Probe Attributes*

Field	Action
Port	Enter the port number that the probe is to use. By default, the probe uses the port number based on its type.
Is Connection	Select the check box to indicate that connection parameters are configured. Clear the check box to indicate that connection parameters are not configured.
Open Timeout	Enter the number of seconds to wait when opening a connection with a real server. Valid entries are integers from 1 to 65535, and the default value is 10.
User Name	Enter the user identifier to be used for authentication on the real server. Valid entries are unquoted text strings with a maximum of 64 characters.
Password	Enter the password to be used for authentication on the real server. Valid entries are unquoted text strings with a maximum of 64 characters. Reenter the password in the Confirm field.
Request Method	Enter the request method command for this probe. Valid entries are text strings with a maximum of 32 characters and no spaces.

Draft - CISCO CONFIDENTIAL**RADIUS Probe Attributes****Table 5-20 RADIUS Probe Attributes**

Field	Action
Port	Enter the port number that the probe is to use. By default, the probe uses the port number based on its type.
User Secret	Enter the shared secret to be used to allow probe access to the RADIUS server. Valid entries are case-sensitive strings with no spaces and a maximum of 128 characters.
User Name	Enter the user identifier to be used for authentication on the real server. Valid entries are unquoted text strings with a maximum of 64 characters.
Password	Enter the password to be used for authentication on the real server. Valid entries are unquoted text strings with a maximum of 64 characters. Reenter the password in the Confirm field.
NAS IP Address	Enter the IP address of the Network Access Server (NAS) in dotted-decimal format, such as 192.168.11.1.

RTSP Probe Attributes**Table 5-21 RTSP Probe Attributes**

Field	Action
Port	Enter the port number that the probe is to use. By default, the probe uses the port number based on its type.
Is Connection	Select the check box to indicate that connection parameters are configured. Clear the check box to indicate that connection parameters are not configured.
Open Timeout	Enter the number of seconds to wait when opening a connection with a real server. Valid entries are integers from 1 to 65535, and the default value is 10.
RTSP Require Header Name	Enter the Require header for this probe.
RTSP Proxy-Require Header Name	Enter the Proxy-Require header for this probe.
RTSP Request Method Type	Select the request method type: - N/A—No request method is selected. - Describe—This probe is to use the Describe request type.

To configure probe expect statuses for RTSP probes, see [Configuring Health Monitoring Expect Status, page 5-42](#).

Scripted Probe Attributes

Table 5-22 **Scripted Probe Attributes**

Field	Action
Port	Enter the port number that the probe is to use. By default, the probe uses the port number based on its type.
Script needs to be copied from remote location?	Select this check box to indicate that the file needs to be copied from a remote server. Clear this check box to indicate that the script resides locally.
Protocol	This field appears if the script is to be copied from a remote server. Select the protocol to be used for copying the script: - FTP—The script is to be copied using FTP. - TFTP—The script is to be copied using TFTP.
Username	This field appears if FTP is selected in the Protocol field. Enter the name of the user account on the remote server.
Password	This field appears if FTP is selected in the Protocol field. Enter the password for the user account on the remote server. Reenter the password in the Confirm field.
Source File Name	This field appears if the script is to be copied from a remote server. Enter the host IP address, path, and filename of the file on the remote server in the format <i>host-ip/path/filename</i> where: <i>host-ip</i> represents the IP address of the remote server. <i>path</i> represents the directory path of the file on the remote server. <i>filename</i> represents the filename of the file on the remote server. For example, your entry might resemble 192.168.11.2/usr/bin/my-script.ext.
Script Name	Enter the local name that you want to assign to this file on the ACE. This file can reside in the disk0: directory or the probe: directory (if the probe: directory exists).  Note The script file must first be established on the ACE device and the name must be entered exactly as is appears on the device. Please refer to your ACE documentation for more details. Valid entries are unquoted text strings with no spaces and a maximum of 255 characters.
Script Arguments	Valid arguments are unquoted text strings with no spaces; separate multiple arguments with a space. The field limit is 255 characters.

Draft - CISCO CONFIDENTIAL**SIP-TCP Probe Attributes****Table 5-23 SIP-TCP Probe Attributes**

Field	Action
Port	Enter the port number that the probe is to use. By default, the probe uses the port number based on its type.
Is Connection	Select the check box to indicate that connection parameters are configured. Clear the check box to indicate that connection parameters are not configured.
Open Timeout	Enter the number of seconds to wait when opening a connection with a real server. Valid entries are integers from 1 to 65535, and the default value is 10.
Expect Regex	Enter the expected response data from the probe destination. Valid entries are text strings with a maximum of 255 characters. This field accepts both single and double quotes. Double quotes are considered delimiters so they don't appear on the device. Single quotes will appear on the device.
Expect Regex Offset	Enter the number of characters into the received message or buffer where the ACE is to begin looking for the string specified in the Expect Regex field. Value entries are integers from 1 to 4000.

To configure probe expect statuses for SIP-TCP probes, see [Configuring Health Monitoring Expect Status, page 5-42](#).

SIP-UDP Probe Attributes**Table 5-24 SIP-UDP Probe Attributes**

Field	Action
Port	Enter the port number that the probe is to use. By default, the probe uses the port number based on its type.
Expect Regex	Enter the expected response data from the probe destination. Valid entries are text strings (quotes allowed) with a maximum of 255 characters.
Expect Regex Offset	Enter the number of characters into the received message or buffer where the ACE is to begin looking for the string specified in the Expect Regex field. Value entries are integers from 1 to 4000.

To configure probe expect statuses for SIP-UDP probes, see [Configuring Health Monitoring Expect Status, page 5-42](#).

SMTP Probe Attributes

Table 5-25 SMTP Probe Attributes

Field	Action
Port	Enter the port number that the probe is to use. By default, the probe uses the port number based on its type.
Is Connection	Select the check box to indicate that connection parameters are configured. Clear the check box to indicate that connection parameters are not configured.
Open Timeout	Enter the number of seconds to wait when opening a connection with a real server. Valid entries are integers from 1 to 65535, and the default value is 10.

To configure probe expect statuses for SMTP probes, see [Configuring Health Monitoring Expect Status, page 5-42](#).

SNMP Probe Attributes

Table 5-26 SNMP Probe Attributes

Field	Action
SNMP Community String	Enter the SNMP community string. Valid entries are unquoted text strings with no spaces and a maximum of 32 characters.
SNMP Version Number	Select the SNMP version for this probe: - N/A—No version is selected. - SNMPv1—This probe is to use SNMP version 1. - SNMPv2c—This probe is to use SNMP version 2c.

To configure the SNMP OID for SNMP probes, see [Configuring an OID for SNMP Probes, page 5-43](#).

TCP Probe Attributes

Table 5-27 TCP Probe Attributes

Field	Action
Port	Enter the port number that the probe is to use. By default, the probe uses the port number based on its type.
Is Connection	Select the check box to indicate that connection parameters are configured. Clear the check box to indicate that connection parameters are not configured.
Open Timeout	Enter the number of seconds to wait when opening a connection with a real server. Valid entries are integers from 1 to 65535, and the default value is 10.
Send Data	Enter the ASCII data that the probe is to send to the server. Valid entries are unquoted text strings with no spaces and a maximum of 255 characters.

Draft - CISCO CONFIDENTIAL**Table 5-27 TCP Probe Attributes (continued)**

Field	Action
Expect Regex	Enter the expected response data from the probe destination. Valid entries are text strings (quotes allowed) with a maximum of 255 characters.
Expect Regex Offset	Enter the number of characters into the received message or buffer where the ACE is to begin looking for the string specified in the Expect Regex field. Value entries are integers from 1 to 4000.

Telnet Probe Attributes**Table 5-28 Telnet Probe Attributes**

Field	Action
Port	Enter the port number that the probe is to use. By default, the probe uses the port number based on its type.
Is Connection	Select the check box to indicate that connection parameters are configured. Clear the check box to indicate that connection parameters are not configured.
Open Timeout	Enter the number of seconds to wait when opening a connection with a real server. Valid entries are integers from 1 to 65535, and the default value is 10.

UDP Probe Attributes**Table 5-29 UDP Probe Attributes**

Field	Action
Port	Enter the port number that the probe is to use. By default, the probe uses the port number based on its type.
Send Data	Enter the ASCII data that the probe is to send to the server. Valid entries are unquoted text strings with no spaces and a maximum of 255 characters.
Expect Regex	Enter the expected response data from the probe destination. Valid entries are text strings (quotes allowed) with a maximum of 255 characters.
Expect Regex Offset	Enter the number of characters into the received message or buffer where the ACE is to begin looking for the string specified in the Expect Regex field. Value entries are integers from 1 to 4000.

Configuring DNS Probe Expect Addresses

When a DNS probe sends a domain name resolve request to the server, it verifies the returned IP address by matching the received IP address with the configured addresses.

Use this procedure to specify the IP address that the ACE expects to receive in response to a DNS request.

Assumption

A DNS probe has been configured. See [Configuring Health Monitoring for Real Servers, page 5-25](#) for more information.

Procedure

-
- Step 1** Select **Config > Devices > context > Load Balancing > Health Monitoring**. The Health Monitoring table appears.
- Step 2** Select the DNS probe that you want to configure with an expected IP address. The Expect Addresses table appears.
- Step 3** Click **Add** to add an entry to the Expect Addresses table. The Expect Address configuration pane appears.



Note You cannot modify an entry in the Expect Addresses table. Instead, delete the existing entry, then add a new one.

- Step 4** In the IP Address field, enter the IP address that the ACE is to expect as a server response to a DNS request. Valid entries are unique IP addresses in dotted-decimal notation, such as 192.168.11.1.
- Step 5** Click:
- **Deploy Now** to deploy this configuration.
 - **Cancel** to exit this procedure without saving your entry and to return to the Expect Addresses table.
 - **Next** to deploy your entry and to add another IP Address to the Expect Addresses table.
-

Related Topics

- [Configuring Health Monitoring for Real Servers, page 5-25](#)
- [DNS Probe Attributes, page 5-30](#)

Configuring Headers for HTTP and HTTPS Probes

Use this procedure to specify header fields for HTTP and HTTPS probes.

Assumption

An HTTP or HTTPS probe has been configured. See [Configuring Health Monitoring for Real Servers, page 5-25](#) for more information.

Procedure

-
- Step 1** Select **Config > Devices > context > Load Balancing > Health Monitoring**. The Health Monitoring table appears.
- Step 2** Select the HTTP or HTTPS probe that you want to configure with a header. The Probe Headers table appears.
- Step 3** Click **Add** to add an entry, or select an existing entry, then click **Edit** to modify it. The Probe Headers configuration pane appears.

Draft - CISCO CONFIDENTIAL

- Step 4** In the Header Name field, select the HTTP header the probe is to use.
- Step 5** In the Header Value field, enter the string to assign to the header field. Valid entries are text strings with a maximum of 255 characters. If the string includes spaces, enclose the string with quotes.
- Step 6** Click:
- **Deploy Now** to deploy this configuration.
 - **Cancel** to exit this procedure without saving your entry and to return to the Probe Headers table.
 - **Next** to deploy your entry and to add another header entry to the Probe Headers table.
-

Related Topics

- [Configuring Health Monitoring for Real Servers, page 5-25](#)
- [HTTP Probe Attributes, page 5-31](#)
- [HTTPS Probe Attributes, page 5-33](#)

Configuring Health Monitoring Expect Status

When the ACE receives a response from the server, it expects a status code to mark a server as passed. By default, there are no status codes configured on the ACE. If you do not configure a status code, any response code from the server is marked as failed.

Expect status codes can be configured for FTP, HTTP, HTTPS, RTSP, SIP-TCP, SIP-UDP, and SMTP probes.

Use this procedure to configure a single or range of code responses that the ACE expects from the probe destination.

Assumption

An FTP, HTTP, HTTPS, RTSP, SIP-TCP, SIP-UDP or SMTP probe has been configured. See [Configuring Health Monitoring for Real Servers, page 5-25](#) for more information.

Procedure

-
- Step 1** Select **Config > Devices > context > Load Balancing > Health Monitoring**. The Health Monitoring table appears.
- Step 2** Select the probe that you want to configure for expect status codes, then click the Expect Status tab. The Expect Status table appears.
- Step 3** Click **Add** to add an entry, or select an existing entry, then click **Edit** to modify it. The Expect Status configuration pane appears.
- Step 4** To configure a single expect status code:
- a. In the Min Expect Status Code field, enter the expect status code for this probe. Valid entries are integers from 0 to 999.
 - b. In the Max Expect Status code, enter the same expect status code that you entered in the Min Expect Status Code field.

- Step 5** To configure a range of expect status codes:
- In the Min Expect Status Code, enter the lower limit of the range of status codes. Valid entries are integers from 0 to 999.
 - In the Max Expect Status Code, enter the upper limit of a range of status codes. Valid entries are integers from 0 to 999. The value in this field must be greater than or equal to the value in the Min Expect Status Code field.
- Step 6** Click:
- Deploy Now** to deploy this configuration on the ACE.
 - Cancel** to exit this procedure without saving your entries and to return to the Expect Status table.
 - Next** to deploy your entries and to add another expect status code to the Expect Status table.
-

Related Topics

- [Configuring Health Monitoring for Real Servers, page 5-25](#)
- [FTP Probe Attributes, page 5-31](#)
- [HTTP Probe Attributes, page 5-31](#)
- [SMTP Probe Attributes, page 5-39](#)

Configuring an OID for SNMP Probes

When the ACE sends a probe with an SNMP OID query, the ACE uses the retrieved value as input to the least-loaded algorithm for load-balancing decisions. Least-loaded load balancing bases the server selection on the server with the lowest load value. If the retrieved value is within the configured threshold, the server is marked as passed. If the threshold is exceeded, the server is marked as failed.

The ACE allows a maximum of eight OID queries to probe the server.

Assumption

An SNMP probe has been configured. See [Configuring Health Monitoring for Real Servers, page 5-25](#) for more information.

Procedure

-
- Step 1** Select **Config > Devices > context > Load Balancing > Health Monitoring**. The Health Monitoring table appears.
- Step 2** Select the SNMP probe for which you want to specify an OID. The SNMP OID for Server Load Query table appears.
- Step 3** Click **Add** to add an entry, or select an existing entry, then click **Edit** to modify it. The SNMP OID configuration pane appears.
- Step 4** In the SNMP OID field, enter the OID that the probe is to use to query the server for a value. Valid entries are unquoted strings with a maximum of 255 alphanumeric characters in dotted-decimal notation, such as .1.3.6.1.4.2021.10.1.3.1. The OID string is based on the server type.
- Step 5** In the Maximum Absolute Server Load Value field, enter the OID value in the form of an integer and to indicate that the retrieved OID value is an absolute value instead of a percent. Valid entries are integers from 1 to 4294967295.

Draft - CISCO CONFIDENTIAL

When the ACE sends a probe with an SNMP OID query, the ACE uses the retrieved value as input to the least-loaded algorithm for load-balancing decisions. By default, the ACE assumes that the retrieved OID value is a percentile value. Use this option to specify that the retrieved OID value is an absolute value.

Step 6 In the Server Load Threshold Value field, specify the threshold at which the server is to be taken out of service:

- When the OID value is based on a percent, valid entries are integers from 0 to 100.
- When the OID is based on an absolute value, valid entries are from 0 to the value specified in the Maximum Absolute Server Load Value field.

Step 7 In the Server Load Weighting field, enter the weight to assign to this OID for the SNMP probe. Valid entries are integers from 0 to 16000.

Step 8 Click:

- **Deploy Now** to deploy this configuration.
 - **Cancel** to exit this procedure without saving your entries and to return to the SNMP OID table.
 - **Next** to deploy your entries and to add another item to the SNMP OID table.
-

Related Topics

- [Configuring Health Monitoring for Real Servers, page 5-25](#)
- [SNMP Probe Attributes, page 5-39](#)



CHAPTER 6

Configuring Stickiness

Revised Date: 3/25/09

This section provides information about sticky behavior and procedures for configuring stickiness with the ANM. Sections include:

- [Stickiness Overview, page 6-1](#)
- [Sticky Types, page 6-2](#)
- [Sticky Groups, page 6-6](#)
- [Sticky Table, page 6-6](#)
- [Configuring Sticky Groups, page 6-7](#)

Stickiness Overview

When customers visit an e-commerce site, they usually start out by browsing the site, the Internet equivalent of window shopping. Depending on the application, the site may require that the client become “stuck” to one server once the connection is established, or the application may not require this until the client starts to build a shopping cart.

In either case, once the client adds items to the shopping cart, it is important that all of the client requests get directed to the same server so that all the items are contained in one shopping cart on one server. An instance of a customer's shopping cart is typically local to a particular Web server and is not duplicated across multiple servers.

E-commerce applications are not the only types of applications that require stickiness. Any Web application that maintains client information may require stickiness, such as banking applications or online trading. Other uses include FTP and HTTP file transfers.

Stickiness allows the same client to maintain multiple simultaneous or subsequent TCP or IP connections with the same real server for the duration of a session. A session, as used here, is defined as a series of transactions between a client and a server over some finite period of time (from several minutes to several hours). This feature is particularly useful for e-commerce applications where a client needs to maintain multiple connections with the same server while shopping online, especially while building a shopping cart and during the checkout process.

Depending on the configured SLB policy, the ACE “sticks” a client to an appropriate server after the ACE has determined which load-balancing method to use. If the ACE determines that a client is already stuck to a particular server, then the ACE sends that client request to that server, regardless of the load-balancing criteria specified by the matched policy. If the ACE determines that the client is not stuck to a particular server, it applies the normal load-balancing rules to the content request.

For information on stickiness, see:

- [Sticky Types, page 6-2](#)
- [Sticky Groups, page 6-6](#)
- [Sticky Table, page 6-6](#)

Related Topics

- [Configuring Virtual Server Default Layer 7 Load Balancing, page 4-35](#)
- [Configuring Sticky Groups, page 6-7](#)

Sticky Types

All ACE devices support stickiness based on:

- HTTP cookies
- HTTP headers
- IP addresses

ACE 2.0 modules also support stickiness based on:

- HTTP content
- Layer 4 payloads
- RADIUS attributes
- RTSP headers
- SIP headers

Related Topics

- [HTTP Content Stickiness, page 6-3](#)
- [HTTP Cookie Stickiness, page 6-3](#)
- [HTTP Header Stickiness, page 6-4](#)
- [IP Netmask Stickiness, page 6-4](#)
- [Layer 4 Payload Stickiness, page 6-4](#)
- [RADIUS Stickiness, page 6-5](#)
- [RTSP Header Stickiness, page 6-5](#)
- [SIP Header Stickiness, page 6-5](#)

HTTP Content Stickiness

HTTP content stickiness allows you to stick a client to a server based on the content of an HTTP packet. You can specify a beginning pattern and ending pattern, the number of bytes to parse, and an offset that specifies how many bytes to ignore from the beginning of the data.

Related Topics

- [Configuring Stickiness, page 6-1](#)
- [Sticky Types, page 6-2](#)
- [Sticky Groups, page 6-6](#)
- [Sticky Table, page 6-6](#)

HTTP Cookie Stickiness

Client *cookies* uniquely identify clients to the ACE and the servers providing content. A cookie is a small data structure within the HTTP header that is used by a server to deliver data to a Web client and request that the client store the information. In certain applications, the client returns the information to the server to maintain the connection state or persistence between the client and the server.

When the ACE examines a request for content and determines through policy matching that the content is sticky, it examines any cookie or URL present in the content request. The ACE uses the information in the cookie or URL to direct the content request to the appropriate server.

The ACE supports the following types of cookie stickiness:

- Dynamic cookie learning

You can configure the ACE to look for a specific cookie name and automatically learn its value either from the client request HTTP header or from the server Set-Cookie message in the server response. Dynamic cookie learning is useful when dealing with applications that store more than just the session ID or user ID within the same cookie. Only very specific bytes of the cookie value are relevant to stickiness.

By default, the ACE learns the entire cookie value. You can optionally specify an offset and length to instruct the ACE to learn only a portion of the cookie value.

Alternatively, you can specify a secondary cookie value that appears in the URL string in the HTTP request. This option instructs the ACE to search for (and eventually learn or stick to) the cookie information as part of the URL. URL learning is useful with applications that insert cookie information as part of the HTTP URL. In some cases, you can use this feature to work around clients that reject cookies.

- Cookie insert

The ACE inserts the cookie on behalf of the server upon the return request, so that the ACE can perform cookie stickiness even when the servers are not configured to set cookies. The cookie contains information that the ACE uses to ensure persistence to a specific real server.

Related Topics

- [Configuring Stickiness, page 6-1](#)
- [Sticky Types, page 6-2](#)
- [Sticky Groups, page 6-6](#)
- [Sticky Table, page 6-6](#)

HTTP Header Stickiness

You can use HTTP-header information to provide stickiness. With HTTP header stickiness, you can specify a header offset to provide stickiness based on a unique portion of the HTTP header.

Related Topics

- [Configuring Stickiness, page 6-1](#)
- [Sticky Types, page 6-2](#)
- [Sticky Groups, page 6-6](#)
- [Sticky Table, page 6-6](#)

IP Netmask Stickiness

You can use the source IP address, the destination IP address, or both to uniquely identify individual clients and their requests for stickiness purposes based on their IP netmask. However, if an enterprise or a service provider uses a megaproxy to establish client connections to the Internet, the source IP address no longer is a reliable indicator of the true source of the request. In this case, you can use cookies or one of the other sticky methods to ensure session persistence.

Related Topics

- [Configuring Stickiness, page 6-1](#)
- [Sticky Types, page 6-2](#)
- [Sticky Groups, page 6-6](#)
- [Sticky Table, page 6-6](#)

Layer 4 Payload Stickiness

Layer 4 payload stickiness allows you to stick a client to a server based on the data in Layer 4 frames. You can specify a beginning pattern and ending pattern, the number of bytes to parse, and an offset that specifies how many bytes to ignore from the beginning of the data.

Related Topics

- [Configuring Stickiness, page 6-1](#)
- [Sticky Types, page 6-2](#)
- [Sticky Groups, page 6-6](#)
- [Sticky Table, page 6-6](#)

RADIUS Stickiness

RADIUS stickiness can be based on the following RADIUS attributes:

- Calling station ID
- Username

Related Topics

- [Configuring Stickiness, page 6-1](#)
- [Sticky Types, page 6-2](#)
- [Sticky Groups, page 6-6](#)
- [Sticky Table, page 6-6](#)

RTSP Header Stickiness

RTSP stickiness is based on information in the RTSP session header. With RTSP header stickiness, you can specify a header offset to provide stickiness based on a unique portion of the RTSP header.

Related Topics

- [Configuring Stickiness, page 6-1](#)
- [Sticky Types, page 6-2](#)
- [Sticky Groups, page 6-6](#)
- [Sticky Table, page 6-6](#)

SIP Header Stickiness

SIP header stickiness is based on the SIP Call-ID header field. SIP header stickiness requires the entire SIP header, so you cannot specify an offset.

Related Topics

- [Configuring Stickiness, page 6-1](#)
- [Sticky Types, page 6-2](#)
- [Sticky Groups, page 6-6](#)
- [Sticky Table, page 6-6](#)

Sticky Groups

The ACE uses the concept of sticky groups to configure stickiness. A sticky group allows you to specify sticky attributes. After you configure a sticky group and its attributes, you associate the sticky group with a Layer 7 policy-map action in a Layer 7 SLB policy map. You can create a maximum of 4096 sticky groups in each context. Each sticky group that you configure on the ACE contains a series of parameters that determine:

- Sticky method
- Timeout
- Replication
- Sticky method-specific attributes

**Note**

The context in which you configure a sticky group must be associated with a resource class that allocates a portion of ACE resources to stickiness. See [Using Resource Classes, page 3-32](#) for information about configuring ACE resources.

Related Topics

- [Configuring Stickiness, page 6-1](#)
- [Sticky Types, page 6-2](#)
- [Sticky Table, page 6-6](#)

Sticky Table

The ACE uses a sticky table to keep track of sticky connections. Table entries include:

- Sticky groups
- Sticky methods
- Sticky connections
- Real servers

The sticky table can hold a maximum of four million entries (four million simultaneous users). When the table reaches the maximum number of entries, additional sticky connections cause the table to wrap and the first users become unstuck from their respective servers.

The ACE uses a configurable timeout mechanism to age out sticky table entries. When an entry times out, it becomes eligible for reuse. High connection rates may cause the premature aging out of sticky entries. In this case, the ACE reuses the entries that are closest to expiration first.

Sticky entries can be either dynamic (generated by the ACE on-the-fly) or static (user-configured). When you create a static sticky entry, the ACE places the entry in the sticky table immediately. Static entries remain in the sticky database until you remove them from the configuration. You can create a maximum of 4096 static sticky entries in each context.

If the ACE takes a real server out of service for whatever reason (probe failure, no inservice command, or ARP timeout), the ACE removes from the database any sticky entries that are related to that server.

Related Topics

- [Configuring Stickiness, page 6-1](#)
- [Sticky Types, page 6-2](#)
- [Sticky Groups, page 6-6](#)

Configuring Sticky Groups

Stickiness (or session persistence) is a feature that allows the same client to maintain multiple simultaneous or subsequent TCP connections with the same real server for the duration of a session. A session, as used here, is defined as a series of transactions between a client and a server over some finite period of time (from several minutes to several hours). This feature is particularly useful for e-commerce applications where a client needs to maintain multiple TCP connections with the same server while shopping online, especially while building a shopping cart and during the checkout process.

E-commerce applications are not the only types of applications that require stickiness. Any Web application that maintains client information may require stickiness, such as banking applications or online trading. Other uses include FTP and HTTP file transfers.

The ACE uses the concept of sticky groups to configure stickiness. A sticky group allows you to specify sticky attributes. After you configure a sticky group and its attributes, you associate the sticky group with a Layer 7 policy-map action in a Layer 7 SLB policy map.

Use this procedure to configure sticky groups.

**Note**

The context in which you configure a sticky group must be associated with a resource class that allocates a portion of ACE resources to stickiness. See [Using Resource Classes, page 3-32](#) for information about configuring ACE resources.

Assumption

The context in which you are configuring a sticky group is associated with a resource class that allocates resources to stickiness.

Procedure

- Step 1** Select **Config > Devices > context > Load Balancing > Stickiness**. The Sticky Groups table appears.
- Step 2** Click **Add** to add a new sticky group, or select an existing sticky group you want to modify, then click **Edit**.
- Step 3** Configure the sticky group using the information in [Table 6-1](#).

Table 6-1 **Sticky Group Attributes**

Field	Description
Group Name	The sticky group identifier. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
Type	Select the method to be used when establishing sticky connections and configure any type-specific attributes: • HTTP Cookie—The ACE either learns a cookie from the HTTP header of a client request or inserts a cookie in the Set-Cookie header of the response from the server to the client, and then uses the learned cookie to provide stickiness between the client and server for the duration of the transaction. See Table 6-3 for additional configuration options. • HTTP Header—The ACE sticks client connections to the same real server based on HTTP headers. See Table 6-4 for additional configuration options. • IP Netmask—The ACE sticks a client to the same server for multiple subsequent connections as needed to complete a transaction using the client source IP address, the destination IP address, or both. See Table 6-5 for additional configuration options. Note If an organization uses a megaproxy to load balance client requests across multiple proxy servers when a client connects to the Internet, the source IP address is no longer a reliable indicator of the true source of the request. In this situation, you can use cookies or another sticky method to ensure session persistence. • HTTP Content—The ACE sticks client connections to the same real server based on a string in the data portion of the HTTP packet. See Table 6-2 for additional configuration options. • Layer 4 Payload—The ACE sticks client connections to the same real server based on a string in the payload portion of the Layer 4 protocol packet. See Table 6-6 for additional configuration options. • RADIUS—The ACE sticks client connections to the same real server based on a RADIUS attribute. See Table 6-7 for additional configuration options. • RTSP Header—The ACE sticks client connections to the same real server based on the RTSP Session header field. See Table 6-8 for additional configuration options. • SIP Header—The ACE sticks client connections to the same real server based on the SIP Call-ID header field.
Sticky Server Farm	Select a server farm you want to associate with this sticky group.
Backup Server Farm	Select a backup server farm to be associated with this sticky group. If the primary server farm is down, the ACE uses the backup server farm.
Aggregate State	This field appears when a server farm and backup server farm are selected. Select this check box to indicate that the state of the backup server farm is tied to the virtual server state. Clear this check box if the backup server farm is not tied to the virtual server state.
Sticky Enabled on Backup Server Farm	This field appears when a server farm and backup server farm are selected. Select this check box to indicate that the backup server farm is sticky. Clear this check box if the backup server farm is not sticky.

Table 6-1 **Sticky Group Attributes (continued)**

Field	Description
Replicate	Select this check box to indicate that the ACE to replicate sticky table entries on the standby ACE. If a failover occurs and this option is selected, the new active ACE can maintain the existing sticky connections. Clear this check box to indicate that the ACE is not to replicate sticky table entries on the standby ACE.
Timeout	Enter the number of minutes that the ACE keeps the sticky information for a client connection in the sticky table after the latest client connection terminates. Valid entries are integers from 1 to 65535; the default is 1440 minutes (24 hours).
Timeout Active Connections	Select this check box to specify that the ACE is to time out sticky table entries even if active connections exist after the sticky timer expires. Clear this check box to specify that the ACE is not to time out sticky table entries even if active connections exist after the sticky timer expires. This is the default behavior.

Step 4 Click:

- **Deploy Now** to deploy this configuration on the ACE. To configure sticky statics, see [Configuring Sticky Statics, page 6-14](#).
- **Cancel** to exit the procedure without saving your entries and to return to the Sticky Groups table.
- **Next** to deploy your entries and to configure another sticky group.

Related Topics

- [Configuring Sticky Statics, page 6-14](#)
- [Configuring Virtual Context Class Maps, page 11-6](#)
- [Configuring Virtual Context Policy Maps, page 11-30](#)
- [Configuring Real Servers, page 5-4](#)
- [Configuring Server Farms, page 5-12](#)

Sticky Group Attribute Tables

Refer to the following topics for sticky group type-specific attributes:

- [HTTP Content Sticky Group Attributes, page 6-10](#)
- [HTTP Cookie Sticky Group Attributes, page 6-11](#)
- [HTTP Header Sticky Group Attributes, page 6-11](#)
- [IP Netmask Sticky Group Attributes, page 6-12](#)
- [Layer 4 Payload Sticky Group Attributes, page 6-12](#)
- [RADIUS Sticky Group Attributes, page 6-13](#)
- [RTSP Header Sticky Group Attributes, page 6-14](#)

HTTP Content Sticky Group Attributes

Table 6-2 *HTTP Content Sticky Group Attributes*

Field	Description
HTTP Content	HTTP content may change over time with only a portion remaining constant throughout a transaction between the client and a server. Select the check box to configure the ACE to use the constant portion of HTTP content to make persistent connections to a specific server. Clear the check box to identify specific content for stickiness in the Offset, Length, Begin Pattern, and End Pattern fields.
Offset	Enter the number of bytes the virtual server is to ignore starting with the first byte of the cookie. Valid entries are integers from 0 to 999. The default is 0 (zero), which indicates that the virtual server does not exclude any portion of the cookie.
Length	Enter the length of the portion of the cookie (starting with the byte after the offset value) that the ACE is to use for sticking the client to the server. Valid entries are integers from 1 to 1000.
Begin Pattern	Enter the beginning pattern of the HTTP content payload and the pattern string to match before hashing. If you do not specify a beginning pattern, the ACE begins parsing immediately after the offset byte. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. You can enter a text string with spaces provided that you enclose the entire string in quotation marks ("). The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions.
End Pattern	Enter the pattern that marks the end of hashing. If you do not specify an end pattern or a length, the ACE continues to parse the data until it reaches the end of the field or packet, or until it reaches the maximum body parse length. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. You can enter a text string with spaces provided that you enclose the entire string in quotation marks ("). The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions.

HTTP Cookie Sticky Group Attributes

Table 6-3 HTTP Cookie Sticky Group Attributes

Field	Description
Cookie Name	Enter a unique identifier for the cookie. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
Enable Insert	Select the check box if the virtual server is to insert a cookie in the Set-Cookie header of the response from the server to the client. This option is useful when you want to use a session cookie for persistence but the server is not currently setting the appropriate cookie. When selected, the virtual server selects a cookie value that identifies the original server from which the client received a response. For subsequent connections of the same transaction, the client uses the cookie to stick to the same server. Clear the check box to disable cookie insertion.
Offset	Enter the number of bytes the virtual server is to ignore starting with the first byte of the cookie. Valid entries are integers from 0 to 999. The default is 0 (zero), which indicates that the virtual server does not exclude any portion of the cookie.
Length	Enter the length of the portion of the cookie (starting with the byte after the offset value) that the ACE is to use for sticking the client to the server. Valid entries are integers from 1 to 1000.
Secondary Name	Enter an alternate cookie name that is to appear in the URL string of the Web page on the server. The virtual server uses this cookie to maintain a sticky connection between a client and a server and adds a secondary entry in the sticky table. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters.

HTTP Header Sticky Group Attributes

Table 6-4 HTTP Header Sticky Group Attributes

Field	Description
Offset	Enter the number of bytes the virtual server is to ignore starting with the first byte of the cookie. Valid entries are integers from 0 to 999. The default is 0 (zero), which indicates that the virtual server does not exclude any portion of the cookie.
Length	Enter the length of the portion of the cookie (starting with the byte after the offset value) that the ACE is to use for sticking the client to the server. Valid entries are integers from 1 to 1000.
Header Name	Select the HTTP header to use for sticking client connections.

IP Netmask Sticky Group Attributes

Table 6-5 *IP Netmask Sticky Group Attributes*

Field	Description
Netmask	Select the netmask to apply to the source IP address, destination IP address, or both.
Address Type	Indicate whether this sticky type is to be applied to the client source IP address, the destination IP address, or both: - Both—The sticky type is to be applied to both the source IP address and the destination IP address. - Source—The sticky type is to be applied to the source IP address only. - Destination—The sticky type is to be applied to the destination IP address only.

Layer 4 Payload Sticky Group Attributes

Table 6-6 *Layer 4 Payload Sticky Group Attributes*

Field	Description
Layer 4 Payload	A Layer 4 payload may change over time with only a portion remaining constant throughout a transaction between the client and a server. Select the check box to configure the ACE to use the constant portion of a payload to make persistent connections to a specific server. Clear the check box to identify specific criteria for stickiness in the Offset, Length, Begin Pattern, and End Pattern fields.
Offset	Enter the number of bytes the virtual server is to ignore starting with the first byte of the cookie. Valid entries are integers from 0 to 999. The default is 0 (zero), which indicates that the virtual server does not exclude any portion of the cookie.
Length	Enter the length of the portion of the cookie (starting with the byte after the offset value) that the ACE is to use for sticking the client to the server. Valid entries are integers from 1 to 1000, and the default is 1000.
Begin Pattern	Enter the beginning pattern of the Layer 4 payload and the pattern string to match before hashing. If you do not specify a beginning pattern, the ACE begins parsing immediately after the offset byte. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. You can enter a text string with spaces provided that you enclose the entire string in quotation marks ("). The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions.

Table 6-6 Layer 4 Payload Sticky Group Attributes (continued)

Field	Description
End Pattern	Enter the pattern that marks the end of hashing. If you do not specify an end pattern or a length, the ACE continues to parse the data until it reaches the end of the field or packet, or until it reaches the maximum body parse length. You cannot configure different beginning and ending patterns for different server farms that are part of the same traffic classification. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. You can enter a text string with spaces provided that you enclose the entire string in quotation marks (""). The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions.
Sticky Server Farm	Select a server farm you want to associate with this sticky group.
Replicate	Select this check box to indicate that the ACE to replicate sticky table entries on the standby ACE. If a failover occurs and this option is selected, the new active ACE can maintain the existing sticky connections. Clear this check box to indicate that the ACE is not to replicate sticky table entries on the standby ACE.
Timeout	Enter the number of minutes that the ACE keeps the sticky information for a client connection in the sticky table after the latest client connection terminates. Valid entries are integers from 1 to 65535; the default is 1440 minutes (24 hours).
Timeout active connections	Select this check box to specify that the ACE is to time out sticky table entries even if active connections exist after the sticky timer expires. Clear this check box to specify that the ACE is not to time out sticky table entries even if active connections exist after the sticky timer expires. This is the default behavior.

RADIUS Sticky Group Attributes

Table 6-7 RADIUS Sticky Group Attributes

Field	Description
RADIUS Types	Select the RADIUS attribute to use for sticking client connections: - N/A—This option is not configured. - RADIUS Calling ID—Stickiness is based on the RADIUS framed IP attribute and the calling station ID attribute. - RADIUS User Name—Stickiness is based on the RADIUS framed IP attribute and the username attribute.

RTSP Header Sticky Group Attributes

Table 6-8 *RTSP Header Sticky Group Attributes*

Field	Description
Offset	Enter the number of bytes the virtual server is to ignore starting with the first byte of the cookie. Valid entries are integers from 0 to 999. The default is 0 (zero), which indicates that the virtual server does not exclude any portion of the cookie.
Length	Enter the length of the portion of the cookie (starting with the byte after the offset value) that the ACE is to use for sticking the client to the server. Valid entries are integers from 1 to 1000, and the default is 1000.

Viewing All Sticky Groups by Context

Use this procedure to view all sticky groups associated with a virtual context.

Procedure

-
- Step 1** Select **Config > Devices**. The Virtual Contexts table appears.
- Step 2** Select the virtual context with the sticky groups you want to view, then select **Load Balancing > Stickiness**. The Sticky Groups table appears, listing the sticky groups associated with the selected context.
-

Related Topics

- [Configuring Sticky Groups, page 6-7](#)
- [Configuring Sticky Statics, page 6-14](#)

Configuring Sticky Statics

Use this procedure to configure sticky statics.

Assumption

A sticky group has been configured. See [Configuring Sticky Groups, page 6-7](#) for more information.

Procedure

-
- Step 1** Select **Config > Devices > context > Load Balancing > Stickiness**. The Sticky Groups table appears.
- Step 2** Select the sticky group you want to configure for sticky statics. The Sticky Statics table appears.
- Step 3** Click **Add** to add a new entry to the table, or select an existing entry, then click **Edit** to modify it. The Sticky Statics configuration screen appears.

Step 4 In the Seqnumber field, either accept the automatically incremented number for this entry or enter a new sequence number. The sequence number indicates the order in which multiple sticky static configurations are applied.

Step 5 In the Type field, confirm that the correct sticky group type is selected.

- **HTTP Cookie**—The ACE is either to learn a cookie from the HTTP header of a client request or to insert a cookie in the Set-Cookie header of the response from the server to the client, and then use the learned cookie to provide stickiness between the client and server for the duration of the transaction.
- **HTTP Header**—The ACE is to stick client connections to the same real server based on HTTP headers.
- **IP Netmask**—The ACE is to stick a client to the same server for multiple subsequent connections as needed to complete a transaction using the client source IP address, the destination IP address, or both.

**Note**

If an organization uses a megaproxy to load balance client requests across multiple proxy servers when a client connects to the Internet, the source IP address is no longer a reliable indicator of the true source of the request. In this situation, you can use cookies or another sticky method to ensure session persistence.

- **HTTP Content**—The ACE sticks client connections to the same real server based on a string in the data portion of the HTTP packet.
- **Layer 4 Payload**—The ACE sticks client connections to the same real server based on a string in the payload portion of the Layer 4 protocol packet. .
- **RADIUS**—The ACE sticks client connections to the same real server based on a RADIUS attribute. .
- **RTSP Header**—The ACE sticks client connections to the same real server based on the RTSP .
- **SIP Header**—The ACE sticks client connections to the same real server based on the SIP Call-ID header field.

Step 6 If you select either HTTP Cookie or HTTP Header for sticky type, in the Static Value field, enter the cookie string value. Valid entries are unquoted text strings with a maximum of 255 alphanumeric characters. If the string includes spaces, enclose the string with quotes.

Step 7 If you select IP Netmask for the sticky type:

- a. In the Static Source field, enter the source IP address of the client.
- b. In the Static Destination field, enter the destination IP address of the client.

Step 8 In the Named Real Server field, select the real server to associate with this static sticky entry.

Step 9 In the Port field, enter the port number of the real server. Valid entries are integers from 1 to 65535.

Step 10 Click:

- **Deploy Now** to deploy this configuration on the ACE.
- **Cancel** to exit the procedure without saving your entries and to return to the Sticky Statics table.
- **Next** to deploy your entries and to configure another sticky static entry.

Related Topic

[Configuring Sticky Groups, page 6-7](#)



Draft - CISCO CONFIDENTIAL

CHAPTER 7

Configuring Parameter Maps

Revised Date: 3/25/09

Parameter maps provide a means of performing actions on traffic ingressing an ACE interface based on certain criteria, such as protocol or connection attributes. After you configure a parameter map, you associate it with a policy map to implement configured behavior. [Table 7-1](#) describes the parameter maps you can configure using the ANM and the ACE devices that support them.

Table 7-1 *Parameter Map Types and ACE Support*

Parameter Map	Description	ACE Modules and Devices			
		ACE 1.0 Module	ACE 2.0 Module	ACE 4710 Running Image A1(8)	ACE 4710 Running Image A3(1.0)
Connection	Connection parameter maps combine all IP and TCP connection-related behaviors pertaining to: - TCP normalization, termination, and server reuse - IP normalization, fragmentation, and reassembly	X	X	X	X
Generic	Generic parameter maps combine related generic protocol actions for server load-balancing connections.		X	X	X
HTTP	HTTP parameter maps configure ACE behavior for HTTP load-balanced connections.	X	X	X	X
Optimization	Optimization parameter maps specify optimization-related commands that pertain to application acceleration and optimization functions performed by the ACE.			X	X
RTSP	RTSP parameter maps configure advanced RTSP behavior for server load-balancing connections.		X	X	X
SIP	Session Initiation Protocol (SIP) parameter maps configure SIP deep packet inspection on the ACE.		X	X	X
Skinny	Skinny Client Control Protocol (SCCP) parameter maps configure SCCP packet inspection on the ACE.		X	X	X

Draft - CISCO CONFIDENTIAL**Related Topics**

- [Configuring Connection Parameter Maps, page 7-2](#)
- [Configuring Generic Parameter Maps, page 7-7](#)
- [Configuring HTTP Parameter Maps, page 7-8](#)
- [Configuring Optimization Parameter Maps, page 7-10](#)
- [Configuring RTSP Parameter Maps, page 7-17](#)
- [Configuring SIP Parameter Maps, page 7-18](#)
- [Configuring Skinny Parameter Maps, page 7-20](#)
- [Configuring Traffic Policies, page 11-1](#)
- [Configuring Parameter Maps, page 7-1](#)
- [Configuring Virtual Contexts, page 3-5](#)

Configuring Connection Parameter Maps

Connection parameter maps combine all IP and TCP connection-related behaviors pertaining to:

- TCP normalization, termination, and server reuse
- IP normalization, fragmentation, and reassembly

Use this procedure to configure a Connection parameter map for use with a Layer 3/Layer 4 policy map.

Procedure

-
- Step 1** Select **Config > Devices > context > Load Balancing > Parameter Maps > Connection Parameter Map**. The Connection Parameter Map table appears.
- Step 2** Click **Add** to add a new parameter map, or select an existing parameter map, then click **Edit** to modify it. The Connection Parameter Map configuration screen appears.
- Step 3** Configure the parameter map using the information in [Table 7-2](#).

Table 7-2 *Connection Parameter Map Attributes*

Field	Description
Parameter Name	Enter a unique name for the parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
Exceeds MSS	Indicate how the ACE is to handle segments that exceed the maximum segment size (MSS): • Allow—The ACE is to permit segments that exceed the configured MSS. • Drop—The ACE is to discard segments that exceed the configured MSS.
Max Connection Limit	This option appears for ACE 2.0 modules and the ACE 4710 A3(1.0) release only. Enter the maximum number of concurrent connections to allow for the parameter map. Valid entries are integers from 0-4000000.

Table 7-2 **Connection Parameter Map Attributes (continued)**

Field	Description
Nagle	The Nagle algorithm instructs a sender to buffer any data to be sent until all outstanding data has been acknowledged or until there is a full segment of data to send. Enabling the Nagle algorithm increases throughput, but it can increase latency in your TCP connection. Select the check box to enable the Nagle algorithm. Clear the check box to disable the Nagle algorithm. Note Disable the Nagle algorithm when you observe unacceptable delays in TCP connections.
Random Sequence Number	Randomizing TCP sequence numbers adds a measure of security to TCP connections by making it more difficult for a hacker to guess or predict the next sequence number in a TCP connection. Select the check box to enable the use of random TCP sequence numbers. Clear the check box to disable the use of random TCP sequence numbers. This option is enabled by default.
Bandwidth Rate Limit	This option appears for ACE 2.0 modules only. Enter the bandwidth-rate limit in bytes per second for the parameter map. Valid entries are integers from 0-300000000 bytes.
Connection Rate Limit	This option appears for ACE 2.0 modules and the ACE 4710 A3(1.0) release only. Enter the connection-rate limit in connections per second. Valid entries are integers from 0-350000.
Reserved Bits	Indicate how the ACE is to handle segments with the reserved bits set in the TCP header: • Allow—Segments with the reserved bits are to be permitted. • Drop—Segments with the reserved bits are to be discarded. • Clear—Reserved bits in TCP headers are to be cleared and segments are to be allowed.
Type-of-Service IP Header	The type of service for an IP packet determines how the network handles the packet and balances its precedence, throughput, delay, reliability, and cost. Enter the type-of-service value to be applied to IP packets. Valid entries are integers from 0 to 255. For more information about type of service, refer to RFCs 791, 1122, 1349, and 3168.
ACK Delay Time	Enter the number of milliseconds that the ACE is to wait before sending an acknowledgement from a client to a server. Valid entries are integers from 0 to 400.
TCP Buffer Share	This option appears for only ACE 2.0 modules and ACE 1.0 modules running software versions 3.0(0)A1(6.2) and later. To improve throughput and overall performance, the ACE buffers the number of bytes you specify before processing received data or transmitting data. Use this option to increase the default buffer size and thereby realize improved network performance. Enter the maximum size of the TCP buffer in bytes. Valid entries are integers from 8192 to 262143 bytes. Default is 32768. Note If you enter a value in this field for an ACE device that does not support this option, an error message appears. Leave this field blank when creating or modifying a connection parameter map for devices that do not support this option.
Smallest TCP MSS	Enter the size of the smallest segment of TCP data that the ACE is to accept. Valid entries are integers from 0 to 65535 bytes. The value 0 indicates that the ACE is not to set a minimum limit.
Largest TCP MSS	Enter the size of the largest segment of TCP data that the ACE is to accept. Valid entries are integers from 0 to 65535 bytes. The value 0 indicates that the ACE is not to set a maximum limit.

Draft - CISCO CONFIDENTIAL**Table 7-2 Connection Parameter Map Attributes (continued)**

Field	Description
SYN Retries	Enter the number of attempts that the ACE is to make to transmit a TCP segment when initiating a Layer 7 connection. Valid entries are integers from 1 to 15 with a default of 4.
TCP WAN Optimization RTT	This option specifies how the ACE is to apply TCP optimizations to packets on a connection associated with a Layer 7 policy map using a round-trip time (RTT) value: - An entry of 0 (zero) indicates that the ACE is to apply TCP optimizations to packets for the life of a connection. - An entry of 65535 (the default) indicates that the ACE is to perform normal operations (that is, without optimizations) for the life of a connection. - Entries from 1 to 65534 indicate that the ACE is to use the following guidelines: - If the actual client RTT is less than the configured RTT, the ACE performs normal operations for the life of the connection. - If the actual client RTT is greater than or equal to the configured RTT, the ACE performs TCP optimizations on the packets for the life of a connection. Valid entries are integers from 0 to 65535.
Timeout for Embryonic Connections	An embryonic connection is a TCP three-way handshake for a connection that does not complete for some reason. Enter the number of seconds that the ACE is to wait before timing out an embryonic connection. Valid entries are integers from 0 to 4294967295 with a default of 5. A value of 0 indicates that the ACE is never to time out an embryonic connection.
Half Closed Timeout	A half-closed connection is one in which the client or server sends a FIN and the server or client acknowledges the FIN without sending a FIN itself. Enter the number of seconds the ACE is to wait before closing a half-closed connection. Valid entries are integers from 0 to 4294967295 with a default of 3600 (1 hour). A value of 0 indicates that the ACE is never to time out a half-closed connection.
Inactivity Timeout	Enter the number of seconds that the ACE is to wait before disconnecting idle connections. Valid entries are integers from 0-3217203. A value of 0 indicates that ACE is never to time out a TCP connection.
Slow Start Algorithm	When enabled, the slow start algorithm increases TCP window size as ACK handshakes arrive so that new segments are injected into the network at the rate at which acknowledgements are returned by the host at the other end of the connection. Select this check box to enable the slow start algorithm, and clear this check box to disable the slow start algorithm. This option is disabled by default.
SYN Segments with Data	Indicate how the ACE is to handle TCP SYN segments that contain data: - Allow—The ACE is to permit SYN segments that contain data and mark them for processing. - Drop—The ACE is to discard SYN segments that contain data.
Urgent Pointer Policy	Urgent data, as indicated by a control bit in the TCP header, indicates that urgent data is to be processed as soon as possible, even before normal data. Indicate how the ACE is to handle urgent data as identified by the Urgent data control bit: - Allow—The ACE is to permit the status of the Urgent control bit. - Clear—The ACE is to set the Urgent control bit to 0 (zero) and thereby invalidate the Urgent Pointer which provides segment information.

Table 7-2 Connection Parameter Map Attributes (continued)

Field	Description
TCP Window-Scale Factor	The TCP window scaling extension expands the definition of the TCP window to 32 bits and uses a scale factor to carry the 32-bit value in the 16-bit window of the TCP header. Increasing the window size improves TCP performance in network paths with large bandwidth, long-delay characteristics. Enter the window scale factor in this field. Valid entries are integers from 0 to 14 (the maximum scale factor). For more information on TCP window scaling, refer to RFC 1323.
Action for TCP Options Range	Indicate how the ACE is to handle the TCP options: • Selective ACK • Timestamps • TCP Window Scaling by selecting one of the options: • N/A—This option is not set. • Allow—The ACE is to allow any segment with the specified option set. • Drop—The ACE is to discard any segment with the specified option set.
Lower TCP Options	Appears if you select Allow or Drop for the Action for TCP Options Range. Enter the lower limit of the TCP option range. Valid entries are 6, 7, or an integer from 9 to 255. See Table 7-3 for information on TCP options.
Upper TCP Options	Appears if you select Allow or Drop for the Action for TCP Options Range. Enter the upper limit of the TCP option range. Valid entries are 6, 7, or an integer from 9 to 255. See Table 7-3 for information on TCP options.
Selective ACK	Indicate how the ACE is to handle the selective ACK option that is specified in SYN segments: • Allow—The ACE is to allow any segment with the specified option set. • Clear—The ACE is to clear the specified option from any segment that has it set and allow the segment.
Timestamps	Indicate how the ACE is to handle the timestamp option that is specified in SYN segments: • Allow—The ACE is to allow any segment with the specified option set. • Clear—The ACE is to clear the specified option from any segment that has it set and allow the segment.
TCP Window Scale Factor	Indicate how the ACE is to handle the TCP window scale factor option that is specified in SYN segments: • Allow—The ACE is to allow any segment with the specified option set. • Clear—The ACE is to clear the specified option from any segment that has it set and allow the segment. • Drop—The ACE is to discard any segment with the specified option set.

Draft - CISCO CONFIDENTIAL**Table 7-3 TCP Options for Connection Parameter Maps¹**

Kind	Length	Meaning
6	6	Echo (obsoleted by option 8)
7	6	Echo Reply (obsoleted by option 8)
9	2	Partial Order Connection Permitted
10	3	Partial Order Service Profile
11		CC
12		CC.NEW
13		CC.ECHO
14	3	TCP Alternate Checksum Request
15	N	TCP Alternate Checksum Data
16		Skeeter
17		Bubba
18	3	Trailer Checksum Option
19	18	MD5 Signature Option
20		SCPS Capabilities
21		Selective Negative Acknowledgements (SNACK)
22		Record Boundaries
23		Corruption Experienced
24		SNAP
25		Unassigned (released 12/18/2000)
26		TCP Compression Filter

1. For more information on TCP options, refer to the *Cisco 4700 Series Application Control Engine Appliance Security Configuration Guide*.

Step 4 Click:

- **Deploy Now** to deploy this configuration on the ACE.
- **Cancel** to exit this procedure without accepting your entries and to return to the Parameter Map table.
- **Next** to accept your entries and to add another parameter map.

Related Topics

- [Configuring Parameter Maps, page 7-1](#)
- [Configuring Traffic Policies, page 11-1](#)
- [Configuring Virtual Contexts, page 3-5](#)

Configuring Generic Parameter Maps

Generic parameter maps are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.

Generic parameter maps allow you to specify nonprotocol-specific behavior for data parsing. Generic parameter maps examine the payload and make decisions regardless of the protocol.

Use this procedure to configure a generic parameter map.

Procedure

- Step 1** Select **Config > Devices > context > Load Balancing > Parameter Maps > Generic Parameter Map**. The Generic Parameter Map table appears.
- Step 2** Click **Add** to add a new parameter map, or select an existing parameter map, then click **Edit** to modify it. The Parameter Maps configuration screen appears.
- Step 3** Configure the parameter map using the information in [Table 7-4](#).

Table 7-4 **Generic Parameter Map Attributes**

Field	Description
Parameter Name	Enter a unique name for the parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
Case-insensitive	Select this check box to indicate that the ACE is to be case insensitive for this parameter map. Clear this check box to indicate that the ACE is to be case sensitive for this parameter map.
Max Parse Length	Enter the number of bytes to parse for the total length of all generic headers. Valid entries are integers from 1 to 65535 with a default of 2048 bytes.

- Step 4** Click:
 - **Deploy Now** to deploy this configuration.
 - **Cancel** to exit this procedure without saving your entries and to return to the Generic Parameter Map table.
 - **Next** to deploy your entries and to configure another generic parameter map.

Related Topics

- [Configuring Parameter Maps, page 7-1](#)
- [Configuring Traffic Policies, page 11-1](#)
- [Configuring Parameter Maps, page 7-1](#)
- [Configuring Virtual Contexts, page 3-5](#)

Draft - CISCO CONFIDENTIAL

Configuring HTTP Parameter Maps

HTTP parameter maps allow you to configure ACE behavior for HTTP load-balanced connections.

Use this procedure to configure an HTTP parameter map for use with a Layer 3/Layer 4 policy map.

Procedure

- Step 1** Select **Config > Devices > context > Load Balancing > Parameter Maps > HTTP Parameter Map**. The HTTP Parameter Map table appears.
- Step 2** Click **Add** to add a new parameter map, or select an existing parameter map, then click **Edit** to modify it. The Parameter Maps configuration screen appears.
- Step 3** Configure the parameter map using the information in [Table 7-5](#).

Table 7-5 HTTP Parameter Map Attributes

Field	Description
Parameter Name	Enter a unique name for the parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
Case-insensitive	Select this check box to indicate that the ACE is to be case insensitive. Clear this check box to indicate that the ACE is to be case sensitive. This check box is cleared by default.
Header Modify Per-Request	This option appears for ACE 2.0 modules and the ACE 4710 A3(1.0) release only. Select the check box to require SSL information be inserted for every HTTP GET request. Current functionality only requires that the information be inserted at the first GET request.
Exceed Max Parse Length	Indicate how the ACE is to handle cookies, HTTP headers, and URLs that exceed the maximum parse length: - Continue—The ACE is to continue load balancing. When this option is selected, the HTTP Persistence Rebalance option is disabled if the total length of all cookies, HTTP headers, and URLs exceeds the maximum parse value. - Drop—The ACE is to stop load balancing and to discard the packet.
HTTP Persistence Rebalance	Select this check box to indicate that the ACE is to: - Separately load balance each subsequent HTTP request on the same TCP connection. - Insert the header and cookie for every request instead of only the first request. Clear this check box to indicate that this option is disabled. This option is enabled by default.

Table 7-5 HTTP Parameter Map Attributes (continued)

Field	Description
TCP Server Connection Reuse	Select this check box to indicate that the ACE is to reduce the number of open connections on a server by allowing connections to persist and be reused by multiple client connections. If you enable this feature: • Ensure that the ACE maximum segment size (MSS) is the same as the server maximum segment size. • Configure port address translation (PAT) on the interface that is connected to the real server. • Configure on the ACE the same TCP options that exist on the TCP server. • Ensure that each server farm is homogeneous (all real servers within a server farm have identical configurations). Clear this check box to disable this option.
Content Max Parse Length	Enter the maximum number of bytes to parse in HTTP content. Valid entries are integers from 1 to 65535 with a default of 4096.
Header Max Parse Length	Enter the maximum number of bytes to parse for the total length of cookies, HTTP headers, and URLs. Valid entries are integers from 1 to 65535 with a default of 4096.
Secondary Cookie Delimiters	Enter the ASCII-character delimiters to be used to separate cookies in a URL string. Valid entries are unquoted text strings with no spaces and a maximum of 4 characters. The default delimiters are /&#+.
MIME Type to Compress	This option appears for ACE appliances only. In the field on the left, enter the Multipurpose Internet Mail Extension (MIME) type to compress, then click Add. The MIME type appears in the column on the right. To remove or change a MIME type, select it in the column on the right, then click Remove. The selected MIME type appears in the field on the left where you can modify or delete it. To specify the sequence in which compression is to be applied, select MIME types in the column on the right, then click Up or Down to arrange the MIME types. Supported MIME Types, page 7-21 lists the supported MIME types. You can use an asterisk (*) to indicate a wildcard, such as <code>text/*</code>, which would include all text MIME types (text/html, text/plain, and so on).

Draft - CISCO CONFIDENTIAL**Table 7-5 HTTP Parameter Map Attributes (continued)**

Field	Description
User Agent Not to Compress	This option appears for ACE appliances only. A user agent is a client that initiates a request. Examples of user agents include browsers, editors, and other end-user tools. When you specify a user agent string in this field, the ACE does not compress the response to a request when the request contains the matching user agent string. In the field on the left, enter the user agent string to be matched, then click Add. The string appears in the column on the right. To remove or change a user agent string, select it in the column on the right, then click Remove. The selected string appears in the field on the left where you can modify or delete it. To specify the sequence in which strings are to be matched, select strings in the column on the right, then click Up or Down to arrange the strings in the desired sequence. Valid entries are 64 characters.
Minimum Size to Compress	This option appears for ACE appliances only. Enter the threshold at which compression is to occur. The ACE compresses files that are the minimum size or larger. Valid entries are integers from 1 to 4096 bytes.

Step 4 Click:

- **Deploy Now** to deploy this configuration on the ACE.
- **Cancel** to exit this procedure without accepting your entries and to return to the Parameter Map table.
- **Next** to accept your entries and to add another parameter map.

Related Topics

- [Configuring Parameter Maps, page 7-1](#)
- [Configuring Traffic Policies, page 11-1](#)
- [Configuring Parameter Maps, page 7-1](#)
- [Configuring Virtual Contexts, page 3-5](#)

Configuring Optimization Parameter Maps

Optimization parameter maps are available for ACE appliances only.

Optimization parameter maps specify optimization-related commands that pertain to application acceleration and optimization functions performed by the ACE.

Use this procedure to configure an Optimization parameter map for use with a Layer 3/Layer 4 policy map.

Refer to [Configuring Application Acceleration and Optimization, page 12-1](#) or the *Cisco 4700 Series Application Control Engine Appliance Application Acceleration and Optimization Configuration Guide* for more information about application acceleration and optimization.

Procedure

- Step 1** Select **Config > Devices > context > Load Balancing > Parameter Maps > Optimization Parameter Map**. The Optimization Parameter Map table appears.
- Step 2** Click **Add** to add a new parameter map, or select an existing parameter map, then click **Edit** to modify it. The Optimization Parameter Map configuration screen appears.
- Step 3** Configure the parameter map using the information in [Table 7-6](#).

Table 7-6 Optimization Parameter Map Attributes

Field	Description
Parameter Name	Enter a unique name for the parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
Set Browser Freshness Period	Select the method that the ACE is to use to determine the freshness of objects in the client's browser: - N/A—This option is not configured. - Set freshness similar to FlashForward objects—The ACE is to set freshness similar to that used for FlashForwarded objects and to use the values specified in the <i>Maximum Time for Cache Time-to-Live</i> and <i>Minimum Time for Cache Time-to-Live</i> fields. - Disable browser object freshness control—Browser freshness control is not to be used.
Duration for Browser Freshness (seconds)	This field appears if the Set Browser Freshness Period option is not configured. Enter the number of seconds that objects in the client's browser are considered fresh. Valid entries are 0 to 2147483647 seconds.
Response Codes to Ignore	Enter a comma-separated list of HTTP response codes for which the response body must not be read. For example, an entry of 302 indicates that the ACE is to ignore the response body of a 302 (redirect) response from the origin server. Valid entries are unquoted text strings with a maximum of 64 alphanumeric characters and integers from 100 to 599, inclusive.
Allow URL Mapping on non-HTML Files	URL mapping refers to the capability of ACEs to modify URLs and other content in the data stream between the origin server and the client browser. Normally, URL mapping applies only to HTML files unless non-HTML file mapping is enabled. Select this check box to enable URL mapping on files other than HTML files. Clear this check box to indicate that the ACE is not to apply URL mapping to non-HTML files.
Appscope Optimize Rate (%)	Enter the percentage of all requests or sessions to be sampled for performance with acceleration (or optimization) applied. All applicable optimizations for the class will be performed. Valid entries are from 0 to 100 percent, with a default of 10 percent. The sum of this value and the value entered in the Passthru Rate Percent field must not exceed 100.
Appscope Passthrough Rate (%)	Enter the percentage of all requests or sessions to be sampled for performance without optimization. No optimizations for the class will be performed. Valid entries are from 0 to 100, with a default of 10 percent. The sum of this value and the value entered in the Optimize Rate Percent field must not exceed 100.
Max Number for Parameter Summary Log (bytes)	Enter the maximum number of bytes that are to be logged for each parameter value in the parameter summary of a transaction log entry in the statistics log. If a parameter value exceeds this limit, it is truncated at the specified limit. Valid entries are 0 to 10,000 bytes.
Max for POST Data to Scan for Logging (kBytes)	Enter the maximum number of kilobytes of POST data the ACE is to scan for parameters for the purpose of logging transaction parameters in the statistics log. Valid entries are 0 to 1000 KB.

Draft - CISCO CONFIDENTIAL**Table 7-6 Optimization Parameter Map Attributes (continued)**

Field	Description
Specify String for Grouping Requests	Enter the string the ACE is to use to sort requests for AppScope reporting. The string can contain a URL regular expression that defines a set of URLs in which URLs that differ only by their query parameters are to be treated as separate URLs in AppScope reports. For example, to define a string that is used to identify the URLs <code>http://server/catalog.asp?region=asia</code> and <code>http://server/catalog.asp?region=america</code> as two separate reporting categories, you would enter <code>http_query_param(region)</code>. Valid entries contain 1 to 255 characters and can contain the parameter expander functions listed in Table 12-4.
Specify Base File Anonymous Level	Information that is common to a large set of users is generally not confidential or user-specific. Conversely, information that is unique to a specific user or a small set of users is generally confidential or user-specific. The anonymous base file feature enables the ACE to create and deliver condensed base files that contain only information that is common to a large set of users. No information unique to a particular user, or across a very small subset of users, is included in anonymous base files. Enter the value for base file anonymity for the all-user condensation method. Valid entries are integers from 0 to 50; the default value of 0 disables the base file anonymity feature.
Specify Cache-Key Modifier Expression	A cache object key is a unique identifier that is used to identify a cached object to be served to a client, replacing a trip to the origin server. The cache key modifier feature allows you to modify the canonical form of a URL; that is, the portion before “?” in a URL. For example, the canonical URL of “<code>http://www.xyz.com/somepage.asp?action=browse&level=2</code>” is “<code>http://www.xyz.com/somepage.asp</code>”. Enter a regular expression containing embedded variables as described in Table 12-4. The ACE transforms URLs specified in class maps for this virtual server with the expression and variable entered here. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. If the string includes spaces, enclose the string with quotation marks (“”).
Maximum Time for Cache Time-to-Live (seconds)	Enter the maximum number of seconds that an object without an explicit expiration time should be considered fresh in the ACE cache. Valid entries are 0 to 2147483647 seconds.
Minimum Time for Cache Time-to-Live (seconds)	Enter the minimum number of seconds that an object without an explicit expiration time should be considered fresh in the ACE cache. This value specifies the minimum time that content can be cached. If the ACE is configured for FlashForward optimization, this value should normally be 0. If the ACE is configured for dynamic caching, this value should indicate how long the ACE should cache the page. (See Table 4-16 for information about these configuration options.) Valid entries are 0 to 2147483647 seconds.
Cache Time-to-Live Duration (%)	Enter the percent of an object’s age at which an embedded object without an explicit expiration time is considered fresh. Valid entries are 0 to 100 percent.

Table 7-6 Optimization Parameter Map Attributes (continued)

Field	Description
Expression to Modify Cache Key Query Parameter	The cache parameter feature allows you to modify the query parameter of a URL; that is, the portion after “?” in a URL. For example, the query parameter portion of “http://www.xyz.com/somepage.asp?action=browse&level=2” is “action=browse&level=2”. Enter a regular expression containing embedded variables as described in Table 12-4. The ACE transforms URLs specified in class maps for this virtual server with the expression and variable entered here. If no string is specified, the query parameter portion of the URL is used as the default value for this portion of the cache key. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters.
Canonical URL Expressions	The ACE uses the canonical URL feature to eliminate the “?” and any characters that follow to identify the general part of the URL. This general URL is then used to create the base file. In this way, the ACE maps multiple URLs to a single canonical URL. Enter a comma-separated list of parameter expander functions as defined in Table 12-4 to identify the URLs to associate with this parameter map. Valid entries are unquoted text strings with a maximum of 255 alphanumeric characters.
Enable Cacheable Content Optimization	This feature allows the ACE to detect content that can be cached and perform delta optimization on it. Select the check box to enable delta optimization of content that can be cached. Clear the check box to disable this feature.
Enable Delta Optimization on First Visit to Web Page	Select the check box to enable condensation on the first visit to a Web page. Clear the check box to disable this feature.
Minimum page size for Delta Optimization (bytes)	Enter the minimum page size, in bytes, that can be condensed. Valid entries are integers from 1 to 250000 bytes.
Maximum page size for Delta Optimization (bytes)	Enter the maximum page size, in bytes, that can be condensed. Valid entries are integers from 1 to 250000 bytes.
Set Default Client Script	Indicate the scripting language that the ACE is to recognize on condensed content pages: • N/A—This option is not configured. • Javascript—The default scripting language is JavaScript. • Visual Basic Script—The default scripting language is Visual Basic.
Exclude Iframes from Delta Optimization	Select the check box to indicate that delta optimization is not to be applied to IFrames (inline frames). Clear the check box to indicate that delta optimization is to be applied to IFrames.
Exclude Non-ASCII Data from Delta Optimization	Select the check box to indicate that delta optimization is not to be applied to non-ASCII data. Clear the check box to indicate that delta optimization is to be applied to non-ASCII data.
Exclude JavaScripts from Delta Optimization	Select the check box to indicate that delta optimization is not to be applied to JavaScript. Clear the check box to indicate that delta optimization is to be applied to JavaScript.

Draft - CISCO CONFIDENTIAL**Table 7-6 Optimization Parameter Map Attributes (continued)**

Field	Description
MIME Types to Exclude from Delta Optimization	1. In the first field, enter a comma-separated list of the MIME (Multipurpose Internet Mail Extension) type messages that are not to have delta optimization applied, such as image/Jpeg, text/html, application/msword, or audio/mpeg. See Supported MIME Types, page 7-21 for a list of supported MIME types. 2. Click Add to add the entry to the list box on the right. You can position the entries in the list box by using the Up and Down buttons.
Remove HTML META Elements from Documents	Select the check box to indicate that HTML META elements are to be removed from documents to prevent them from being condensed. Clear the check box to indicate that HTML META elements are not to be removed from documents.
Set FlashForward Refresh Policy	Select the method the ACE is to use to refresh stale embedded objects: • N/A—This option is not configured. • Allow FlashForward to indirect refresh of objects—The ACE is to use FlashForward to indirectly refresh embedded objects. • Bypass FlashForward to direct refresh of objects—The ACE is to bypass FlashForward for stale embedded objects so that they are refreshed directly.
Rebase Delta Optimization Threshold (%)	Enter the delta threshold, expressed as a percent, when rebasing is to be triggered. This entry represents the size of a page delta relative to total page size, expressed as a percent. This entry triggers rebasing when the delta response size exceeds the threshold as a percentage of base file size. Valid entries are 0 to 10000 percent.
Rebase FlashForward Threshold (%)	Enter the threshold, expressed as a percent, when rebasing is to be triggered based on the percent of FlashForwarded URLs in the response. This entry triggers rebasing when the difference between the percentages of FlashForwarded URLs in the delta response and the base file exceeds the threshold. Valid entries are 0 to 10000 percent.
Rebase History Size (pages)	Enter the number of pages to be stored before the ACE resets all rebase control parameters to zero and starts over. This option prevents the base file from becoming too rigid. Valid entries are 10 to 2147483647.
Rebase Modify Cool-off Period (seconds)	Enter the number of seconds after the last modification before performing a rebase. Valid entries are 1 to 14400 seconds (4 hours).
Rebase Reset Period (seconds)	Enter the period of time, in seconds, for performing a meta data refresh. Valid entries are 1 to 900 seconds (15 minutes).
Override Client Request Headers	Indicate how the ACE is to handle client request headers (primarily for embedded objects): • N/A—This feature is not enabled. • All cache request headers are ignored—The ACE is to ignore all cache request headers. • Overrides the Cache-Control: no cache HTTP header from a request—The ACE is to ignore cache control request headers that state <i>no cache</i>.

Table 7-6 Optimization Parameter Map Attributes (continued)

Field	Description
Override Server Response Headers	Indicate how the ACE is to handle origin server response headers (primarily for embedded objects): • N/A—This feature is not enabled. • All cache response headers are ignored—The ACE is to ignore all response headers. • Overrides the Cache-Control: private HTTP header from a response—The ACE is to ignore cache control response headers that state <i>private</i>.
UTF-8 Character Set Threshold	The UTF-8 (8-bit Unicode Transformation Format) character set is an international standard that allows Web pages to display non-ASCII or non-English multibyte characters. It can represent any universal character in the Unicode standard and is backwards compatible with ASCII. Enter the number of UTF-8 characters that need to appear on a page to constitute a UTF-8 character set page. Valid entries are integers from 1 to 1,000,000.
Hosts Limit for FlashConnect	FlashConnect dynamically renames embedded objects by adding a prefix and changing the hostname so that the objects appear to reside on different hosts. FlashConnect then has the browser open a separate connection to the origin server for each object and retrieve the objects in parallel instead of sequentially. Enter the maximum number of artificial hosts that FlashConnect can create for retrieving embedded objects. Valid entries are integers from 0 to 99.
Server Load Threshold Trigger (%)	The server load threshold trigger indicates that the time-to-live (TTL) period for cached objects is to be based dynamically on server load. With this method, TTL periods increase if the current response time from the origin sever is greater than the average response time and decrease if the current response time from the origin server is less than the average response time when the difference in response times exceeds a specified threshold amount. Enter the threshold, expressed as a percent, at which the TTL for cached objects is to be changed. Valid entries are from 0 to 100 percent.
Server Load Time-to-Live Change (%)	This option specifies the percentage by which the cache TTL is increased or decreased in response to a change in server load. For example, if this value is set to 20 and the current TTL for a response is 300 seconds, and if the current server response times exceeds the trigger threshold, the cache TTL for the response is raised to 360 seconds. Enter the percent by which the cache TTL is to be increased or decreased when the server load threshold trigger is met. Valid entries are from 0 to 100 percent.
Enable XSLT Merge Debug	Select the check box to enable the XSLT merge debug function. Clear the check box to disable the XSLT merge debug function.
Specify XSLT Stylesheet for PreTransform	Enter the URL of an XSLT style sheet to indicate that the ACE is to perform a pretransformation of the style sheet.
Specify XSLT Stylesheet for XSLT Merge	Enter the URL of an XSLT style sheet to force the use of this style sheet, regardless of any XSL specified in the XML source file.

Draft - CISCO CONFIDENTIAL**Table 7-6 Optimization Parameter Map Attributes (continued)**

Field	Description
Specify Delta Optimization Mode	Select the method by which delta optimization is to be implemented: • N/A—This option is not configured. • Enable all-user mode for delta optimization—The ACE is to generate the delta against a single base file that is shared by all users of the URL. This option is usable in most cases if the structure of a page is common across all users, and the disk space overhead is minimal. • Enable the per-user mode for delta optimization—The ACE is to generate the delta against a base file that is created specifically for that user. This option is useful when page contents, including layout elements, are different for each user, and delivers the highest level of condensation. However, this increases disk space requirements because a copy of the base page that is delivered to each user is cached. This option is useful when privacy is required because base pages are not shared among users.
Smooth Transform of Image	Select the check box to indicate that the ACE is to apply a smoothing transformation to images, if needed. Clear the check box to indicate that the ACE is not to apply a smoothing transformation to images.
Ignore Thumbnail Images	Select the check box to indicate that the ACE is to ignore small thumbnail images without transforming them in any way. Clear the check box to indicate that the ACE is not to ignore thumbnail images.
Progressive Rendering of Image	Select the check box to indicate that the ACE is to transform images so that they are rendered progressively by the browser. When enabled, this feature results in slightly larger image sizes. Because images render progressively, this feature might not be useful in fast networking environments, such as LANs. Clear the check box to indicate that the ACE is not to transform images so that they are rendered progressively by the browser.
High Quality Transform of Image	Select the check box to indicate that the ACE is to apply higher quality transformation with less compression to images. When enabled, this option results in images that are larger than those compressed without this option, but they have less visual deterioration. Image size is smaller with this option than for uncompressed images. Clear the check box to indicate that the ACE is not to apply higher quality transformation to images.
Grayscale Transform of Image	Select the check box to indicate that the ACE is to optimize images by transforming JPEG and PNG images to grayscale images. Clear the check box to indicate that the ACE is not to optimize images by transforming JPEG and PNG images to grayscale images.
String To Be Used for Server HTTP Header	Use this option to define a string that is to be sent in the server header for an HTTP response. This option provides you with a method for uniquely tagging the context or URL match statement by setting the server header value to a particular string. The server header string can be used when a particular URL is not being transmitted to the correct target context or match statement. Enter the string that is to appear in the server header. Valid entries are quoted text strings with a maximum of 64 alphanumeric characters.

Step 4 Click:

- **Deploy Now** to save your entries. The ACE validates the parameter map configuration and deploys it.
- **Cancel** to exit this procedure without accepting your entries and to return to the Parameter Map table.
- **Next** to accept your entries and to add another parameter map.

Related Topics

- [Configuring Parameter Maps, page 7-1](#)
- [Configuring Traffic Policies, page 11-1](#)
- [Configuring Parameter Maps, page 7-1](#)
- [Configuring Virtual Contexts, page 3-5](#)

Configuring RTSP Parameter Maps

RTSP parameter maps are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.

RTSP parameter maps allow you to configure advanced RTSP behavior for server load-balancing connections.

Use this procedure to configure an [RTSP](#) parameter map.

Procedure

- Step 1** Select **Config > Devices > context > Load Balancing > Parameter Maps > RTSP Parameter Map**. The RTSP Parameter Map table appears.
- Step 2** Click **Add** to add a new parameter map, or select an existing parameter map, then click **Edit** to modify it. The Parameter Maps configuration screen appears.
- Step 3** Configure the parameter map using the information in [Table 7-7](#).

Table 7-7 *RTSP Parameter Map Attributes*

Field	Description
Parameter Name	Enter a unique name for the parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
Case-insensitive	Select this check box to indicate that the ACE is to be case insensitive. Clear this check box to indicate that the ACE is to be case sensitive.
Header Max Parse Length	Enter the number of bytes to parse for the total length of RTSP headers. Valid entries are integers from 1 to 65535 with a default of 2048 bytes.

Draft - CISCO CONFIDENTIAL**Step 4** Click:

- **Deploy Now** to deploy this configuration.
- **Cancel** to exit this procedure without saving your entries and to return to the RTSP Parameter Map table.
- **Next** to deploy your entries and to configure another RTSP parameter map.

Related Topics

- [Configuring Parameter Maps, page 7-1](#)
- [Configuring Traffic Policies, page 11-1](#)
- [Configuring Parameter Maps, page 7-1](#)
- [Configuring Virtual Contexts, page 3-5](#)

Configuring SIP Parameter Maps

SIP parameter maps are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.

[SIP](#) parameter maps allow you to configure SIP deep-packet inspection policy maps on the ACE.

Use this procedure to configure a SIP parameter map.

Procedure

- Step 1** Select **Config > Devices > context > Load Balancing > Parameter Maps > SIP Parameter Map**. The SIP Parameter Map table appears.
- Step 2** Click **Add** to add a new parameter map, or select an existing parameter map, then click **Edit** to modify it. The Parameter Maps configuration screen appears.
- Step 3** Configure the parameter map using the information in [Table 7-8](#).

Table 7-8 *SIP Parameter Map Attributes*

Field	Description
Parameter Name	Enter a unique name for the parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
Instant Messaging	Select the check box to enable instant messaging (IM) over SIP after it has been disabled. Clear this check box to disable this feature.
Max Forward Validation	This option allows you to configure the ACE to validate the value of the Max-Forward header field. Specify how the ACE is to handle the validation of Max-Forward header fields: • N/A—The ACE is not to validate Max-Forward header fields. • Drop—The ACE is to drop the SIP message if it does not pass Max-Forward header validation. • Reset—The ACE is to reset the SIP connection if it does not pass Max-Forward header validation.

Table 7-8 **SIP Parameter Map Attributes (continued)**

Field	Description
Log Max Forward Validation Event	Select the check box to indicate that the ACE is to log Max-Forward validation events. Clear the check box to disable this feature.
Mask UA Software Version	If the software version of a user agent is exposed, that user agent might be vulnerable to attacks from hackers who exploit the security holes present in that particular software version. This option allows you to mask or log the user agent software version so that it is not exposed. Select the check box to indicate that the ACE is to mask the user agent software version. Clear the check box to disable this feature.
Log UA Software Version	Select the check box to indicate that the ACE is to log the user agent software version. Clear the check box to disable this feature.
Strict Header Validation	You can ensure the validity of SIP packet headers by configuring the ACE to check for the presence of the following mandatory SIP header fields: • From • To • Call-ID • CSeq • Via • Max-Forwards If one of the header fields is missing in a SIP packet, the ACE considers that packet invalid. The ACE also checks for forbidden header fields, according to RFC 3261. Specify how the ACE is to handle header validation. • N/A—The ACE is not to perform header validation. • Drop—The ACE is to drop the SIP message if the SIP packet does not pass header validation. • Reset—The ACE is to reset the connection if the SIP packet does not pass header validation.
Log Strict Header Validation	Select the check box to indicate that the ACE is to log header validation events. Clear the check box to disable this feature.
Mask non-SIP URI	This option and the next enable the detection of non-SIP URIs in SIP messages. Select the check box to indicate that the ACE is to mask non-SIP URIs in SIP messages. Clear the check box to disable this feature.
Log non-SIP URI	Select the check box to indicate that the ACE is to log non-SIP URIs in SIP messages. Clear the check box to disable this feature.
SIP Media Pinhole Timeout	Specify the timeout period for SIP media pinhole (secure port) connections in seconds. Valid entries are integers from 1 to 65535 seconds. Default is 5.

Draft - CISCO CONFIDENTIAL**Step 4** Click:

- **Deploy Now** to deploy this configuration.
- **Cancel** to exit this procedure without saving your entries and to return to the SIP Parameter Map table.
- **Next** to deploy your entries and to configure another SIP parameter map.

Related Topics

- [Configuring Parameter Maps, page 7-1](#)
- [Configuring Traffic Policies, page 11-1](#)
- [Configuring Parameter Maps, page 7-1](#)
- [Configuring Virtual Contexts, page 3-5](#)

Configuring Skinny Parameter Maps

Skinny parameter maps are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.

Skinny Client Control Protocol ([SCCP](#) or [Skinny](#)) parameter maps allow you to configure SCCP packet inspection on the ACE.

Use this procedure to configure a Skinny parameter map.

Procedure

-
- Step 1** Select **Config > Devices > context > Load Balancing > Parameter Maps > Skinny Parameter Map**. The Skinny Parameter Map table appears.
- Step 2** Click **Add** to add a new parameter map, or select an existing parameter map, then click **Edit** to modify it. The Parameter Maps configuration screen appears.
- Step 3** Configure the parameter map using the information in [Table 7-9](#).

Table 7-9 *Skinny Parameter Map Attributes*

Field	Description
Parameter Name	Enter a unique name for the parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
Enforce Registration	You can configure the ACE to allow only registered Skinny clients to make calls. To accomplish this task, the ACE maintains the state of each Skinny client. After a client registers with CCM , the ACE opens a secure port (pinhole) to allow that client to make a call. Select the check box to enable Skinny registration enforcement. Clear the check box to disable this feature.
Message Id Max	Enter the largest value for the station message ID in hexadecimal that the ACE is to accept. Valid entries are hexadecimal values from 0 to 4000 with a default value of 0x181. If a packet arrives with a station message ID greater than the specified value, the ACE drops the packet and generates a syslog message.

Table 7-9 *Skinny Parameter Map Attributes (continued)*

Field	Description
SCCP Prefix Length Max	This feature allows you to configure the ACE so that it checks the maximum SCCP prefix length. The ACE drops Skinny message packets that fail this check and generates a syslog message. Enter the maximum SCCP prefix length in bytes. Valid entries are integers from 4 to 4000 bytes.
SCCP Prefix Length Min	By default, the ACE drops SCCP messages that have an SCCP Prefix length that is less than the message ID. The ACE drops Skinny message packets that fail this check and generates a syslog message. Enter the minimum SCCP prefix length in bytes. Valid entries are integers from 4 to 4000 bytes.

Step 4 Click:

- **Deploy Now** to deploy this configuration.
- **Cancel** to exit this procedure without saving your entries and to return to the Skinny Parameter Map table.
- **Next** to deploy your entries and to configure another Skinny parameter map.

Related Topics

- [Configuring Parameter Maps, page 7-1](#)
- [Configuring Traffic Policies, page 11-1](#)
- [Configuring Parameter Maps, page 7-1](#)
- [Configuring Virtual Contexts, page 3-5](#)

Supported MIME Types

The ACE supports following MIME types:

- application/msexcel
- application/mspowerpoint
- application/msword
- application/octet-stream
- application/pdf
- application/postscript
- application/x-gzip
- application/x-java-archive
- application/x-java-vm
- application/x-messenger
- application/zip

Draft - CISCO CONFIDENTIAL

- audio/*
- audio/basic
- audio/midi
- audio/mpeg
- audio/x-adpcm
- audio/x-aiff
- audio/x-ogg
- audio/x-wav
- image/*
- image/gif
- image/jpeg
- image/png
- image/tiff
- image/x-3ds
- image/x-bitmap
- image/x-niff
- image/x-portable-bitmap
- image/x-portable-greymap
- image/x-xpm
- text/*
- text/css
- text/html
- text/plain
- text/richtext
- text/sgml
- text/xmcd
- text/xml
- video/*
- video/flc
- video/mpeg
- video/quicktime
- video/sgi
- video/x-fli



Draft - CISCO CONFIDENTIAL

CHAPTER 8

Configuring SSL

Revised Date: 3/25/09

This topic describes the steps required to configure your ACE (both the ACE module and the ACE appliance) as a virtual Secure Sockets Layer (SSL) server for SSL initiation or termination. The topics included in this section are:

- [SSL Overview, page 8-1](#)
- [SSL Configuration Prerequisites, page 8-2](#)
- [Summary of SSL Configuration Steps, page 8-3](#)
- [SSL Setup Sequence, page 8-4](#)
- [Using SSL Certificates, page 8-5](#)
- [Using SSL Keys, page 8-8](#)
- [Configuring SSL Parameter Maps, page 8-15](#)
- [Configuring SSL Chain Group Parameters, page 8-18](#)
- [Configuring SSL CSR Parameters, page 8-19](#)
- [Generating CSRs, page 8-21](#)
- [Configuring SSL Proxy Service, page 8-22](#)
- [Enabling Client Authentication, page 8-23](#)

SSL Overview

SSL is an application-level protocol that provides encryption technology for the Internet, ensuring secure transactions such as the transmission of credit card numbers for e-commerce Web sites. SSL initiation occurs when the ACE device (either an ACE module or an ACE appliance) acts as a client and initiates the SSL session between it and the SSL server. SSL termination occurs when the ACE, acting as an SSL server, terminates an SSL connection from a client and then establishes a TCP connection to an HTTP server.

SSL provides the secure transaction of data between a client and a server through a combination of privacy, authentication, and data integrity. SSL relies upon certificates and private-public key exchange pairs for this level of security.

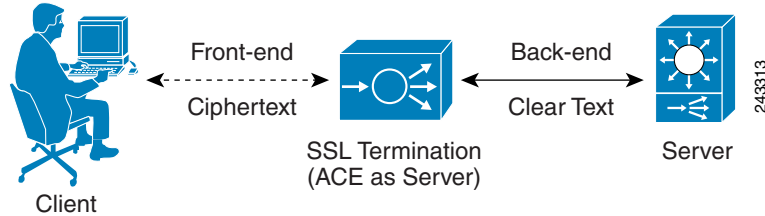
[Figure 8-1](#) shows the following network connections in which the ACE terminates the SSL connection with the client:

- Client to ACE—SSL connection between a client and the ACE acting as an SSL proxy server

Draft - CISCO CONFIDENTIAL

- ACE to Server—TCP connection between the ACE and the HTTP server

Figure 8-1 *SSL Termination with Client*
SSL Termination with a Client



The ACE uses parameter maps, SSL proxy services, and class maps to build the policy maps that determine the flow of information between the client, the ACE, and the server. SSL termination is a Layer 3 and Layer 4 application because it is based on the destination IP addresses of the inbound traffic flow from the client. For this type of application, you create a Layer 3 and Layer 4 policy map that the ACE applies to the inbound traffic.

If you need to delete any of the SSL objects (authorization groups, chain groups, parameter maps, keys, CRLs, or certificates), you must remove the dependency from within the proxy service first before removing the SSL object.

Before configuring the ACE for SSL, see [SSL Configuration Prerequisites, page 8-2](#).

SSL Configuration Prerequisites

Before configuring your ACE for SSL operation, you must first ensure:

- Your ACE hardware is configured for server load balancing (SLB).



Note

During the real server and server farm configuration process, when you associate a real server with a server farm, ensure that you assign an appropriate port number for the real server. The default behavior by the ACE is to automatically assign the same destination port that was used by the inbound connection to the outbound server connection if you do not specify a port.

- Your policy map is configured to define the SSL session parameters and client/server authentication tools, such as the certificate and RSA key pair.
- Your class map is associated with the policy map to define the virtual SSL server IP address that the destination IP address of the inbound traffic must match.
- You must import a digital certificate and its corresponding public and private key pair to the desired ACE context.
- At least one SSL certificate is available.
- If you do not have a certificate and corresponding key pair, you can generate an [RSA](#) key pair and a *certificate signing request (CSR)*. Create a CSR when you need to apply for a certificate from a *certificate authority (CA)*. The CA signs the CSR and returns the authorized digital certificate to you.

**Note**

You cannot generate a CSR in Building Blocks (**Config > Global > All Building Blocks**); SSL CSR generation is available only in virtual context configuration.

Summary of SSL Configuration Steps

Table 8-1 describes the steps for using SSL keys and certificates.

Table 8-1 *SSL Key and Certificate Procedure Overview*

Task	Description
Create an SSL parameter map.	Create an SSL parameter map to specify the options that apply to SSL sessions such as the method to be used to close SSL connections, the cipher suite, and version of SSL or TLS. See Configuring SSL Parameter Maps, page 8-15 .
Create an SSL key pair file.	Create an SSL RSA key pair file to generate a CSR, create a digital signature, and encrypt packet data during the SSL handshake with an SSL peer. See Generating SSL Key Pairs, page 8-11 .
Configure CSR parameters.	Set CSR parameters to define the distinguished name attributes of a CSR. See Configuring SSL CSR Parameters, page 8-19 .
Create a CSR.	Create a CSR to submit with the key pair file when you apply for an SSL certificate. See Generating CSRs, page 8-21 .
Copy and paste the CSR into the Certificate Authority (CA) Web-based application or e-mail the CSR to the CA.	Using the SSL key pair and CSR, apply for an approved certificate from a Certificate Authority. Use the method specified by the CA for submitting your request.
Save the approved certificate from the CA in its received format on an FTP, SFTP, or TFTP server.	When you receive the approved certificate, save it in the format in which it was received on a network server accessible via FTP, SFTP, or TFTP.
Import the approved certificate and key pair into the desired virtual context.	Import the approved certificate and the associated SSL key pair into the appropriate context using ANM. See: • Importing SSL Certificates, page 8-6 • Importing SSL Key Pairs, page 8-9

Draft - CISCO CONFIDENTIAL**Table 8-1 SSL Key and Certificate Procedure Overview (continued)**

Task	Description
Confirm that the public key in the key pair file matches the public key in the certificate file.	Examine the contents of the files to confirm that the key pair information is the same in both the key pair file and the certificate file.
Configure the virtual context for SSL.	See Configuring Traffic Policies, page 11-1 .
Configure authorization group.	Create a group of certificates that are trusted as certificate signers by creating an authentication group. See Configuring SSL Authentication Groups, page 8-24 .
Configure CRL.	See Configuring CRLs for Client Authentication, page 8-25 .

For more information about using SSL with ACE, see the *Cisco 4700 Series Application Control Engine Appliance SSL Configuration Guide* or *Cisco Application Control Engine Module SSL Configuration Guide*.

SSL Setup Sequence

The SSL setup sequence provides detailed instructions with illustrations for configuring SSL on ACE devices from ANM ([Figure 8-2](#)). The purpose of this option is to provide a visual guide for performing typical SSL operations, like SSL CSR generation, SSL proxy creation, and so on. This option does not replace any existing SSL functions or configuration screens already present in ANM. It is only intended as an additional guide for anyone unfamiliar or unclear with the SSL operations that need to be performed on the ACE device. From the SSL setup sequence, you are allowed to configure all SSL operations, without duplicating the edit/delete/table/view operations that the other SSL configuration screens provide.

The purpose of this option is to provide details about typical SSL flows and the operations involved in doing typical SSL operations, including the following:

- SSL Import/Create Keys
- SSL Import Certificates
- SSL CSR generation
- SSL proxy creation

For more information on SSL configuration features, see [Summary of SSL Configuration Steps](#).

Figure 8-2 *SSL Setup Sequence*



Related Topics

- [Configuring SSL, page 8-1](#)
- [Importing SSL Certificates, page 8-6](#)
- [Importing SSL Key Pairs, page 8-9](#)
- [Configuring SSL Parameter Maps, page 8-15](#)
- [Configuring SSL Chain Group Parameters, page 8-18](#)
- [Configuring SSL Proxy Service, page 8-22](#)

Using SSL Certificates

Digital certificates and key pairs are a form of digital identification for user authentication. Certificate Authorities issue certificates that attest to the validity of the public keys they contain. A client or server certificate includes the following identification attributes:

- Name of the Certificate Authority and Certificate Authority digital signature
- Name of the client or server (the certificate subject) that the certificate authenticates
- Issuer
- Time stamps that indicate the certificate's start date
- Time stamps that indicate the certificate's expiration date
- CA certificate

A Certificate Authority has one or more signing certificates that it uses for creating SSL certificates and certificate revocation lists (CRL). Each signing certificate has a matching private key that is used to create the Certificate Authority signature. The Certificate Authority makes the signing certificates (with the public key embedded) available to the public, enabling anyone to access and use the signing certificates to verify that an SSL certificate or CRL was actually signed by a specific Certificate Authority.

All certificates have an expiration date, usually one year after the certificate was issued. You can monitor certificate expiration status by going to **Monitor > Alarm Notifications > Threshold Groups**. ANM will issue a warning email daily before the certificate expiration date (See [Configuring Alarm Notifications, page 14-25](#)). You establish how many days before the expiration date that the warning email messages begin in the Threshold Groups settings page.

Step 1 Select **Monitor > Alarm Notifications > Threshold Groups**, then click **Add**.

Draft - CISCO CONFIDENTIAL

ACE require certificates and corresponding key pairs for:

- SSL termination—The ACE acts as an SSL proxy server and terminates the SSL session between it and the client. For SSL termination, you must obtain a server certificate and corresponding key pair.
- SSL initiation—The ACE acts as a client and initiates the SSL session between it and the SSL server. For SSL initiation, you must obtain a client certificate and corresponding key pair.

Related Topics

- [Configuring SSL, page 8-1](#)
- [Exporting SSL Certificates, page 8-12](#)
- [Importing SSL Certificates, page 8-6](#)
- [Using SSL Keys, page 8-8](#)
- [Importing SSL Key Pairs, page 8-9](#)
- [Configuring SSL CSR Parameters, page 8-19](#)
- [Generating CSRs, page 8-21](#)

Importing SSL Certificates

Use this procedure to import SSL certificates.

Assumptions

- You have configured the ACE for server load balancing. (See [Load Balancing Overview, page 4-1](#).)
- You have obtained an SSL certificate from a certificate authority (CA) and have placed it on a network server accessible by the ACE.



Note You cannot import SSL certificates in Building Blocks (**Config > Global > All Building Blocks**); SSL certificate imports are available only in virtual context configuration.

Procedure

- Step 1** To configure a virtual context, select **Config > Devices > context > SSL > Certificates**.
The Certificates table appears, listing any valid SSL certificates.
- Step 2** Click **Import**. The Import dialog box appears.
- Step 3** Enter the information in [Table 8-2](#).

Table 8-2 *SSL Certificate Management Import Attributes*

Field	Description
Protocol	Specify the method to be used for accessing the network server: - FTP—Indicates that FTP is to be used to access the network server when importing the SSL certificate. - TFTP—Indicates that TFTP is to be used to access the network server when importing the SSL certificate. - SFTP—Indicates that SFTP is to be used to access the network server when importing the SSL certificate. - TERMINAL—Indicates that you will import the file using cut and paste by pasting the certificate information to the terminal display. You can use the terminal method to display only PEM files, which are in ASCII format.
IP Address	This field appears for FTP, TFTP, and SFTP. Enter the IP address of the remote server on which the SSL certificate file resides.
Remote Filename	This field appears for FTP, TFTP, and SFTP. Enter the directory and filename of the certificate file on the network server.
Local Filename	Enter the filename to be used for the SSL certificate file when it is imported to the ACE.
Username	This field appears for FTP and SFTP. Enter the name of the user account on the network server.
Password	This field appears for FTP and SFTP. Enter the password for the user account on the network server.
Confirm	This field appears for FTP and SFTP. Reenter the password.
Passphrase	This field appears for FTP, SFTP, and TERMINAL. Enter the passphrase that was created with the file. Without this phrase, you cannot use the file. Passphrases are used only with encrypted PEM and PKCS files.
Confirm	This field appears for FTP, SFTP, and TERMINAL. Reenter the passphrase.
Nonexportable	The ability to export SSL certificates allows you to copy signed certificates to another server on your network so that you can then import them onto another ACE or Web server. Exporting is similar to copying in that the original files are not deleted. Select the check box to indicate that this certificate file cannot be exported from the ACE.
Import Text	This field appears for Terminal. Cut the certificate information from the remote server and paste it into this field.

Draft - CISCO CONFIDENTIAL**Step 4** Click:

- **OK** to accept your entries and to return to the Certificates table. ANM updates the Certificates table with the newly installed certificate.
 - **Cancel** to exit this procedure without saving your entries and to return to the Certificates table.
-

Related Topics

- [Configuring SSL, page 8-1](#)
- [Using SSL Keys, page 8-8](#)
- [Importing SSL Key Pairs, page 8-9](#)
- [Configuring SSL Parameter Maps, page 8-15](#)
- [Configuring SSL Chain Group Parameters, page 8-18](#)
- [Configuring SSL CSR Parameters, page 8-19](#)
- [Configuring SSL Proxy Service, page 8-22](#)

Using SSL Keys

The ACE and its peer use a public key cryptographic system named Rivest, Shamir, and Adelman Signatures (RSA) for authentication during the SSL handshake to establish an SSL session. The RSA system uses *key pairs* that consist of a public key and a corresponding private (secret) key. During the handshake, the RSA key pairs encrypt the session key that both devices will use to encrypt the data that follows the handshake.

Use this procedure to view options for working with SSL and SSL keys.

Procedure**Step 1** Select the item to configure:

- To configure a virtual context, select **Config > Devices > context > SSL > Keys**.
- To configure a building block, select **Config > Global > building_block > SSL > Keys**.

The Keys table appears.

Step 2 Continue with one of the following options:

- Generate a key pair—See [Generating SSL Key Pairs, page 8-11](#).
 - Import a key pair—See [Importing SSL Key Pairs, page 8-9](#).
 - Export a key pair—See [Exporting SSL Key Pairs, page 8-14](#).
 - Generate a CSR—See [Generating CSRs, page 8-21](#).
-

Related Topics

- [Generating SSL Key Pairs, page 8-11](#)
- [Importing SSL Key Pairs, page 8-9](#)
- [Generating SSL Key Pairs, page 8-11](#)

- [Exporting SSL Key Pairs, page 8-14](#)
- [Configuring SSL, page 8-1](#)

Importing SSL Key Pairs

Use this procedure to import an SSL key pair file.

Assumptions

- You have configured the ACE for server load balancing. (See [Load Balancing Overview, page 4-1.](#))
- You have obtained an SSL key pair from a certificate authority (CA) and have placed the pair on a network server accessible by the ACE.

Procedure

- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > context > SSL > Keys.**
 - To configure a building block, select **Config > Global > building_block > SSL > Keys.**
- The Keys table appears, listing existing SSL keys.
- Step 2** Click **Import**. The Import dialog box appears.
- Step 3** Enter the information in [Table 8-3](#).

Table 8-3 *SSL Key Pair Import Attributes*

Field	Description
Protocol	Specify the method to be used for accessing the network server: • FTP—Indicates that FTP is to be used to access the network server when importing the SSL key pair file. • TFTP—Indicates that TFTP is to be used to access the network server when importing the SSL key pair file. • SFTP—Indicates that SFTP is to be used to access the network server when importing the SSL key pair file. • TERMINAL—Indicates that you will import the file using cut and paste by pasting the certificate and key pair information to the terminal display. You can use the terminal method to display only PEM files, which are in ASCII format.
IP Address	This field appears for FTP, TFTP, and SFTP. Enter the IP address of the remote server on which the SSL key pair file resides.
Remote Filename	This field appears for FTP, TFTP, and SFTP. Enter the directory and filename of the key pair file on the network server.
Local Filename	Enter the filename to be used for the SSL key pair file when it is imported to the ACE.

Draft - CISCO CONFIDENTIAL**Table 8-3** *SSL Key Pair Import Attributes (continued)*

Field	Description
Username	This field appears for FTP and SFTP. Enter the name of the user account on the network server.
Password	This field appears for FTP and SFTP. Enter the password for the user account on the network server.
Confirm	This field appears for FTP, SFTP, and TERMINAL. Reenter the password.
Passphrase	This field appears for FTP, SFTP, and TERMINAL. Enter the passphrase that was created with the file. Without this phrase, you cannot use the file. Passphrases are used only with encrypted PEM and PKCS files.
Confirm	This field appears for FTP and SFTP. Reenter the passphrase.
Nonexportable	The ability to export SSL key pair files allows you to copy key pair files to another server on your network so that you can then import them onto another ACE or Web server. Exporting is similar to copying in that the original files are not deleted. Select the check box to indicate that this key pair file cannot be exported from the ACE. Clear the check box to indicate that this key pair file can be exported from the ACE.
Import Text	This field appears for Terminal. Cut the key pair information from the remote server and paste it into this field.

Step 4 Click:

- **OK** to accept your entries and to return to the Keys table. ANM updates the Keys table with the imported key pair file information.
- **Cancel** to exit this procedure without saving your entries and to return to the Keys table.

Related Topics

- [Configuring SSL, page 8-1](#)
- [Importing SSL Certificates, page 8-6](#)
- [Configuring SSL Parameter Maps, page 8-15](#)
- [Configuring SSL Chain Group Parameters, page 8-18](#)
- [Configuring SSL CSR Parameters, page 8-19](#)
- [Configuring SSL Proxy Service, page 8-22](#)

Generating SSL Key Pairs

If you do not have any matching key pairs, you can use ANM to generate a key pair.

Use this procedure to generate SSL RSA key pairs.

Procedure

- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > context > SSL > Keys**.
 - To configure a building block, select **Config > Global > building_block > SSL > Keys**.

The Keys table appears.

- Step 2** Click **Add** to add a new key pair. The Keys configuration screen appears.



Note You cannot modify an existing entry in the Keys table. Instead, delete the existing entry, then add a new one.

- Step 3** Enter the information in [Table 8-4](#).

Table 8-4 Key Attributes

Field	Description
Name	Enter the name of the SSL key pair. Valid entries are alphanumeric strings up to 64 characters.
Size	Select the key pair security strength. The number of bits in the key pair file defines the size of the RSA key pair used to secure Web transactions. Longer keys produce more secure implementations by increasing the strength of the RSA security policy. Options and their relative levels of security are: • 1024—High security, level 1 • 1536—High security, level 2 • 2048—High security, level 3 • 512—Least security • 768—Normal security
Type	RSA is a public-key cryptographic system used for authentication.
Exportable Key	Select the check box to indicate that the key pair file can be exported. Clear the check box to indicate that the key pair file cannot be exported.

- Step 4** Click:
- **Deploy Now** to deploy this configuration on the ACE.
 - **Cancel** to exit this procedure without saving your entries and to return to the Keys table.
 - **Next** to deploy your entries and to define another RSA key pair.

Draft - CISCO CONFIDENTIAL

After generating an RSA key pair, you can:

- Create a CSR parameter set. The CSR parameter set defines the distinguished name attributes for the ACE to use during the CSR-generating process. For details on defining a CSR parameter set, see the [Configuring SSL CSR Parameters, page 8-19](#).
- Generate a CSR for the RSA key pair file and transfer the CSR request to the certificate authority for signing. This provides an added layer of security because the RSA private key originates directly within the ACE and does not have to be transported externally. Each generated key pair must be accompanied by a corresponding certificate to work. For details on generating a CSR, see [Generating CSRs, page 8-21](#).

Related Topics

- [Configuring SSL, page 8-1](#)
- [Importing SSL Certificates, page 8-6](#)
- [Importing SSL Key Pairs, page 8-9](#)
- [Configuring SSL Chain Group Parameters, page 8-18](#)
- [Configuring SSL CSR Parameters, page 8-19](#)
- [Configuring SSL Proxy Service, page 8-22](#)

Exporting SSL Certificates

The ability to export SSL certificates allows you copy signed certificates to another server on your network so that you can then import them onto another ACE or Web server. Exporting certificates is similar to copying in that the original certificates are not deleted.

Use this procedure to export SSL certificates from the ACE to a remote server.

Assumption

The SSL certificate can be exported. (See [Importing SSL Certificates, page 8-6](#).)



Note You cannot export an SSL certificate in Building Blocks (**Config > Global > All Building Blocks**); SSL certificate export is available only in virtual context configuration.

Procedure

-
- Step 1** To configure a virtual context, select **Config > Devices > context > SSL > Certificates**.
The Certificates table appears, listing any valid SSL certificates.
- Step 2** Select the certificate you want to export, then click **Export**. The Export dialog box appears.
- Step 3** Enter the information in [Table 8-5](#).

Table 8-5 **SSL Certificate Export Attributes**

Field	Description
Protocol	Specify the method to be used for exporting the SSL certificate: - FTP—Indicates that FTP is to be used to access the network server when exporting the SSL certificate. - TFTP—Indicates that TFTP is to be used to access the network server when exporting the SSL certificate. - SFTP—Indicates that SFTP is to be used to access the network server when exporting the SSL certificate. - TERMINAL—Indicates that you will export the certificate using cut and paste by pasting the certificate and key pair information to the terminal display. You can use the terminal method to display only PEM files, which are in ASCII format.
IP Address	This field appears for FTP, TFTP, and SFTP. Enter the IP address of the remote server to which the SSL certificate file is to be exported.
Remote Filename	This field appears for FTP, TFTP, and SFTP. Enter the directory and filename to be used for the SSL certificate file on the remote network server.
Username	This field appears for FTP and SFTP. Enter the name of the user account on the remote network server.
Password	This field appears for FTP and SFTP. Enter the password for the user account on the remote network server.
Confirm	This field appears for FTP and SFTP. Reenter the password.

Step 4 Click:

- **OK** to export the certificate and to return to the Certificates table.
- **Cancel** to exit this procedure without exporting the certificate and to return to the Certificates table.

Related Topics

- [Configuring SSL, page 8-1](#)
- [Importing SSL Certificates, page 8-6](#)
- [Importing SSL Key Pairs, page 8-9](#)
- [Generating SSL Key Pairs, page 8-11](#)
- [Configuring SSL Chain Group Parameters, page 8-18](#)
- [Configuring SSL CSR Parameters, page 8-19](#)
- [Configuring SSL Proxy Service, page 8-22](#)

Draft - CISCO CONFIDENTIAL

Exporting SSL Key Pairs

The ability to export SSL key pairs allows you copy SSL key pair files to another server on your network so that you can then import them onto another ACE or Web server. Exporting key pair files is similar to copying in that the original key pairs are not deleted.

Use this procedure to export SSL key pairs from the ACE to a remote server.

Assumption

The SSL key pair can be exported (see [Generating SSL Key Pairs](#), page 8-11).

Procedure

-
- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > context > SSL > Keys**.
 - To configure a building block, select **Config > Global > building_block > SSL > Keys**.
- The Keys table appears.
- Step 2** Select the key entry you want to export, then click **Export**. The Export dialog box appears.
- Step 3** Enter the information in [Table 8-6](#).

Table 8-6 **SSL Key Export Attributes**

Field	Description
Protocol	Specify the method to be used for exporting the SSL key pair: - FTP—Indicates that FTP is to be used to access the network server when exporting the SSL key pair. - TFTP—Indicates that TFTP is to be used to access the network server when exporting the SSL key pair. - SFTP—Indicates that SFTP is to be used to access the network server when exporting the SSL key pair. - TERMINAL—Indicates that you will export the key pair using cut and paste by pasting the key pair information to the terminal display. You can use the terminal method to display only PEM files, which are in ASCII format.
IP Address	This field appears for FTP, TFTP, and SFTP. Enter the IP address of the remote server to which the SSL key pair is to be exported.
Remote Filename	This field appears for FTP, TFTP, and SFTP. Enter the directory and filename to be used for the SSL key pair file on the remote network server.
Username	This field appears for FTP and SFTP. Enter the name of the user account on the remote network server.

Table 8-6 *SSL Key Export Attributes (continued)*

Field	Description
Password	This field appears for FTP and SFTP. Enter the password for the user account on the remote network server.
Confirm	This field appears for FTP and SFTP. Reenter the password.

Step 4 Click:

- **OK** to export the key pair and to return to the Keys table.
- **Cancel** to exit this procedure without exporting the key pair and to return to the Keys table.

Related Topics

- [Configuring SSL, page 8-1](#)
- [Importing SSL Certificates, page 8-6](#)
- [Importing SSL Key Pairs, page 8-9](#)
- [Generating SSL Key Pairs, page 8-11](#)
- [Configuring SSL Chain Group Parameters, page 8-18](#)
- [Configuring SSL CSR Parameters, page 8-19](#)
- [Configuring SSL Proxy Service, page 8-22](#)

Configuring SSL Parameter Maps

An SSL parameter map defines the SSL session parameters that the ACE applies to an SSL proxy service. SSL parameter maps let you apply the same SSL session parameters to different proxy services.

Use this procedure to create SSL parameter maps.

Procedure

-
- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > context > SSL > Parameter Map**.
 - To configure a building block, select **Config > Global > building_block > SSL > Parameter Map**.
- The Parameter Map table appears.
- Step 2** Click **Add** to add a new SSL parameter map, or select an existing entry to modify, then click **Edit**. The Parameter Map configuration screen appears.

Draft - CISCO CONFIDENTIAL

Step 3 Enter the information in [Table 8-7](#).

Table 8-7 *SSL Parameter Map Attributes*

Field	Description
Parameter Map Name	Enter a unique name for the parameter map. Valid entries are alphanumeric strings with a maximum of 64 characters.
Queue Delay Timeout	Sets the amount of time (in milliseconds) to wait before emptying the queued data for encryption. If disabled (set to 0), the ACE module encrypts the data from the server as soon as it arrives and then sends the encrypted data to the client. Note The Queue Delay Timeout is only applied to data that the SSL module sends to the client. This avoids a potentially long delay in passing a small HTTP GET to the real server.
Session Cache Timeout	Allows the ACE module to reuse the master key on subsequent connections with the client, which can speed up the SSL negotiation process. Specifies a timeout value of an SSL session ID to remain valid before the ACE module requires the full SSL handshake to establish a new SSL session. Specifying 0 causes the ACE module to implement a least recently used (LRU) timeout policy. By disabling this option (with the no command), the full SSL handshake occurs for each new connection with the ACE module.
Reject Expired CRLs	Configures whether expired CRLs can be used. If checked, no expired CRLs are allowed.
Close Protocol Behavior	Select the method to be used to close the SSL connection. The default is None; allowed options are None and Disabled. • N/A or None—Indicates that the ACE is not to send a close-notify alert message to the SSL peer, nor does the ACE expect a close-notify alert message from the peer. The ACE preserves the session information so that SSL resumption can be used for future SSL connections. • Disabled—Indicates that the ACE is to send a close-notify alert message to the SSL peer; however, the SSL peer does not expect a close-notify alert before removing the session. Whether the SSL peer sends a close-notify alert message or not, the session information is preserved, allowing session resumption for future SSL connections. Note Where ACE 1.0 is already configured with the Strict option, ANM interprets it as the option None. This is due to the change in ACE 1.0 configuration (which no longer allows the Strict option).

Table 8-7 *SSL Parameter Map Attributes (continued)*

Field	Description
SSL Version	Enter the version of SSL to be used during SSL communications: - All—Indicates that the ACE is to use both SSL v3 and TLS v1 in its communications with peer ACE. - SSL3—Indicates that the ACE is to use only SSL v3 in its communications with peer ACE. - TLS1—Indicates that the ACE is to use only TLS v1 in its communications with peer ACE.
Ignore Authentication Failure	 Note This is applicable to ACE 2.0 modules versions 3.0(0)A2(1.1) forward, and ACE 4710 devices running image A3(1.0). This feature is <i>not applicable</i> to ACE 2.0 modules 3.0(0)A2(1.0a)/ACE 4710 devices A1(7x) and earlier releases. If checked this feature enables the ACE to ignore expired or invalid server certificates and to continue setting up the back-end connection in an SSL initiation configuration. This command allows the ACE to ignore the following nonfatal errors with respect to server certificates: - Certificate not yet valid - Certificate has expired - Unable to get issuer certificate - Certificate revoked

Step 4 In the Parameter Map Cipher table, click **Add** to add a cipher, or select an existing cipher, then click **Edit**.

Step 5 Enter the information in [Table 8-8](#).

Table 8-8 *SSL Parameter Map Cipher Configuration Attributes*

Field	Description
Cipher Name	Select the cipher you want to use. For more information on the SSL cipher suites that ACE supports, see <i>Cisco 4700 Series Application Control Engine Appliance SSL Configuration Guide</i> or <i>Cisco Application Control Engine Module SSL Configuration Guide</i>.
Cipher Priority	Enter the priority you want to assign to this cipher suite. The priority indicates the cipher's preference for use. Valid entries are integers from 1 to 10 with 1 indicating the least preferred and 10 indicating the most preferred. When determining which cipher suite to use, the ACE selects the cipher suite with the highest priority.

Draft - CISCO CONFIDENTIAL

- Step 6** On the Parameter Map Cipher table, click:
- **Deploy Now** to deploy the Parameter Map Cipher on the ACE.
 - **Cancel** to exit the procedure without saving your entries and to return to the Parameter Map Cipher table.
 - **Next** to deploy your entries and to add another entry to the Parameter Map Cipher table.
- Step 7** On the Parameter Map table, click:
- **Deploy Now** to deploy this configuration on the ACE.
 - **Cancel** to exit the procedure without saving your entries and to return to the Parameter Map table.
 - **Next** to deploy your entries and to add another entry to the Parameter Map table.
-

Related Topics

- [Configuring SSL, page 8-1](#)
- [Importing SSL Certificates, page 8-6](#)
- [Importing SSL Key Pairs, page 8-9](#)
- [Generating SSL Key Pairs, page 8-11](#)
- [Configuring SSL Chain Group Parameters, page 8-18](#)
- [Configuring SSL CSR Parameters, page 8-19](#)
- [Configuring SSL Proxy Service, page 8-22](#)

Configuring SSL Chain Group Parameters

A chain group specifies the *certificate chains* that the ACE sends to its peer during the handshake process. A certificate chain is a hierarchal list of certificates that includes the ACE's certificate, the root certificate authority certificate, and any intermediate certificate authority certificates. Using the information provided in a certificate chain, the certificate verifier searches for a trusted authority in the certificate hierarchal list up to and including the root certificate authority. If the verifier finds a trusted authority before reaching the root certificate authority certificate, it stops searching further.

Use this procedure to configure certificate chains for a virtual context.

Assumption

At least one SSL certificate is available.

Procedure

-
- Step 1** Select **Config > Devices > context > SSL > Chain Group Parameters**. The Chain Group Parameters table appears.
- Step 2** Click **Add** to add a new chain group, or select an existing chain group, then click **Edit** to modify it. The Chain Group Parameters configuration screen appears.
- Step 3** In the Chain Group Name field, enter a unique name for the chain group. Valid entries are alphanumeric strings with a maximum of 64 characters.

Step 4 Click:

- **Deploy Now** to deploy this configuration on the ACE. The updated Chain Group Parameters screen appears along with the Chain Group Certificates table. Continue with [Step 5](#).
- **Cancel** to exit the procedure without saving your entries and to return to the Chain Group Parameters table.
- **Next** to deploy your entries and to add another entry to the Chain Group Parameters table.

Step 5 In the Chain Group Certificates table, click **Add** to add an entry. The Chain Group Certificates configuration screen appears.**Note**

You cannot modify an existing entry in the Chain Group Certificates table. Instead, delete the entry, then add a new one.

Step 6 In the Certificate Name field, select the certificate to add to this chain group.**Step 7** Click:

- **Deploy Now** to deploy this configuration on the ACE.
- **Cancel** to exit the procedure without saving your entries and to return to the Chain Group Certificates table.
- **Next** to deploy your entries and to add another certificate to this chain group table.

Related Topics

- [Configuring SSL, page 8-1](#)
- [Importing SSL Certificates, page 8-6](#)
- [Importing SSL Key Pairs, page 8-9](#)
- [Generating SSL Key Pairs, page 8-11](#)
- [Configuring SSL Parameter Maps, page 8-15](#)
- [Configuring SSL CSR Parameters, page 8-19](#)
- [Configuring SSL Proxy Service, page 8-22](#)

Configuring SSL CSR Parameters

A *certificate signing request* (CSR) is a message you send to a certificate authority such as VeriSign and Thawte to apply for a digital identity certificate. The CSR contains information that identifies the SSL site, such as location and a serial number, and a public key that you choose. A corresponding private key is not included in the CSR, but is used to digitally sign the request. The CSR may be accompanied by other credentials or proofs of identity required by the certificate authority, and the certificate authority may contact the applicant for more information.

If the request is successful, the certificate authority returns a digitally signed (with the private key of the certificate authority) identity certificate.

CSR parameters define the *distinguished name* attributes the ACE applies to the CSR during the CSR-generating process. These attributes provide the certificate authority with the information it needs to authenticate your site. Defining a CSR parameter set lets you to generate multiple CSRs with the same distinguished name attributes.

Draft - CISCO CONFIDENTIAL

Each context on the ACE can contain up to eight CSR parameter sets.

Use this procedure to define the distinguished name attributes for SSL CSRs.

Procedure

- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > context > SSL > CSR Parameters**.
 - To configure a building block, select **Config > Global > building_block > SSL > CSR Parameters**.

The CSR Parameters table appears.

- Step 2** Click **Add** to add new set of CSR attributes, or select an existing entry to modify, then click **Edit**. The CSR Parameters configuration screen appears.

- Step 3** Enter the information in [Table 8-9](#).

Table 8-9 SSL CSR Parameter Attributes

Field	Description
Name	Enter a unique name for this parameter set. Valid entries are alphanumeric strings with a maximum of 64 characters.
Country	Enter the name of the country where the SSL site resides. Valid entries are 2 alphabetic characters representing the country, such as <i>US</i> for the United States. The International Organization for Standardization (ISO) maintains the complete list of valid country codes on its Web site (www.iso.org).
State	Enter the name of the state or province where the SSL site resides.
Locality	Enter the name of the city where the SSL site resides.
Common Name	Enter the name of the domain or host of the SSL site. Valid entries are strings with a maximum of 64 characters. Special characters are allowed.
Serial Number	Enter a serial number to assign to the certificate. Valid entries are alphanumeric strings with a maximum of 16 characters.
Organization Name	Enter the name of the organization to include in the certificate. Valid entries are alphanumeric strings with a maximum of 64 characters.
Email	Enter the site e-mail address. Valid entries are text strings, including alphanumeric and special characters (for example, @ symbol in email address) with a maximum of 40 characters.
Organization Unit	Enter the name of the organization to include in the certificate. Valid entries are alphanumeric strings with a maximum of 64 characters.

- Step 4** Click:
- Deploy Now** to deploy this configuration on the ACE.
 - Cancel** to exit this procedure without saving your entries and to return to the CSR Parameters table.
 - Next** to deploy your entries and to define another set of CSR attributes.

Related Topics

- [Configuring SSL, page 8-1](#)

- [Importing SSL Certificates, page 8-6](#)
- [Importing SSL Key Pairs, page 8-9](#)
- [Configuring SSL Parameter Maps, page 8-15](#)
- [Configuring SSL Chain Group Parameters, page 8-18](#)
- [Configuring SSL Proxy Service, page 8-22](#)

Generating CSRs

A *certificate signing request* (CSR) is a message you send to a certificate authority such as VeriSign and Thawte to apply for a digital identity certificate. Create a CSR when you need to apply for a certificate from a certificate authority. When the certificate authority approves a request, it signs the CSR and returns the authorized digital certificate to you. This certificate includes the private key of the certificate authority. When you receive the authorized certificate and key pair, you can import them for use (see [Importing SSL Certificates, page 8-6](#) and [Importing SSL Key Pairs, page 8-9](#)).

Use this procedure to generate SSL CSRs.



Note

You cannot generate a CSR in Building Blocks (**Config > Global > All Building Blocks**); SSL CSR generation is available only in virtual context configuration.

Assumption

You have configured SSL CSR parameters (see [Configuring SSL CSR Parameters, page 8-19](#)).

Procedure

-
- Step 1** Select **Config > Devices > context > SSL > Keys**. The Keys table appears.
 - Step 2** Select a key in the table, then click **Generate CSR**. The Generate a Certificate Signing Request dialog box appears.
 - Step 3** In the CSR Parameter field, select the CSR parameter to be used.
 - Step 4** Click:
 - **OK** to generate the CSR. The CSR appears in a popup window which you can now submit to a certificate authority for approval. Work with your certificate authority to determine the method of submission, such as e-mail or a Web-based application. Click **Close** to close the popup window and to return to the Keys table.
 - **Cancel** to exit this procedure without generating the CSR and to return to the Keys table.
-

Related Topics

- [Configuring SSL, page 8-1](#)
- [Importing SSL Certificates, page 8-6](#)
- [Importing SSL Key Pairs, page 8-9](#)
- [Configuring SSL Parameter Maps, page 8-15](#)
- [Configuring SSL Chain Group Parameters, page 8-18](#)

Draft - CISCO CONFIDENTIAL

- [Configuring SSL Proxy Service, page 8-22](#)

Configuring SSL Proxy Service

SSL proxy service defines the SSL parameter map, key pair, certificate, and chain group the ACE uses during SSL handshakes. By configuring an SSL proxy *server* service on the ACE, the ACE can act as an SSL server.

Use this procedure to define the attributes that the ACE is to use during SSL handshakes so that it can act as an SSL server.

Assumption

You have configured at least one SSL key pair, certificate, chain group, or parameter map to apply to this proxy service.

Procedure

- Step 1** Select **Config > Devices > context > SSL > Proxy Service**. The Proxy Service table appears.
- Step 2** Click **Add** to add a new proxy service, or select an existing service, then click **Edit** to modify it. The Proxy Service configuration screen appears.
- Step 3** Enter the information in [Table 8-10](#).

Table 8-10 SSL Proxy Service Attributes

Field	Description
Proxy Service Name	Enter a unique name for this proxy service. Valid entries are alphanumeric strings with a maximum of 40-65 characters, depending on your module and hardware version.
Key List	Select the key pair that the ACE is to use during the SSL handshake for data encryption.
Certificate List	Select the certificate that the ACE is to use during the SSL handshake to prove its identity.
Chain Group Name	Select the chain group that the ACE is to use during the SSL handshake. To create a chain group, see Configuring SSL Chain Group Parameters, page 8-18 .
Auth Group Name	Select the authorization group name that the ACE is to use during the SSL handshake. To create an authorization group, see Configuring SSL Authentication Groups, page 8-24 .
CRL Best -effort	Displays only when Auth Group Name is selected. Allows ANM to search client certificates for the service to determine if it contains a CRL in the extension. ANM then retrieves the value, if it exists.
CRL Name	Name of the CRL.
Parameter Map Name	Select the SSL parameter map to associate with this SSL proxy server service.

- Step 4** Click:

- **Deploy Now** to deploy this configuration on the ACE.
- **Cancel** to exit this procedure without saving your entries and to return to the Proxy Service table.
- **Next** to deploy your entries and to add another proxy service.
- **Delete** to remove this configuration on the ACE.



Note When an authorization group is deleted, the CRL Name object (if it exists) is deleted automatically.

Related Topics

- [Configuring SSL, page 8-1](#)
- [Importing SSL Certificates, page 8-6](#)
- [Importing SSL Key Pairs, page 8-9](#)
- [Configuring SSL Parameter Maps, page 8-15](#)
- [Configuring SSL Chain Group Parameters, page 8-18](#)
- [Configuring SSL CSR Parameters, page 8-19](#)

Enabling Client Authentication

During the flow of a normal SSL handshake, the SSL server sends its certificate to the client. Then the client verifies the identity of the server through the certificate. However, the client does not send any identification of its own to the server. When you enable the client authentication feature enabled on the ACE, it will require that the client send a certificate to the server. Then the server verifies the following information on the certificate:

- A recognized CA issued the certificate.
- The valid period of the certificate is still in effect.
- The certificate signature is valid and not tampered.
- The CA has not revoked the certificate.
- At least one SSL certificate is available.

Use the following procedures to enable or disable client authentication:

- [Configuring SSL Proxy Service, page 8-22](#)
- [Configuring SSL Authentication Groups, page 8-24](#)
- [Configuring CRLs for Client Authentication, page 8-25](#)

Draft - CISCO CONFIDENTIAL

Configuring SSL Authentication Groups

On the ACE, you can implement a group of certificates that are trusted as certificate signers by creating an authentication group. After creating the authentication group and assigning its certificates, then you can assign the authentication group to a proxy service in an SSL termination configuration to enable client authentication. For information on client authentication, see [Enabling Client Authentication, page 8-23](#).

For information on server authentication and assigning an authentication group, see [Configuring SSL Proxy Service, page 8-22](#).

Use this procedure to specify the certificate authentication groups that the ACE uses during the SSL handshake and enable client authentication on this SSL-proxy service. The ACE includes the certificates configured in the group along with the certificate that you specified for the SSL proxy service.

**Note**

You cannot create an authorization group in Building Blocks (**Config > Global > All Building Blocks**); You can only create SSL authentication groups while configuring virtual contexts in specific modules.

Assumptions

- At least one SSL certificate is available.
- Your ACE module supports authentication groups. See your *Supported Devices Table for the Cisco Application Networking Manager 1.2* for details on supported modules.

Procedure

-
- Step 1** Select **Config > Devices > context > SSL > Auth Group Parameters**.
- The Auth Group Parameters table appears.
- Step 2** Click **Add** to add an authentication group, or select an existing authorization group, then click **Edit** to modify it. The Auth Group Parameters configuration screen appears.
- Step 3** In the Auth Group Name field, enter a unique name for the authorization group. Valid entries are alphanumeric strings with a maximum of 64 characters.
- Step 4** Click:
- **Deploy Now** to deploy this configuration on the ACE. The updated Auth Group Parameters screen appears along with the Auth Group Certificates table. Continue with [Step 5](#).
 - **Cancel** to exit the procedure without saving your entries and to return to the Auth Group Parameters table.
 - **Next** to deploy your entries and to add another entry to the Auth Group Parameters table.
- Step 5** In the Auth Group Certificates field, click **Add** to add an entry. The Auth Group Certificates configuration screen appears.
-
-  **Note** You cannot modify an existing entry in the Auth Group Certificates table. Instead, delete the entry, then add a new one.
-
- Step 6** In the Certificate Name field, select the certificate to add to this authorization group.
- Step 7** Click:
- **Deploy Now** to deploy this configuration on the ACE.

- **Cancel** to exit the procedure without saving your entries and to return to the Auth Group Parameters table.
- **Next** to deploy your entries and to add another entry to the Auth Group Parameters table.

Step 8 You can repeat the previous step to add more certificates to the authorization group or click **Deploy Now**.

Step 9 After you configure authorization group parameters, you can configure the SSL proxy service to use a CRL. See [Configuring CRLs for Client Authentication, page 8-25](#).

**Note**

When you enable client authentication, a significant performance decrease may occur. Additional latency may occur when you configure CRL retrieval.

Related Topics

- [Configuring SSL Chain Group Parameters, page 8-18](#)
- [Configuring CRLs for Client Authentication, page 8-25](#)

Configuring CRLs for Client Authentication

By default, ACE does not use certificate revocation lists (CRLs) during client authentication. You can configure the SSL proxy service to use a CRL by having the ACE scan each client certificate for the service to determine if it contains a CRL in the extension and then retrieve the value, if it exists. For more information about SSL termination on the ACE, see the *Cisco Application Control Engine Module SSL Configuration Guide*.

**Note**

When you enable client authentication, a significant performance decrease may occur. Additional latency may occur when you configure CRL retrieval.

Use this procedure to configure ACE to scan for CRLs and retrieve them.

Assumption

A CRL cannot be configured on an SSL proxy without first configuring an authorization group.

Procedure

- Step 1** Select **Config > Devices > context > SSL > Certificate Revocation List**. The Certificate Revocation List table appears.
- Step 2** Click **Add** to add a CRL or select an existing CRL, then click **Edit** to modify it. The Certificate Revocation List screen appears.

Draft - CISCO CONFIDENTIAL

Step 3 Enter the information in [Table 8-11](#).

Table 8-11 *SSL Certificate Revocation List*

Field	Description
Name	Enter the CRL name. Valid entries are unquoted alphanumeric strings with a maximum of 64 characters.
URL	Enter the URL where the ACE retrieves the CRL. Valid entries are unquoted alphanumeric strings with a maximum of 255 characters. Only HTTP URLs are supported. ACE checks the URL and displays an error if it does not match.

Step 4 Click:

- **Deploy Now** to deploy this configuration on the ACE. The updated Certificate Revocation List table appears.
- **Cancel** to exit the procedure without saving your entries and to return to the Certificate Revocation List table.
- **Next** to deploy your entries and to add another entry to the Certificate Revocation List table.

Related Topics

- [Configuring SSL Proxy Service, page 8-22](#)
- [Configuring SSL Authentication Groups, page 8-24](#)



CHAPTER 9

Configuring Network Access

Revised Date: 3/25/09

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

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

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

VLAN Overview

The following sections describe VLANs:

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

ACE Module VLAN Overview

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

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

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

Related Topics

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

ACE Appliance VLAN Overview

The ACE appliance has four physical Ethernet interface ports. All VLANs are allocated to the physical ports. After the VLANs are assigned, you can configure the corresponding VLAN interfaces as either routed or bridged for use. When you configure an IP address on an interface, the ACE appliance automatically makes it a routed mode interface.

Similarly, when you configure a bridge group on an interface VLAN, the ACE appliance automatically makes it a bridged interface. Then, you associate a bridge-group virtual interface (BVI) with the bridge group.

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

In routed mode, the ACE is considered a router hop in the network. In the Admin or user contexts, the ACE supports static routes only. The ACE supports up to eight equal cost routes for load balancing.

Related Topics

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

Configuring VLAN Interfaces

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



Note

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

Procedure

-
- Step 1** Select the item to configure:

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

The VLAN Interface table appears.

Step 2 Click **Add** to add a new VLAN interface, or select an existing VLAN interface, then click **Edit** to modify it.



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

Step 3 Enter the VLAN interface attributes (see [Table 9-1](#)).

Enable MAC address autogenerate.



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

Table 9-1 *VLAN Interface Attributes*

Field	Description
VLAN	Either accept the automatically incremented entry or enter a different value. Valid entries are integers from 2 to 4094.
Description	Enter a brief description for this interface.
IP Address	Enter the IP address assigned to this interface.
Alias IP Address	Enter the IP address of the alias this interface is associated with.
Peer IP Address	Enter the IP address of the remote peer.
Netmask	Select the subnet mask to be used.
Admin Status	Indicate whether you want the interface to be up or down.
Max Fragment Chains Allowed	Enter the maximum number of fragments belonging to the same packet that the ACE appliance is to accept for reassembly. Valid entries are integers from 1 to 256, and the default is 112.

Table 9-1 VLAN Interface Attributes (continued)

Field	Description
ARP Inspection Type	By default, ARP inspection is disabled on all interfaces, allowing all ARP packets through the ACE. When you enable ARP inspection, the ACE appliance uses the IP address and interface ID (ifID) of an incoming ARP packet as an index into the ARP table. ARP inspection operates only on ingress bridged interfaces. ARP inspection prevents malicious users from impersonating other hosts or routers, known as ARP spoofing. ARP spoofing can enable a "man-in-the-middle" attack. For example, a host sends an ARP request to the gateway router. The gateway router responds with the gateway router MAC address.  Note If ARP inspection fails, then the ACE does not perform source MAC validation. The options are as follows: • N/A—ARP inspection is disabled. • Flood—Enables ARP forwarding of nonmatching ARP packets. The ACE appliance forwards all ARP packets to all interfaces in the bridge group. This is the default setting. In the absence of a static ARP entry, this option bridges all packets. • No-flood—Disables ARP forwarding for the interface and drops nonmatching ARP packets. In the absence of a static ARP entry, this option does not bridge any packets.
Fragment Min MTU Value	Enter the minimum Maximum Transmission Units (MTUs) for each allowable fragment. Valid entries are integers from 28-9216 with no default.
Min MTU Value	Enter number of bytes for MTU). Valid entries are integers from 68 to 9216, and the default is 1500.
Reassembly Timeout	Enter the number of seconds that the ACE appliance is to wait before it abandons the fragment reassembly process if it doesn't receive any outstanding fragments for the current fragment chain (that is, fragments belonging to the same packet). Valid entries are 1 to 30 seconds.
Reverse Path Forwarding (RPF)	Select the checkbox to indicate that the ACE appliance is to discard IP packets if no reverse route is found or if the route does not match the interface on which the packets arrived. Clear the check box to indicate that the ACE appliance is not to filter or discard packets based on the ability to verify the source IP address.
Bridge Group Number	Enter the number of the bridge group to be configured on this VLAN. When you configure a bridge group on a VLAN, the ACE appliance automatically makes it bridged. Valid entries are from 1 to 4094.

Table 9-1 **VLAN Interface Attributes (continued)**

Field	Description
Enable MAC Sticky	Select the check box to indicate that the ACE appliance is to convert dynamic MAC addresses to sticky secure MAC addresses and add this information to the running configuration. Clear the check box to indicate that the ACE appliance is not to convert dynamic MAC addresses to sticky secure MAC addresses.
Enable ICMP Guard	Select the check box to indicate that ICMP Guard is to be enabled on the ACE appliance. Clear the check box to indicate that ICMP Guard is not to be enabled on ACE appliance.  Caution Disabling ICMP security checks may expose your ACE appliance and network to potential security risks. When you disable ICMP Guard, the ACE appliance no longer performs NAT translations on the ICMP header and payload in error packets, which can potentially reveal real host IP addresses to attackers.
Enable DHCP Relay	Select the check box to indicate that the ACE appliance is to accept DHCP requests from clients on this interface and to enable the DHCP relay agent. Clear the check box to indicate that the ACE appliance is not to accept DHCP requests or enable the DHCP relay agent.
Enable Normalization	Select the check box to indicate that normalization is to be enabled on this interface. Clear the check box to indicate that normalization is to be disabled on this interface.  Caution Disabling normalization may expose your ACE appliance and network to potential security risks. Normalization protects your networking environment from attackers by enforcing strict security policies that are designed to examine traffic for malformed or malicious segments.
Action for DF Bit	Indicate how the ACE appliance is to handle a packet that has its DF (Don't Fragment) bit set in the IP header: • Allow—Indicates that the ACE appliance is to permit the packet with the DF bit set. If the packet is larger than the next-hop MTU, ACE appliance discards the packet and sends an ICMP unreachable message to the source host. • Clear—Indicates that the ACE appliance is to clear the DF bit and permit the packet. If the packet is larger than the next-hop MTU, the ACE appliance fragments the packet.

Table 9-1 *VLAN Interface Attributes (continued)*

Field	Description
Action for IP Header Options	Select the action the ACE appliance is to take when an IP option is set in a packet: • Allow—Indicates that the ACE appliance is to allow the IP packet with the IP options set. • Clear—Indicates that the ACE appliance is to clear all IP options from the packet and to allow the packet. • Clear-Invalid—Indicates that the ACE appliance is to clear the invalid IP options from the packet and then allow the packet. • Drop—Indicates that the ACE appliance is to discard the packet regardless of any options that are set.
Min TTL IP Header Value	Enter the minimum number of hops a packet is allowed to reach its destination. Valid entries are integers from 1 to 255. Each router along the packet's path decrements the TTL by one. If the packet's TTL reaches zero before the packet reaches its destination, the packet is discarded.
Enable Syn Cookie Threshold Value	For ACE 2.0 and 3.0 devices only. Embryonic connection threshold above which the ACE applies SYN-cookie DoS protection. Valid entries are integers from 2 to 65535.
UDP Config Commands	For ACE 2.0 and 3.0 devices only. Select the UDP boost command: • N/A—not applicable • IP-Destination-Hash—Perform source IP hash during connection lookup • IP-Source-Hash—Perform destination IP hash during connection
Enable MAC Address Autogenerate	Allows you to configure a different MAC address for the VLAN interface.

Step 4 Click:

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

Related Topic

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

Viewing All VLAN Interfaces

Use this procedure to view all VLAN interfaces.

Procedure

-
- Step 1** Select **Config > Devices > context > Network > VLAN Interfaces**.
The VLAN Interface table appears listing all VLAN interfaces for the selected virtual context.
-

Related Topics

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

Configuring VLAN Interface Options

After adding a VLAN interface, you can configure other VLAN interface attributes such as policy map use, access groups, static ARP entries, and so on.

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

Configuration options for VLAN interfaces are:

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

Configuring VLAN Interface Policy Map Use

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



Note

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

Assumptions

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

Procedure

-
- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > context > Network > VLAN Interfaces**.

- To configure a configuration building block, select **Config > Global > All Building Blocks > building_block > Network > VLAN Interfaces**.
- Step 2** Select the VLAN interface you want to associate with a policy map, then select the Policy tab. The Policy configuration table appears.
- Step 3** Click **Add** to add a policy. The Policy configuration screen appears.
- Step 4** In the Policy Map field, select the policy map to be associated with this VLAN interface.
- Step 5** In the Direction field, select the traffic this policy map applies to:
- **Input**—Specifies that this policy map is to be applied to the inbound direction of the interface; that is, all traffic received by this interface.
 - **Output**—Specifies that this policy map is to be applied to the outbound direction of the interface; that is, all traffic sent by this interface.
- Step 6** Click:
- **Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts.
 - **OK** to save your entry. This option appears for configuration building blocks.
 - **Cancel** to exit this procedure without saving your entries and to return to the previous table.
 - **Next** to deploy your entries and to add another policy to this interface.

Related Topics

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

Configuring VLAN Interface Access Control

The ACE Device Manager uses access control lists to limit access to and from VLAN interfaces in a virtual context. Use this procedure to configure access control for a VLAN interface.



Note

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

Assumptions

- You have successfully configured at least one VLAN interface (see [Configuring VLAN Interfaces, page 9-2](#)).
- An access control list has been configured for this virtual context. Entering an ACL name does not configure the ACL; you must configure the ACL on the ACE appliance. For more information, see [Configuring Security with ACLs, page 3-43](#).

Procedure

-
- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > *context* > Network > VLAN Interfaces**.
 - To configure a configuration building block, select **Config > Global > All Building Blocks > *building_block* > Network > VLAN Interfaces**.
- The VLAN Interface table appears.
- Step 2** Select the VLAN interface you want to associate with an ACL, then select the Access Group tab. The Access Group configuration table appears.
- Step 3** Click **Add** to associate a new ACL with the selected VLAN interface. The Access Group configuration screen appears.
- Step 4** In the ACL Name field, select the ACL group to be associated with this VLAN interface.
- Step 5** In the Direction field, select the traffic this access group applies to:
- **Input**—Specifies that this access group is to be applied to the inbound direction of the interface; that is, all traffic received by this interface.
 - **Output**—Specifies that this access group is to be applied to the outbound direction of the interface; that is, all traffic sent by this interface.
- Step 6** Click:
- **Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts.
 - **OK** to save your entry. This option appears for configuration building blocks.
 - **Cancel** to exit this procedure without saving your entries and to return to the previous screen.
 - **Next** to deploy your entries and to apply another access group to this interface.
-

Related Topics

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

Configuring VLAN Interface Static ARP Entries

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



Note

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

Assumption

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

Procedure

-
- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > *context* > Network > VLAN Interfaces**.
 - To configure a configuration building block, select **Config > Global > All Building Blocks > *building_block* > Network > VLAN Interfaces**.
- The VLAN Interface table appears.
- Step 2** Select the VLAN interface for which you want to configure static ARP entries, then click the Static ARP Entries tab. The Static ARP Entries configuration table appears.
- Step 3** In the Static ARP table, click **Add** to configure static ARP entries for the selected VLAN interface.
- Step 4** In the ARP IP Address field, enter the IP address in dotted-decimal notation (for example, 192.168.11.2).
- Step 5** In the ARP MAC Address field, enter the hardware MAC address for the ARP table entry (for example, 00.02.9a.3b.94.d9).
- Step 6** Click:
- **Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts.
 - **OK** to save your entry. This option appears for configuration building blocks.
 - **Cancel** to exit this procedure without saving your entries and to return to the previous screen.
 - **Next** to deploy your entries and to add another static ARP entry.
-

Related Topics

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

Configuring VLAN Interface NAT Pools

Network Address Translation (NAT) is designed to simplify and conserve IP addresses. It allows private IP networks that use unregistered IP addresses to connect to the Internet. NAT operates on a router, usually connecting two networks, and translates the private (not globally unique) addresses in the internal network into legal addresses before the packets are forwarded to another network.

The ACE Device Manager allows you to configure NAT so that it advertises only one address for the entire network to the outside world. This effectively hides the entire internal network behind that address, thereby offering both security and address conservation.

Several internal addresses can be translated to only one or a few external addresses by using Port Address Translation (PAT) in conjunction with NAT. With PAT, you can configure static address translations at the port level and use the remainder of the IP address for other translations. PAT effectively extends NAT from one-to-one to many-to-one by associating the source port with each flow.

Use this procedure to configure NAT pools for a VLAN interface.

**Note**

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

Assumption

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

Procedure

-
- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > *context* > Network > VLAN Interfaces**.
 - To configure a configuration building block, select **Config > Global > All Building Blocks > *building_block* > Network > VLAN Interfaces**.
- Step 2** Select the VLAN interface you want to configure a NAT pool for, then select NAT Pool tab. The NAT Pool configuration table appears.
- Step 3** Click **Add** to add a new entry.
- Step 4** In the NAT Id field, either accept the automatically incremented entry or enter a new number to uniquely identify this pool. Valid entries are integers from 1 to 2147483647.
- Step 5** In the Start IP Address field, enter an IP address in dotted-decimal notation (such as 192.168.11.2). This entry identifies either a single IP address or, if using a range of IP addresses, the first IP address in a range of global addresses for this NAT pool.
- Step 6** In the End IP Address field, enter the highest IP address in a range of global IP addresses for this NAT pool. Enter the IP address in dotted-decimal notation, such as 192.168.11.2.
- Leave this field blank if you want to identify only the single IP address in the Start IP Address field.
- Step 7** In the Netmask field, select the subnet mask for the global IP addresses in the NAT pool.
- Step 8** Select the PAT Enabled check box to indicate that the ACE appliance is to perform port address translation (PAT) in addition to NAT. Clear the check box to indicate that the ACE appliance is not to perform port address translation (PAT) in addition to NAT.
- Step 9** Click:
- **Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts.
 - **OK** to save your entry. This option appears for configuration building blocks.
 - **Cancel** to exit this procedure without saving your entries and to return to the previous table.
 - **Next** to deploy your entries and to add another NAT Pool entry.
-

Related Topics

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

Configuring VLAN Interface DHCP Relay

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

**Note**

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

Assumption

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

Procedure

-
- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > *context* > Network > VLAN Interfaces**.
 - To configure a configuration building block, select **Config > Global > All Building Blocks > *building_block* > Network > VLAN Interfaces**.
- Step 2** Select the VLAN interface you want to configure DHCP relay for, then select the DHCP Relay Configuration tab. The DHCP Relay Configuration table appears.
- Step 3** Click **Add** to add a new entry.
- Step 4** In the IP Address field, enter the IP address of the DHCP server to which the DHCP relay agent is to forward client requests. Enter the IP address in dotted-decimal notation, such as 192.168.11.2.
- Step 5** Click:
- **Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts.
 - **OK** to save your entry. This option appears for configuration building blocks.
 - **Cancel** to exit this procedure without saving your entries and to return to the previous table.
 - **Next** to deploy your entries and to add another DHCP relay entry.
-

Related Topics

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

Configuring Virtual Context BVI Interfaces

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

**Note**

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

Procedure

Step 1 Select the item to configure:

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

The BVI Interface configuration table appears.

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

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

Table 9-2 BVI Interface Attributes

Field	Description
Bridge Group Number	Either accept the automatically incremented entry or enter a different, unique value. Valid entries are integers from 1 to 4094.
Description	Enter a brief description for this interface.
IP Address	Enter the IP address assigned to this interface.
Alias IP Address	Enter the IP address of the alias this interface is associated with.
Peer IP Address	Enter the IP address of the remote peer.
Netmask	Select the subnet mask to be used.
Admin Status	Indicate whether you want the interface to be up or down.

Step 4 Click:

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

Related Topics

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

Viewing All BVI Interfaces by Context

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

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

Table 9-3 *BVI Interface Fields*

Field	Description
Bridge Group Number	Name of the interface
Description	Description for this interface
IP Address	IP address assigned to this interface
Netmask	Subnet mask for this interface
Admin Status	Status of the interface, which can be up or down

Related Topics

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

Configuring Virtual Context Static Routes



Note

This functionality is available for only Admin virtual contexts.

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

Procedure

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

The Static Routes configuration table appears.

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

**Note**

You cannot modify an existing static route. To make changes to an existing static route, you must delete the static route and then add it back.

- Step 3** In the Destination Prefix field, enter the IP address for the route. The address you specify for the static route is the address that is in the packet before entering the ACE appliance and performing network address translation. Enter the address in dotted-decimal IP notation (for example, 192.168.11.2).
- Step 4** In the Destination Prefix Mask field, select the subnet to use for this route.
- Step 5** In the Next Hop field, enter the IP address of the gateway router for this route. The gateway address must be in the same network as a VLAN interface for this context.
- Step 6** Click:
- **Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts.
 - **OK** to save your entry. This option appears for configuration building blocks.
 - **Cancel** to exit this procedure without saving your entries and to return to the previous table.
 - **Next** to deploy your entries and to add another static route.

Related Topics

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

Viewing All Static Routes by Context

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

Procedure

- Step 1** Select **Config > Devices > context > Network > Static Routes**.

The Static Route table appears with the following information:

- Destination prefix
- Destination prefix mask
- Next hop IP address

Related Topics

- [Configuring Port Channel Interfaces, page 9-21](#)
- [Configuring VLAN Interfaces, page 9-2](#)

Configuring Global IP DHCP

ANM can configure the DHCP relay agent on the ACE. When you configure the ACE as a DHCP relay agent, it is responsible for forwarding the requests and responses that are negotiated between the DHCP clients and the server. By default, the DHCP relay agent is disabled. You must configure a DHCP server when you enable the DHCP relay agent.

The following steps show you how to configure the DHCP relay agent at the context level so the configuration applies to all interfaces associated with the context.



Note

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

Procedure

-
- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > *context* > Network > Global IP DHCP**.
 - To configure a configuration building block, select **Config > Global > All Building Blocks > *building_block* > Network > Global IP DHCP**.
- The Global IP DHCP configuration table appears.
- Step 2** Click **Enable DHCP relay for the context** to enable DHCP relay for the context and all interfaces associated with this context.
- Step 3** Select a relay agent information forwarding policy, which can be
- N/A—Specifies to not configure the DHCP relay to identify what is to be performed if a forwarded message already contains relay information.
 - Keep—Specifies that existing information is left unchanged on the DHCP relay agent.
 - Replace—Specifies that existing information is overwritten on the DHCP relay agent.
- Step 4** In the IP DHCP Server field, select the IP DHCP server to which the DHCP relay agent is to forward client requests.
- Step 5** Click:
- Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts.
 - OK** to save your entry. This option appears for configuration building blocks.
 - Cancel** to exit this procedure without saving your entries and to return to the previous table.
 - Next** to deploy your entries and to add another DHCP relay entry.
-

Configuring Static VLANs for Over 8 K Static NAT Configurations



Note

This feature is for ACE 2.0 devices only.

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

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

Procedure

-
- Step 1** Select **Config > Devices > *context* > Network > Static NAT Overwrite**.
The Static NAT Overwrite configuration table appears.
- Step 2** Click **Add** to add a new static NAT.
- Step 3** In the Mapped IP Addr field, enter the IP address to which the real IP address is translated. In a context, the mapped IP address must be different in each static NAT configuration.
- Step 4** In the Real VLAN number field, select the VLAN number of the interface connected to the real IP address network.
- Step 5** In the Mapped VLAN number field, select the VLAN number of the interface connected to the mapped IP address network. In a context, the mapped interface must be the same in each static NAT configuration.
- Step 6** In the Real IP address field, enter the real server IP address to be translated. In a context, you must configure a different address for configurations that have the same real server interface.
- Step 7** In the Real IP netmask field, enter the subnet mask for the real server address.
- Step 8** Click:
- **Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts.
 - **Cancel** to exit this procedure without saving your entries and to return to the previous table.
 - **Next** to deploy your entries and to add another DHCP relay entry.
-

Configuring Gigabit Ethernet Interfaces



Note

This feature is for ACE appliances only.

The ACE appliance provides physical Ethernet ports to connect servers, PCs, routers, and other devices to the ACE appliance. The ACE appliance supports four Layer 2 Ethernet ports for performing Layer 2 switching. You can configure the four Ethernet ports to provide an interface for connecting to 10-Mbps, 100-Mbps, or 1000-Mbps networks. Each Layer 2 Ethernet port supports autonegotiate, full-duplex, or half-duplex operation on an Ethernet LAN, and can carry traffic within a designated VLAN.

A Layer 2 Ethernet port can be configured as:

- **Member of Port-Channel Group**—The port is configured as a member of a port-channel group, which associates a physical port on the ACE appliance to a logical port to create a port-channel logical interface. The VLAN association is derived from port-channel configuration. The port is configured as a Layer 2 EtherChannel, where each EtherChannel bundles the individual physical Ethernet data ports into a single logical link that provides the aggregate bandwidth of up to four physical links on the ACE.
- **Access VLAN**—The port is assigned to a single VLAN. This port is referred to as an access port and provides a connection for end users or node devices, such as a router or server.
- **Trunk port**—The port is associated with IEEE 802.1Q encapsulation-based VLAN trunking to allocate VLANs to ports and to pass VLAN information (including VLAN identification) between switches for all Ethernet channels defined in a Layer 2 Ethernet data port or a Layer 2 EtherChannel (port-channel) group on the ACE appliance.

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

Procedure

-
- Step 1** Select **Config > Devices > context > Network > Gigabit Ethernet Interfaces**. The Physical Interface table appears.
- Step 2** Select an existing gigabit Ethernet interface, then click **Edit** to modify it.
- Step 3** Enter the gigabit Ethernet physical interface attributes (see [Table 9-4](#)).

Table 9-4 Physical Interface Attributes

Field	Description
Interface Name	Name of the gigabit interface, which is the <i>slot_number/port_number</i> where <i>slot_number</i> is the physical slot on the ACE for the specified port, and <i>port_number</i> is the physical Ethernet data port on the ACE for the specified port.
Description	Enter a brief description for this interface.
Admin Status	Indicate whether you want the interface to be up or down.
Speed	Specifies the port speed, which can be • Auto—Autonegotiate with other devices • 1000 Mbps • 100 Mbps • 10 Mbps

Table 9-4 Physical Interface Attributes (continued)

Field	Description
Duplex	Specifies an interface duplex mode, which can be: • Auto—Resets the specified Ethernet port to automatically negotiate port speed and duplex of incoming signals. This is the default setting. • Half—Configures the specified Ethernet port for half-duplex operation. A half-duplex setting ensures that data only travels in one direction at any given time. • Full—Configures the specified Ethernet port for full-duplex operation, which allows data to travel in both directions at the same time.
Port Operation Mode	Specifies the port operation mode, which can be: • N/A—Indicates that this option is not to be used. • Channel-group—Specifies to map the port to a port channel. You must specify: – Port channel group number—Specify the port channel group number. – FT VLAN—Specify the fault tolerant (FT) VLAN used for communication between the members of the FT group. • Switchport—Specifies the interface switchport type: – Access—Specifies that the port interface is an access port. You must specify a VLAN as an access port in the Access VLAN field. – Trunk—Specifies that the port interface is a trunk port. When you select Trunk, you must complete one or both of the following fields: - Trunk Native VLAN - Trunk Allowed VLANs
FT Vlan	Specify the fault tolerant (FT) VLAN used for communication between the members of the FT group.

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

Field	Description
Carrier Delay	Adds a configurable delay at the physical port level to address any issues with transition time, based on the variety of peers. Valid values are 0 to 120 seconds. The default is 0 (no carrier delay).  Note If you connect an ACE to a Catalyst 6500 series switch, your configuration on the Catalyst may include the Spanning-Tree Protocol (STP). However, the ACE does not support STP. In this case, you may find that the Layer 2 convergence time is much longer than the physical port up time. For example, the physical port would normally be up within 3 seconds, but STP moving to the forward state may need approximately 30 seconds. During this transitional time, although the ACE declares the port to be up, the traffic will not pass. In this case, specify a carrier delay
QoS Trust COS	Enables Quality of Service (QoS) for the physical Ethernet port. By default, QoS is disabled for each physical Ethernet port on the ACE. QoS for a configured physical Ethernet port based on VLAN Classes of Service (CoS) bits (priority bits that segment the traffic in eight different classes of service). When you enable QoS on a port (a trusted port), traffic is mapped into different ingress queues based on their VLAN CoS bits. If there are no VLAN CoS bits, or QoS is not enabled on the port (untrusted port), the traffic is then mapped into the lowest priority queue. You can enable QoS for an Ethernet port configured for fault tolerance. In this case, heartbeat packets are always tagged with COS bits set to 7 (a weight of High).  Note We recommend that you enable QoS on the FT VLAN port to provide higher priority for FT traffic.

Step 4 Click:

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

Related Topics

- [Configuring VLAN Interfaces, page 9-2](#)
- [Configuring Virtual Context BVI Interfaces, page 9-12](#)
- [Configuring Port Channel Interfaces, page 9-21](#)

Configuring Port Channel Interfaces

**Note**

This feature is for ACE appliances only.

You can group physical ports together on the ACE appliance to form a logical Layer 2 interface called the port-channel. All the ports belonging to the same port-channel must be configured with same values; for example, port parameters, VLAN membership, and trunk configuration. Only one port-channel in a channel group is allowed, and a physical port can belong to a single port-channel interface only.

Step 1 Select **Config > Devices > context > Network > Port Channel Interfaces**. The Port Channel Interface table appears.

Step 2 Click **Add** to add a port channel interface, or select an existing port channel interface, then click **Edit** to modify it.

**Note**

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

Step 3 Enter the port channel interface attributes (see [Table 9-5](#)).

Table 9-5 Port Channel Interface Attributes

Field	Description
Port Channel Number	Specify a channel number for the port-channel interface, which can be from 1 to 255.
Description	Enter a brief description for this interface.
FT Vlan	Specify the fault tolerant (FT) VLAN used for communication between the members of the FT group.
Admin Status	Indicate whether you want the interface to be up or down.

Table 9-5 Port Channel Interface Attributes (continued)

Field	Description
ARP Inspection Type	Instructs the ACE to check the source MAC address in an Ethernet header against the sender's MAC address in an ARP payload for every ARP packet received by the ACE on the specified interface. The ACE does not learn or update the ARP or MAC tables for packets with different MAC addresses. By default, source MAC validation is disabled. Note If ARP inspection fails, then the ACE does not perform source MAC validation. The options are as follows: • N/A—Source MAC validation is disabled. • Flood—Enables ARP forwarding for the interface and forwards ARP packets with nonmatching source MAC addresses to all interfaces in the bridge group. This is the default option when you enable source MAC validation. • No-flood—Disables ARP forwarding for the interface and drops ARP packets with nonmatching source MAC addresses.

Table 9-5 Port Channel Interface Attributes (continued)

Field	Description
Load Balancing Method	Specify one of the following load balancing methods: • dst-ip—Loads distribution on the destination IP address. • dst-mac—Loads distribution on the destination MAC address. • dst-port—Loads distribution on the destination TCP or UDP port. • src-dst-ip—Loads distribution on the source or destination IP address. • src-dst-mac—Loads distribution on the source or destination MAC address. • src-dst-port—Loads distribution on the source or destination port. • src-ip—Loads distribution on the source IP address. • src-mac—Loads distribution on the source MAC address. • src-port—Loads distribution on the TCP or UDP source port.
Switchport Type	Specify the interface switchport type: • N/A—Indicates that the switchport type is not specified. • Access—Specifies that the port interface is an access port. You must specify a VLAN as an access port in the Access VLAN field. • Trunk—Specifies that the port interface is a trunk port. When you select Trunk, you must complete the following fields: – Trunk Native VLAN – Trunk Allowed VLANs

Step 4 Click:

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

Related Topic

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



CHAPTER 10

Configuring High Availability

Revised Date: 3/25/09

High Availability (or fault tolerance) ensures that your network services and applications are always available. High availability (HA) provides seamless switchover of flows in case an ACE Device Manager becomes unresponsive or a critical host or interface fails. High Availability uses two nodes, where one node is that *active* node and the other is the *standby* node.

The ANM high availability feature includes:

- Automatic determination of node status, whether *active* or *standby*, using heartbeat counts
- Designation of the virtual IP address (VIP), which is associated with the active node
- Near real-time replication of ANM configuration and events after a failover occurs
- Automatic inspection of certificate/key presence on HA peer upon SSL certificate or key import.

For information about ACE redundancy, see [Understanding ACE Redundancy, page 10-20](#).

Related Topics

- [Understanding High Availability, page 10-1](#)
- [Understanding High Availability Processes, page 10-2](#)
- [Configuring High Availability Overview, page 10-4](#)

Understanding High Availability

During normal operation, high availability performs the following actions:

- The two nodes constantly exchange heartbeat packets over both interfaces.
- Database operations that occur on the active node's database are replicated on the standby node's database.
- The monitor function ensures that the necessary processes are running on both the active and standby node. For example, not all processes necessarily run on the standby node, so after a node changes from active to standby, the ANM high availability function stops certain processes on the standby node.

When you log into the ANM, you log in via a virtual IP address (VIP) that associates with the active node. The VIP is the only IP address you need to remember. If the current active node fails, the standby node takes over as the active node and the VIP automatically associates with the node that has just become active. When a failover occurs and the standby node becomes the active node, all existing web

sessions are lost. In addition, there is a slight delay while the standby node takes over as the active node. After the switchover is complete and the ANM fully initializes, you can log into the ANM using the same VIP. All ANM functions remain the same.

The ANM uses heartbeat counts to determine when a failover should occur. Because both nodes are constantly sending and receiving heartbeat packets, if heartbeat packets are no longer being received on a node, its peer node is determined to be dead. If this peer node was the active node, then the standby node takes over as the active node. The VIP automatically associates with the newly active node, and the monitoring process starts any necessary processes on the newly active node that were not already running.

Similarly, if you manually issue a failover to cause the active node to become the standby node, the heartbeat process disassociates the VIP from the node and tells the monitoring function to stop processes that are not normally run on the standby node.

Related Topics

- [Understanding High Availability Processes, page 10-2](#)
- [Configuring High Availability Overview, page 10-4](#)

Understanding High Availability Processes

During normal high availability operation, the active node runs all ANM processes required for normal operation of the ANM. The standby node runs only a minimal set of processes. [Table 10-3](#) lists the processes, their descriptions, and on which node they run.



Note

If you are running standalone ANM, all processes show in [Table 10-3](#), with the exception of the heartbeat process, are constantly running.

Table 10-1 ANM High Availability Processes

Process	Description	Node on Which Process Runs
Monit	Starts, stops, restarts, and monitors local ANM processes	Active and standby
Heartbeat	Provides UDP-based heartbeat between nodes, helps determine active vs. standby states, and associates the VIP	Active and standby
Mysql	Provides persistent storage and implements database replication between active and standby nodes	Active and standby
DCM	Java process	Active node only
DAL	Java process	Active node only
Ip-disc	Java process	Active node only
Licman	Java process for license management	Active and standby

Related Topics

- [CLI Commands for High Availability Processes, page 10-3](#)
- [Understanding High Availability, page 10-1](#)
- [Configuring High Availability Overview, page 10-4](#)

CLI Commands for High Availability Processes

You can use two commands to view ANM processes:

- You can use the `/opt/CSCOanm/bin/anm-tool` command to start and stop the ANM processes and to view the status of the ANM processes.
- You can use the `/opt/CSCOanm/bin/anm-ha` command to check high availability configuration or to force a node to become standby or active.

Table 10-2 lists the sub-commands and their descriptions.

Table 10-2 CLI Sub-commands for Processes

Command	Sub-command	Description
/opt/CSCOanm/bin/anm-tool	info-services	Indicates the state of all ANM processes. This command does not return process status if <i>monit</i> is not running.
	stop-services	Stops all ANM processes, including <i>monit</i> . Note <i>Monit</i> must be running in order for the info-services command to provide status information.
	start-services	Starts the relevant ANM processes.
	restart-services	Restarts the relevant ANM processes.
	info	Provides additional information (state, whether running or stopped, start time, and PID) regarding the Java processes. <i>Monit</i> need not be running for this command to return information.
/opt/CSCOanm/bin/anm-ha	check	Checks the local node's high availability configuration. If errors are returned, it's likely that HA will not function correctly until you fix the errors. Note You must run this command on both the active and standby node. While errors might indicate a problem, they could also simply indicate a known condition. For example, you receive a warning if the ANM cannot ping the peer node via either of the specified IP addresses; however, if the peer is down, the warning can be ignored because this is a known issue. It is also possible that no error might be returned even though there is a configuration problem. For example, the configuration of the two nodes must match; however the check sub-command cannot validate that the configurations match.
	active	Forces the local node to become <i>active</i> and the peer node to become the <i>standby</i> node.
	standby	Forces the local node to become <i>standby</i> and the peer node to become the <i>active</i> node.

Related Topics

- [Understanding High Availability Processes, page 10-2](#)
- [Understanding High Availability, page 10-1](#)
- [Configuring High Availability Overview, page 10-4](#)

Configuring High Availability Overview

The ANM high availability consists of two nodes, which both run the ANM software. Each node must have at least two network interfaces:

- A primary interface, normally used to access the node.
- A heartbeat interface, which is used to provide additional redundancy. The heartbeat interfaces of the two nodes must be connected via a crossover Ethernet connection.
- The two Ethernet interfaces used on one of the hosts should match the two interfaces used on the other host, with regard to the subnets they participate in. For example, if HA Node 1 uses eth0 for the primary interface and eth1 for the heartbeat interface, then HA Node 2 should also use eth0 for the primary interface and eth1 for the heartbeat interface.



Note

The ANM does not configure the primary and heartbeat IP addresses of the nodes' interfaces. You must manually configure the node's interfaces.

When you installed the ANM, you provided values for high availability parameters, determined the node IDs of the two nodes designated as *Node 1* and *Node 2*. For additional information about the installation parameters, see the *Installation Guide for the Cisco Application Networking Manager 2.0*.

Related Topics

- [Understanding High Availability, page 10-1](#)
- [Configuring High Availability Groups, page 10-8](#)
- [Configuring ACE High Availability, page 10-4](#)

Configuring ACE High Availability

The tasks involved with configuring high availability on ACE devices are described in [Table 10-3](#).

Table 10-3 High Availability Task Overview

	Task	Reference
Step 1	Create a fault-tolerant VLAN and identify peer IP addresses and configure peer devices for heartbeat count and interval.	Configuring ACE High Availability Peers, page 10-5
Step 2	Reconcile SSL certificates and keys, create a fault-tolerant group, assign peer priorities, associate the group with a context, place the group in service, and enable automatic synchronization.	Configuring High Availability Groups, page 10-8
Step 3	Configure tracking for switchover.	High Availability Tracking and Failure Detection Overview, page 10-13

Related Topics

- [Understanding ACE Redundancy, page 10-20](#)
- [Configuring ACE High Availability Peers, page 10-5](#)

- [Configuring High Availability Groups, page 10-8](#)
- [High Availability Tracking and Failure Detection Overview, page 10-13](#)

Configuring ACE High Availability Peers



Note

This functionality is available for only Admin contexts.

Fault-tolerant peers transmit and receive heartbeat packets and state and configuration replication packets. The standby member uses the heartbeat packet to monitor the health of the active member, while the active member uses the heartbeat packet to monitor the health of the standby member. When the heartbeat packets are not received from the active member when expected, switchover occurs and the standby member assumes all active communications previously on the active member.

Use this procedure to:

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

Assumption

- At least one fault-tolerant VLAN has been configured.



Note

A fault-tolerant VLAN cannot be used for other network traffic.

Procedure

- Step 1** Select **Config > Devices > admin_context > High Availability (HA) > Setup**. The HA Management window appears with two columns: One for the selected ACE Device Manager and one for a peer ACE Device Manager.
- Step 2** Click **Edit**, then enter the information for the primary ACE and the peer ACE as described in [Table 10-4](#).

Table 10-4 High Availability Management Configuration Attributes

Field	This Module	Peer Module
Module	Name of the ACE	
VLAN	Specify a fault-tolerant VLAN to be used for this high availability pair. Valid entries are integers from 2 to 4094. Note This VLAN cannot be used for other network traffic.	Not applicable.

Table 10-4 High Availability Management Configuration Attributes (continued)

Field	This Module	Peer Module
IP Address	Enter an IP address for the fault-tolerant VLAN in dotted-decimal format, such as 192.168.11.2.	Enter the IP address of the peer interface in dotted-decimal format so that the peer ACE can communicate on the fault-tolerant VLAN.
Netmask	Select the subnet mask that is to be used for the fault-tolerant VLAN.	Not applicable.
Query VLAN	Select the VLAN that the standby ACE is to use to determine whether the active ACE is down or if there is a connectivity problem with the fault-tolerant VLAN.	
Heartbeat Count	Enter the number of heartbeat intervals that must occur with no heartbeat packet received by the standby ACE before the standby ACE determines that the active member is not available. Valid entries are integers from 10 to 50.	Not applicable.
Heartbeat Interval	Enter the number of milliseconds that the active ACE is to wait between each heartbeat it sends to the standby ACE. Valid entries are integers from 100 to 1000.	Not applicable.
Interface Enabled	Select the Interface Enabled check box to enable the high availability interface. Clear the check box to disable the high availability interface.	Not applicable.
HA State	This is a read-only field with the current state of high availability on the ACE.	Not applicable.

Step 3 Click:

- **Deploy Now** to save your entries and to continue with configuring high availability groups. The HA Management screen appears at the top of the content area and the HA Groups table appears at the bottom. See [Configuring High Availability Groups, page 10-8](#) to configure a high availability group.
- **Cancel** to exit this procedure without saving your entries and to view the HA Management screen.

Related Topics

- [Understanding High Availability, page 10-1](#)
- [Configuring High Availability Overview, page 10-4](#)
- [Configuring High Availability Groups, page 10-8](#)
- [Synchronizing ACE High Availability Configurations, page 10-19](#)
- [Tracking VLAN Interfaces for High Availability, page 10-13](#)

Clearing High Availability Pairs

**Note**

This functionality is available for only Admin contexts.

Use this procedure to remove a high availability link between two ACEs.

Procedure

-
- Step 1** Select **Config > Devices > *admin_context* > High Availability (HA) > Setup**. The HA Management screen appears.
- Step 2** Select the ACE pair whose high availability configuration you want to remove, then click **Clear**. A message appears asking you to confirm the clearing of the high availability link.
- Step 3** Click:
- **OK** to confirm the removal of this high availability link and to return to the HA Management screen.
 - **Cancel** to exit this procedure without removing this high availability link and to return to the HA Management screen.
-

Related Topics

- [Understanding High Availability, page 10-1](#)
- [Configuring ACE High Availability Peers, page 10-5](#)
- [Editing High Availability Groups, page 10-9](#)
- [High Availability Tracking and Failure Detection Overview, page 10-13](#)
- [Tracking VLAN Interfaces for High Availability, page 10-13](#)
- [Tracking Hosts for High Availability, page 10-14](#)

Configuring High Availability Groups

**Note**

This functionality is available for only Admin contexts.

A fault-tolerant group consists of a maximum of two contexts: One active context on one ACE and one standby context on the peer ACE. You can create multiple fault-tolerant groups on each ACE up to a maximum of 251 groups (250 user contexts and 1 Admin context).

Use this procedure to configure high availability groups.

Assumption

At least one high availability pair has been configured. (See [Configuring ACE High Availability Peers, page 10-5](#).)

Procedure

-
- Step 1** **Config > Devices > *admin_context* > High Availability (HA) > Setup.** The HA Management screen appears at the top of the content area and the HA Groups table appears at the bottom.
- Step 2** In the HA Groups table, click **Add** to add a new high availability group. The table refreshes with the configurable fields.
- Step 3** Select the Enabled check box to enable the high availability group. Clear the Enabled check box to disable the high availability group.
- Step 4** In the Context field, select the virtual context to associate with this high availability group.
- Step 5** In the Priority (Actual) field, enter the priority you want to assign to the first device in the group. Valid entries are integers from 1 to 255.
- A member of a fault-tolerant group becomes the active member through a process based on the priority assigned. In this process, the group member with the higher priority becomes the active member. When you set up a fault-tolerant pair, use a higher priority for the group where the active member initially resides.
- Step 6** Select the Preempt check box to indicate that the group member with the higher priority is to always assert itself and become the active member. Clear the Preempt check box to indicate that you do not want the group member with the higher priority to always become the active member.
- Step 7** In the Priority (Actual) field, enter the priority you want to assign to the peer device in the group. Valid entries are integers from 1 to 255.
- A member of a fault-tolerant group becomes the active member through a process based on the priority assigned. In this process, the group member with the higher priority becomes the active member. When you set up a fault-tolerant pair, use a higher priority for the group where the active member initially resides.
- Step 8** Leave the Autosync Run check box *unchecked* to enable automatic synchronization of the running configuration files. Clear the Autosync Run check box to disable automatic synchronization of the running configuration files. If you disable automatic synchronization, you need to update the configuration of the standby context manually. See [Synchronizing Virtual Context Configurations, page 3-66](#).

**Note**

If you check **Autosync Run** for the HA group, you must manually sync the standby context in order for ANM to allow subsequent configuration changes. Until you have done this, the standby context will be marked out of sync. See [Synchronizing Virtual Context Configurations in High Availability Mode, page 10-19](#).

Step 9 Select the Autosync Startup check box to enable automatic synchronization of the startup configuration files. Clear the Autosync Run check box to disable automatic synchronization of the startup configuration files. If you disable automatic synchronization, you need to update the configuration of the standby context manually. See [Synchronizing Virtual Context Configurations, page 3-66](#).

Step 10 Click:

- **Deploy Now** to accept your entries. The HA Groups table refreshes with the new high availability group.
- **Cancel** to exit this procedure without saving your entries and to return to the HA Management screen and HA Groups table.

Related Topics

- [Configuring ACE High Availability Peers, page 10-5](#)
- [Editing High Availability Groups, page 10-9](#)
- [Synchronizing Virtual Context Configurations, page 3-66](#)
- [Tracking VLAN Interfaces for High Availability, page 10-13](#)
- [Tracking Hosts for High Availability, page 10-14](#)

Editing High Availability Groups

Use this procedure to modify the attributes of a high availability group.

**Note**

This functionality is available for only Admin contexts.

**Note**

If you need to modify a fault-tolerant group, take the group out of service before making any other changes (see [Taking a High Availability Group Out of Service, page 10-10](#)). When you finish making all changes, place the group back into service (see [Enabling a High Availability Group, page 10-11](#)).

Procedure

- Step 1** Select **Config > Devices > *admin_context* > High Availability (HA) > Setup**. The HA Management screen appears at the top of the content area and the HA Groups table appears at the bottom.
- Step 2** In the HA Groups table, select the high availability group you want to modify, then click **Edit**. The table refreshes with configurable fields.
- Step 3** Modify the fields as desired. For information on these fields, see [Configuring High Availability Groups, page 10-8](#).

**Note**

If you leave unchecked **Autosync Run** for the HA group, you must manually sync the standby context in order for ANM to allow subsequent configuration changes. Until you have done this, the standby context will be marked out of sync. See [Synchronizing Virtual Context Configurations in High Availability Mode, page 10-19](#).

- Step 4** When you finish modifying this group, click:
- **Deploy Now** to accept your entries and to return to the HA Groups table.
 - **Cancel** to exit this procedure without saving your entries and to return to the HA Management screen.

Related Topics

- [Configuring High Availability Groups, page 10-8](#)
- [Taking a High Availability Group Out of Service, page 10-10](#)
- [Enabling a High Availability Group, page 10-11](#)
- [Configuring ACE High Availability Peers, page 10-5](#)
- [High Availability Tracking and Failure Detection Overview, page 10-13](#)

Taking a High Availability Group Out of Service

**Note**

This functionality is available for only Admin contexts.

If you need to modify a fault-tolerant group, you must first take the group out of service before making any other changes. Use this procedure to take a high availability group out of service.

Procedure

- Step 1** Select **Config > Devices > admin_context > High Availability (HA) > Setup**. The HA Management screen appears at the top of the content area and the HA Groups table appears at the bottom.
- Step 2** In the HA Groups table, select the high availability group you want to take out of service, then click **Edit**. The table refreshes with configurable fields.
- Step 3** Clear the **Enabled** check box.
- Step 4** Click **Deploy Now** to take the high availability group out of service and to return to the HA Groups table. You can now make the necessary modifications to the high availability group. To put the high availability group back in service, see [Enabling a High Availability Group, page 10-11](#).

Related Topic

- [Enabling a High Availability Group, page 10-11](#)

Enabling a High Availability Group

**Note**

This functionality is available for only Admin contexts.

After you take a high availability group out of service to modify it, you need to reenable the group. Use the following procedure to put a high availability group back in service.

Procedure

- Step 1** Select **Config > Devices > *admin_context* > High Availability (HA) > Setup**. The HA Management screen appears at the top of the content area and the HA Groups table appears at the bottom.
- Step 2** In the HA Groups table, select the high availability group you want to take out of service, then click **Edit**. The table refreshes with configurable fields.
- Step 3** Select the **Enabled** check box.
- Step 4** Click **Deploy Now** to put the high availability group in service and to return to the HA Groups table.

Related Topic

- [Taking a High Availability Group Out of Service, page 10-10](#)

Switching Over a High Availability Group

**Note**

This functionality is available for only Admin contexts.

You may need to cause a switchover when you want to make a particular context the standby (for example, for maintenance or a software upgrade on the currently active context). If the standby group member can statefully become the active member of the high availability group, a switchover occurs.

Use this procedure to force the failover of a high availability group.

Procedure

- Step 1** Select **Config > Devices > *admin_context* > High Availability (HA) > Setup**. The HA Management screen appears at the top of the content area and the HA Groups table appears at the bottom.
- Step 2** In the HA Groups table, select the group you want to switch over, then click **Switchover**. The standby group member becomes active, while the previously active group member becomes the standby member.

**Note**

You must manually sync the standby context in order for ANM to allow subsequent configuration changes. Until you have done this, the standby context will be marked out of sync. See [Synchronizing Virtual Context Configurations in High Availability Mode, page 10-19](#).

Related Topics

- [Understanding High Availability, page 10-1](#)
- [Configuring ACE High Availability Peers, page 10-5](#)
- [Configuring High Availability Groups, page 10-8](#)
- [Tracking VLAN Interfaces for High Availability, page 10-13](#)

Deleting High Availability Groups

**Note**

This functionality is available for only Admin contexts.

Use this procedure to remove a high availability group from ACE Device Manager management.

Procedure

- Step 1** Select **Config > Devices > *admin_context* > High Availability (HA) > Setup**. The HA Management screen appears at the top of the content area and the HA Groups table appears at the bottom.
- Step 2** In the HA Groups table, select the high availability group that you want to remove, then click **Delete**. A message appears asking you to confirm the deletion.
- Step 3** Click:
 - **Deploy Now** to delete the high availability group and to return to the HA Groups table. The selected group no longer appears.
 - **Cancel** to exit this procedure without deleting the high availability group and to return to the HA Groups table.

Related Topics

- [Configuring ACE High Availability Peers, page 10-5](#)
- [Configuring High Availability Groups, page 10-8](#)
- [Tracking VLAN Interfaces for High Availability, page 10-13](#)

High Availability Tracking and Failure Detection Overview

The ANM supports the tracking and detection of failures to ensure that switchover occurs as soon as the criteria are met (see [Configuring ACE High Availability Peers](#), page 10-5). You can track and detect failures on:

- Hosts—See [Tracking Hosts for High Availability](#), page 10-14.
- Interfaces—See [Tracking VLAN Interfaces for High Availability](#), page 10-13.

When the active member of a fault-tolerant group becomes unresponsive, the following occurs:

1. The active member's priority is reduced by 10.
2. If the resulting priority value is less than that of the standby member, the active member switches over and the standby member becomes the new active member. All active flows continue uninterrupted.
3. When the failed member comes back up, its priority is incremented by 10.
4. If the resulting priority value is greater than that of the currently active member, a switchover occurs again, returning the flows to the originally active member.

**Note**

In a user context, the ACE allows a switchover only of the fault-tolerant groups belonging to that context. In an Admin context, the ACE allows a switchover of all fault-tolerant groups on all configured contexts on the ACE.

Related Topics

- [Configuring High Availability Groups](#), page 10-8
- [Tracking VLAN Interfaces for High Availability](#), page 10-13
- [Tracking Hosts for High Availability](#), page 10-14

Tracking VLAN Interfaces for High Availability

Use this procedure to configure a tracking and failure detection process for a VLAN interface.

Procedure

- Step 1** Select **Config > Devices > *admin_context* > HA Tracking and Failure Detection > Interfaces**. The Track Interface table appears.
- Step 2** Click **Add** to add a new tracking process to this table, or select an existing entry, then click **Edit** to modify it. The Track Interface configuration screen appears.
- Step 3** In the Track Object Name field, enter a unique identifier for the tracking process. Valid entries are unquoted text strings with no spaces.
- Step 4** In the Priority field, enter the priority for the interface on the active member. Valid entries are integers from 0 to 255 with higher values indicating higher priorities. The values that you enter here and in the Interface Peer Priority field (see [Step 6](#)) reflect the point at which you want switchover to occur. If the tracked interface goes down, the priority of that fault-tolerant group is decremented by the value entered in the Priority field. If the priority of the fault-tolerant group on the active member falls below that of the standby member, a switchover occurs.

- Step 5** In the VLAN Interface field, select the fault-tolerant VLAN that you want the active member to track.
- Step 6** In the Interface Peer Priority field, enter the priority for the interface on the standby member. Valid entries are integers from 0 to 255 with higher values indicating higher priorities. The values that you enter here and in the Priority field (See [Step 4](#)) reflect the point at which you want switchover to occur. If the tracked interface goes down, the priority of that fault-tolerant group is decremented by the value entered in the Interface Peer Priority field. If the priority of the fault-tolerant group on the active member falls below that of the standby member, a switchover occurs.
- Step 7** In the Peer VLAN Interface field, enter the identifier of an existing fault-tolerant VLAN that you want the standby member to track. Valid entries are integers from 1 to 4096.
- Step 8** Click:
- **Deploy Now** to save your entries and to return to the Track Interface table.
 - **Cancel** to exit this procedure without saving your entries and to return to the Track Interface table.
 - **Next** to deploy your entries and to configure the next entry in the Track Interface table.
-

Related Topics

- [Configuring ACE High Availability Peers, page 10-5](#)
- [Configuring High Availability Groups, page 10-8](#)
- [Tracking Hosts for High Availability, page 10-14](#)

Tracking Hosts for High Availability

Use this procedure to configure a tracking and failure detection process for a gateway or host.

Procedure

- Step 1** Select **Config > Devices > *admin_context* > HA Tracking and Failure Detection > Hosts**. The Track Host table appears.
- Step 2** Click **Add** to add a new tracking process to the table, or select an existing entry, then click **Edit** to modify it. The Track Host configuration screen appears.
- Step 3** In the Track Object Name field, enter a unique identifier for the tracking process. Valid entries are unquoted text strings with no spaces.
- Step 4** In the Track Host/IP Address field, enter the IP address or hostname of the gateway or host that you want the active member of the high availability group to track. Enter the IP address in dotted-decimal format, such as 192.168.11.2.
- Step 5** In the Priority field, enter the priority of the probe sent by the active member. Valid entries are integers from 0 to 255. Higher values indicate higher priorities. Assign a priority value based on the relative importance of the host that the probe is tracking. If the probe goes down, the ACE decrements the priority of the fault-tolerant group on the active member by the value in the Priority field.
- Step 6** In the Peer Host/IP Address field, enter the IP address or hostname of the host that you want the standby member to track. Enter the IP address using dotted-decimal notation, such as 192.168.11.2.

Step 7 In the Peer Priority field, enter the priority of the probe sent by the standby member. Valid entries are integers from 0 to 255. Higher values indicate higher priorities. Assign a priority value based on the relative importance of the host that the probe is tracking. If the probe goes down, the ACE decrements the priority of the fault-tolerant group on the standby member by the value in the Priority field.

Step 8 Click:

- **Deploy Now** to save your entries and to continue with configuring track host probes. See [Configuring Host Tracking Probes, page 10-15](#).
 - **Cancel** to exit this procedure without saving your entries and to return to the Track Host table.
 - **Next** to deploy your entries and to configure another tracking process.
-

Related Topics

- [Configuring Host Tracking Probes, page 10-15](#)
- [Configuring ACE High Availability Peers, page 10-5](#)
- [Configuring High Availability Groups, page 10-8](#)
- [Tracking VLAN Interfaces for High Availability, page 10-13](#)

Configuring Host Tracking Probes

Use this procedure to configure probes on the active high availability group member to track the health of the gateway or host.

Assumptions

- At least one host tracking process for high availability has been configured (see [Tracking Hosts for High Availability, page 10-14](#).)
- At least one health monitoring probe has been configured (see [Configuring Health Monitoring for Real Servers, page 5-25](#)).

Procedure

Step 1 Select **Config > Devices > *admin_context* > HA Tracking and Failure Detection > Hosts**. The Track Host table appears.

- Step 2** Select the tracking process you want to modify, then select the Peer Track Host Probe tab. The Peer Track Host Probes table appears.
- Step 3** In the Peer Track Host Probes table, click **Add** to add a peer host tracking probe, or select an existing peer host tracking probe, then click Edit to modify it. The Peer Track Host Probes configuration screen appears.
- Step 4** In the Probe Name field, select the name of the probe to be used for the peer host tracking process.
- Step 5** In the Priority field, enter a priority for the host you are tracking by the active member. Valid entries are integers from 1 to 255 with higher values indicating higher priorities. Assign a priority value based on the relative importance of the gateway or host that the probes are tracking. If the host goes down, the ACE decrements the priority of the high availability group on the standby member by the value in this Priority field.
- Step 6** Click:
- **Deploy Now** to save your entries and to return to the Track Host Probe table. The table includes the added probe.
 - **Cancel** to exit this procedure without saving your entries and to return to the Track Host Probe table.
 - **Next** to deploy your entries and to configure another track host probe.
-

Related Topics

- [Configuring Peer Host Tracking Probes, page 10-17](#)
- [Configuring ACE High Availability Peers, page 10-5](#)
- [Configuring High Availability Groups, page 10-8](#)
- [Tracking VLAN Interfaces for High Availability, page 10-13](#)

Deleting Host Tracking Probes

Use this procedure to remove a high availability host tracking probe.

Procedure

- Step 1** Select **Config > Devices > ACE *admin_context* > HA Tracking and Failure Detection > Hosts**. The Track Host table appears.
- Step 2** Select the tracking process you want to modify, then select the Track Host Probe tab. The Track Host Probe table appears.
- Step 3** In the Track Host table, select the probe you want to remove, then click **Delete**. The probe is deleted and the Track Host Probe table refreshes without the deleted probe.
-

Related Topics

- [Configuring Peer Host Tracking Probes, page 10-17](#)
- [Configuring ACE High Availability Peers, page 10-5](#)
- [Configuring High Availability Groups, page 10-8](#)
- [Tracking VLAN Interfaces for High Availability, page 10-13](#)

Configuring Peer Host Tracking Probes

Use this procedure to configure probes on the standby member of a high availability group to track the health of the gateway or host.

Assumptions

- At least one host tracking process for high availability has been configured (see [Tracking Hosts for High Availability](#), page 10-14.)
- At least one health monitoring probe has been configured (see [Configuring Health Monitoring for Real Servers](#), page 5-25).

Procedure

-
- Step 1** Select **Config > Devices > ACE admin_context > HA Tracking and Failure Detection > Hosts**. The Track Host table appears.
- Step 2** Select the tracking process you want to modify, then select the Peer Track Host Probe tab. The Peer Track Host Probes table appears.
- If the Track Host Probe and Peer Track Host Probes tabs do not appear below the Track Host table, click **Show Tabs** below the Track Host table name.
- Step 3** In the Peer Track Host Probes table, click **Add** to add a peer host tracking probe, or select an existing peer host tracking probe, then click **Edit** to modify it. The Peer Track Host Probes configuration screen appears.
- Step 4** In the Probe Name field, select the name of the probe to be used for the peer host tracking process.
- Step 5** In the Priority field, enter a priority for the host you are tracking by the standby member of the high availability group. Valid entries are integers from 0 to 255 with higher values indicating higher priorities. Assign a priority value based on the relative importance of the gateway or host that the probes are tracking. If the host goes down, the ACE decrements the priority of the high availability group on the standby member by the value in this Priority field.
- Step 6** Click:
- **Deploy Now** to save your entries and to return to the Peer Track Host Probes table. The table includes the added probe.
 - **Cancel** to exit this procedure without saving your entries and to return to the Peer Track Host Probes table.
 - **Next** to deploy your entries and to configure another peer track host probe.
-

Related Topics

- [Configuring Host Tracking Probes](#), page 10-15
- [Configuring ACE High Availability Peers](#), page 10-5
- [Configuring High Availability Groups](#), page 10-8
- [Tracking VLAN Interfaces for High Availability](#), page 10-13

Deleting Peer Host Tracking Probes

Use this procedure to remove a high availability peer host tracking probe.

Procedure

-
- Step 1** Select **Config > Devices > ACE admin_context > HA Tracking and Failure Detection > Hosts**. The Track Host table appears.
- Step 2** Select the tracking process you want to modify then, select the Peer Track Host Probe tab. The Peer Track Host Probes table appears.
- If the Track Host Probe and Peer Track Host Probes tabs do not appear below the Track Host table, click **Show Tabs** below the Track Host table name.
- Step 3** In the Peer Track Host Probes table, select the probe you want to remove, then click **Delete**. The probe is deleted and the Peer Track Host Probes table refreshes without the deleted probe.
-

Related Topics

- [Configuring Peer Host Tracking Probes, page 10-17](#)
- [Configuring Host Tracking Probes, page 10-15](#)
- [Tracking VLAN Interfaces for High Availability, page 10-13](#)

Configuring ACE HSRP Groups

This section describes how to add or edit a Hot Standby Router Protocol (HSRP) group.

Assumptions

- At least one host tracking process for high availability has been configured (see [Tracking Hosts for High Availability, page 10-14](#).)
- Before you configure an HSRP tracking and failure detection process on the ACE, you must configure the HSRP group on the Catalyst 6500 Supervisor.

Procedure

-
- Step 1** Select **Config > Devices > ACE admin_context > HA Tracking and Failure Detection > HSRP Groups**. The HSRP Groups table appears.
- Step 2** Click **Add** to add a new HSRP group or select an existing entry, then click **Edit** to modify it. The HSRP Group configuration screen appears.
- Step 3** In the Track Object Name field, enter a unique identifier for the tracking process. Valid entries are unquoted text strings with no spaces.
- Step 4** In the Priority field, enter the priority of the HSRP group as an integer from 0 to 255. The default is 0. Higher values indicate higher priorities. Assign a priority value based on the relative importance of the HSRP group that you are tracking. If the HSRP group goes down, the ACE decrements the priority of the FT group on the active member. If the priority of the FT group on the active member falls below the priority of the FT group on the standby member, a switchover occurs.

- Step 5** In the HSRP Group Name, enter a name for the HSRP group.
- Step 6** In the HSRP Peer Priority field, enter the priority of the HSRP group as an integer from 0 to 255. The default is 0. Higher values indicate higher priorities. Assign a priority value based on the relative importance of the HSRP group you are tracking. If the HSRP group goes down, the ACE decrements the priority of the FT group on the standby member.
- Step 7** In the HSRP Group Name of Peer field, enter a name for the HSRP group on the peer ACE.
- Step 8** Click:
- **Deploy Now** to save your entries and to return to the HSRP Groups table. The table includes the added HSRP group.
 - **Cancel** to exit this procedure without saving your entries and to return to the HSRP Groups table.

Synchronizing ACE High Availability Configurations

When two ACE Device Manager devices are configured as high availability peers, their configurations must be synchronized at all times so that the standby member can take over for the active member seamlessly. As they synchronize, however, the configuration on the hot standby ACE can become out of sync with the ACE Device Manager-maintained configuration data for that ACE.



Note

The Application Networking Manager manages local configurations only.



Note

Although a context might have been configured for syslog notification, changes applied to the standby ACE configuration can change syslog notification configuration so that you are not notified of the out-of-sync configurations. **As a result, it is important for you to manually synchronize the ACE Device Manager with the standby ACE.**

Synchronizing configuration files for the standby ACE requires:

1. Auditing the standby ACE to confirm that its configuration does not agree with the ACE Device Manager-maintained configuration data for the ACE. See [Synchronizing Virtual Context Configurations](#), page 3-66.
2. Uploading the configuration from the standby ACE to the ACE Device Manager server. See [Synchronizing Virtual Context Configurations](#), page 3-66.
3. Ensuring that the SSL certificate/keys are imported and identical for the pair. See [Synchronizing SSL Certificate and Key Pairs on Both Peers](#), page 10-20.
4. For an Admin context, uploading configurations on any newly imported user contexts. If new user contexts are not updated, they cannot be managed using ACE Device Manager.

Synchronizing Virtual Context Configurations in High Availability Mode

In a high availability pair, the two configured virtual contexts synchronize with each other as part of their ongoing communications. However, their copies do not synchronize in ACE Device Manager and the configuration on the standby member can become out of sync with the configuration on the ACE appliance.

After the active member of a high availability pair fails and the standby member becomes active, the newly active member detects any out-of-sync virtual context configurations and reports that status in the Virtual Contexts table so that you can synchronize the virtual context configurations.

For information on synchronizing virtual context configurations, see [Synchronizing Virtual Context Configurations](#), page 3-66.

Related Topics

- [Configuring ACE High Availability Peers](#), page 10-5
- [Configuring High Availability Groups](#), page 10-8
- [Synchronizing Virtual Context Configurations](#), page 3-66

Synchronizing SSL Certificate and Key Pairs on Both Peers

When SSL certificate/key import is attempted on a peer that is configured in HA, ACE Device Manager automatically detects the HA state and also imports the same cert/key into the other HA peer. In addition, when you are configuring two peers in HA from ANM, a warning message appears asking you to perform certificate/key reconciliation and offers the appropriate screen enabling you to do this.

Understanding ACE Redundancy

ACE redundancy (or fault tolerance) uses a maximum of two ACEs in the same Catalyst 6500 switch or in separate switches to ensure that your network remains operational even if one of the modules becomes unresponsive.



Note

High Availability is supported between ACEs of the same type only.

For additional information about ACE redundancy, see the *Cisco Application Control Engine Module Administration Guide*.

Related Topics

- [ACE High Availability Polling](#), page 10-20
- [ACE Redundancy Protocol](#), page 10-21

ACE High Availability Polling

Approximately every two minutes, the ANM issues the **show ft group** command to the ACE to gather the redundancy statistics of each virtual context. The state information is displayed in the HA State and HA Autosync fields when you click **Config > Devices > virtual context**.

The possible HA states are:

- Active—Local member of the FT group is active and processing flows.
- Standby Cold—Indicates if the FT VLAN is down but the peer ACE is still alive, or the configuration or application state synchronization failed. When a context is in this state and a switchover occurs, the transition to the ACTIVE state is stateless.

- Standby Bulk—Local standby context is waiting to receive state information from its active peer context. The active peer context receives a notification to send a snapshot of the current state information for all applications to the standby context.
- Standby Hot—Local standby context has all the state information it needs to statefully assume the active state if a switchover occurs.

Related Topics

- [ACE High Availability Polling, page 10-20](#)
- [ACE Redundancy Protocol, page 10-21](#)

ACE Redundancy Protocol

You can configure a maximum of two ACEs of the same type (peers) for redundancy in the same Catalyst 6500 switch or in different chassis for redundancy. Each peer ACE can contain one or more fault-tolerant (FT) groups. Each FT group consists of two members: one active context and one standby context. An FT group has a unique group ID that you assign.

One virtual MAC address (VMAC) is associated with each FT group. The format of the VMAC is: 00-0b-fc-fe-1b-*groupID*. Because a VMAC does not change upon switchover, the client and server ARP tables does not require updating. The ACE selects a VMAC from a pool of virtual MACs available to it. For more information, see [Configuring Virtual Contexts, page 3-5](#).

Each FT group acts as an independent redundancy instance. When a switchover occurs, the active member in the FT group becomes the standby member and the original standby member becomes the active member. A switchover can occur for the following reasons:

- The active member becomes unresponsive.
- A tracked host or interface fails.
- You force a switchover for a high availability group by clicking **Switchover** in the HA Groups table (see [Switching Over a High Availability Group, page 10-11](#)).

To outside nodes (clients and servers), the active and standby FT group members appear as one node with respect to their IP addresses and associated VMAC. ACE provides active-active redundancy with multiple contexts only when there are multiple FT groups configured on each ACE and both devices contain at least one active group member (context). With a single context, the ACE supports active-backup redundancy and each group member is an Admin context.

The ACE sends and receives all redundancy-related traffic (protocol packets, configuration data, heartbeats, and state replication packets) on a dedicated FT VLAN. You cannot use this dedicated VLAN for normal traffic.

To optimize the transmission of heartbeat packets for multiple FT groups and to minimize network traffic, the ACE sends and receives heartbeat messages using a separate process. The ACE uses the heartbeat to probe the peer ACE, rather than probe each context. When an ACE does not receive a heartbeat from the peer ACE, all the contexts in the standby state become active. The ACE sends heartbeat packets over UDP. You can set the frequency with which the ACE sends heartbeat packets as part of the FT peer configuration. For details about configuring the heartbeat, see [Configuring ACE High Availability Peers, page 10-5](#).

The election of the active member within each FT group is based on a priority scheme. The member configured with the higher priority is elected as the active member. If a member with a higher priority is found after the other member becomes active, the new member becomes active because it has a higher priority. This behavior is known as preemption and is enabled by default. You can override this default

behavior by disabling preemption. To disable preemption, use the `Preempt` parameter. Enabling `Preempt` causes the member with the higher priority to assert itself and become active. For details about configuring preemption, see [Configuring High Availability Groups, page 10-8](#).

For additional information about ACE redundancy, see the *Cisco Application Control Engine Module Administration Guide*.

Related Topics

- [Understanding ACE Redundancy, page 10-20](#)
- [ACE High Availability Polling, page 10-20](#)

ACE Stateful Failover

The ACE replicates flows on the active FT group member to the standby group member per connection for each context. The replicated flows contain all the flow-state information necessary for the standby member to take over the flow if the active member becomes unresponsive. If the active member becomes unresponsive, the replicated flows on the standby member become active when the standby member assumes mastership of the context. The active flows on the former active member transition to a standby state to fully back up the active flows on the new active member.



Note

By default, connection replication is enabled in the ACE.

After a switchover occurs, the same connection information is available on the new active member. Supported end-user applications do not need to reconnect to maintain the same network session.

The state information passed to the standby ACE Device Manager includes the following data:

- Network Address Translation (NAT) table based on information synchronized with the connection record
- All Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) connections not terminated by the ACE
- HTTP connection states (Optional)
- Sticky table



Note

In a user context, the ACE allows a switchover only of the FT group that belongs to that context. In the Admin context, the ACE allows a switchover of all FT groups in all configured contexts in the ACE.

To ensure that bridge learning occurs quickly upon a switchover in a Layer 2 configuration in the case where a VMAC moves to a new location, the new active member sends a gratuitous ARP on every interface associated with the active context. Also, when there are two VLANs on the same subnet and servers need to send packets to clients directly, the servers must know the location of the gateway on the client-side VLAN. The active member acts as the bridge for the two VLANs. In order to initiate learning of the new location of the gateway, the new active member sends an ARP request to the gateway on the client VLAN and bridges the ARP response onto the server VLAN.

For additional information about ACE redundancy, see the *Cisco Application Control Engine Module Administration Guide*.

Related Topic

- [Understanding ACE Redundancy, page 10-20](#)

ACE Fault-Tolerant VLAN

ACE redundancy uses a dedicated fault-tolerant VLAN between redundant ACE Device Managers of the same type to transmit flow-state information and the redundancy heartbeat. Do not use this dedicated VLAN for normal network traffic. You must configure this same VLAN on both peers. You also must configure a different IP address within the same subnet on each ACE for the fault-tolerant VLAN.

The two redundant ACE Device Managers constantly communicate over the fault-tolerant VLAN to determine the operating status of each ACE. The standby member uses the heartbeat packet to monitor the health of the active member. The active member uses the heartbeat packet to monitor the health of the standby member. Communications over the switchover link include the following data:

- Redundancy protocol packets
- State information replication data
- Configuration synchronization information
- Heartbeat packets

For multiple contexts, the fault-tolerant VLAN resides in the system configuration data. Each fault-tolerant VLAN on the ACE has one unique MAC address associated with it. The ACE uses these ACE MAC addresses as the source or destination MACs for sending or receiving redundancy protocol state and configuration replication packets.

**Note**

The IP address and the MAC address of the fault-tolerant VLAN do not change at switchover.

For additional information about ACE redundancy, see the *Cisco Application Control Engine Module Administration Guide*.

Related Topic

[Understanding ACE Redundancy, page 10-20](#)

ACE Configuration Synchronization

For redundancy to function properly, both members of an fault-tolerant group must have identical configurations. The ACE automatically replicates the active configuration on the standby member using a process called *configuration synchronization* (config sync). Config sync automatically replicates any changes made to the configuration of the active member to the standby member. After the ACE synchronizes the redundancy configuration from the active member to the standby peer, it disables configuration mode on the standby. See [Configuring ACE High Availability Peers, page 10-5](#).

**Note**

The Application Networking Manager manages local configurations only.

For additional information about ACE redundancy, see the *Cisco Application Control Engine Module Administration Guide*.

Related Topic

[Understanding ACE Redundancy, page 10-20](#)

ACE Redundancy Configuration Requirements and Restrictions

Follow these requirements and restrictions when configuring the ACE redundancy feature.

- In bridged mode (Layer 2), two contexts cannot share the same VLAN.
- To achieve active-active redundancy, a minimum of two contexts and two fault-tolerant groups are required on each ACE.
- When you configure redundancy, the ACE keeps all interfaces that do not have an IP address in the Down state. The IP address and the peer IP address that you assign to a VLAN interface should be in the same subnet, but different IP addresses. For more information about configuring VLAN interfaces, see [Configuring VLAN Interfaces, page 9-2](#).

For additional information about ACE redundancy, see the *Cisco Application Control Engine Module Administration Guide*.

Related Topic

[Understanding ACE Redundancy, page 10-20](#)



CHAPTER 11

Configuring Traffic Policies

Revised Date: 3/25/09

Cisco Application Networking Manager helps you configure class maps and policy maps to provide a global level of classification for filtering traffic received by or passing through the ACE. This section includes the following topics about traffic policies:

- [Traffic Policy Overview, page 11-1](#)
- [Class Map and Policy Map Overview, page 11-2](#)
- [Configuring Virtual Context Class Maps, page 11-6](#)
- [Setting Match Conditions for Class Maps, page 11-8](#)
- [Configuring Virtual Context Policy Maps, page 11-30](#)
- [Configuring Rules and Actions for Policy Maps, page 11-33](#)

Traffic Policy Overview

Cisco Application Networking Manager helps you configure class maps and policy maps to provide a global level of classification for filtering traffic received by or passing through the ACE. You create traffic policies and attach these policies to one or more VLAN interfaces associated with the ACE to apply feature-specific actions to the matching traffic. The ACE uses the individual traffic policies to implement functions such as:

- FTP command inspection
- IP normalization and fragment reassembly
- Network Address Translation (NAT)
- Optimization of HTTP traffic
- Protocol deep packet inspection
- Remote access using Secure Shell (SSH) or Telnet
- Secure Socket Layer (SSL) security services between a Web browser (the client) and the HTTP connection (the server)
- Server load balancing
- TCP termination, normalization, and reuse

Related Topics

- [Class Map and Policy Map Overview, page 11-2](#)
- [Configuring Virtual Context Class Maps, page 11-6](#)
- [Configuring Virtual Context Policy Maps, page 11-30](#)

Class Map and Policy Map Overview

You classify inbound network traffic destined to, or passing through, the ACE based on a series of flow match criteria specified by a class map. Each class map defines a traffic classification; that is, network traffic that is of interest to you. A policy map defines a series of actions (functions) that you want applied to a set of classified inbound traffic.

Class maps enable you to classify network traffic based on the following criteria:

- Layer 3 and Layer 4 traffic flow information—Source or destination IP address, source or destination port, virtual IP address, or IP protocol
- Layer 7 protocol information—HTTP cookie, HTTP URL, HTTP header, HTTP content, FTP request commands, RADIUS, RDP, RTSP, Skinny, or SIP

The policies that you can configure depend on the ACE you are configuring. [Table 11-1](#) lists the available policies and the ACE devices that support them.

Table 11-1 Traffic Policies and ACE Device Support

Policy Map	Description	ACE Device		
		ACE 1.0 Module	ACE 2.0 Module	ACE Appliance
Generic Server Load Balancing	Generic Layer 7 policy map for server load balancing		X	
Layer 3/4 Management Traffic	Layer 3 and Layer 4 policy map for network management traffic received by the ACE	X	X	X
Layer 3/4 Network Traffic	Layer 3 and Layer 4 policy map for traffic passing through the ACE	X	X	X
Layer 7 FTP Command Inspection	Layer 7 policy map for inspection of FTP commands	X	X	X
Layer 7 HTTP Deep Packet Inspection	Layer 7 policy map for inspection of HTTP packets	X	X	X
Layer 7 HTTP Optimization	Layer 7 policy map for optimizing HTTP traffic			X
Layer 7 Server Load Balancing	Layer 7 policy map for HTTP server load balancing	X	X	X
Layer 7 SIP Deep Packet Inspection	Layer 7 policy map for inspection of SIP packets		X	
Layer 7 Skinny Deep Packet Inspection	Layer 7 policy map for inspection of Skinny Client Control Protocol (SCCP)		X	
RADIUS Server Load Balancing	Layer 7 policy map for RADIUS server load balancing		X	
RDP Server Load Balancing	Layer 7 policy map for RDP server load balancing		X	

Table 11-1 **Traffic Policies and ACE Device Support (continued)**

Policy Map	Description	ACE Device		
		ACE 1.0 Module	ACE 2.0 Module	ACE Appliance
RTSP Server Load Balancing	Layer 7 policy map for RTSP server load balancing		X	
SIP Server Load Balancing	Layer 7 policy map for SIP server load balancing		X	

The traffic classification process consists of the following three steps:

1. Creating a class map, which comprise a set of match criteria related to Layer 3 and Layer 4 traffic classifications or Layer 7 protocol classifications.
2. Creating a policy map, which refers to the class maps and identifies a series of actions to perform based on the traffic match criteria.
3. Activating the policy map and attaching it to a specific VLAN interface or globally to all VLAN interfaces associated with a context by configuring a virtual context global traffic policy to filter traffic received by the ACE.

The following overview topics describe the components that define a traffic policy:

- [Class Maps, page 11-3](#)
- [Policy Maps, page 11-4](#)
- [Parameter Maps and Their Use in Layer 3 and Layer 4 Policy Maps, page 11-5](#)
- [Configuring Virtual Context Global Traffic Policies, page 3-26](#)

Class Maps

A class map defines each type of Layer 3 and Layer 4 traffic class and each Layer 7 protocol class. You create class maps to classify the traffic received and transmitted by the ACE.

- Layer 3 and Layer 4 traffic classes contain match criteria that identify the IP network traffic that can pass through the ACE or network management traffic that can be received by the ACE.
- Layer 7 protocol-specific classes identify:
 - Server load-balancing traffic on generic, HTTP, RADIUS, RTSP, or SIP traffic
 - HTTP or SIP traffic for deep packet inspection
 - FTP traffic for inspection of commands

A traffic class contains the following components:

- Class map name
- Class map type
- One or more match conditions that define the match criteria for the class map
- Instructions on how the ACE evaluates match conditions when you specify more than one match statement in a traffic class (match-any, match-all)

The individual match conditions specify the criteria for classifying Layer 3 and Layer 4 network traffic as well as the Layer 7 server load balancing and application protocol-specific fields. The ACE evaluates the packets to determine whether they match the specified criteria. If a statement matches, the ACE

considers that packet to be a member of the class and forwards the packet according to the specifications set in the traffic policy. Packets that fail to meet any of the matching criteria are classified as members of the default traffic class if one is specified.

The ACE allows you to configure two Layer 7 load-balancing class maps in a nested traffic class configuration to create a single traffic class. You can nest Layer 7 class maps to achieve complex logical expressions. The ACE restricts the nesting of class maps to two levels to prevent you from including one nested class map under a different class map.

Related Topics

- [Class Map and Policy Map Overview, page 11-2](#)
- [Policy Maps, page 11-4](#)
- [Parameter Maps and Their Use in Layer 3 and Layer 4 Policy Maps, page 11-5](#)
- [Configuring Traffic Policies, page 11-1](#)
- [Configuring Virtual Context Class Maps, page 11-6](#)

Policy Maps

A policy map creates the traffic policy. The purpose of a traffic policy is to implement specific ACE functions associated with a traffic class. A traffic policy contains the following components:

- Policy map name
- Previously created traffic class map or, optionally, the class-default class map
- One or more of the individual Layer 3 and Layer 4 or Layer 7 policies that specify the actions to be performed by the ACE

A Layer 7 policy map is always associated within a Layer 3 and Layer 4 policy map to provide an entry point for traffic classification. Layer 7 policy maps are considered to be child policies and can only be nested under a Layer 3 and Layer 4 policy map. Only a Layer 3 and Layer 4 policy map can be activated on a VLAN interface; a Layer 7 policy map cannot be directly applied on an interface. For example, to associate a Layer 7 load-balancing policy map, you nest the load-balancing policy map by using the Layer 3 and Layer 4 Policy Map action type.

If none of the classifications specified in policy maps match, then the ACE executes the default actions specified against the class map configured with the Use Class Default option to use a default class map (if specified). All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. The Use Class Default feature has an implicit **match-any** match statement and is used to match any traffic classification.

The ACE supports flexible class map ordering within a policy map. The ACE executes only the actions for the first matching traffic classification, so the order of class maps within a policy map is very important. The policy lookup order is based on the security features of the ACE. The policy lookup order is implicit, irrespective of the order in which you configure policies on the interface.

The policy lookup order of the ACE is as follows:

1. Access control (permit or deny a packet)
2. Permit or deny management traffic
3. TCP/UDP connection parameters
4. Load balancing based on a virtual IP (VIP)
5. Application protocol inspection

6. Source NAT
7. Destination NAT

The sequence in which the ACE applies the actions for a specific policy is independent of the actions configured for a class map inside a policy.

Related Topics

- [Class Map and Policy Map Overview, page 11-2](#)
- [Class Maps, page 11-3](#)
- [Parameter Maps and Their Use in Layer 3 and Layer 4 Policy Maps, page 11-5](#)
- [Configuring Traffic Policies, page 11-1](#)
- [Configuring Virtual Context Policy Maps, page 11-30](#)

Parameter Maps and Their Use in Layer 3 and Layer 4 Policy Maps

Parameter maps allow you to combine related actions in a Layer 3 and Layer 4 policy map. For example, an HTTP parameter map provides a means of performing actions on traffic ingressing an ACE interface based on certain criteria such as HTTP header and cookie settings, server connection reuse, action to be taken when an HTTP header, cookie, or URL exceeds a configured maximum length, and so on.

The ACE uses policy maps to combine class maps and parameter maps into traffic policies and to perform certain configured actions on the traffic that matches the specified criteria in the policies.

See [Table 7-1](#) for a list of the available parameter maps and the ACE devices that support them.

Related Topic

- [Configuring Parameter Maps, page 7-1](#)
- [Class Map and Policy Map Overview, page 11-2](#)
- [Class Maps, page 11-3](#)
- [Policy Maps, page 11-4](#)

Protocol Inspection Overview

Certain applications require special handling of the data portion of a packet as the packets pass through the ACE. Application protocol inspection helps to verify the protocol behavior and identify unwanted or malicious traffic passing through the ACE. Based on the specifications of the traffic policy, the ACE accepts or rejects the packets to ensure the secure use of applications and services.

For information about application protocol inspection as configured and performed by the ACE, see the related topics.

Related Topics

- [Configuring Virtual Context Policy Maps, page 11-30](#)
- [Setting Match Conditions for Layer 7 FTP Command Inspection Class Maps, page 11-21](#)
- [Setting Policy Map Rules and Actions for Layer 7 HTTP Deep Packet Inspection, page 11-47](#)
- [Setting Policy Map Rules and Actions for Layer 7 SIP Deep Packet Inspection, page 11-62](#)

Configuring Virtual Context Class Maps

Class maps are used to define each Layer 3 and Layer 4 traffic class and each Layer 7 protocol class. You create class maps to classify the traffic received and transmitted by the ACE.

- Layer 3 and Layer 4 traffic classes contain match criteria that identify the IP network traffic that can pass through the ACE or network management traffic that can be received by the ACE.
- Layer 7 protocol-specific classes identify:
 - Server load-balancing traffic on generic, HTTP, RADIUS, RTSP, or SIP traffic
 - HTTP or SIP traffic for deep packet inspection
 - FTP traffic for inspection of commands

A traffic class contains the following components:

- Class map name
- Class map type
- One or more match conditions that define the match criteria for the class map
- Instructions on how the ACE evaluates match conditions when you specify more than one match statement in a traffic class (match-any, match-all)



Note

To successfully delete a class map from a context, the class map must no longer be in use. To delete multiple class maps, none of the class maps must be in use. If you attempt to delete multiple class maps and one of the class maps is still in use, none of the class maps are deleted and a message appears stating that one of the class maps is in use. Remove the class map that is still in use from your selection, then click **Delete**. The selected class maps are removed.

Procedure

- Step 1** Select **Config > Virtual Contexts > context > Expert > Class Map**. The Class Map table appears.
- Step 2** Click **Add** to add a new class map, or select an existing class map, then click **Edit** to modify it.
- Step 3** The Name field contains an automatically incremented number for the class map. You can leave the number as it is or enter a different, unique number.
- Step 4** In the Class Map Type field, select the type of class map you are creating.
The types that are available depend on the ACE that you are configuring. [Table 11-2](#) lists the available class map types and the ACE devices that support them.

Table 11-2 *Class Maps and ACE Module and Device Support*

Class Map	ACE Modules and Devices			
	ACE 1.0 Module	ACE 2.0 Module	ACE Appliance Running Image A1(8)	ACE Appliance Running Image A3(1.0)
Generic Server Load Balancing		X		
Layer 3/4 Management Traffic	X	X	X	X
Layer 3/4 Network Traffic	X	X	X	X

Table 11-2 *Class Maps and ACE Module and Device Support (continued)*

Class Map	ACE Modules and Devices			
	ACE 1.0 Module	ACE 2.0 Module	ACE Appliance Running Image A1(8)	ACE Appliance Running Image A3(1.0)
Layer 7 FTP Command Inspection	X	X	X	X
Layer 7 HTTP Deep Packet Inspection	X	X	X	X
Layer 7 Server Load Balancing	X	X	X	X
Layer 7 SIP Deep Packet Inspection		X		
RADIUS Server Load Balancing		X		
RTSP Server Load Balancing		X		
SIP Server Load Balancing		X		

Step 5 In the Match Type field, select the method to be used to evaluate multiple match statements when multiple match conditions exist:

- **Match Any**—A match exists if at least one of the match conditions is satisfied. If you select Match Any, you can specify only one type of match condition.
- **Match All**—A match exists only if all match conditions are satisfied. If you select Match All, you can specify multiple types of match conditions.

This field does not appear for Layer 7 FTP Command Inspection class maps.

Step 6 In the Description field, enter a brief description for the class map.

Step 7 Click:

- **Deploy Now** to deploy this configuration on the ACE and to configure match conditions for the class map. See [Setting Match Conditions for Class Maps, page 11-8](#) for more information.
- **Cancel** to exit the procedure without saving your entries and to return to the Class Map table.
- **Next** to deploy your entries and to configure another class map.

Related Topics

- [Using Virtual Contexts, page 3-1](#)
- [Deleting Class Maps, page 11-8](#)
- [Setting Match Conditions for Class Maps, page 11-8](#)
- [Configuring Virtual Context Policy Maps, page 11-30](#)

Deleting Class Maps

To successfully delete a class map from a context, the class map must no longer be in use. To delete multiple class maps, none of the class maps must be in use.

Assumption

The class map to be deleted is not being used.

Procedure

-
- Step 1** Select **Config > Virtual Contexts > context > Expert > Class Map**. The Class Map table appears.
- Step 2** Select the class maps you want to delete, then click **Delete**. A window appears, asking you to confirm the deletion.
- If you attempt to delete multiple class maps and one of the class maps is still in use, none of the class maps are deleted and a message appears stating that one of the class map is in use. Remove the class map that is still in use from your selection, then click **Delete**. The Class Map table refreshes and the deleted class maps no longer appear.
- Step 3** Click **OK** to confirm the deletion or **Cancel** to retain the class map and to return to the Class Map table.
-

Related Topics

- [Class Map and Policy Map Overview, page 11-2](#)
- [Configuring Virtual Context Class Maps, page 11-6](#)

Setting Match Conditions for Class Maps

[Table 11-3](#) lists the class maps available for all ACE devices and provides links to topics for setting match conditions:

Table 11-3 *Class Maps Available for All ACE Devices*

Class Map	Related Topic
Layer 3/Layer 4 management traffic	Setting Match Conditions for Layer 3/Layer 4 Management Traffic Class Maps, page 11-12
Layer 3/Layer 4 network traffic	Setting Match Conditions for Layer 3/Layer 4 Network Traffic Class Maps, page 11-9
Layer 7 FTP command inspection	Setting Match Conditions for Layer 7 FTP Command Inspection Class Maps, page 11-21
Layer 7 HTTP deep packet inspection	Setting Match Conditions for Layer 7 HTTP Deep Packet Inspection Class Maps, page 11-15
Layer 7 server load balancing	Setting Match Conditions for Layer 7 Server Load Balancing Class Maps, page 11-13

Table 11-4 lists additional class maps that are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release, and provides links to topics for setting match conditions.

Table 11-4 Additional Class Maps for ACE 2.0 Modules and the ACE 4710 A3(1.0) Release

Class Map	Related Topic
Generic server load balancing	Setting Match Conditions for Generic Server Load Balancing Class Maps, page 11-22
Layer 7 SIP deep packet inspection	Setting Match Conditions for Layer 7 SIP Deep Packet Inspection Class Maps, page 11-28
RADIUS server load balancing	Setting Match Conditions for RADIUS Server Load Balancing Class Maps, page 11-23
RTSP server load balancing	Setting Match Conditions for RTSP Server Load Balancing Class Maps, page 11-25
SIP server load balancing	Setting Match Conditions for SIP Server Load Balancing Class Maps, page 11-27

Setting Match Conditions for Layer 3/Layer 4 Network Traffic Class Maps

Use this procedure to specify the match criteria for a Layer 3/Layer 4 network traffic class map on the ACE.

Assumption

You have configured a Layer 3/Layer 4 network traffic class map and want to establish match conditions.

Procedure

- Step 1** Select **Config > Virtual Contexts > context > Expert > Class Map**. The Class Map table appears.
- Step 2** In the Class Map table, select the Layer 3/4 network traffic class map you want to set match conditions for. The Match Condition table appears.
- Step 3** In the Match Condition table, click **Add** to add match criteria, or select the match condition you want to modify, then click **Edit**. The Match Condition configuration screen appears.
- Step 4** In the Seq Number field, enter an integer from 2 to 255.

- Step 5** In the Match Condition Type field, select the type of match condition to use for this class map and configure any match-specific attributes as described in [Table 11-5](#).

Table 11-5 *Layer 3/Layer 4 Network Traffic Class Map Match Conditions*

Match Condition	Description
Access-list	An access list is the match type for this match condition. In the ACL field, select the ACL to use as the match condition.
Virtual-address	A virtual IP address is the match type for this match condition. 1. In the Virtual IP Address field, enter the virtual server IP (VIP) address to match in dotted-decimal format, such as 192.168.11.1. 2. In the Virtual IP Netmask field, select the subnet mask for the virtual IP address. 3. In the Virtual Address Protocol field, select the protocol to be used for this match condition. For a list of protocols and their respective numbers, see Table 3-12. 4. Depending on the protocol that you select, such as TCP or UDP, additional fields appear. If they appear, enter the information described in the following steps. 5. In the Port Operator field, select the match criteria for the port: – Any—Any port using the selected protocol meets the match condition. – Equal—A specific port using the protocol meets the match condition. In the Port Number field, enter the port to be matched. Valid entries are integers from 0 to 65535. A value of 0 indicates that the ACE is to include all ports. – Range—The port must be one of a range of ports to meet the match condition. Valid entries are integers from 0 to 65535. A value of 0 indicates that the ACE is to include all ports. a. In the Lower Port Number field, enter the first port number in the port range for the match condition. b. In the Upper Port Number field, enter the last port number in the port range for the match condition.
Destination-address	The destination address is the match type for this match condition. 1. In the Destination Address field, enter the destination IP address for this match condition in dotted-decimal format, such as 192.168.11.1. 2. In the Destination Netmask field, select the subnet mask for the destination IP address.
Source-address	The source IP address is the match type for this match condition. 1. In the Source Address field, enter the source IP address for this match condition in dotted-decimal format, such as 192.168.11.1. 2. In the Source Netmask field, select the subnet mask for the source IP address.

Table 11-5 Layer 3/Layer 4 Network Traffic Class Map Match Conditions (continued)

Match Condition	Description
Any	Any Layer 3 or Layer 4 traffic passing through the ACE meets the match condition.
Port	A UDP or TCP port or range of ports is the match type for this match condition. 1. In the Port Protocol field, select TCP or UDP as the protocol to match. 2. In the Port Operator field, select the match criteria for the port: – Any—Any port using the selected protocol meets the match condition. – Equal—A specific port using the protocol meets the match condition. In the Port Number field, enter the port to be matched. Valid entries are integers from 0 to 65535. A value of 0 indicates that the ACE is to include all ports. – Range—The port must be one of a range of ports to meet the match condition. a. In the Lower Port Number field, enter the first port number in the port range for the match condition. b. In the Upper Port Number field, enter the last port number in the port range for the match condition. Valid entries are integers from 0 to 65535. A value of 0 indicates that the ACE is to include all ports.

Step 6 Click:

- **Deploy Now** to deploy this configuration on the ACE and to return to the Match Condition table.



Note If you click **Deploy Now**, the ACE drops the traffic and then restarts it, even if you have not made changes. If you have not altered existing match conditions, click **Cancel** instead of **Deploy Now** to ensure uninterrupted traffic.

- **Cancel** to exit the procedure without saving your entries and to return to the Match Condition table.
- **Next** to deploy your entries and to configure additional match conditions.

Related Topics

- [Configuring Traffic Policies, page 11-1](#)
- [Setting Match Conditions for Layer 3/Layer 4 Management Traffic Class Maps, page 11-12](#)
- [Setting Match Conditions for Layer 7 Server Load Balancing Class Maps, page 11-13](#)
- [Configuring Virtual Context Policy Maps, page 11-30](#)
- [Configuring Virtual Context Class Maps, page 11-6](#)

Setting Match Conditions for Layer 3/Layer 4 Management Traffic Class Maps

Use this procedure to identify the network management protocols that can be received by the ACE.

Assumption

You have configured a Layer 3/Layer 4 network management class map and want to establish match conditions.

Procedure

- Step 1** Select **Config > Virtual Contexts > context > Expert > Class Map**. The Class Map table appears.
- Step 2** In the Class Map table, select the Layer 3/Layer 4 management class map you want to set match conditions for. The Match Condition table appears.
- Step 3** In the Match Condition table, click **Add** to add match criteria, or select the match conditions you want to modify, then click **Edit**. The Match Condition configuration screen appears.
- Step 4** Enter the match conditions (see [Table 11-6](#)).

Table 11-6 Layer 3/Layer 4 Management Traffic Class Map Match Conditions

Field	Description
Seq Number	Enter an integer from 2 to 255 as the line number. The number entered here does not indicate a priority or sequence for the match conditions.
Match Condition Type	Confirm that Management is selected. Note To change the type of match condition, you must delete the class map and add it again with the correct match type.
Mgmt Protocol Type	This field identifies the network management protocols that can be received by the ACE. Select the allowed protocol for this match condition: • HTTP—Specifies the Hypertext Transfer Protocol (HTTP). • HTTPS—Specifies the secure (SSL) Hypertext Transfer Protocol (HTTP) for connectivity with the ANM GUI on the ACE. • ICMP—Specifies the Internet Control Message Protocol (ICMP), commonly referred to as ping. • SNMP—Specifies the Simple Network Management Protocol (SNMP). • SSH—Specifies a Secure Shell (SSH) connection to the ACE. • TELNET—Specifies a Telnet connection to the ACE. • KALAP UDP—Specifies the KeepAlive Appliance Protocol over UDP. This option is available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only. • XML-HTTPS—Specifies HTTPS as the transfer protocol for sending and receiving XML documents between the ACE and a Network Management System (NMS). This option is available for ACE appliances only.

Table 11-6 Layer 3/Layer 4 Management Traffic Class Map Match Conditions (continued)

Field	Description
Traffic Type	Select the type of traffic: - Any—Any client source IP address meets the match condition. - Source-address—A specific source IP address is part of the match condition.
Source Address	This field appears if Source-address is selected for Traffic Type. Enter the source IP address of the client in dotted-decimal notation, such as 192.168.11.1.
Source Netmask	This field appears if Source-address is selected for Traffic Type. Select the subnet mask for the source IP address.

Step 5 Click:

- **Deploy Now** to deploy this configuration on the ACE and to return to the Match Condition table.

**Note**

If you click **Deploy Now**, the ACE drops the traffic and then restarts it, even if you have not made changes. If you have not altered existing match conditions, click **Cancel** instead of **Deploy Now** to ensure uninterrupted traffic.

- **Cancel** to exit the procedure without saving your entries and to return to the Match Condition table.
- **Next** to deploy your entries and to configure additional match conditions.

Related Topics

- [Configuring Traffic Policies, page 11-1](#)
- [Configuring Virtual Context Class Maps, page 11-6](#)
- [Configuring Real Servers, page 5-4](#)
- [Configuring Server Farms, page 5-12](#)
- [Configuring Sticky Groups, page 6-7](#)

Setting Match Conditions for Layer 7 Server Load Balancing Class Maps

Use this procedure to set match conditions for Layer 7 server load balancing class maps.

Assumption

You have configured a load-balancing class map and want to establish the match conditions.

Procedure

- Step 1** Select **Config > Virtual Contexts > context > Expert > Class Map**. The Class Map table appears.
- Step 2** In the Class Map table, select the Layer 7 server load balancing class map you want to set match conditions for. The Match Condition table appears.

- Step 3** In the Match Condition table, click **Add** to add match criteria, or select the match condition you want to modify, then click **Edit**. The Match Condition configuration screen appears.
- Step 4** In the Seq Number field, enter an integer from 2 to 255 as the line number. The number entered here does not indicate a priority or sequence for the match conditions.
- Step 5** In the Match Condition Type field, select the type of match to use and configure condition-specific attributes as described in [Table 11-7](#).

Table 11-7 Layer 7 Server Load Balancing Class Map Match Conditions

Match Condition	Description
Http-cookie	An HTTP cookie is to be used to establish a match condition. 1. In the Cookie Name field, enter a unique cookie name. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. 2. In the Cookie Value field, enter a unique cookie value expression. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. 3. Select the Secondary Cookie Matching check box to indicate that the ACE is to use both the cookie name and the cookie value to satisfy this match condition. Clear this check box to indicate that the ACE is to use either the cookie name or the cookie value to satisfy this match condition.
Http-header	An HTTP header is to be used to establish a match condition. 1. In the Header Name field, specify the header to match in one of the following ways: – To specify an HTTP header that is not one of the standard HTTP headers, select the first radio button, then enter the HTTP header name in the Header Name field. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters. – To specify a standard HTTP header, click the second radio button, then select an HTTP header from the list. 2. In the Header Value field, enter the header value expression string to compare against the value in the specified field in the HTTP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. If the string includes spaces, enclose the string in quotes. See Table 11-35 for a list of the supported characters that you can use in regular expressions.
Http-url	A portion of an HTTP URL is to be used to establish a match condition. 1. In the URL Expr field, enter a URL or a portion of a URL to match. Valid entries are URL strings from 1 to 255 alphanumeric characters and include only the portion of the URL following <code>www.hostname.domain</code>. For example, in the URL <code>www.anydomain.com/latest/whatsnew.html</code>, include only <code>/latest/whatsnew.html</code>. 2. In the Method field, enter the HTTP method to match. Valid entries are method names entered as unquoted text strings with no spaces and a maximum of 15 alphanumeric characters. You can enter either one of the standard HTTP 1.1 method names (OPTIONS, GET, HEAD, POST, PUT, DELETE, TRACE, or CONNECT) or a text string that must be matched exactly (for example, CORVETTE).
Source-address	The source IP address is to be used to establish a match condition. 1. In the Source Address field, enter the source IP address of the client in dotted-decimal notation, such as 192.168.11.1. 2. In the Source Netmask field, select the subnet mask of the source IP address.

Table 11-7 **Layer 7 Server Load Balancing Class Map Match Conditions (continued)**

Match Condition	Description
Class-map	A class map is to be used to establish a match condition. In the Class Map field, select the class map to apply to this match condition.
HTTP Content	This option appears for ACE 2.0 modules and the ACE 4710 A3(1.0) release only. Specific content contained within the HTTP entity-body is used to establish a match condition. 1. In the Content Expression field, enter the content that is to be matched. Valid entries are alphanumeric strings from 1 to 255 characters. 2. In the Content Offset field, enter the number of bytes to be ignored starting with the first byte of the Message body, after the empty line (CR,LF,CR,LF) between the headers and the body of the message. Valid entries are integers from 1 to 255.

Step 6 Click:

- **Deploy Now** to deploy this configuration on the ACE and to return to the Match Condition table.



Note If you click **Deploy Now**, the ACE drops the traffic and then restarts it, even if you have not made changes. If you have not altered existing match conditions, click **Cancel** instead of **Deploy Now** to ensure uninterrupted traffic.

- **Cancel** to exit the procedure without saving your entries and to return to the Match Condition table.
- **Next** to deploy your entries and to configure additional match conditions.

Related Topics

- [Using Virtual Contexts, page 3-1](#)
- [Configuring Virtual Context Class Maps, page 11-6](#)
- [Configuring Virtual Context Policy Maps, page 11-30](#)

Setting Match Conditions for Layer 7 HTTP Deep Packet Inspection Class Maps

The ANM allows you to create Layer 7 class maps and policy maps to be used for HTTP deep packet inspection by the ACE. When these features are configured, the ACE performs a stateful deep packet inspection of the HTTP protocol and permits or restricts traffic based on the actions in the defined policy maps. You can configure the following security features as part of HTTP deep packet inspection to be performed by the ACE:

- Regular expression matching on name in an HTTP header, URL name, or content expressions in an HTTP entity body
- Content, URL, and HTTP header length checks
- MIME-type message inspection
- Transfer-encoding methods
- Content type verification and filtering

- Port 80 misuse by tunneling protocols
- RFC compliance monitoring and RFC method filtering

Use this procedure to configure a Layer 7 class map for deep packet inspection of HTTP traffic.

Assumption

You have configured a Layer 7 HTTP deep packet inspection class map and want to establish match conditions.

Procedure

-
- Step 1** Select **Config > Virtual Contexts > context > Expert > Class Map**. The Class Map table appears.
- Step 2** In the Class Map table, select the Layer 7 HTTP deep packet inspection class map you want to set match conditions for. The Match Condition table appears.
- Step 3** In the Match Condition table, click **Add** to add match criteria, or select the match condition you want to modify, then click **Edit**. The Match Condition configuration screen appears.
- Step 4** In the Seq Number field, enter an integer from 2 to 255 as the line number. The number entered here does not indicate a priority or sequence for the match conditions.

- Step 5** In the Match Condition Type field, select the method by which match decisions are to be made and configure condition-specific attributes as described in [Table 11-8](#).

Table 11-8 *Layer 7 HTTP Deep Packet Inspection Class Map Match Conditions*

Match Condition	Description
Content	Specific content contained within the HTTP entity-body is to be used for protocol inspection decisions. 1. In the Content Expression field, enter the content that is to be matched. Valid entries are alphanumeric strings from 1 to 255 characters. 2. In the Content Offset field, enter the number of bytes to be ignored starting with the first byte of the Message body, after the empty line (CR,LF,CR,LF) between the headers and the body of the message. Valid entries are integers from 1 to 255.
Content Length	The content parse length in an HTTP message is to be used for protocol inspection decisions. 1. In the Content Length Operator field, select the operand to use to compare content length: – Equal—The content length must equal the number in the Content Length Value field. – Greater than—The content length must be greater than the number in the Content Length Value field. – Less than—The content length must be less than the number in the Content Length Value field. – Range—The content length must be within the range specified in the Content Length Lower Value field and the Content Length Higher Value field. 2. Enter values to apply for content length comparison: – If you select Equal, Greater than, or Less than in the Content Length Operator field, the Content Length Value field appears. In the Content Length Value field, enter the number of bytes for comparison. Valid entries are integers from 0 to 4294967295. – If you select Range in the Content Length Operator field, the Content Length Lower Value and the Content Length Higher Value fields appear: a. In the Content Length Lower Value field, enter the lowest number of bytes to be used for this match condition. Valid entries are integers from 0 to 4294967295. The number in this field must be less than the number entered in the Content Length Higher Value field. b. In the Content Length Higher Value field, enter the highest number of bytes to be used for this match condition. Valid entries are integers from 0 to 4294967295. The number in this field must be greater than the number entered in the Content Length Lower Value field.
Header	The name and value in an HTTP header are to be used for protocol inspection decisions. 1. In the Header field, select one of the predefined HTTP headers to be matched, or select HTTP Header to specify a different HTTP header. 2. If you select HTTP Header, in the Header Name field, enter the name of the HTTP header to match. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. 3. In the Header Value field, enter the header value expression string to compare against the value in the specified field in the HTTP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. If the string includes spaces, enclose the string with quotes. All headers in the header map must be matched. See Table 11-35 for a list of the supported characters that you can use in regular expressions.

Table 11-8 Layer 7 HTTP Deep Packet Inspection Class Map Match Conditions (continued)

Match Condition	Description
Header Length	The length of the header in the HTTP message is to be used for protocol inspection decisions. - In the Header Length Type field, specify whether HTTP header request or response messages are to be used for protocol inspection decisions: - Request—HTTP header request messages are to be checked for header length. - Response—HTTP header response messages are to be checked for header length. - In the Header Length Operator field, select the operand to use to compare header length: - Equal—The header length must equal the number in the Header Length Value field. - Greater Than—The header length must be greater than the number in the Header Length Value field. - Less Than—The header length must be less than the number in the Header Length Value field. - Range—The header length must be within the range specified in the Header Length Lower Value field and the Header Length Higher Value field. - Enter values to apply for header length comparison: - If you select Equal, Greater Than, or Less Than in the Header Length Operator field, the Header Length Value field appears. In the Header Length Value field, enter the number of bytes for comparison. Valid entries are integers from 0 to 255. - If you select Range in the Header Length Operator field, the Header Length Lower Value and the Header Length Higher Value fields appear: - In the Header Length Lower Value field, enter the lowest number of bytes to be used for this match condition. Valid entries are integers from 0 to 255. The number in this field must be less than the number entered in the Header Length Higher Value field. - In the Header Length Higher Value field, enter the highest number of bytes to be used for this match condition. Valid entries are integers from 1 to 255. The number in this field must be greater than the number entered in the Header Length Lower Value field.
Header MIME Type	Multipurpose Internet Mail Extension (MIME) message types are to be used for protocol inspection decisions. In the Header MIME Type field, select the MIME message type to use for this match condition.
Port Misuse	The misuse of port 80 (or any other port running HTTP) is to be used for protocol inspection decisions. Select the application category to use for this match condition: - IM—Instant messaging applications are to be used for this match condition. - P2P—Peer-to-peer applications are to be used for this match condition. - Tunneling—Tunneling applications are to be used for this match condition.

Table 11-8 **Layer 7 HTTP Deep Packet Inspection Class Map Match Conditions (continued)**

Match Condition	Description
Request Method	The request method is to be used for protocol inspection decisions. By default, ACEs allow all request and extension methods. This option allows you to configure class maps that define protocol inspection decisions based on compliance to request methods defined in RFC 2616 and by HTTP extension methods. 1. In the Request Method Type field, select the type of compliance to be used for protocol inspection decision: – Ext—An HTTP extension method is to be used for protocol inspection decisions. – RFC—A request method defined in RFC 2616 is to be used for protocol inspection decisions. Depending on your selection, the Ext Request Method field or the RFC Request Method field appears. 2. In the Request Method field, select the specific request method to be used.
Transfer Encoding	An HTTP transfer-encoding type is to be used for protocol inspection decisions. The transfer-encoding general-header field indicates the type of transformation, if any, that has been applied to the HTTP message body to safely transfer it between the sender and the recipient. In the Transfer Encoding field, select the type of encoding that is to be checked: • Chunked—The message body is transferred as a series of chunks. • Compress—The encoding format that is produced by the UNIX file compression program compress. • Deflate—The .zlib format that is defined in RFC 1950 in combination with the DEFLATE compression mechanism described in RFC 1951. • Gzip—The encoding format that is produced by the file compression program GZIP (GNU zip) as described in RFC 1952. • Identity—The default (identity) encoding which does not require the use of transformation.

Table 11-8 Layer 7 HTTP Deep Packet Inspection Class Map Match Conditions (continued)

Match Condition	Description
URL	URL names are to be used for protocol inspection decisions. In the URL field, enter a URL or a portion of a URL to match. Valid entries are URL strings from 1 to 255 alphanumeric characters and include only the portion of the URL following <code>www.hostname.domain</code>. For example, in the URL <code>www.anydomain.com/latest/whatsnew.html</code>, include only <code>/latest/whatsnew.html</code>.
URL Length	URL length is to be used for protocol inspection decisions. - In the URL Length Operator field, select the operand to be used to compare URL length: - Equal—The URL length must equal the number in the URL Length Value field. - Greater Than—The URL length must be greater than the number in the URL Length Value field. - Less Than—The URL length must be less than the number in the URL Length Value field. - Range—The URL length must be within the range specified in the URL Length Lower Value field and the URL Length Higher Value field. - Enter values to apply for URL length comparison: - If you select Equal, Greater Than, or Less Than in the URL Length Operator field, the URL Length Value field appears. In the URL Length Value field, enter the value for comparison. Valid entries are from 1 to 65535 bytes. - If you select Range in the URL Length Operator field, the URL Length Lower Value and the URL Length Higher Value fields appear: - In the URL Length Lower Value field, enter the lowest number of bytes to be used for this match condition. Valid entries are integers from 1 to 65535. The number in this field must be less than the number entered in the URL Length Higher Value field. - In the URL Length Higher Value field, enter the highest number of bytes to be used for this match condition. Valid entries are integers from 1 to 65535. The number in this field must be greater than the number entered in the URL Length Lower Value field.

Step 6 Click:

- **Deploy Now** to deploy this configuration on the ACE.

**Note**

If you click **Deploy Now**, the ACE drops the traffic, then restarts it, even if you have not made changes. If you have not altered existing match conditions, click **Cancel** instead of **Deploy Now** to ensure uninterrupted traffic.

- **Cancel** to exit this procedure without saving your entries and to return to the Match Condition table.
- **Next** to configure another match condition for this class map.

Related Topics

- [Configuring Virtual Context Policy Maps, page 11-30](#)
- [Setting Match Conditions for Layer 3/Layer 4 Network Traffic Class Maps, page 11-9](#)

- [Setting Match Conditions for Layer 3/Layer 4 Management Traffic Class Maps](#), page 11-12
- [Setting Match Conditions for Layer 7 Server Load Balancing Class Maps](#), page 11-13
- [Setting Match Conditions for Layer 7 FTP Command Inspection Class Maps](#), page 11-21

Setting Match Conditions for Layer 7 FTP Command Inspection Class Maps

Use this procedure to set match conditions for a Layer 7 FTP command inspection class map.

Assumption

You have configured a Layer 7 FTP command inspection class map and want to establish match criteria.

Procedure

- Step 1** Select **Config > Virtual Contexts > context > Expert > Class Map**. The Class Map table appears.
- Step 2** In the Class Map table, select the Layer 7 FTP command inspection class map you want to set match conditions for. The Match Condition table appears.
- Step 3** In the Match Condition table, click **Add** to add match criteria, or select the match condition you want to modify, then click **Edit**. The Match Condition configuration screen appears.
- Step 4** In the Seq Number field, enter an integer from 2 to 255.
- Step 5** In the Match Condition Type field, confirm that Request Method Name is selected as the match condition type for this class map.
- Step 6** In the Request Method Name field, select the FTP command to be inspected. [Table 11-9](#) identifies the FTP commands that can be inspected.

Table 11-9 *FTP Commands for Inspection*

FTP Command	Description
appe	Append data to the end of the specified file on the remote host.
cdup	Change to the parent of the current directory.
dele	Delete the specified file.
get	Copy the specified file from the remote host to the local system.
help	List all available FTP commands.
mkd	Create a directory using the specified path and directory name.
put	Copy the specified file from the local system to the remote host.
rmd	Remove the specified directory.
rnfr	Rename a file, specifying the current file name. Used with rnto .
rnto	Rename a file, specifying the new file name. Used with rnfr .
site	Execute a site-specific command.
stou	Store a file on the remote host and give it a unique name.
syst	Query the remote host for operating system information.

Step 7 Click:

- **Deploy Now** to deploy this configuration on the ACE and to return to the Match Condition table.



Note

If you click **Deploy Now**, the ACE drops the traffic and then restarts it, even if you have not made changes. If you have not altered existing match conditions, click **Cancel** instead of **Deploy Now** to ensure uninterrupted traffic.

- **Cancel** to exit this procedure without saving your entries and to return to the Match Condition table.
- **Next** to configure another match condition for this class map.

Related Topics

- [Configuring Virtual Context Class Maps, page 11-6](#)
- [Configuring Virtual Context Policy Maps, page 11-30](#)

Setting Match Conditions for Generic Server Load Balancing Class Maps



Note

Generic server load balancing class maps are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.

Use this procedure to set match conditions for a generic server load balancing class map.

Assumption

You have configured a generic server load balancing class map and want to establish match criteria.

Procedure

- Step 1** Select **Config > Virtual Contexts > context > Expert > Class Map**. The Class Map table appears.
- Step 2** In the Class Map table, select the generic server load balancing class map you want to set match conditions for. The Match Condition table appears.
- Step 3** In the Match Condition table, click **Add** to add match criteria, or select the match condition you want to modify, then click **Edit**. The Match Condition configuration screen appears.
- Step 4** In the Seq Number field, enter an integer from 2 to 255.
- Step 5** In the Match Condition Type field, select the match condition type for this class map and configure any match-specific criteria as described in [Table 11-10](#).

Table 11-10 *Generic Server Load Balancing Class Map Match Conditions*

Match Condition	Description
Source Address	A source IP address is used to establish a match condition. 1. In the Source Address field, enter the source IP address for this match condition in dotted-decimal format, such as 192.168.11.1. 2. In the Source Netmask field, select the subnet mask for the source IP address.
Class Map	A class map is used to establish a match condition. In the Class Map field, select the class map to use for this match condition.
Layer 4 Payload	Generic data parsing is used to establish a match condition. 1. In the Layer 4 Payload Regex field, enter the Layer 4 payload expression contained within the TCP or UDP entity body to use for this match condition. Valid entries are text strings with a maximum of 255 alphanumeric characters. See Table 11-35 for a list of the supported characters that you can use for matching string expressions. 2. In the Layer 4 Payload Offset field, enter the absolute offset where the Layer 4 payload expression search starts. The offset starts at the first byte of the TCP or UDP body. Valid entries are integers from 0 to 999.

Step 6 Click:

- **Deploy Now** to deploy this configuration on the ACE and to return to the Match Condition table.

**Note**

If you click **Deploy Now**, the ACE drops the traffic and then restarts it, even if you have not made changes. If you have not altered existing match conditions, click **Cancel** instead of **Deploy Now** to ensure uninterrupted traffic.

- **Cancel** to exit this procedure without saving your entries and to return to the Match Condition table.
- **Next** to configure another match condition for this class map.

Related Topics

- [Configuring Virtual Context Class Maps, page 11-6](#)
- [Configuring Virtual Context Policy Maps, page 11-30](#)

Setting Match Conditions for RADIUS Server Load Balancing Class Maps

**Note**

RADIUS server load balancing class maps are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.

Use this procedure to set match conditions for a RADIUS server load balancing class map.

Assumption

You have configured a RADIUS server load balancing class map and want to establish match criteria.

Procedure

-
- Step 1** Select **Config > Virtual Contexts > context > Expert > Class Map**. The Class Map table appears.
- Step 2** In the Class Map table, select the RADIUS server load balancing class map you want to set match conditions for. The Match Condition table appears.
- Step 3** In the Match Condition table, click **Add** to add match criteria, or select the match condition you want to modify, then click **Edit**. The Match Condition configuration screen appears.
- Step 4** In the Seq Number field, enter an integer from 2 to 255.
- Step 5** In the Match Condition Type field, select the match condition type for this class map and configure any match-specific criteria as described in [Table 11-11](#).

Table 11-11 RADIUS Server Load Balancing Class Map Match Conditions

Match Condition	Description
Calling Station ID	A unique identifier of the calling station is used to establish a match condition. In the RADIUS Calling Station ID field, enter the calling station identifier to match. Valid entries are strings containing 1 to 64 alphanumeric characters. See Table 11-35 for a list of the supported characters that you can use for matching string expressions.
Username	A username is used to establish a match condition. In the Username field, enter the name to match. Valid entries are strings containing 1 to 64 alphanumeric characters. See Table 11-35 for a list of the supported characters that you can use for matching string expressions.

Step 6 Click:

- **Deploy Now** to deploy this configuration on the ACE and to return to the Match Condition table.

**Note**

If you click **Deploy Now**, the ACE drops the traffic and then restarts it, even if you have not made changes. If you have not altered existing match conditions, click **Cancel** instead of **Deploy Now** to ensure uninterrupted traffic.

- **Cancel** to exit this procedure without saving your entries and to return to the Match Condition table.
 - **Next** to configure another match condition for this class map.
-

Related Topics

- [Configuring Virtual Context Class Maps, page 11-6](#)
- [Configuring Virtual Context Policy Maps, page 11-30](#)

Setting Match Conditions for RTSP Server Load Balancing Class Maps

**Note**

RTSP server load balancing class maps are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.

Use this procedure to set match conditions for a RTSP server load balancing class map.

Assumption

You have configured a RTSP server load balancing class map and want to establish match criteria.

Procedure

- Step 1** Select **Config > Virtual Contexts > context > Expert > Class Map**. The Class Map table appears.
- Step 2** In the Class Map table, select the RTSP server load balancing class map you want to set match conditions for. The Match Condition table appears.
- Step 3** In the Match Condition table, click **Add** to add match criteria, or select the match condition you want to modify, then click **Edit**. The Match Condition configuration screen appears.
- Step 4** In the Seq Number field, enter an integer from 2 to 255.
- Step 5** In the Match Condition Type field, select the match condition type for this class map and configure any match-specific criteria as described in [Table 11-12](#).

Table 11-12 RTSP Server Load Balancing Class Map Match Conditions

Match Condition	Description
Source Address	The source IP address is used to establish a match condition. 1. In the Source Address field, enter the source IP address for this match condition in dotted-decimal format, such as 192.168.11.1. 2. In the Source Netmask field, select the subnet mask for the source IP address.
Class Map	A class map is used to establish a match condition. In the Class Map field, select the class map to use for this match condition.

Table 11-12 RTSP Server Load Balancing Class Map Match Conditions (continued)

Match Condition	Description
RTSP Header	The name and value in an RTSP header are used to establish a match condition. - In the Header Name field, specify the header in one of the following ways: - To specify an RTSP header that is not one of the standard RTSP headers, select the first radio button and enter the RTSP header name in the Header Name field. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters. - To specify one of the standard RTSP headers, select the second radio button and select one of the RTSP headers from the list. - In the Header Value field, enter the header value expression string to compare against the value in the specified field in the RTSP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. If the string includes spaces, enclose the string with quotes. All headers in the header map must be matched. See Table 11-35 for a list of the supported characters that you can use in regular expressions.
RTSP URL	A URL or portion of a URL is used to establish a match condition. - In the URL Expr field, enter a URL, or portion of a URL, to match. The ACE performs matching on whatever URL string appears after the RTSP method, regardless of whether the URL includes the host name. The ACE supports regular expressions for matching URL strings. See Table 11-35 for a list of the supported characters that you can use in regular expressions. - In the Method field, enter the RTSP method to match. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. The method can be either one of the standard RTSP method names (DESCRIBE, ANNOUNCE, GET_PARAMETER, OPTIONS, PAUSE, PLAY, RECORD, REDIRECT, SETUP, SET_PARAMETER, TEARDOWN) or a text string that must be matched exactly (for example, STINGRAY).

Step 6 Click:

- Deploy Now** to deploy this configuration on the ACE and to return to the Match Condition table.

**Note**

If you click **Deploy Now**, the ACE drops the traffic and then restarts it, even if you have not made changes. If you have not altered existing match conditions, click **Cancel** instead of **Deploy Now** to ensure uninterrupted traffic.

- Cancel** to exit this procedure without saving your entries and to return to the Match Condition table.
- Next** to configure another match condition for this class map.

Related Topics

- [Configuring Virtual Context Class Maps, page 11-6](#)
- [Configuring Virtual Context Policy Maps, page 11-30](#)

Setting Match Conditions for SIP Server Load Balancing Class Maps


Note

SIP server load balancing class maps are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.

Use this procedure to set match conditions for a SIP server load balancing class map.

Assumption

You have configured a SIP server load balancing class map and want to establish match criteria.

Procedure

- Step 1** Select **Config > Virtual Contexts > context > Expert > Class Map**. The Class Map table appears.
- Step 2** In the Class Map table, select the SIP server load balancing class map you want to set match conditions for. The Match Condition table appears.
- Step 3** In the Match Condition table, click **Add** to add match criteria, or select the match condition you want to modify, then click **Edit**. The Match Condition configuration screen appears.
- Step 4** In the Seq Number field, enter an integer from 2 to 255.
- Step 5** In the Match Condition Type field, select the match condition type for this class map and configure any match-specific criteria as described in [Table 11-13](#).

Table 11-13 SIP Server Load Balancing Class Map Match Conditions

Match Condition	Description
Source Address	The source IP address is used to establish a match condition. 1. In the Source Address field, enter the source IP address for this match condition in dotted-decimal format, such as 192.168.11.1. 2. In the Source Netmask field, select the subnet mask for the source IP address.
Class Map	A class map is used to establish a match condition. In the Class Map field, select the class map to use for this match condition.
SIP Header	A SIP header name and value are used to establish a match condition. 1. In the Header Name field, specify the header in one of the following ways: – To specify a SIP header that is not one of the standard SIP headers, select the first radio button and enter the SIP header name in the Header Name field. Enter an unquoted text string with no spaces and a maximum of 64 characters. – To specify one of the standard SIP headers, select the second radio button and select one of the SIP headers from the list. 2. In the Header Value field, enter the header value expression string to compare against the value in the specified field in the SIP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. If the string includes spaces, enclose the string with quotes. All headers in the header map must be matched. See Table 11-35 for a list of the supported characters that you can use in regular expressions.

Step 6 Click:

- **Deploy Now** to deploy this configuration on the ACE and to return to the Match Condition table.



Note

If you click **Deploy Now**, the ACE drops the traffic and then restarts it, even if you have not made changes. If you have not altered existing match conditions, click **Cancel** instead of **Deploy Now** to ensure uninterrupted traffic.

- **Cancel** to exit this procedure without saving your entries and to return to the Match Condition table.
- **Next** to configure another match condition for this class map.

Related Topics

- [Configuring Virtual Context Class Maps, page 11-6](#)
- [Configuring Virtual Context Policy Maps, page 11-30](#)

Setting Match Conditions for Layer 7 SIP Deep Packet Inspection Class Maps



Note

SIP deep packet inspection class maps are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.

Use this procedure to set match conditions for a SIP deep packet inspection class map.

Assumption

You have configured a SIP deep packet inspection class map and want to establish match criteria.

Procedure

- Step 1** Select **Config > Virtual Contexts > context > Expert > Class Map**. The Class Map table appears.
- Step 2** In the Class Map table, select the SIP deep packet inspection class map you want to set match conditions for. The Match Condition table appears.
- Step 3** In the Match Condition table, click **Add** to add match criteria, or select the match condition you want to modify, then click **Edit**. The Match Condition configuration screen appears.
- Step 4** In the Seq Number field, enter an integer from 2 to 255.
- Step 5** In the Match Condition Type field, select the match condition type for this class map and configure any match-specific criteria as described in [Table 11-14](#).

Table 11-14 **Layer 7 SIP Deep Packet Inspection Class Map Match Conditions**

Match Condition	Description
Message Path	A message coming from or transiting through certain SIP proxy servers is used to establish a match condition. In the Message Path field, enter a regular expression that identifies the SIP proxy server for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions.
SIP Request Method	A SIP request method is used to establish a match condition. In the Request Method field, select the request method that is to be matched.
IM Subscriber	An IM (instant messaging) subscriber is used to establish a match condition. In the IM Subscriber field, enter a regular expression that identifies the IM subscriber for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions.
Third Party	A third party who is authorized to register other users on their behalf is used to establish a match condition. In the Third Party Registration Entities field, enter a regular expression that identifies a privileged user authorized for third-party registrations for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions.
URI Length	A SIP URI or user identifier is used to establish a match condition. - In the URI Type field, select the type of URI to use: - SIP URI—The calling party URI is used for this match condition. - Tel URI—A telephone number is used for this match condition. - In the URI Operator field, confirm that Greater Than is selected. - In the URI Length field, enter the maximum length of the SIP URI or Tel URI in bytes. Valid entries are integers from 0 to 254 bytes.
Called Party	The destination or called party in the URI of the SIP To header is used to establish a match condition. In the Called Party field, enter a regular expression that identifies the called party in the URI of the SIP To header for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions.
Calling Party	The source or calling party in the URI of the SIP From header is used to establish a match condition. In the Calling Party field, enter a regular expression that identifies the called party in the URI of the SIP To header for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions.

Table 11-14 **Layer 7 SIP Deep Packet Inspection Class Map Match Conditions (continued)**

Match Condition	Description
SIP Content Length	The SIP message body length is used to establish a match condition. 1. In the Content Operator field, confirm that Greater Than is selected. 2. In the Content Length field, enter the maximum size of a SIP message body in bytes that the ACE is to allow without performing SIP protocol inspection. If a SIP message exceeds the specified value, the ACE performs SIP protocol inspection as defined in an associated policy map. Valid entries are integers from 0 to 65534 bytes.
SIP Content Type	The content type in the SIP message body is used to establish a match condition. In the Content Type field, enter the a regular expression that identifies the content type in the SIP message body to use for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions.

Step 6 Click:

- **Deploy Now** to deploy this configuration on the ACE and to return to the Match Condition table.



Note If you click **Deploy Now**, the ACE drops the traffic and then restarts it, even if you have not made changes. If you have not altered existing match conditions, click **Cancel** instead of **Deploy Now** to ensure uninterrupted traffic.

- **Cancel** to exit this procedure without saving your entries and to return to the Match Condition table.
- **Next** to configure another match condition for this class map.

Related Topics

- [Configuring Virtual Context Class Maps, page 11-6](#)
- [Configuring Virtual Context Policy Maps, page 11-30](#)

Configuring Virtual Context Policy Maps

Policy maps establish traffic policy for the ACE. The purpose of a traffic policy is to implement specific ACE functions associated with a traffic class. A traffic policy contains:

- A policy map name.
- A previously created traffic class map or, optionally, the class-default class map.
- One or more of the individual Layer 3/Layer 4 or Layer 7 policies that specify the actions to be performed by the ACE.

The ACE executes actions specified in a policy map on a first-match, multi-match, or all-match basis:

- **First-match**—With a first-match policy map, the ACE executes only the action specified against the first classification that it matches. Layer 3/Layer 4 Management Traffic, Layer 7 Server Load Balancing, Layer 7 FTP Command Inspection, and Layer 7 HTTP Optimization policy maps are first-match policy maps.
- **Multi-match**—With a multi-match policy map, the ACE executes all possible actions applicable for a specific classification. Layer 3/Layer 4 Network Traffic policy maps are multi-match policy maps.
- **All-match**—With an all-match policy map, the ACE attempts to match all specified conditions against the matching classification and executes the actions of all matching classes until it encounters a deny for a match request.

You can view a context's policy maps and their types in the Policy Map table (**Config > Virtual Contexts > context > Expert > Policy Map**.)

The types of policy maps that you can configure depend on the ACE device type. [Table 11-15](#) lists the types of policy maps with brief descriptions and the ACE devices that support them.

Table 11-15 Policy Maps and ACE Device Support

Policy Map	Description	ACE Modules and Device			
		ACE 1.0 Module	ACE 2.0 Module	ACE Appliance Running Image A1(8)	ACE Appliance Running Image A3(1.0)
Generic Server Load Balancing	Generic Layer 7 policy map for server load balancing		X		X
Layer 3/4 Management Traffic	Layer 3 and Layer 4 policy map for network management traffic received by the ACE	X	X	X	X
Layer 3/4 Network Traffic	Layer 3 and Layer 4 policy map for traffic passing through the ACE	X	X	X	X
Layer 7 FTP Command Inspection	Layer 7 policy map for inspection of FTP commands	X	X	X	X
Layer 7 HTTP Deep Packet Inspection	Layer 7 policy map for inspection of HTTP packets	X	X	X	X
Layer 7 HTTP Optimization	Layer 7 policy map for optimizing HTTP traffic			X	X
Layer 7 Server Load Balancing	Layer 7 policy map for HTTP server load balancing	X	X	X	X
Layer 7 SIP Deep Packet Inspection	Layer 7 policy map for inspection of SIP packets		X		
Layer 7 Skinny Deep Packet Inspection	Layer 7 policy map for inspection of Skinny Client Control Protocol (SCCP)		X		X
RADIUS Server Load Balancing	Layer 7 policy map for RADIUS server load balancing		X		X
RDP Server Load Balancing	Layer 7 policy map for RDP server load balancing		X		X

Table 11-15 Policy Maps and ACE Device Support (continued)

Policy Map	Description	ACE Modules and Device			
		ACE 1.0 Module	ACE 2.0 Module	ACE Appliance Running Image A1(8)	ACE Appliance Running Image A3(1.0)
RTSP Server Load Balancing	Layer 7 policy map for RTSP server load balancing		X		X
SIP Server Load Balancing	Layer 7 policy map for SIP server load balancing		X		X

Use this procedure to create a policy map for a virtual context.

Procedure

- Step 1** Select **Config > Virtual Contexts > context > Expert > Policy Map**. The Policy Map table appears.
- Step 2** Click **Add** to add a new policy map, or select an existing policy map, then click **Edit** to modify it.
- Step 3** The Policy Map Name field contains an automatically incremented number for the policy map. Either leave the entry as it is or enter a different, unique number.
- Step 4** In Type, select the type of policy map to create. See [Table 11-15](#) for a list of the policy maps and their availability for the different ACE models.
- Step 5** In the Description field, enter a brief description of the policy map.
- Step 6** Click:
 - **Deploy Now** to deploy this configuration on the ACE. To define rules and actions for the policy map, see [Configuring Rules and Actions for Policy Maps, page 11-33](#).
 - **Cancel** to exit this procedure without saving your entries and to return to the Policy Map table.
 - **Next** to deploy your entries and to configure another policy map.

Related Topics

- [Using Virtual Contexts, page 3-1](#)
- [Configuring Virtual Context Class Maps, page 11-6](#)
- [Configuring Rules and Actions for Policy Maps, page 11-33](#)

Configuring Rules and Actions for Policy Maps

Table 11-16 lists the policy maps and related topics for setting rules and actions.

Table 11-16 **Topic Reference for Policy Map Rules and Actions**

Policy Map	Topic for Setting Rules and Actions
Generic Server Load Balancing	Setting Policy Map Rules and Actions for Generic Server Load Balancing, page 11-34
Layer 3/4 Management Traffic	Setting Policy Map Rules and Actions for Layer 3/Layer 4 Management Traffic, page 11-37
Layer 3/4 Network Traffic	Setting Policy Map Rules and Actions for Layer 3/Layer 4 Network Traffic, page 11-38
Layer 7 FTP Command Inspection	Setting Policy Map Rules and Actions for Layer 7 FTP Command Inspection, page 11-45
Layer 7 HTTP Deep Packet Inspection	Setting Policy Map Rules and Actions for Layer 7 HTTP Deep Packet Inspection, page 11-47
Layer 7 HTTP Optimization	Setting Policy Map Rules and Actions for Layer 7 HTTP Optimization, page 11-53
Layer 7 Server Load Balancing	Setting Policy Map Rules and Actions for Layer 7 Server Load-Balancing Traffic, page 11-56
Layer 7 SIP Deep Packet Inspection	Setting Policy Map Rules and Actions for Layer 7 SIP Deep Packet Inspection, page 11-62
Layer 7 Skinny Deep Packet Inspection	Setting Policy Map Rules and Actions for Layer 7 Skinny Deep Packet Inspection, page 11-64
RADIUS Server Load Balancing	Setting Policy Map Rules and Actions for RADIUS Server Load Balancing, page 11-66
RDP Server Load Balancing	Setting Policy Map Rules and Actions for RDP Server Load Balancing, page 11-68
RTSP Server Load Balancing	Setting Policy Map Rules and Actions for RTSP Server Load Balancing, page 11-70
SIP Server Load Balancing	Setting Policy Map Rules and Actions for SIP Server Load Balancing, page 11-73

Setting Policy Map Rules and Actions for Generic Server Load Balancing



Note

Generic server load balancing policy maps are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.

Use this procedure to configure the rules and actions for generic traffic received by the ACE.

Assumptions

- A generic traffic policy map has been configured.
- A class map has been defined for a class map rule if you do not want to use the class-default class map.

Procedure

- Step 1** Select **Config > Virtual Contexts > context > Expert > Policy Map**. The Policy Map table appears.
- Step 2** In the Policy Map table, select the generic traffic policy map you want to set rules and actions for. The Rule table appears.
- Step 3** In the Rule table, click **Add** to add a new rule, or select the rule you want to modify, then click **Edit**. The Rule screen appears.
- Step 4** In the Rule Type field, configure rules using the information in [Table 11-17](#).

Table 11-17 Generic Server Load Balancing Policy Map Rules

Option	Description
Class Map	A class map is used for this traffic policy. - To use the class-default class map, select the Use Class Default check box. The class-default class map is a reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified by the class-default class map. The class-default class map has an implicit match any statement that enables it to match all traffic. - To use a previously created class map: - Clear the Use Class Default check box. - In the Class Map Name field, select the class map to be used.

Table 11-17 **Generic Server Load Balancing Policy Map Rules (continued)**

Option	Description		
Match Condition	A match condition is used for this traffic policy.		
	Match Condition Name	Enter a name for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.	
	Match Condition Type	Source Address	A client source host IP address and subnet mask are used for the network traffic matching criteria. 1. In the Source IP Address field, enter the source IP address of the client in dotted-decimal notation. 2. In the Source Netmask select the subnet mask for the source IP address.
		Layer 4 Payload	Layer 4 payload data is used for the network matching criteria. 1. In the Layer 4 Payload Regex field, enter a Layer 4 payload expression that is contained within the TCP or UDP entity body. Valid entries are strings containing 1 to 255 alphanumeric characters. Table 11-35 lists the supported characters that you can use for matching string expressions. 2. In the Layer 4 Payload Offset field, enter the absolute offset in the data where the Layer 4 payload expression search string starts. The offset starts at the first byte of the TCP or UDP body. Valid entries are integers from 0 to 999.
Insert Before	1. Indicate whether this rule is to precede another rule for this policy map. – N/A—This option is not configured. – False—This rule is not to precede another rule in this policy map. – True—This rule is to precede another rule in this policy map. 2. If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.		

Step 5 Click:

- **Deploy Now** to deploy this configuration. The screen refreshes and the Action table appears. Continue with [Step 6](#).
- **Cancel** to exit this procedure without saving your entries and to return to the Rule table.

**Note**

If you selected the Insert Before option described in [Table 11-17](#) and specified True, perform the following steps to refresh the Rule tab before adding an action for this rule:

1. Click the Rule tab to refresh the Rule table.
2. In the Rule table, select the newly added rule.

When the screen refreshes, an empty action list appears.

- Step 6** In the Action table, click **Add** to add an entry or select an existing entry to modify, then click **Edit**.
- Step 7** In the Id field, accept the automatically incremented entry or assign a unique identifier for this action.
- Step 8** In the Action Type field, configure actions for this rule using the information in [Table 11-18](#).

Table 11-18 Generic Server Load Balancing Policy Map Actions

Action	Description
Server Farm	The ACE is to load balance client requests for content to a server farm. 1. In the Server Farm field, select the server farm for this policy map action. 2. In the Backup Server Farm field, select the backup server farm for this action. 3. Select the Sticky Enabled check box to indicate that the backup server farm is sticky. Clear this check box if the backup server farm is not sticky. 4. Select the Aggregate State Enabled check box to indicate that the operational state of the backup server farm is taken into consideration when evaluating the state of the load-balancing class in a policy map. Clear this check box to indicate that the operational state of the backup server farm is not taken into consideration when evaluating the state of the load-balancing class in a policy map.
Drop	The ACE is to discard packets that match this policy map. In the Action Log field, specify whether the dropped packets are to be logged in the software.
Forward	The ACE is to forward the traffic that match this policy map to its destination.
Sticky Server Farm	The ACE is to load balance client requests for content to a sticky server farm. In the Sticky Group field, select the sticky server farm that is to be used for requests that match this policy map.
Set IP TOS	The ACE is to set the IP Differentiated Services Code Point (DSCP) bit in the Type of Service (ToS) byte. Once the IP DSCP bit is set, other Quality of Service (QoS) services can then operate on the bit settings. In the IP TOS Rewrite Value field, enter the IP DSCP value. Valid entries are integers from 0 to 255.
Server Farm NAT	The ACE is to apply dynamic NAT to traffic for this policy map. 1. In the NAT Pool ID field, enter the number of the pool of IP addresses that exist under the VLAN specified in the VLAN Id field. Valid entries are integers from 1 to 2147483647. For information on configuring NAT pools, see Configuring VLAN Interface NAT Pools, page 9-10. 2. In the VLAN ID field, select the VLAN to use for NAT. Valid entries are integers from 2 to 4094. 3. In the Server Farm Type field, indicate whether the server farm is a backup or primary server farm.

- Step 9** Click:
- **Deploy Now** to deploy this configuration on the ACE.
 - **Cancel** to exit the procedure without saving your entries and to return to the Action table.
 - **Next** to deploy your entries and to configure another action.

Related Topics

- [Configuring Traffic Policies, page 11-1](#)
- [Configuring Virtual Context Class Maps, page 11-6](#)
- [Configuring Virtual Context Policy Maps, page 11-30](#)
- [Configuring Rules and Actions for Policy Maps, page 11-33](#)

Setting Policy Map Rules and Actions for Layer 3/Layer 4 Management Traffic

Use this procedure to configure the rules and actions for IP management traffic received by the ACE.

Assumptions

- A network management policy map has been configured.
- A class map has been defined for a class map rule if you do not want to use the class-default class map.

Procedure

-
- Step 1** Select **Config > Virtual Contexts > context > Expert > Policy Map**. The Policy Map table appears.
- Step 2** In the Policy Map table, select the Layer 3/Layer 4 management traffic policy map you want to set rules and actions for. The Rule table appears.
- Step 3** In the Rule table, click **Add** to add a new rule, or select the rule you want to modify, then click **Edit**. The Rule screen appears.
- Step 4** In the Rule Type field, confirm that classmap is selected.
- Step 5** To use the class-default class map, select the Use Class Default check box.
- Step 6** To use a previously created class map for this rule:
- a. Clear the Use Class Default check box.
 - b. In the Class Map Name field, select the class map to be used.
 - c. In the Insert Before field, indicate whether this rule is to precede another rule in this policy map.
 - N/A—This option is not configured.
 - False—This rule is not to precede another rule in this policy map.
 - True—This rule is to precede another rule in this policy map.
 - d. If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.
- Step 7** Click:
- **Deploy Now** to deploy this configuration on the ACE. The Action table appears. To define actions for this rule, continue with [Step 8](#).
 - **Cancel** to exit this procedure without saving your entries and to return to the Policy Map table.
 - **Next** to deploy your entries and to configure another rule.

**Note**

If you selected the Insert Before option in [Step 6](#) and specified True, perform the following steps to refresh the Rule tab before adding an action for this rule:

1. Click the Rule tab to refresh the Rule table.
2. In the Rule table, select the newly added rule.

When the screen refreshes, an empty action list appears.

-
- Step 8** In the Action table, click **Add** to add an action or select an existing action, then click **Edit** to modify it. The Action configuration screen appears.
- Step 9** In the Id field, either accept the automatically incremented entry or assign a unique identifier for this action.
- Step 10** In the Action Type field, confirm that Mgmt-permit is selected to indicate that this action permits or denies network management traffic.
- Step 11** In the Action field, specify the action that is to occur:
- Permit—The ACE is to accept network management traffic when this rule is met.
 - Deny—The ACE is to deny network management traffic when this rule is met.
- Step 12** Click:
- **Deploy Now** to deploy this configuration on the ACE.
 - **Cancel** to exit the procedure without saving your entries and to return to the Action table.
 - **Next** to deploy your entries and to configure another action.
-

Related Topics

- [Configuring Virtual Context Class Maps, page 11-6](#)
- [Configuring Virtual Context Policy Maps, page 11-30](#)
- [Configuring Rules and Actions for Policy Maps, page 11-33](#)

Setting Policy Map Rules and Actions for Layer 3/Layer 4 Network Traffic

Use this procedure to configure rules and actions for Layer 3/Layer 4 traffic other than network management traffic.

Assumptions

- You have configured a Layer 3/Layer 4 policy map.
- A class map has been defined if you do not want to use the class-default class map.

Procedure

-
- Step 1** Select **Config > Virtual Contexts > context > Expert > Policy Map**. The Policy Map table appears.
- Step 2** In the Policy Map table, select the Layer 3/Layer 4 network traffic policy map you want to set rules and actions for. The Rule table appears.

- Step 3** In the Rule table, click **Add** to add a new rule, or select the rule you want to modify, then click **Edit**. The Rule configuration screen appears.
- Step 4** In the Rule Type field, confirm that Classmap is selected.
- Step 5** To use the class-default class map, select the Use Class Default check box.
- Step 6** To use a previously created class map for this rule:
- Clear the Use Class Default check box.
 - In the Class Map Name field, select the class map to be used.
 - In the Insert Before field, indicate whether this rule is to precede another rule in this policy map:
 - N/A—This option is not configured.
 - False—This rule is not to precede another rule in this policy map.
 - True—This rule is to precede another rule in this policy map.
 - If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.
- Step 7** Click:
- Deploy Now** to deploy this configuration on the ACE. The screen refreshes and the Action field appears. To configure actions for this rule, continue with [Step 8](#).
 - Cancel** to exit this procedure without saving your entries and to return to the Policy Map table.
 - Next** to deploy your entries and to configure another rule.



Note If you selected the Insert Before option in [Step 6](#) and specified True, perform the following steps to refresh the Rule tab before adding an action for this rule:

- Click the Rule tab to refresh the Rule table.
- In the Rule table, select the newly added rule.

When the screen refreshes, an empty action list appears.

- Step 8** In the Action field, click Edit. The Action table appears.
- Step 9** Click **Add** to add an action or select an existing action, then click **Edit** to modify it. The Action configuration screen appears.
- Step 10** In the Id field, either accept the automatically incremented entry or assign a unique identifier for this action.
- Step 11** In the Action Type field, select the type of action to be taken for this rule, then configure the related attributes. See [Table 11-19](#).

Table 11-19 **Layer 3/Layer 4 Network Traffic Policy Map Actions**

Action	Description/Steps
Vip-advertise	This option appears for ACE modules and the ACE 4710 A3(1.0) release only. The ACE is to advertise the IP address of a virtual server as the host route. 1. In the Active field, indicate how the ACE is to advertise the VIP: – N/A—This option is not configured. – False—The ACE always advertises the IP address of the virtual server whether there is any active real server associated with the VIP. – True—The ACE advertises the IP address of the virtual server as the host route only if there is at least one active real server in the server farm. 2. If you select False in the Active field, in the Metric Distance field, enter the administrative distance to include in the routing table. Valid entries are integers from 1 to 254.
Vip-icmp-reply	A VIP is to send an ICMP ECHO-REPLY response to ICMP requests. In the Active field, indicate the response to ICMP requests: • N/A—This option is not configured. • False—A VIP is not to send an ICMP ECHO-REPLY response to an ICMP request. • True—A VIP is to send an ICMP ECHO-REPLY response to an ICMP request.
Polycymap	The ACE is to associate a Layer 7 server load-balancing policy map with this Layer 3/Layer 4 policy map. In the Policy Map field, select the Layer 7 policy map to associate with this Layer 3/Layer 4 policy map.
Vip-in-service	A VIP is to be enabled for server load-balancing operations.

Table 11-19 **Layer 3/Layer 4 Network Traffic Policy Map Actions (continued)**

Action	Description/Steps
Nat	The ACE is to implement network address translation (NAT) for this rule. - In the NAT Mode field, select the type of NAT to be used: - Static NAT—NAT is to translate each local address to a fixed global address. Continue with Step 2. - Dynamic NAT—NAT is to translate local addresses to a pool of global addresses. Continue with Step 3. - If you select Static NAT: - In the Static Mapped Netmask field, select the subnet mask to apply to the static mapped address. - In the Static Port field, enter the TCP or UDP port to use for static port redirection. Valid entries are integers from 0 to 65535. - In the Static Mapped Address field, enter the IP address to use for static NAT translation. This entry establishes the globally unique IP address of a host as it appears to the outside world. The policy map performs the global IP address translation for the source IP address specified in the ACL (as part of the class-map traffic classification). - In the NAT Protocol field, select the protocol to use for NAT: - N/A—This attribute is not set. - UDP—The ACE is to use UDP for NAT. - TCP—The ACE is to use TCP for NAT. - In the VLAN Id field, select the VLAN to use for NAT. - If you select Dynamic NAT: - In the NAT Pool Id field, enter the number of the pool of IP addresses that exist under the VLAN specified in the VLAN Id field. Valid entries are integers from 1 to 2147483647. See Configuring VLAN Interface NAT Pools, page 9-10. - In the VLAN Id field, select the VLAN to use for NAT. Note For dynamic NAT, ACE allows you to associate a non-configured NAT pool ID to the dynamic NAT action. However, the ANM will not discover the dynamic NAT action when the NAT pool ID is not configured. You must associate the configured NAT pool ID to the dynamic NAT action for ANM discovery to complete successfully.
Ssl-proxy	The ACE is to use an SSL proxy server service to define the SSL parameters the ACE is to use during the handshake and subsequent SSL session. - In the SSL Proxy field, select the SSL proxy server service to use in the handshake and subsequent SSL session when the ACE engages with an SSL client. - In the SSL Proxy Type field, confirm that Server is selected to indicate that the ACE is to be configured so that it is recognized as an SSL server.
Appl-parameter-generic	This option appears for ACE 2.0 modules only. A generic parameter map is to be implemented for this rule. In the Generic Parameter Map field, select the generic parameter map to use.

Table 11-19 **Layer 3/Layer 4 Network Traffic Policy Map Actions (continued)**

Action	Description/Steps
Appl-parameter-rtsp	This option appears for ACE 2.0 modules only. An RTSP parameter map containing RTSP-related actions is to be implemented for this rule. In the RTSP Parameter Map field, select the parameter map to use.
Appl-parameter-sip	This option appears for ACE 2.0 modules only. A SIP parameter map containing SIP-related actions is to be implemented for this rule. In the SIP Parameter Map field, select the parameter map to use.
Appl-parameter-skinny	This option appears for ACE 2.0 modules only. A Skinny parameter map containing Skinny-related actions is to be implemented for this rule. In the Skinny Parameter Map field, select the parameter map to use.
Appl-parameter-http	An HTTP parameter map containing HTTP-related actions is to be implemented for this rule. In the HTTP Parameter Map field, select the HTTP parameter map to use.
Connection	A connection parameter map containing TCP/IP connection-related commands that pertain to normalization and termination is to be implemented for this rule. In the Connection Parameter Map field, select the Connection parameter map that is to be used.
Inspect	Deep packet inspection is to be implemented for this rule. 1. In the Inspect Type field, select the protocol that is to be inspected. 2. Provide any protocol-specific information. Table 11-20 describes the available options for deep packet inspection actions.
UDP-fast-age	This option appears for ACE 2.0 modules only. The ACE is to close the connection immediately after sending a response to the client, thereby enabling per-packet load balancing for UDP traffic.
HTTP Optimize	This option appears for ACE appliances only. In the HTTP Optimization Policy field, select the HTTP optimization policy map to use.

Table 11-20 **Layer 3/Layer 4 Network Traffic Policy Map Deep Packet Inspection Options**

Option	Description
DNS	Domain Name System (DNS) query inspection is to be implemented. DNS requires application inspection so that DNS queries will not be subject to the generic UDP handling based on activity timeouts. Instead, the UDP connections associated with DNS queries and responses are torn down as soon as a reply to a DNS query has been received. The ACE performs the reassembly of DNS packets to verify that the packet length is less than the configured maximum length. In the DNS Maximum Length field, enter the maximum length of a DNS reply in bytes. Default for all modules and ACE 4710 devices is 512. Valid range for ACE 1.0 modules is 64 to 65535, and for all other supported modules and ACE 4710 devices, 64 to 65535.
FTP	FTP inspection is to be implemented. The ACE inspects FTP packets, translates the address and port embedded in the payload, and opens up secondary channel for data. - For ACE 2.0 modules and the ACE 4710 A3(1.0) release only, in the Parameter Map field, specify a previously created parameter map used to define parameters for FTP inspection. - In the FTP Strict field, indicate whether the ACE is to check for protocol RFC compliance and prevent Web browsers from sending embedded commands in FTP requests: - N/A—This attribute is not set. - False—The ACE is not to check for RFC compliance or prevent Web browsers from sending embedded commands in FTP requests. - True—The ACE is to check for RFC compliance and prevent Web browsers from sending embedded commands in FTP requests. - If you select True, in the FTP Inspect Policy field, select the Layer 7 FTP command inspection policy to be implemented for this rule.
HTTP	Enhanced Hypertext Transfer Protocol (HTTP) inspection is to be performed on HTTP traffic. The inspection checks are based on configured parameters in an existing Layer 7 policy map and internal RFC compliance checks performed by the ACE. By default, the ACE allows all request methods. - In the HTTP Inspect Policy field, select the HTTP inspection policy map to be implemented for this rule. If you do not specify a Layer 7 policy map, the ACE performs a general set of Layer 3 and Layer 4 protocol fixup actions and internal RFC compliance checks. - In the URL Logging field, indicate whether Layer 3 and Layer 4 traffic is to be monitored: - N/A—This attribute is not set. - False—Layer 3 and Layer 4 traffic is not to be monitored. - True—Layer 3 and Layer 4 traffic is to be monitored. When enabled, this function logs every URL request that is sent in the specified class of traffic, including the source or destination IP address and the URL that is accessed.

Table 11-20 *Layer 3/Layer 4 Network Traffic Policy Map Deep Packet Inspection Options (continued)*

Option	Description
ICMP	Internet Control Message Protocol (ICMP) payload inspection is to be performed. ICMP inspection allows ICMP traffic to have a “session” so it can be inspected similarly to TCP and UDP traffic. In the ICMP Error field, indicate whether the ACE is to perform name address translation on ICMP error messages: • N/A—This attribute is not set. • False—The ACE is not to perform NAT on ICMP error messages. • True—The ACE is to perform NAT on ICMP error messages. When enabled, the ACE creates translation sessions for intermediate or endpoint nodes that send ICMP error messages based on the NAT configuration. The ACE overwrites the packet with the translated IP addresses.
ILS	Internet Locator Service (ILS) protocol inspection is to be implemented.
RTSP	Real Time Streaming Protocol (RTSP) packet inspection is to be implemented. RTSP is used by RealAudio, RealNetworks, Apple QuickTime 4, RealPlayer, and Cisco IP/TV connections. The ACE monitors Setup and Response (200 OK) messages in the control channel established using TCP port 554 (no UDP support). For ACE 2.0 modules only, in the Parameter Map field, select a previously defined parameter map used to define parameters for RTSP inspection.
SIP	SIP protocol inspection is implemented. SIP is used for call handling sessions and instant messaging. The ACE inspects signaling messages for media connection addresses, media ports, and embryonic connections. The ACE also uses NAT to translate IP addresses that are embedded in the user-data portion of the packet. 1. For ACE 2.0 modules only, in the Parameter Map field, specify a previously created parameter map used to define parameters for SIP inspection. 2. In the SIP Inspect Policy field, select a previously created Layer 7 SIP inspection policy map to implement packet inspection of Layer 7 SIP application traffic. If you do not specify a Layer 7 policy map, the ACE performs a general set of Layer 3 and Layer 4 HTTP fixup actions and internal RFC compliance checks.
Skinny	Cisco Skinny Client Control Protocol (SCCP) protocol inspection is implemented. The SCCP is a Cisco proprietary protocol that is used between Cisco CallManager and Cisco VOiP phones. The ACE uses NAT to translate embedded IP addresses and port numbers in SCCP packet data. 1. For ACE 2.0 modules only, in the Parameter Map field, specify a previously created connection parameter map used to define parameters for Skinny inspection. 2. In the Skinny Inspect Policy field, select a previously created Layer 7 Skinny inspection policy map to implement packet inspection of Layer 7 Skinny application traffic. If you do not specify a Layer 7 policy map, the ACE performs a general set of Layer 3 and Layer 4 HTTP fixup actions and internal RFC compliance checks.

Step 12 Click:

- **Deploy Now** to deploy this configuration on the ACE.
- **Cancel** to exit this procedure without saving your entries and to return to the Action table.
- **Next** to deploy your entries and to configure another Action.

Related Topics

- [Configuring Traffic Policies, page 11-1](#)
- [Configuring Virtual Context Class Maps, page 11-6](#)
- [Configuring Virtual Context Policy Maps, page 11-30](#)

Setting Policy Map Rules and Actions for Layer 7 FTP Command Inspection

File Transfer Protocol (FTP) inspection inspects FTP sessions for address translation in a message, dynamic opening of ports, and stateful tracking of request and response messages. Each specified FTP command must be acknowledged before the ACE allows a new command. Command filtering allows you to restrict specific commands by the ACE. When the ACE denies a command, it closes the connection.

The FTP command inspection process, as performed by the ACE:

- Prepares a dynamic secondary data connection. The channels are allocated in response to a file upload, a file download, or a directory listing event and must be prenegotiated. The port is negotiated through the PORT or PASV commands.
- Tracks the FTP command-response sequence. The ACE performs the command checks listed below. If you specify the FTP Strict field in a Layer 3 and Layer 4 policy map, the ACE tracks each FTP command and response sequence for the anomalous activity outlined below. The FTP Strict parameter is used in conjunction with a Layer 7 FTP policy map (nested within the Layer 3 and Layer 4 policy map) to deny certain FTP commands or to mask the server reply for SYST command.

**Note**

The use of the FTP Strict parameter may affect FTP clients that do not comply with the RFC standards.

- Truncated command—Checks the number of commas in the PORT and PASV reply command against a fixed value of five. If the value is not five, the ACE assumes that the PORT command is truncated and issues a warning message and closes the TCP connection.
- Incorrect command—Checks the FTP command to verify if it ends with <CR><LF> characters, as required by RFC 959. If the FTP command does not end with those characters, the ACE closes the connection.
- Size of RETR and STOR commands—Checked the size of the RETR and STOR commands against a fixed constant of 256. If the size is greater, the ACE logs an error message and closes the connection.
- Command spoofing—Verifies that the PORT command is always sent from the client. If a PORT command is sent from the server, the ACE denies the TCP connection.
- Reply spoofing—Verifies that the PASV reply command (227) is always sent from the server. If a PASV reply command is sent from the client, the ACE denies the TCP connection. This denial prevents a security hole when the user executes “227 xxxxx a1, a2, a3, a4, p1, p2.”
- Invalid port negotiation—Checks the negotiated dynamic port value to verify that it is greater than 1024 (port numbers in the range from 2 to 1024 are reserved for well-known connections). If the negotiated port falls in this range, the ACE closes the TCP connection.
- Command pipelining—Checks the number of characters present after the port numbers in the PORT and PASV reply command against a constant value of 8. If the number of characters is greater than 8, the ACE closes the TCP connection.

- Translates embedded IP addresses in conjunction with NAT. FTP command inspection translates the IP address within the application payload. Refer to RFC 959 for background details.

Use this procedure to add rules and actions for Layer 7 FTP command inspection policy maps.

Procedure

- Step 1** Select **Config > Virtual Contexts > context > Expert > Policy Map**. The Policy Map table appears.
- Step 2** In the Policy Map table, select the Layer 7 FTP command inspection policy map you want to set rules and actions for. The Rule table appears.
- Step 3** In the Rule table, click **Add** to add a new rule, or select an existing rule, then **Edit** to modify it. The Rule configuration screen appears.
- Step 4** In the Rule Type field, configure rules using the information in [Table 11-21](#).

Table 11-21 Layer 7 FTP Command Inspection Policy Map Rules

Option	Description
Class Map	Specify a class map to use for this traffic policy: - To use the class-default class map, select the Use Class Default check box. The class-default class map is a reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified by the class-default class map. The class-default class map has an implicit match any statement that enables it to match all traffic. - To use a previously created class map: - Clear the Use Class Default check box. - In the Class Map Name field, select the class map to be used.
Match Condition	Specify a match condition to use for this traffic policy: - In the Match Condition Name field, enter a name for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. - In the Match Condition Type field, confirm that Request Method Name is selected. - In the Request Method Name field, select the FTP command to be inspected for this rule. Table 11-9 describes the FTP commands that can be inspected.
Insert Before	- Indicate whether this rule is to precede another rule for this policy map. - N/A—This option is not configured. - False—This rule is not to precede another rule in this policy map. - True—This rule is to precede another rule in this policy map. - If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.

- Step 5** Click:
 - **Deploy Now** to deploy this configuration on the ACE. The screen refreshes and the Action table appears. Continue with [Step 6](#).
 - **Cancel** to exit this procedure without saving your entries and to return to the Policy Map table.

- **Next** to deploy your entries and to configure another rule.



Note If you selected the Insert Before option described in [Table 11-21](#) and specified True, perform the following steps to refresh the Rule tab before adding an action for this rule:

1. Click the Rule tab to refresh the Rule table.
2. In the Rule table, select the newly added rule.

When the screen refreshes, an empty action list appears.

- Step 6** In the Action table, click **Add** to add an entry, or select an existing entry, then click **Edit** to modify it. The Action configuration screen appears.
- Step 7** In the Id field, either accept the automatically incremented entry or assign a unique identifier for this action.
- Step 8** In the Action Type field, specify the action to be taken for this rule:
- Deny—The ACE is to deny the specified FTP command when this rule is met.
 - Mask-reply—The ACE is to mask the reply to the FTP **syst** command by filtering sensitive information from the command output. The action applies to the FTP **syst** command only.
- Step 9** Click:
- **Deploy Now** to deploy this configuration on the ACE.
 - **Cancel** to exit this procedure without saving your entries and to return to the Action table.
 - **Next** to deploy your entries and to configure another action for this rule.

Related Topics

- [Configuring Traffic Policies, page 11-1](#)
- [Configuring Virtual Context Class Maps, page 11-6](#)
- [Configuring Virtual Context Policy Maps, page 11-30](#)

Setting Policy Map Rules and Actions for Layer 7 HTTP Deep Packet Inspection

The ACE performs a stateful deep packet inspection of the HTTP protocol. Deep packet inspection is a special case of application inspection where the ACE examines the application payload of a packet or a traffic stream and makes decisions based on the content of the data. During HTTP deep inspection, the main focus of the application inspection process is on HTTP attributes such as HTTP header, URL, and to a limited extent, the payload. User-defined regular expressions can also be used to detect “signatures” in the payload.

You define policies to permit or deny the traffic, or to send a TCP reset message to the client or server to close the connection.

The security features covered by HTTP application inspection include:

- RFC compliance monitoring and RFC method filtering
- Content, URL, and HTTP header length checks

- Transfer-encoding methods
- Content type verification and filtering
- Port 80 misuse

Use this procedure to add rules and actions for Layer 7 HTTP deep packet inspection policy maps.

Procedure

- Step 1** Select **Config > Virtual Contexts > context > Expert > Policy Map**. The Policy Map table appears.
- Step 2** In the Policy Map table, select the Layer 7 deep packet inspection policy map that you want to set rules and actions for. The Rule table appears.
- Step 3** In the Rule table, click **Add** to add a new rule, or select an existing rule, then **Edit** to modify it. The Rule configuration screen appears.
- Step 4** In the Rule Type field, configure rules using the information in [Table 11-22](#).

Table 11-22 Layer 7 HTTP Deep Packet Inspection Policy Map Rules

Option	Description
Class Map	Specify a class map to use for this traffic policy: - To use the class-default class map, select the Use Class Default check box. The class-default class map is a reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified by the class-default class map. The class-default class map has an implicit match any statement that enables it to match all traffic. - To use a previously created class map: - Clear the Use Class Default check box. - In the Class Map Name field, select the class map to be used.
Match Condition	Specify a match condition to use for this traffic policy: - In the Match Condition Name field, enter a name for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. - In the Match Condition Type field, select the method by which match decisions are to be made and their corresponding conditions. See Table 11-23 for information about these selections.
Insert Before	- Indicate whether this rule is to precede another rule for this policy map. - N/A—This option is not configured. - False—This rule is not to precede another rule in this policy map. - True—This rule is to precede another rule in this policy map. - If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.

Table 11-23 Layer 7 HTTP Deep Packet Inspection Policy Map Match Conditions

Match Condition	Description
Content	Specific content contained within the HTTP entity-body is used for protocol inspection decisions. 1. In the Content Expression field, enter the content that is to be matched. Valid entries are alphanumeric strings from 1 to 255 characters. 2. In the Content Offset field, enter the number of bytes to be ignored starting with the first byte of the Message body, after the empty line (CR,LF,CR,LF) between the headers and the body of the message. Valid entries are from 1 to 255 bytes.
Content Length	The content parse length in an HTTP message is used for protocol inspection decisions. 1. In the Content Length Operator field, select the operand to be used to compare content length: – Equal—The content length must equal the number in the Content Length Value field. – Greater than—The content length must be greater than the number in the Content Length Value field. – Less than—The content length must be less than the number in the Content Length Value field. – Range—The content length must be within the range specified in the Content Length Lower Value field and the Content Length Higher Value field. 2. Enter values to apply for content length comparison: – If you select Equal, Greater than, or Less than in the Content Length Operator field, the Content Length Value field appears. In the Content Length Value field, enter the number of bytes for comparison. Valid entries are integers from 0 to 4294967295. – If you select Range in the Content Length Operator field, the Content Length Lower Value and the Content Length Higher Value fields appear: a. In the Content Length Lower Value field, enter the lowest number of bytes to be used for this match condition. Valid entries are integers from 0 to 4294967295. The number in this field must be less than the number entered in the Content Length Higher Value field. b. In the Content Length Higher Value field, enter the highest number of bytes to be used for this match condition. Valid entries are integers from 1 to 4294967295. The number in this field must be greater than the number entered in the Content Length Lower Value field.
Content-type Verification	Verifies the content MIME-type messages with the header MIME-type. This inline match command limits the MIME-types in HTTP messages allowed through the ACE. It verifies that the header MIME-type value is in the internal list of supported MIME-types and the header MIME-type matches the actual content in the data or entity body portion of the message. If they do not match, the ACE performs the specified Layer 7 policy map action.

Table 11-23 Layer 7 HTTP Deep Packet Inspection Policy Map Match Conditions (continued)

Match Condition	Description
Header	The name and value in an HTTP header are used for protocol inspection decisions. 1. In the Header field, select one of the predefined HTTP headers to be matched, or select HTTP Header to specify a different HTTP header. 2. If you select HTTP Header, in the Header Name field, enter the name of the HTTP header to match. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. 3. In the Header Value field, enter the header value expression string to compare against the value in the specified field in the HTTP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. To include spaces in the string, enclose the entire string in quotes. All headers in the header map must be matched. See Table 11-35 for a list of the supported characters that you can use in regular expressions.
Header Length	The length of the header in the HTTP message is used for protocol inspection decisions. 1. In the Header Length Type field, specify whether HTTP header request or response messages are to be used for protocol inspection decisions: – Request—HTTP header request messages are to be checked for header length. – Response—HTTP header response messages are to be checked for header length. 2. In the Header Length Operator field, select the operand to be used to compare header length: – Equal—The header length must equal the number in the Header Length Value field. – Greater Than—The header length must be greater than the number in the Header Length Value field. – Less Than—The header length must be less than the number in the Header Length Value field. – Range—The header length must be within the range specified in the Header Length Lower Value field and the Header Length Higher Value field. 3. Enter values to apply for header length comparison: – If you select Equal, Greater Than, or Less Than in the Header Length Operator field, the Header Length Value field appears. In the Header Length Value field, enter the number of bytes for comparison. Valid entries are integers from 0 to 255. – If you select Range in the Header Length Operator field, the Header Length Lower Value and the Header Length Higher Value fields appear: a. In the Header Length Lower Value field, enter the lowest number of bytes to be used for this match condition. Valid entries are integers from 0 to 255. The number in this field must be less than the number entered in the Header Length Higher Value field. b. In the Header Length Higher Value field, enter the highest number of bytes to be used for this match condition. Valid entries are integers from 1 to 255. The number in this field must be greater than the number entered in the Header Length Lower Value field.
Header MIME Type	Multipurpose Internet Mail Extension (MIME) message types are used for protocol inspection decisions. In the Header MIME Type field, select the MIME message type to be used for this match condition.

Table 11-23 **Layer 7 HTTP Deep Packet Inspection Policy Map Match Conditions (continued)**

Match Condition	Description
Port Misuse	The misuse of port 80 (or any other port running HTTP) is used for protocol inspection decisions. In the Port Misuse field, select the application category to be used for this match condition: • IM—Instant messaging applications are to be used for this match condition. • P2P—Peer-to-peer applications are to be used for this match condition. • Tunneling—Tunneling applications are to be used for this match condition.
Request Method	The request method is used for protocol inspection decisions. By default, ACEs allow all request and extension methods. This option allows you to configure class maps that define protocol inspection decisions based on compliance to request methods defined in RFC 2616 and by HTTP extension methods. 1. In the Request Method Type field, select the type of compliance to be used for protocol inspection decision: – Ext—An HTTP extension method is to be used for protocol inspection decisions. – RFC—A request method defined in RFC 2616 is to be used for protocol inspection decisions. 2. In the Request Method field, select the specific request method to be used.
Strict HTTP	Internal compliance checks are performed to verify that a message is compliant with the HTTP RFC standard, RFC 2616. If the HTTP message is not compliant, the ACE performs the specified Layer 7 policy map action.
Transfer Encoding	An HTTP transfer-encoding type is used for protocol inspection decisions. The transfer-encoding general-header field indicates the type of transformation, if any, that has been applied to the HTTP message body to safely transfer it between the sender and the recipient. In the Transfer Encoding field, select the type of encoding that is to be checked: • Chunked—The message body is transferred as a series of chunks. • Compress—The encoding format that is produced by the UNIX file compression program compress. • Deflate—The .zlib format that is defined in RFC 1950 in combination with the DEFLATE compression mechanism described in RFC 1951. • Gzip—The encoding format that is produced by the file compression program GZIP (GNU zip) as described in RFC 1952. • Identity—The default (identity) encoding which does not require the use of transformation.

Table 11-23 Layer 7 HTTP Deep Packet Inspection Policy Map Match Conditions (continued)

Match Condition	Description
URL	URL names are used for protocol inspection decisions. In the URL field, enter a URL or a portion of a URL to match. Valid entries are URL strings from 1 to 255 alphanumeric characters and include only the portion of the URL following <code>www.hostname.domain</code>. For example, in the URL <code>www.anydomain.com/latest/whatsnew.html</code>, include only <code>/latest/whatsnew.html</code>.
URL Length	URL length is used for protocol inspection decisions. - In the URL Length Operator field, select the operand to be used to compare URL length: - Equal—The URL length must equal the number in the URL Length Value field. - Greater Than—The URL length must be greater than the number in the URL Length Value field. - Less Than—The URL length must be less than the number in the URL Length Value field. - Range—The URL length must be within the range specified in the URL Length Lower Value field and the URL Length Higher Value field. - Enter values to apply for URL length comparison: - If you select Equal, Greater Than, or Less Than in the URL Length Operator field, the URL Length Value field appears. In the URL Length Value field, enter the value for comparison. Valid entries are from 1 to 65535 bytes. - If you select Range in the URL Length Operator field, the URL Length Lower Value and the URL Length Higher Value fields appear: - In the URL Length Lower Value field, enter the lowest number of bytes to be used for this match condition. Valid entries are integers from 1 to 65535. The number in this field must be less than the number entered in the URL Length Higher Value field. - In the URL Length Higher Value field, enter the highest number of bytes to be used for this match condition. Valid entries are integers from 1 to 65535. The number in this field must be greater than the number entered in the URL Length Lower Value field.

Step 5 Click:

- **Deploy Now** to deploy this configuration on the ACE. The screen refreshes and the Action table appears. To define actions for this rule, continue with [Step 6](#).
- **Cancel** to exit this procedure without saving your entries and to return to the Policy Map table.
- **Next** to deploy your entries and to configure another rule.

**Note**

If you selected the Insert Before option described in [Table 11-22](#) and specified True, perform the following steps to refresh the Rule tab before adding an action for this rule:

1. Click the Rule tab to refresh the Rule table.
2. In the Rule table, select the newly added rule.

When the screen refreshes, an empty action list appears.

- Step 6** In the Action table, click **Add** to add a new action, or select an existing action, then click **Edit** to modify it. The Action configuration screen appears.
- Step 7** In the Id field, either accept the automatically incremented entry or assign a unique identifier for this action.
- Step 8** In the Action Type field, select the action to be taken for this rule:
- **Permit**—The HTTP traffic is to be allowed if it meets the match criteria.
 - **Reset**—The HTTP traffic is to be denied if it meets the match criteria. A TCP reset message is sent to the client or server to close the connection.
- Step 9** In the Action Log field, specify whether the action taken is to be logged.
- Step 10** Click:
- **Deploy Now** to deploy this configuration on the ACE.
 - **Cancel** to exit this procedure without saving your entries and to return to the Action table.
 - **Next** to configure another action for this policy map and rule.

Related Topics

- [Configuring Traffic Policies, page 11-1](#)
- [Configuring Virtual Context Class Maps, page 11-6](#)
- [Configuring Virtual Context Policy Maps, page 11-30](#)
- [Configuring Rules and Actions for Policy Maps, page 11-33](#)

Setting Policy Map Rules and Actions for Layer 7 HTTP Optimization



Note

HTTP optimization policy maps are available for ACE appliances only.

Use this procedure to add rules and actions for Layer 7 HTTP optimization policy maps.

Assumptions

- An action list has been configured. See [Configuring Action Lists for Application Acceleration and Optimization, page 12-3](#) for more information.
- A class map has been defined if you are not using the class-default class map. See [Configuring Virtual Context Class Maps, page 11-6](#) for more information.

Procedure

- Step 1** Select **Config > Virtual Contexts > context > Expert > Policy Map**. The Policy Map table appears.
- Step 2** In the Policy Map table, select the Layer 7 HTTP optimization policy map you want to set rules and actions for. The Rule table appears.
- Step 3** In the Rule table, click **Add** to add a new rule, or select an existing rule, then **Edit** to modify it. The Rule configuration screen appears.
- Step 4** In the Rule Type field, configure rules using the information in [Table 11-24](#).

Table 11-24 **Layer 7 HTTP Optimization Policy Map Rules**

Option	Description
Class Map	Specify a class map to use for this traffic policy: - To use the class-default class map, select the Use Class Default check box. The class-default class map is a reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified by the class-default class map. The class-default class map has an implicit match any statement that enables it to match all traffic. - To use a previously created class map: - Clear the Use Class Default check box. - In the Class Map Name field, select the class map to be used.
Match Condition	Specify a match condition to use for this traffic policy: - In the Match Condition Name field, enter a name for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. - In the Match Condition Type field, select the method by which match decisions are to be made and their corresponding conditions. See Table 11-25 for information about these selections.
Insert Before	- Indicate whether this rule is to precede another rule for this policy map. - N/A—This option is not configured. - False—This rule is not to precede another rule in this policy map. - True—This rule is to precede another rule in this policy map. - If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.

Table 11-25 Layer 7 HTTP Optimization Policy Map Match Conditions

Match Condition	Procedure
Cookie	An HTTP cookie is to be used to establish a match condition. 1. In the Cookie Name field, enter a unique cookie name. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. 2. In the Cookie Value field, enter a unique cookie value expression. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. 3. In the Secondary field, indicate whether the ACE is to use both the cookie name and the cookie value to satisfy this match condition: – N/A—This option is not configured. – False—The ACE is to use either the cookie name or the cookie value to satisfy this match condition. – True—The ACE is to use both the cookie name and the cookie value to satisfy this match condition.
Header	An HTTP header is to be used to establish a match condition. 1. In the Header field, select one of the predefined HTTP headers to be matched, or select HTTP Header to specify a different HTTP header. 2. If you select HTTP Header, in the Header Name field, enter the name of the HTTP header to match. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. 3. In the Header Value field, enter the header value expression string to compare against the value in the specified field in the HTTP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. To include spaces in the string, enclose the entire string in quotes. All headers in the header map must be matched. See Table 11-35 for a list of the supported characters that you can use in regular expressions.
Http-url	A portion of an HTTP URL is to be used to establish a match condition. 1. In the URL Expr field, enter a URL or a portion of a URL to match. Valid entries are URL strings from 1 to 255 alphanumeric characters and include only the portion of the URL following <code>www.hostname.domain</code>. For example, in the URL <code>www.anydomain.com/latest/whatsnew.html</code>, include only <code>/latest/whatsnew.html</code>. 2. In the Method field, enter the HTTP method to match. Valid entries are method names entered as unquoted text strings with no spaces and a maximum of 15 alphanumeric characters. You can enter either one of the standard HTTP 1.1 method names (OPTIONS, GET, HEAD, POST, PUT, DELETE, TRACE, or CONNECT) or a text string that must be matched exactly (for example, CORVETTE).

Step 5 Click:

- **Deploy Now** to deploy this configuration on the ACE. The screen refreshes and the Action table appears. To define actions for this rule, continue with [Step 6](#).
- **Cancel** to exit this procedure without saving your entries and to return to the Rule table.
- **Next** to deploy your entries and to configure another rule.

**Note**

If you selected the Insert Before option described in [Table 11-24](#) and specified True, perform the following steps to refresh the Rule tab before adding an action for this rule:

1. Click the Rule tab to refresh the Rule table.
2. In the Rule table, select the newly added rule.

When the screen refreshes, an empty action list appears.

-
- Step 6** In the Action table, click **Add** to add a new action, or select an existing action, then click **Edit** to modify it. The Action configuration screen appears.
- Step 7** In the Id field, either accept the automatically incremented entry or assign a unique identifier for this action.
- Step 8** In the Action Type field, confirm that Action-list is selected.
- Step 9** In the Action List field, select the action list to apply to this policy map and rule.
- Step 10** In the Optimization Parameter Map field, select the optimization parameter map to apply to this policy map and rule.
- Step 11** Click:
- **Deploy Now** to deploy this configuration on the ACE.
 - **Cancel** to exit this procedure without saving your entries and to return to the Action table.
 - **Next** to deploy your entries and to configure another action for this rule.
-

Related Topics

- [Configuring Traffic Policies, page 11-1](#)
- [Configuring Virtual Context Class Maps, page 11-6](#)
- [Configuring Virtual Context Policy Maps, page 11-30](#)
- [Configuring Rules and Actions for Policy Maps, page 11-33](#)

Setting Policy Map Rules and Actions for Layer 7 Server Load-Balancing Traffic

Use this procedure to set rules and actions for Layer 7 server load-balancing policy maps.

Assumptions

- You have configured a load-balancing policy map and want to establish the corresponding rules and actions.
- If you want to configure an SSL proxy action, you have configured SSL proxy service for this context.

Procedure

-
- Step 1** Select **Config > Virtual Contexts > context > Expert > Policy Map**. The Policy Map table appears.

- Step 2** In the Policy Map table, select the load-balancing policy map you want to set rules and actions for. The Rule table appears.
- Step 3** In the Rule table, click **Add** to add a new rule, or select an existing rule, then **Edit** to modify it. The Rule configuration screen appears.
- Step 4** In the Rule Type field, configure rules using the information in [Table 11-26](#).

Table 11-26 Layer 7 Server Load Balancing Policy Map Rules

Option	Description
Class Map	Specify a class map to use for this traffic policy: - To use the class-default class map, select the Use Class Default check box. The class-default class map is a reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified by the class-default class map. The class-default class map has an implicit match any statement that enables it to match all traffic. - To use a previously created class map: - Clear the Use Class Default check box. - In the Class Map Name field, select the class map to be used.
Match Condition	Specify a match condition to use for this traffic policy: - In the Match Condition Name field, enter a name for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. - In the Match Condition Type field, select the method by which match decisions are to be made and their corresponding conditions. See Table 11-27 for information about these selections.
Insert Before	- Indicate whether this rule is to precede another rule for this policy map. - N/A—This option is not configured. - False—This rule is not to precede another rule in this policy map. - True—This rule is to precede another rule in this policy map. - If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.

Table 11-27 Layer 7 Server Load Balancing Policy Map Match Conditions

Match Condition	Description
Http-cookie	HTTP cookies are to be used for this match condition. 1. In the Cookie Name field, enter a unique cookie name. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. 2. In the Cookie Value field, enter a unique cookie value expression. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching string expressions. Table 11-35 lists the supported characters that you can use for matching string expressions.
Http-header	The HTTP header and a corresponding value are to be used for this match condition. 1. In the Header Name field, specify the header to match in one of the following ways: – To specify an HTTP header that is not one of the standard HTTP headers, select the first radio button, then enter the HTTP header name in the Header Name field. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters. – To specify a standard HTTP header, click the second radio button, then select an HTTP header from the list. 2. In the Header Value field, enter the header-value expression string to compare against the value in the specified field in the HTTP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. To include spaces, enclose the entire string in quotes. All headers in the header map must be matched. See Table 11-35 for a list of the supported characters that you can use in regular expressions.
Http-url	This rule is to perform regular expression matching against the received packet data from a particular connection based on the HTTP URL string. 1. In the URL Expr field, enter a URL, or portion of a URL, to match. Valid entries are URL strings from 1 to 255 alphanumeric characters. Include only the portion of the URL following <code>www.hostname.domain</code> in the match statement. For example, in the URL <code>www.anydomain.com/latest/whatsnew.html</code>, include only <code>/latest/whatsnew.html</code>. To match the <code>www.anydomain.com</code> portion, the URL string can take the form of a URL regular expression. The ACE supports regular expressions for matching URL strings. See Table 11-35 for a list of the supported characters that you can use in regular expressions. 2. In the Method Expr field, enter the HTTP method to match. Valid entries are unquoted text strings with no spaces and a maximum of 15 alphanumeric characters. The method can either be one of the standard HTTP 1.1 method names (OPTIONS, GET, HEAD, POST, PUT, DELETE, TRACE, or CONNECT) or a text string that must be matched exactly (for example, CORVETTE).

Table 11-27 Layer 7 Server Load Balancing Policy Map Match Conditions (continued)

Match Condition	Description
Source-address	A client source IP address is used to establish match conditions. 1. In the Source IP Address field, enter the source IP address of the client. Enter the IP address in dotted-decimal notation (for example, 192.168.11.2). 2. In the Source Netmask field, enter the subnet mask of the IP address. Enter the netmask in dotted-decimal notation (for example, 255.255.255.0). The default is 255.255.255.255.
Http-content	This option appears for ACE 2.0 modules only. Specific content contained within the HTTP entity-body is used to establish a match condition. 1. In the Content Expression field, enter the content that is to be matched. Valid entries are alphanumeric strings from 1 to 255 characters. 2. In the Content Offset field, enter the number of bytes to be ignored starting with the first byte of the Message body, after the empty line (CR,LF,CR,LF) between the headers and the body of the message. Valid entries are integers from 1 to 255.

Step 5 Click:

- **Deploy Now** to deploy the configuration on the ACE. The screen refreshes and the Action table appears. To define the actions for this rule, continue with [Step 6](#).
- **Cancel** to exit this procedure without saving your entries and to return to the Rule table.
- **Next** to deploy your entries and to configure another rule.

**Note**

If you selected the Insert Before option described in [Table 11-26](#) and specified True, perform the following steps to refresh the Rule tab before adding an action for this rule:

1. Click the Rule tab to refresh the Rule table.
2. In the Rule table, select the newly added rule.

When the screen refreshes, an empty action list appears.

Step 6 In the Action table, click **Add** to add a new action, or select an existing action, then click **Edit** to modify it.

Step 7 In the Id field, either accept the automatically incremented entry or assign a unique identifier for this action.

Step 8 In the Action Type field, select the action to be taken and configure any action-specific attributes as described in [Table 11-28](#).

Table 11-28 **Layer 7 Server Load Balancing Policy Map Actions**

Action	Description
Serverfarm	The ACE is to load balance client requests for content to a server farm. 1. In the Server Farm field, select the server farm to which requests for content are to be sent. 2. In the Backup Server Farm field, select the backup server farm to which requests for content are to be sent. Select N/A to indicate that no backup server farm is to be used. 3. ~~Select the Sticky Enabled check box to indicate that the sticky group associated with this policy and applied to the primary server farm is applied to the backup server farm. Clear the Sticky Enabled check box to indicate that the sticky group associated with this policy and applied to the primary server farm in that policy is not applied to the backup server farm.~~ 4. Select the Aggregate State Enabled check box to indicate that the operational state of the backup server farm is taken into consideration when evaluating the state of the load-balancing class in a policy map. Clear this check box to indicate that the operational state of the backup server farm is not taken into consideration when evaluating the state of the load-balancing class in a policy map.
Drop	The ACE is to discard packets that match the rule. In the Action Log field, specify whether the dropped packets are to be logged in the software.
Forward	The ACE is to forward requests that match this policy map without load balancing the requests.
Insert-http	The ACE is to insert an HTTP header for Layer 7 load balancing for requests that match this policy map. This option allows the ACE to identify a client whose IP address has been translated using NAT by inserting a generic header and string value in the client HTTP request. 1. In the HTTP Header Name field, enter the name of the generic field in the HTTP header. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. 2. In the HTTP Header Value field, enter the value to be inserted into the HTTP header. Valid entries are unquoted text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. To include spaces, enclose the entire string in quotes. All headers in the header map must be matched. See Table 11-35 for a list of the supported characters that you can use in regular expressions.
Sticky-serverfarm	Requests matching this policy map be load balanced to a sticky server farm. In the Sticky Group field, select the sticky server farm that is to be used for requests that match this policy map.
Ssl-proxy	The ACE is to use an SSL proxy client service to define the SSL parameters the ACE is to use during the handshake and subsequent SSL session. 1. In the SSL Proxy field, select the SSL proxy service to be used for this action. 2. In the SSL Proxy Type field, confirm that Client is selected to indicate that the ACE is to be configured so that it is recognized as an SSL client.

Table 11-28 **Layer 7 Server Load Balancing Policy Map Actions (continued)**

Action	Description
Compress	 Note This option appears for ACE appliances. The ACE is to compress packets that match this policy map. This option is available only when you associate an HTTP-type class map with a policy map. In the Compress Method field, specify the method that the ACE is to use to compress packets: • Deflate—Indicates that the ACE is to use the DEFLATE compression method when the client browser supports both the DEFLATE and GZIP compression methods. • Gzip—Indicates that ACE is to use the GZIP compression method when the client browser supports both the DEFLATE and GZIP compression methods.
Action	This option appears for ACE 2.0 modules and the ACE 4710 A3(1.0) release only. The ACE is to implement an action list for the rule. In the Action List field, select an action list to associate with this rule.
Set IP TOS	The ACE is to set the IP Differentiated Services Code Point (DSCP) bit in the Type of Service (ToS) byte. Once the IP DSCP bit is set, other Quality of Service (QoS) services can then operate on the bit settings. In the IP TOS Rewrite Value field, enter the IP DSCP value. Valid entries are integers from 0 to 255.
Server Farm NAT	This option appears for ACE 2.0 modules only. The ACE is to apply dynamic NAT to traffic for this policy map. 1. In the NAT Pool ID field, enter the number of the pool of IP addresses that exist under the VLAN specified in the VLAN Id field. Valid entries are integers from 1 to 2147483647. For information on configuring NAT pools, see Configuring VLAN Interface NAT Pools, page 9-10. 2. In the VLAN ID field, select the VLAN to use for NAT. Valid entries are integers from 2 to 4094. 3. In the Server Farm Type field, indicate whether the server farm is a backup or primary server farm.

Step 9 Click:

- **Deploy Now** to deploy this configuration on the ACE.
- **Cancel** to exit the procedure without saving your entries and to return to the Action table.
- **Next** to deploy your entries and to configure another action.

Related Topics

- [Configuring Traffic Policies, page 11-1](#)
- [Configuring Virtual Context Class Maps, page 11-6](#)
- [Configuring Virtual Context Policy Maps, page 11-30](#)
- [Configuring Rules and Actions for Policy Maps, page 11-33](#)

Setting Policy Map Rules and Actions for Layer 7 SIP Deep Packet Inspection

**Note**

SIP deep packet inspection policy maps are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.

Use this procedure to configure the rules and actions for a SIP deep packet inspection policy map.

Assumptions

- A SIP deep packet inspection policy map has been configured.
- A class map has been defined for a class map rule if you do not want to use the class-default class map.

Procedure

- Step 1** Select **Config > Virtual Contexts > context > Expert > Policy Map**. The Policy Map table appears.
- Step 2** In the Policy Map table, select the SIP deep packet inspection policy map you want to set rules and actions for. The Rule table appears.
- Step 3** In the Rule table, click **Add** to add a new rule, or select the rule you want to modify, then click **Edit**. The Rule screen appears.
- Step 4** In the Rule Type field, configure rules using the information in [Table 11-29](#).

Table 11-29 Layer 7 SIP Deep Packet Inspection Policy Map Rules

Option	Description
Class Map	Specify a class map to use for this traffic policy: 1. To use the class-default class map, select the Use Class Default check box. The class-default class map is a reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified by the class-default class map. The class-default class map has an implicit match any statement that enables it to match all traffic. 2. To use a previously created class map: a. Clear the Use Class Default check box. b. In the Class Map Name field, select the class map to be used.

Table 11-29 Layer 7 SIP Deep Packet Inspection Policy Map Rules (continued)

Option	Description
Match Condition	Specify a match condition to use for this traffic policy: 1. In the Match Condition field, enter a name for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. 2. In the Match Condition Type field, select the type of match condition to use for this policy map and configure any type-specific options using the information in Table 4-10.
Insert Before	1. Indicate whether this rule is to precede another rule for this policy map. – N/A—This option is not configured. – False—This rule is not to precede another rule in this policy map. – True—This rule is to precede another rule in this policy map. 2. If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.

Step 5 Click:

- **Deploy Now** to deploy this configuration. The screen refreshes and the Action table appears. Continue with [Step 6](#).
- **Cancel** to exit this procedure without saving your entries and to return to the Rule table.
- **Next** to deploy your entries and to add another rule.

**Note**

If you selected the Insert Before option described in [Table 11-29](#) and specified True, perform the following steps to refresh the Rule tab before adding an action for this rule:

1. Click the Rule tab to refresh the Rule table.
2. In the Rule table, select the newly added rule.

When the screen refreshes, an empty action list appears.

Step 6 In the Action table, click **Add** to add an entry or select an existing entry to modify, then click **Edit**.

Step 7 In the Id field, accept the automatically incremented entry or assign a unique identifier for this action.

Step 8 In the Action Type field, select the action to be taken for this rule:

- **Drop**—The SIP traffic is to be dropped if it meets the specified match criteria.
- **Permit**—The SIP traffic is to be allowed if it meets the specified match criteria.
- **Reset**—The SIP traffic is to be denied if it meets the specified match criteria. A TCP reset message is sent to the client or server to close the connection.

Step 9 In the Action Log field, specify whether the action taken is to be logged.

Step 10 Click:

- **Deploy Now** to deploy this configuration on the ACE.
- **Cancel** to exit the procedure without saving your entries and to return to the Action table.

- **Next** to deploy your entries and to configure another action.

Related Topics

- [Configuring Traffic Policies, page 11-1](#)
- [Configuring Virtual Context Class Maps, page 11-6](#)
- [Configuring Virtual Context Policy Maps, page 11-30](#)
- [Configuring Rules and Actions for Policy Maps, page 11-33](#)

Setting Policy Map Rules and Actions for Layer 7 Skinny Deep Packet Inspection



Note

Skinny deep packet inspection policy maps are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.

Use this procedure to configure the rules and actions for a Skinny Client Control Protocol (SCCP) deep packet inspection policy map.

Assumptions

- A Skinny deep packet inspection policy map has been configured.
- A class map has been defined for a class map rule if you do not want to use the class-default class map.

Procedure

- Step 1** Select **Config > Virtual Contexts > context > Expert > Policy Map**. The Policy Map table appears.
- Step 2** In the Policy Map table, select the Skinny deep packet inspection policy map you want to set rules and actions for. The Rule table appears.
- Step 3** In the Rule table, click **Add** to add a new rule, or select the rule you want to modify, then click **Edit**. The Rule screen appears.
- Step 4** In the Rule Type field, confirm that Match Condition is selected.
- Step 5** In the Match Condition Name field, enter a name for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
- Step 6** In the Match Condition Type field, confirm that Message ID is selected.
- Step 7** In the Message ID Operator field, indicate whether the match criteria is for a single message identifier or for a range of message identifiers:
 - **Equal**—A single message identifier is used for this match condition.
In the Message ID Value field, enter the numerical identifier of a SCCP message. Valid entries are integers from 0 to 65535.
 - **Range**—A range of message identifiers is used for this match condition.
 - a. In the Message ID Low Range Value field, enter the lowest numerical identifier of a range of SCCP messages. Valid entries are integers from 0 to 65535.

b. In the Message ID High Range Value field, enter the highest numerical identifier of a range of SCCP messages. Valid entries are integers from 0 to 65535, and the value in this field must equal or be greater than the value in the Message ID Low Range Value field.

- Step 8** In the Insert Before field, indicate whether this rule is to precede another rule in this policy map:
- N/A—This option is not configured.
 - False—This rule is not to precede another rule in this policy map.
 - True—This rule is to precede another rule in this policy map.
- Step 9** If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.
- Step 10** Click:
- **Deploy Now** to deploy the configuration on the ACE. The screen refreshes and the Action table appears. To define the actions for this rule, continue with [Step 11](#).
 - **Cancel** to exit this procedure without saving your entries and to return to the Rule table.
 - **Next** to deploy your entries and to configure another rule.



Note If you selected the Insert Before option in [Step 8](#) and specified True, perform the following steps to refresh the Rule tab before adding an action for this rule:

1. Click the Rule tab to refresh the Rule table.
2. In the Rule table, select the newly added rule.

When the screen refreshes, an empty action list appears.

- Step 11** In Action table, click **Add** to add a new action, or select an existing action, then click **Edit** to modify it. The Action configuration screen appears.
- Step 12** In the ID field, accept the automatically incremented entry or assign a unique identifier for this action.
- Step 13** In the Action Type field, confirm that Reset is selected.
- Step 14** In the Action Log field, specify whether the action taken is to be logged.
- Step 15** Click:
- **Deploy Now** to deploy this configuration on the ACE.
 - **Cancel** to exit the procedure without saving your entries and to return to the Action table.
 - **Next** to deploy your entries and to configure another action.

Related Topics

- [Configuring Traffic Policies, page 11-1](#)
- [Configuring Virtual Context Class Maps, page 11-6](#)
- [Configuring Virtual Context Policy Maps, page 11-30](#)
- [Configuring Rules and Actions for Policy Maps, page 11-33](#)

Setting Policy Map Rules and Actions for RADIUS Server Load Balancing

**Note**

RADIUS server load balancing policy maps are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.

Use this procedure to configure the rules and actions for RADIUS traffic received by the ACE.

Assumptions

- A RADIUS server load balancing traffic policy map has been configured.
- A class map has been defined for a class map rule if you do not want to use the class-default class map.

Procedure

-
- Step 1** Select **Config > Virtual Contexts > context > Expert > Policy Map**. The Policy Map table appears.
- Step 2** In the Policy Map table, select the RADIUS server load balancing policy map you want to set rules and actions for. The Rule table appears.
- Step 3** In the Rule table, click **Add** to add a new rule, or select the rule you want to modify, then click **Edit**. The Rule screen appears.

Step 4 In the Rule Type field, configure rules using the information in [Table 11-30](#).

Table 11-30 RADIUS Server Load Balancing Policy Map Rules

Option	Description
Class Map	Specify a class map to use for this traffic policy: - To use the class-default class map, select the Use Class Default check box. The class-default class map is a reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified by the class-default class map. The class-default class map has an implicit match any statement that enables it to match all traffic. - To use a previously created class map: - Clear the Use Class Default check box. - In the Class Map Name field, select the class map to be used.
Match Condition	Specify a match condition to use for this traffic policy: - In the Match Condition Name field, enter a name for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. - In the Match Condition Type field, select the type of match condition to use for this policy map: - Calling Station ID—A unique identifier of the calling station is used to establish a match condition. In the RADIUS Calling Station ID field, enter the calling station identifier to match. Valid entries are strings containing 1 to 64 alphanumeric characters. See Table 11-35 for a list of the supported characters that you can use for matching string expressions. - Username—A username is used to establish a match condition. In the Username field, enter the name to match. Valid entries are strings containing 1 to 64 alphanumeric characters. See Table 11-35 for a list of the supported characters that you can use for matching string expressions.
Insert Before	- Indicate whether this rule is to precede another rule for this policy map. - N/A—This option is not configured. - False—This rule is not to precede another rule in this policy map. - True—This rule is to precede another rule in this policy map. - If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.

Step 5 Click:

- **Deploy Now** to deploy this configuration. The screen refreshes and the Action table appears. To enter actions for this rule, continue with [Step 6](#).
- **Cancel** to exit this procedure without saving your entries and to return to the Rule table.
- **Next** to deploy your entries and to configure another rule.

**Note**

If you selected the Insert Before option described in [Table 11-30](#) and specified True, perform the following steps to refresh the Rule tab before adding an action for this rule:

1. Click the Rule tab to refresh the Rule table.
2. In the Rule table, select the newly added rule.

When the screen refreshes, an empty action list appears.

-
- Step 6** In the Action table, click **Add** to add an entry or select an existing entry to modify, then click **Edit**.
- Step 7** In the Id field, accept the automatically incremented entry or assign a unique identifier for this action.
- Step 8** In the Action Type field, configure actions for this rule using the information in [Table 11-18](#).
- Step 9** Click:
- **Deploy Now** to deploy this configuration on the ACE.
 - **Cancel** to exit the procedure without saving your entries and to return to the Action table.
 - **Next** to deploy your entries and to configure another action.
-

Related Topics

- [Configuring Traffic Policies, page 11-1](#)
- [Configuring Virtual Context Class Maps, page 11-6](#)
- [Configuring Virtual Context Policy Maps, page 11-30](#)
- [Configuring Rules and Actions for Policy Maps, page 11-33](#)

Setting Policy Map Rules and Actions for RDP Server Load Balancing

**Note**

RDP server load balancing policy maps are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.

Use this procedure to configure the rules and actions for RDP traffic received by the ACE.

Assumptions

- An RDP server load balancing traffic policy map has been configured.
- A class map has been defined for a class map rule if you do not want to use the class-default class map.

Procedure

-
- Step 1** Select **Config > Virtual Contexts > context > Expert > Policy Map**. The Policy Map table appears.
- Step 2** In the Policy Map table, select the RDP server load balancing policy map you want to set rules and actions for. The Rule table appears.

Step 3 In the Rule table, click **Add** to add a new rule, or select the rule you want to modify, then click **Edit**. The Rule screen appears.

Step 4 In the Rule Type field, confirm that Class Map is selected.

Step 5 To use the class-default class map, select the Use Class Default check box.

The class-default class map is a reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified by the class-default class map. The class-default class map has an implicit **match any** statement that enables it to match all traffic.

Step 6 To use a previously created class map:

- a. Clear the Use Class Default check box.
- b. In the Class Map Name field, select the class map to be used.

Step 7 In the Insert Before field, indicate whether this rule is to precede another rule for this policy map.

- N/A—This option is not configured.
- False—This rule is not to precede another rule in this policy map.
- True—This rule is to precede another rule in this policy map.

If you select True in the Insert Before field, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.

Step 8 Click:

- **Deploy Now** to deploy this configuration. The screen refreshes and the Action table appears. To enter actions for this rule, continue with [Step 9](#).
- **Cancel** to exit this procedure without saving your entries and to return to the Rule table.
- **Next** to deploy your entries and to configure another rule.



Note If you selected the Insert Before option in [Step 7](#) and specified True, perform the following steps to refresh the Rule tab before adding an action for this rule:

1. Click the Rule tab to refresh the Rule table.
2. In the Rule table, select the newly added rule.

When the screen refreshes, an empty action list appears.

Step 9 In the Action table, click **Add** to add an entry or select an existing entry to modify, then click **Edit**.

Step 10 In the Id field, accept the automatically incremented entry or assign a unique identifier for this action.

Step 11 In the Action Type field, configure actions for this rule using the information in [Table 11-18](#).

Step 12 Click:

- **Deploy Now** to deploy this configuration on the ACE.
- **Cancel** to exit the procedure without saving your entries and to return to the Action table.
- **Next** to deploy your entries and to configure another action.

Related Topics

- [Configuring Traffic Policies, page 11-1](#)
- [Configuring Virtual Context Class Maps, page 11-6](#)
- [Configuring Virtual Context Policy Maps, page 11-30](#)
- [Configuring Rules and Actions for Policy Maps, page 11-33](#)

Setting Policy Map Rules and Actions for RTSP Server Load Balancing

**Note**

RTSP server load balancing policy maps are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.

Use this procedure to configure the rules and actions for RTSP traffic received by the ACE.

Assumptions

- An RTSP server load balancing traffic policy map has been configured.
- A class map has been defined for a class map rule if you do not want to use the class-default class map.

Procedure

- Step 1** Select **Config > Virtual Contexts > context > Expert > Policy Map**. The Policy Map table appears.
- Step 2** In the Policy Map table, select the RTSP server load balancing policy map you want to set rules and actions for. The Rule table appears.
- Step 3** In the Rule table, click **Add** to add a new rule, or select the rule you want to modify, then click **Edit**. The Rule screen appears.

Step 4 In the Rule Type field, configure rules using the information in [Table 11-31](#).

Table 11-31 RTSP Server Load Balancing Policy Map Rules

Option	Description
Class Map	Specify a class map to use for this traffic policy: - To use the class-default class map, select the Use Class Default check box. The class-default class map is a reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified by the class-default class map. The class-default class map has an implicit match any statement that enables it to match all traffic. - To use a previously created class map: - Clear the Use Class Default check box. - In the Class Map Name field, select the class map to be used.
Match Condition	Specify a match condition to use for this traffic policy: - In the Match Condition field, enter a name for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. - In the Match Condition Type field, select the type of match condition to use for this policy map and configure any type-specific options using the information in Table 11-32.
Insert Before	- Indicate whether this rule is to precede another rule for this policy map. - N/A—This option is not configured. - False—This rule is not to precede another rule in this policy map. - True—This rule is to precede another rule in this policy map. - If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.

Table 11-32 RTSP Policy Map Match Conditions

Match Condition	Description
Source Address	The source IP address is used for match criteria. 1. In the Source Address field, enter the source IP address for this match condition in dotted-decimal format, such as 192.168.11.1. 2. In the Source Netmask field, select the subnet mask for the source IP address.
RTSP Header	RTSP header information is used for matching criteria. 1. In the Header Name field, specify the header to match in one of the following ways: – To specify an RTSP header that is not one of the standard RTSP headers, select the first radio button, then enter the RTSP header name in the Header Name field. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters. – To specify a standard RTSP header, click the second radio button, then select an RTSP header from the list. 2. In the Header Value field, enter the header value expression string to compare against the value in the specified field in the RTSP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. If the string includes spaces, enclose the string with quotes. All headers in the header map must be matched. See Table 11-35 for a list of the supported characters that you can use in regular expressions.
RTSP URL	A URL or portion of a URL is used for match criteria. 1. In the URL Expr field, enter a URL, or portion of a URL, to match. The ACE performs matching on whatever URL string appears after the RTSP method, regardless of whether the URL includes the host name. The ACE supports regular expressions for matching URL strings. See Table 11-35 for a list of the supported characters that you can use in regular expressions. 2. In the Method Expr field, enter the RTSP method to match. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. The method can be either one of the standard RTSP method names (DESCRIBE, ANNOUNCE, GET_PARAMETER, OPTIONS, PAUSE, PLAY, RECORD, REDIRECT, SETUP, SET_PARAMETER, TEARDOWN) or a text string that must be matched exactly (for example, STINGRAY).

- Step 5** In the Insert Before field, indicate whether this rule is to precede another rule for this policy map.
- N/A—This option is not configured.
 - False—This rule is not to precede another rule in this policy map.
 - True—This rule is to precede another rule in this policy map.
- If you select True in the Insert Before field, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.

- Step 6** Click:
- **Deploy Now** to deploy this configuration. The screen refreshes and the Action table appears. Continue with [Step 7](#).
 - **Cancel** to exit this procedure without saving your entries and to return to the Rule table.
 - **Next** to deploy your entries and to add another rule.

**Note**

If you selected the Insert Before option in [Table 11-32](#) and specified True, perform the following steps to refresh the Rule tab before adding an action for this rule:

1. Click the Rule tab to refresh the Rule table.
2. In the Rule table, select the newly added rule.

When the screen refreshes, an empty action list appears.

- Step 7** In the Action table, click **Add** to add an entry or select an existing entry to modify, then click **Edit**.
- Step 8** In the Id field, accept the automatically incremented entry or assign a unique identifier for this action.
- Step 9** In the Action Type field, configure actions for this rule using the information in [Table 11-18](#).
- Step 10** Click:
- **Deploy Now** to deploy this configuration on the ACE.
 - **Cancel** to exit the procedure without saving your entries and to return to the Action table.
 - **Next** to deploy your entries and to configure another action.

Related Topics

- [Configuring Traffic Policies, page 11-1](#)
- [Configuring Virtual Context Class Maps, page 11-6](#)
- [Configuring Virtual Context Policy Maps, page 11-30](#)
- [Configuring Rules and Actions for Policy Maps, page 11-33](#)

Setting Policy Map Rules and Actions for SIP Server Load Balancing

**Note**

SIP server load balancing policy maps are available for ACE 2.0 modules and the ACE 4710 A3(1.0) release only.

Use this procedure to configure the rules and actions for SIP traffic received by the ACE.

Assumptions

- A SIP server load balancing traffic policy map has been configured.
- A class map has been defined for a class map rule if you do not want to use the class-default class map.

Procedure

- Step 1** Select **Config > Virtual Contexts > context > Expert > Policy Map**. The Policy Map table appears.
- Step 2** In the Policy Map table, select the SIP server load balancing policy map you want to set rules and actions for. The Rule table appears.

- Step 3** In the Rule table, click **Add** to add a new rule, or select the rule you want to modify, then click **Edit**. The Rule screen appears.
- Step 4** In the Rule Type field, configure rules using the information in [Table 11-33](#).

Table 11-33 SIP Server Load Balancing Policy Map Rules

Option	Description
Class Map	Specify a class map to use for this traffic policy: - To use the class-default class map, select the Use Class Default check box. The class-default class map is a reserved, well-known class map created by the ACE. You cannot delete or modify this class. All traffic that fails to meet the other matching criteria in the named class map belongs to the default traffic class. If none of the specified classifications matches the traffic, then the ACE performs the action specified by the class-default class map. The class-default class map has an implicit match any statement that enables it to match all traffic. - To use a previously created class map: - Clear the Use Class Default check box. - In the Class Map Name field, select the class map to be used.
Match Condition	Specify a match condition to use for this traffic policy: - In the Match Condition field, enter a name for this match condition. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters. - In the Match Condition Type field, select the type of match condition to use for this policy map and configure any type-specific options using the information in Table 11-34.
Insert Before	- Indicate whether this rule is to precede another rule for this policy map. - N/A—This option is not configured. - False—This rule is not to precede another rule in this policy map. - True—This rule is to precede another rule in this policy map. - If you select True, the Insert Before Policy Rule field appears. Select the rule that you want the current rule to precede.

Table 11-34 SIP Server Load Balancing Policy Map Match Conditions

Match Condition	Description
Source Address	The source IP address is used for match criteria. 1. In the Source Address field, enter the source IP address for this match condition in dotted-decimal format, such as 192.168.11.1. 2. In the Source Netmask field, select the subnet mask for the source IP address.
SIP Header	SIP header information is used for matching criteria. 1. In the Header Name field, specify the header to match in one of the following ways: – To specify a SIP header that is not one of the standard SIP headers, select the first radio button, then enter the SIP header name in the Header Name field. Valid entries are unquoted text strings with no spaces and a maximum of 64 characters. – To specify a standard SIP header, click the second radio button, then select an SIP header from the list. 2. In the Header Value field, enter the header value expression string to compare against the value in the specified field in the SIP header. Valid entries are text strings with a maximum of 255 alphanumeric characters. The ACE supports regular expressions for matching. If the string includes spaces, enclose the string with quotes. All headers in the header map must be matched. See Table 11-35 for a list of the supported characters that you can use in regular expressions.

Step 5 Click:

- **Deploy Now** to deploy this configuration. The screen refreshes and the Action table appears so you can enter actions for this rule. Continue with [Step 6](#).
- **Cancel** to exit this procedure without saving your entries and to return to the Rule table.
- **Next** to deploy your entries and to add another rule.

Step 6 In the Action table, click **Add** to add an entry or select an existing entry to modify, then click **Edit**.

Step 7 In the Id field, accept the automatically incremented entry or assign a unique identifier for this action.

Step 8 In the Action Type field, configure actions for this rule using the information in [Table 11-18](#).

Step 9 Click:

- **Deploy Now** to deploy this configuration on the ACE.
- **Cancel** to exit the procedure without saving your entries and to return to the Action table.

- **Next** to deploy your entries and to configure another action.



Note If you selected the Insert Before option in [Table 11-33](#) and specified True, perform the following steps to refresh the Rule tab before adding an action for this rule:

1. Click the Rule tab to refresh the Rule table.
2. In the Rule table, select the newly added rule.

When the screen refreshes, an empty action list appears.

Related Topics

- [Configuring Traffic Policies, page 11-1](#)
- [Configuring Virtual Context Class Maps, page 11-6](#)
- [Configuring Virtual Context Policy Maps, page 11-30](#)
- [Configuring Rules and Actions for Policy Maps, page 11-33](#)

Special Characters for Matching String Expressions

[Table 11-35](#) identifies the special characters that can be used in matching string expressions.

Table 11-35 *Special Characters for Matching String Expressions*

Convention	Description
.	One of any character.
.*	Zero or more of any character.
\.	Period (escaped).
\xhh	Non-printable character.
[charset]	Match any single character from the range.
[^charset]	Do not match any character in the range. All other characters represent themselves.
()	Expression grouping.
expr1 expr2	OR of expressions.
(expr)*	0 or more of expression.
(expr)+	1 or more of expression.
.\a	Alert (ASCII 7).
.\b	Backspace (ASCII 8).
.\f	Form-feed (ASCII 12).
.\n	New line (ASCII 10).
.\r	Carriage return (ASCII 13).
.\t	Tab (ASCII 9).

Table 11-35 *Special Characters for Matching String Expressions (continued)*

Convention	Description
.\\v	Vertical tab (ASCII 11).
.\\0	Null (ASCII 0).
.\\	Backslash.
.\\x##	Any ASCII character as specified in two-digit hexadecimal notation.

Related Topics

- [Configuring Traffic Policies, page 11-1](#)
- [Configuring Virtual Context Class Maps, page 11-6](#)
- [Configuring Virtual Context Policy Maps, page 11-30](#)
- [Configuring Rules and Actions for Policy Maps, page 11-33](#)



Draft - CISCO CONFIDENTIAL

CHAPTER 12

Configuring Application Acceleration and Optimization

Revised Date: 3/25/09

With application acceleration and optimization features on ACE appliances, you can configure application delivery and application acceleration options that increase productivity and efficiency. The application acceleration features optimize network performance and improve access to critical business information. This capability accelerates the performance of Web applications, including customer relationship management, portals, and online collaboration by up to 10 times.

This section includes:

- [Optimization Overview, page 12-1](#)
- [Optimization Traffic Policies and Typical Configuration Flow, page 12-2](#)
- [Configuring Action Lists for Application Acceleration and Optimization, page 12-3](#)
- [Configuring Optimization Parameter Maps, page 12-12](#)
- [Configuring Traffic Policies for HTTP Optimization, page 12-13](#)
- [Enabling HTTP Optimization Using Virtual Servers, page 12-16](#)
- [Configuring Global Application Acceleration and Optimization, page 12-16](#)

Optimization Overview

The application acceleration functions of the ACE appliance apply several optimization technologies to accelerate application performance. This functionality enables enterprises to optimize network performance and improve access to critical business information.

The ACE appliance provides the following application acceleration and optimization functionality:

- Delta optimization eliminates redundant traffic on the network by computing and transmitting only the changes that occur in a Web page between successive downloads of the same page or similar pages.
- FlashForward object acceleration technology eliminates network delays associated with embedded Web objects able to be cached, such as images, style sheets, and JavaScript files by placing the responsibility for validating object freshness on the ACE appliance, rather than on the client, making the client more efficient.
- Just-in-time object acceleration enables acceleration of non-cacheable embedded objects, resulting in improved application response time by eliminating the need for clients to download these objects on each request.

- Smart image optimization automatically reduces image file sizes while optimizing image quality, resulting in faster image download times, faster page renders, and more efficient bandwidth utilization.
- Smart redirect enables the ACE appliance to automatically and transparently convert HTML META tag-based redirections into more efficient HTTP header-based redirections in order to eliminate the need for unnecessary freshness validation requests.
- Adaptive dynamic caching accelerates enterprise application performance and improves server system scalability by enabling the ACE appliance itself to fulfill requests for dynamic content, which offloads application servers and databases.

Refer to [Configuring Application Acceleration and Optimization, page 12-1](#) or the *Cisco 4700 Series Application Control Engine Appliance Application Acceleration and Optimization Configuration Guide* for more information about application acceleration and optimization.

Related Topics

- [Optimization Traffic Policies and Typical Configuration Flow, page 12-2](#)
- [Configuring Traffic Policies for HTTP Optimization, page 12-13](#)
- [Configuring Global Application Acceleration and Optimization, page 12-16](#)

Optimization Traffic Policies and Typical Configuration Flow

To define the different optimization and application acceleration functions that you want the ACE appliance to perform, you must configure at least one each of the following:

- HTTP optimization action list—This action list specifies the actions that the ACE is to perform for application acceleration and optimization. You can configure action lists when configuring a virtual server, or as a separate procedure. See:
 - [Configuring Application Acceleration and Optimization, page 4-37](#)
 - [Configuring Action Lists for Application Acceleration and Optimization, page 12-3](#)
- Layer 7 server load-balancing class map—This class map identifies the Layer 7 server load-balancing match criteria to apply to incoming traffic, such as URL, HTTP cookie, HTTP header, or source IP address. See [Configuring Virtual Context Policy Maps, page 11-30](#)
- Layer 7 HTTP optimization policy map—This policy map applies the HTTP optimization action list and optionally an optimization parameter map to Layer 7 HTTP traffic. See [Configuring Virtual Context Policy Maps, page 11-30](#).
- Layer 3 and Layer 4 class map—By using match criteria, this class map identifies the network traffic that can pass through the ACE appliance. The match criteria includes the VIP address for the network traffic. The ACE appliance uses these Layer 3 and Layer 4 traffic classes to perform server load balancing. See [Configuring Virtual Context Policy Maps, page 11-30](#).
- Layer 3 and Layer 4 policy map—This policy map associates server load-balancing actions and HTTP optimization action lists with the VIP. See [Setting Policy Map Rules and Actions for Layer 3/Layer 4 Network Traffic, page 11-38](#) and [Configuring Traffic Policies for HTTP Optimization, page 12-13](#).
- Layer 7 server load-balancing policy map—This policy map specifies the server load-balancing actions that the ACE appliance is to perform. See [Configuring Virtual Context Policy Maps, page 11-30](#).

You can also configure:

- Optimization parameter maps—Optimization parameter maps allow you to configure specific options for action list items. You can configure optimization parameter maps when configuring a virtual server or as a separate procedure.

When you configure a parameter map with an action list for a class map, the ACE appliance validates the action list and parameter map configurations before deploying them.

See:

- [Configuring Application Acceleration and Optimization, page 4-37](#)
- [Configuring Optimization Parameter Maps, page 7-10.](#)
- Global application acceleration and optimization options—The acceleration and optimization options allow you to apply specific acceleration and optimization features for logging and debugging on a global level on the ACE appliance. See [Configuring Global Application Acceleration and Optimization, page 12-16.](#)

Related Topics

- [Configuring Traffic Policies for HTTP Optimization, page 12-13](#)
- [Optimization Overview, page 12-1](#)

Configuring Action Lists for Application Acceleration and Optimization

An action list groups a series of individual application acceleration and optimization functions that are applicable to a specific type of operation.

Action lists are available for ACE 2.0 modules and ACE appliances. For information on configuring action lists for these devices, see:

- [Configuring Action Lists for ACE 2.0 Modules and ACE 4710 A3\(1.0\) Appliances, page 12-3](#)
- [Configuring Action Lists for ACE Appliances, page 12-6](#)

Configuring Action Lists for ACE 2.0 Modules and ACE 4710 A3(1.0) Appliances

Use this procedure to configure an action list for ACE 2.0 module and ACE 4710 A3(1.0) application acceleration and optimization.

Procedure

-
Step 1	Select Config > Devices > <i>context</i> > Expert > HTTP Header Modify Action List . The Action List table appears.
Step 2	Click Add to add an action list, or select an existing action list, then click Edit to modify it. The HTTP Header Modify Action List configuration screen appears.
Step 3	In the Action List Name field, enter a unique name for the action list. Valid entries are unquoted text strings with a maximum of 64 alphanumeric characters.

Step 4 Click:

- **Deploy Now** to deploy the action list. If this is a new action list, the screen refreshes with additional tables. Continue with [Step 5](#)
- **Cancel** to exit this procedure without saving your entry and to return to the Action List table.
- **Next** to deploy your entries and to add another action list.

Step 5 Click the Header Action tab. The Header Action table appears.**Step 6** Click **Add** to add an entry, or select an existing entry, then click **Edit** to modify it.**Step 7** Configure the header action using the information in [Table 12-1](#).**Table 12-1** HTTP Header Modify Action List

Field	Option	Description
Header Name		Enter the name of an HTTP header. Valid entries are unquoted text strings with a maximum of 255 alphanumeric characters.
Operator	Insert	The ACE is to insert a header value in an HTTP client request, server response, or both. In the Header Value field, enter the value that you want to insert into the identified HTTP header. Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. You can also use the following dynamic replacement strings: • %is—Insert the source IP address in the HTTP header. • %id—Insert the destination IP address in the HTTP header. • %ps—Insert the source port in the HTTP header. • %pd—Insert the destination port in the HTTP header.
	Delete	The ACE is to delete the specified HTTP header from a client request, server response, or both.
	Rewrite	The ACE is to rewrite the specified HTTP header in client request packets, server response packets, or both. 1. In the Header Value field, enter the value of the HTTP header that you want to replace. Valid entries are text strings containing 1 to 255 alphanumeric characters. The ACE supports the use of regular expressions for matching data strings. Use parenthesized expressions for dynamic replacement using %1 and %2 in the replacement pattern. Note When matching data strings, note that the period (.) and question mark (?) characters do not have a literal meaning in regular expressions. Use brackets ([]) to match these symbols (for example, enter <code>www[.]xyz[.]com</code> instead of <code>www.xyz.com</code>). You can also use a backslash (\) to escape a dot (.) or a question mark (?). 2. In the Replace field, enter the pattern string that you want to substitute for the header value regular expression. For dynamic replacement of the first and second parenthesized expressions from the header value, use %1 and %2, respectively.

Table 12-1 HTTP Header Modify Action List (continued)

Field	Option	Description
Type	Request	The ACE performs the insertion, deletion, or rewrite on the HTTP request packets from clients.
	Response	The ACE performs the insertion, deletion, or rewrite on the HTTP response packets from servers.
	Both	The ACE performs the insertion, deletion, or rewrite on both the HTTP request packets and the response packets.

Step 8 Click:

- **Deploy Now** to deploy this configuration.
- **Cancel** to exit this procedure without saving your entry and to return to the Header Action table.
- **Next** to deploy your entries and to add another header action.

Step 9 Click the SSL Action tab. The SSL Action table appears.**Step 10** Click **Add** to add a new action, or select an existing entry, then click **Edit** to modify it. The SSL Action configuration screen appears.**Step 11** In the URL Expression field, enter the URL regular expression string that is to be matched in the Location header. If the URL in the Location header matches the string that you specify, the ACE rewrites the URL from http:// to https:// and rewrites the port number if configured.

Valid entries are unquoted text strings with no spaces and a maximum of 255 alphanumeric characters. You can enter a text string with spaces provided that you enclose the entire string in quotation marks ("). The ACE supports the use of regular expressions for matching data strings.

Step 12 In the Port field, enter the SSL port number from which the ACE translates a clear port number before sending the server redirect response to the client. Valid entries are integers from 1 to 65535. The default is 443.**Step 13** In the Clear Port field, enter the clear port number to which the ACE translates the SSL port number before sending a server redirect response to the client. Valid entries are integers from 1 to 65535. The default is 443.**Step 14** Click:

- **Deploy Now** to deploy this configuration.
- **Cancel** to exit this procedure without saving your entry and to return to the SSL Action table.
- **Next** to deploy your entries and to add another SSL action.

Related Topics

- [Configuring Action Lists for ACE Appliances, page 12-6](#)
- [Configuring Pattern Replacements, page 12-10](#)

Configuring Action Lists for ACE Appliances

Use this procedure to configure an action list for ACE appliance application acceleration and optimization.



Tip

You can also configure action lists when configuring a virtual server. For more information, see [Configuring Application Acceleration and Optimization, page 4-37](#).

Procedure

Step 1

Select the item to configure:

- To configure a virtual context, select **Config > Devices > context > Expert > Action List**. The Action List table appears.
- To configure a configuration building block, select **Config > Global > All Building Blocks > building_block > Expert > Action List**.



Note

The options in this procedure appear for ACE 4710-type configuration building blocks only.

Step 2

Click **Add** to add a new action list, or select an existing action list, then click **Edit** to modify it.

Step 3

Configure the action list using the information in [Table 12-2](#).

Table 12-2 Action List Configuration Options

Field	Description
Action List Name	Enter a unique name for the action list. Valid entries are unquoted text strings with a maximum of 64 alphanumeric characters.
Enable Delta	Delta optimization dynamically updates client browser caches directly with content differences, or deltas, resulting in faster page downloads. Select the check box to enable delta optimization for the specified URLs. Clear the check box to disable this feature.
Enable AppScope	AppScope runs on the Management Console of the optional Cisco AVS 3180A Management Station and measures end-to-end application performance. Select the check box to enable AppScope performance monitoring for use with the ACE appliance. Clear the check box to disable this feature.
Fast Redirect	The Fast Redirect feature specifies that the ACE appliance is to intercept 302 responses from the origin server and make a second request on behalf of the client for the redirect URL, fetch it, and send it to the client. This feature applies only to redirects within the same domain. Select the check box to enable the fast redirect feature. Clear the check box to disable this feature.

Table 12-2 **Action List Configuration Options (continued)**

Field	Description
FlashForward	The FlashForward feature reduces bandwidth usage and accelerates embedded object downloading by combining local object storage with dynamic renaming of embedded objects, thereby enforcing object freshness within the parent HTML page. Specify FlashForward implementation: • N/A—This option is not configured. • FlashForward—FlashForward is to be enabled for the specified URLs and that embedded objects are to be transformed. • FlashForward Object—FlashForward static caching is to be enabled for the objects that the corresponding URLs refer to, such as Cascading Style Sheets (CSS), JPEG, and GIF files.
FlashConnect	The FlashConnect feature reduces bandwidth usage and accelerates the downloading of objects that are embedded within HTML pages. FlashConnect dynamically renames embedded objects by adding a prefix and changing the hostname so that the objects appear to reside on different hosts. FlashConnect then has the browser open a separate connection to the origin server for each object and retrieve the objects in parallel instead of sequentially. Note If you enable this feature, you must configure DNS so that all requests for the rewritten object URLs are resolved back to the ACE appliance that rewrote them initially. Use the CLI to configure DNS on the ACE appliance. Specify FlashConnect implementation: • N/A—This option is not configured. • Flash Connect—FlashConnect is to be enabled for the specified URLs. • Flash Connect Object—FlashConnect is to be enabled for corresponding embedded object URLs.
Cache Dynamic	Select this check box to enable Adaptive Dynamic Caching for the specified URLs even if the expiration settings in the response indicate that the content is dynamic. The expiration of cache objects is controlled by the cache expiration settings based on time or server load. Clear this check box to disable this feature.
Cache Forward	Specify cache forwarding implementation: • N/A—This option is not configured. • With Wait—Cache forwarding is enabled with the wait option for the specified URL. If the object has expired but the maximum cache TTL time period has not yet expired, the ACE appliance sends a request to the origin server for the object. A user requesting this page continues to receive content from the cache during this time but must wait for the object to be updated before the request is satisfied. When the fresh object is returned, it is sent to the requesting user and the cache is updated. • Without Wait—Cache forwarding is enabled without the wait option.
Dynamic Etag	This feature enables the acceleration of noncacheable embedded objects, which results in improved application response time. When enabled, this feature eliminates the need for users to download noncacheable objects on each request. Select the check box to indicate that the ACE appliance is to implement just-in-time object acceleration for embedded objects not able to be cached. Clear the check box to disable this feature.

Table 12-2 **Action List Configuration Options (continued)**

Field	Description
Meta Refresh	The Meta Refresh feature enables the ACE appliance to automatically and transparently convert HTML META tag redirections into more efficient HTTP header-based redirections. When enabled, this feature eliminates the need for unnecessary requests to validate freshness and results in significantly faster page response time. Select the check box to enable the smart URL redirection. Clear the check box to disable this feature.
XSLT Merge	Select the check box to indicate that the ACE appliance is to apply XSL style sheet transformations to an XML source document and return the resulting HTML document to the requestor. The ACE appliance applies other optimizations after the XML is transformed, but before the result is returned to the requestor. Clear the check box to disable this feature.
Image Type	Image optimization controls how the ACE appliance compresses JPEG and PNG images. Image optimization is not applied to small images, such as thumbnails, or when optimization reduces the file size by less than 10 percent. Image optimization is not intended for images with many high-frequency components that do not compress well. Specify how the ACE appliance is to handle image optimization: • N/A—This option is not configured. • Standard—The ACE appliance is to perform standard image optimization and smooth the image, if needed, to reduce noise. • Advanced—The ACE appliance is to override standard settings and control individual optimization options.

Step 4 Click:

- **Deploy Now** to immediately deploy this configuration. The ACE appliance validates the action list configuration, and the URL Map table appears. To add URL mappings, continue with [Step 5](#).
- **OK** to save your entries. This option appears for configuration building blocks. To add URL mappings, continue with [Step 5](#).
- **Cancel** to exit this procedure without saving your entries and to return to the Action List table.
- **Next** to deploy your entries and to configure another action list.

Step 5 Click the URL Map tab. The URL Map table appears.**Step 6** Click **Add** to add a new URL mapping. The URL Map configuration screen appears.

Note You cannot modify an existing URL mapping. Instead, delete the existing mapping, then add a new one.

Step 7 Configure a URL mapping using the information in [Table 12-3](#).

Table 12-3 **URL Mapping Configuration Options**

Field	Description
URL Scope	Select the portion of the URL that is to be remapped: • All—URLs are to be altered, regardless of their locations. • Content—The content is to be altered, not just that which appears in URLs. • Cookie—The domain section of cookies are to be altered. • Header—URLs only within the Location response-header field are to be altered. • Html—URLs only within the URL attribute of META HTTP-EQUIV tags and within the SRC attribute of the HTML tags BASE, HREF, IMG, LINK, SCRIPT, and STYLE are to be altered.
Replacement Directive	Indicate how the URL is to be altered: • Host—The host portion of the URL that is specified in the Source field is to be replaced with the string specified in the Destination field. • Pattern—The portion of the input stream specified in the Source field is to be replaced with the string specified in the Destination field. • Port—The port of the URL that is specified in the Source field is to be replaced with the port specified in the Destination field. • Protocol—The URL protocol HTTP is to be replaced with HTTPS or that HTTPS is to be replaced with HTTP.
Source	Enter the string or value that is to be replaced: • For Host replacements, enter the host portion that is to be replaced. • For Pattern replacements, enter a regular expression that defines subexpressions within the input stream that are to be replaced. • For Port replacements, enter the port number that is to be replaced. • For Protocol replacement, enter HTTP or HTTPS as the protocol to be replaced.
Destination	Enter the string or value that is to replace the entry in the Source field: • For Host replacements, enter the new host string. Valid entries contain a maximum of 64 alphanumeric characters • For Pattern replacements, enter the pattern that is to replace the existing pattern. Valid entries contain a maximum of 64 alphanumeric characters. For more information on Pattern replacements, see Configuring Pattern Replacements, page 12-10. • For Port replacements, enter the port number that is to replace the existing port number. Valid entries are integers from 0 to 65535. • For Protocol replacements, enter HTTP or HTTPS as the protocol to replace the existing protocol.

Step 8 Click:

- **Deploy Now** to immediately deploy this configuration. This option appears for virtual contexts.
- **OK** to save your entries. This option appears for configuration building blocks.
- **Cancel** to exit this procedure without saving your entries and to return to the URL Map table.
- **Next** to deploy your entries and to add another URL mapping.

Related Topics

- [Optimization Traffic Policies and Typical Configuration Flow, page 12-2](#)
- [Configuring Optimization Parameter Maps, page 12-12](#)
- [Configuring Traffic Policies for HTTP Optimization, page 12-13](#)
- [Configuring Global Application Acceleration and Optimization, page 12-16](#)

Configuring Pattern Replacements

When configuring Pattern replacements, use regular expression syntax to define subexpressions within the input stream that are to be altered. Subexpressions are delimited using parentheses (). The numbering of the subexpressions begins with 1 and is the number of the left-parenthesis “(“ counting from the left.

For example, the following pattern defines three subexpressions in the input stream:

```
(.*) (fast) (.*)
```

The first subexpression is everything before the word “fast.” The second subexpression is the word “fast.” The third subexpression is everything after the word “fast.”

When configuring replacement directives in action lists (see [Configuring Action Lists for Application Acceleration and Optimization, page 12-3, Step 7](#)), the string identified in the Source field is replaced by the string specified in the Destination field. In the Destination field, you can use any of the parameter expander functions listed in [Table 12-4](#), or one or more `urlmap_pattern(number)` variables, which refer to specific subexpressions in the original input stream. For example, `$urlmap_pattern(0)` matches the entire input stream, `$urlmap_pattern(1)` matches the first subexpression, `$urlmap_pattern(2)` matches the second subexpression, and so on.

If the specified subexpression does not exist in the input stream, then the variable evaluates to the empty string.

**Note**

The parameter expander functions listed in [Table 12-4](#) apply only to the context of the HTTP request from the client, not to the data stream being sent as a response to the client. For example, the function `$http_query_string()` evaluates to the query string of the request URL.

[Table 12-4](#) lists the parameter expander functions that you can use.

Table 12-4 **Parameter Expander Functions**

Variable	Description
<code>\$(number)</code>	Expands to the corresponding matching subexpression (by <i>number</i>) in the URL pattern. Subexpressions are marked in a URL pattern using parentheses (). The numbering of the subexpressions begins with 1 and is the number of the left-parenthesis “(“ counting from the left. You can specify any positive integer for the number. <code>\$(0)</code> matches the entire URL. For example, if the URL pattern is <code>((http://server/.*)/(.*)/a.jsp)</code>, and the URL that matches it is <code>http://server/main/sub/a.jsp?category=shoes&session=99999</code>, then the following are correct: <code>\$(0)</code> = <code>http://server/main/sub/a.jsp</code> <code>\$(1)</code> = <code>http://server/main/sub/</code> <code>\$(2)</code> = <code>http://server/main</code> <code>\$(3)</code> = <code>sub</code> If the specified subexpression does not exist in the URL pattern, then the variable expands to the empty string.
<code>\$http_query_string()</code>	Expands to the value of the whole query string in the URL. For example, if the URL is <code>http://myhost/dotthis?param1=value1&param2=value2</code>, then the following is correct: <code>\$http_query_string()</code> = <code>param1=value1&param2=value2</code> This function applies to both GET and POST requests.
<code>\$http_query_param(query-param-name)</code> The obsolete syntax is also supported: <code>\$param(query-param-name)</code>	Expands to the value of the named query parameter (case-sensitive). For example, if the URL is <code>http://server/main/sub/a.jsp?category=shoes&session=99999</code>, then the following are correct: <code>\$http_query_param(category)</code> = <code>shoes</code> <code>\$http_query_param(session)</code> = <code>99999</code> If the specified parameter does not exist in the query, then the variable expands to the empty string. This function applies to both GET and POST requests.
<code>\$http_cookie(cookie-name)</code>	Evaluates to the value of the named cookie. For example, <code>\$http_cookie(cookiexyz)</code>. The cookie name is case-sensitive.
<code>\$http_header(request-header-name)</code>	Evaluates to the value of the specified HTTP request header. In the case of multivalued headers, it is the single representation as specified in the HTTP specification. For example, <code>\$http_header(user-agent)</code>. The HTTP header name is not case-sensitive.
<code>\$http_method()</code>	Evaluates to the HTTP method used for the request, such as GET or POST.

Table 12-4 Parameter Expander Functions (continued)

Variable	Description
Boolean Functions: \$http_query_param_present(<i>query-param-name</i>) \$http_query_param_notpresent(<i>query-param-name</i>) \$http_cookie_present(<i>cookie-name</i>) \$http_cookie_notpresent(<i>cookie-name</i>) \$http_header_present(<i>request-header-name</i>) \$http_header_notpresent(<i>request-header-name</i>) \$http_method_present(<i>method-name</i>) \$http_method_notpresent(<i>method-name</i>)	Evaluates to a Boolean value: True or False, depending on the presence or absence of the element in the request. The elements are a specific query parameter (<i>query-param-name</i>), a specific cookie (<i>cookie-name</i>), a specific request header (<i>request-header-name</i>), or a specific HTTP method (<i>method-name</i>). All identifiers are case-sensitive except for the HTTP request header name.
\$regex_match(<i>param1</i> , <i>param2</i>)	Evaluates to a Boolean value: True if the two parameters match and False if they do not match. The two parameters can be any two expressions, including regular expressions, that evaluate to two strings. For example, this function: <pre>\$regex_match(\$http_query_param(URL), .*Store\.asp.*)</pre> compares the query URL with the regular expression string <code>.*Store\.asp.*</code> . If the URL matches this regular expression, this function evaluates to True.

Configuring Optimization Parameter Maps

Use this procedure to configure an Optimization parameter map for use with a Layer 3/Layer 4 policy map.

Optimization parameter maps can be configured for ACE appliances and ACE 4710-type configuration building blocks only.



Tip

You can also configure optimization parameter maps when configuring a virtual server. For more information, see [Configuring Application Acceleration and Optimization, page 4-37](#).

Procedure

- Step 1** Select the item to configure:
- To configure a virtual context, select **Config > Devices > context > Load Balancing > Parameter Maps > Optimization Parameter Map**.
 - To configure a configuration building block, select **Config > Global > All Building Blocks > building_block > Load Balancing > Parameter Maps > Optimization Parameter Map**.
- The Optimization Parameter Map table appears.
- Step 2** Click **Add** to add a new parameter map, or select an existing parameter map, then click **Edit** to modify it. The Optimization Parameter Map configuration screen appears.

- Step 3** In the Parameter Name field, enter a unique name for this parameter map. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
- Step 4** Configure optimization using the information in [Table 7-6](#).
- Step 5** Click:
- **Deploy Now** to immediately deploy this configuration. The ACE validates the parameter map configuration and deploys it. This option appears for virtual contexts.
 - **OK** to save your entries. This option appears for configuration building blocks.
 - **Cancel** to exit this procedure without saving your entries and to return to the Parameter Map table.
 - **Next** to accept your entries and to add another parameter map.
-

Related Topics

- [Optimization Traffic Policies and Typical Configuration Flow](#), page 12-2
- [Configuring Action Lists for Application Acceleration and Optimization](#), page 12-3
- [Configuring Traffic Policies for HTTP Optimization](#), page 12-13
- [Configuring Global Application Acceleration and Optimization](#), page 12-16

Configuring Traffic Policies for HTTP Optimization

[Table 12-5](#) provides a high-level overview of the steps required to configure HTTP optimization on an ACE appliance.



Note

[Table 12-5](#) includes only the significant steps in each task. For detailed information on configuring these items, select the links provided, click **Help** in the ANM GUI, or refer to [Configuring Traffic Policies](#), page 11-1.

Assumption

A virtual IP address has been configured for the context in which you configure HTTP optimization.

Table 12-5 *Configuring Traffic Policies for HTTP Optimization*

	Task	Procedure
Step 1	Create a Layer 7 class map for server load balancing.	1. Select Config > Devices > context > Expert > Class Map. 2. Click Add to add a new class map. 3. In the Class Map Type field, select Layer 7 Server Load Balancing. 4. In the Match Type field, select the method the ACE appliance is to use to evaluate multiple match statements when multiple match conditions exist in the class map. 5. Click Deploy Now. 6. Configure match conditions for this class map. For more information, see: • Configuring Virtual Context Class Maps, page 11-6 • Setting Match Conditions for Layer 7 Server Load Balancing Class Maps, page 11-13
Step 2	Create an HTTP optimization action list to specify the optimization actions that are to be performed.	1. Select Config > Devices > context > Expert > Action List. 2. Click Add to add a new action list. 3. Configure the action list using the information in Table 12-2. 4. Click Deploy Now. 5. In the URL Map table, click Add to add a new URL mapping. 6. Configure a URL mapping using the information in Table 12-3. 7. Click Deploy Now. For more information, see Configuring Action Lists for Application Acceleration and Optimization, page 12-3.
Step 3	Create a Layer 7 HTTP optimization policy map and associate it with the server load-balancing class map in Step 1 and the action list configured in Step 2 .	1. Select Config > Devices > context > Expert > Policy Map. 2. Click Add to add a new policy map. 3. In the Type field, select Layer 7 HTTP Optimization. 4. Click Deploy Now. 5. In the Rules table, add the server load-balancing class map created in Step 1. 6. In the Action table, add the action list created in Step 2. For more information, see: • Configuring Virtual Context Policy Maps, page 11-30 • Setting Policy Map Rules and Actions for Layer 7 HTTP Optimization, page 11-53

Table 12-5 **Configuring Traffic Policies for HTTP Optimization (continued)**

Task	Procedure
Step 4 Create a Layer 3/Layer 4 class map for server load balancing.	1. Select Config > Devices > context > Expert > Class Map. 2. Click Add to add a new class map. 3. In the Class Map Type field, select Layer 3/4 Network Traffic. 4. In the Match Type field, select the method the ACE appliance is to use to evaluate multiple match statements when multiple match conditions exist in the class map. 5. Click Deploy Now. 6. Configure Virtual Address match conditions for this class map. For more information, see: • Configuring Virtual Context Class Maps, page 11-6 • Setting Match Conditions for Layer 3/Layer 4 Network Traffic Class Maps, page 11-9
Step 5 Create a Layer 7 policy map for server load balancing and associate it with the Layer 7 server load-balancing class map from Step 1 .	1. Select Config > Devices > context > Expert > Policy Map. 2. Click Add to add a new policy map. 3. In the Type field, select Layer 7 Server Load Balancing. 4. Click Deploy Now. 5. Associate the Layer 7 server load-balancing class map configured in Step 1 with this policy map by adding it to the Rule table. For more information, see: • Configuring Virtual Context Policy Maps, page 11-30 • Setting Policy Map Rules and Actions for Layer 7 Server Load-Balancing Traffic, page 11-56
Step 6 Create a Layer 3/Layer 4 network traffic policy map and associate it with the: • Layer 3/Layer 4 server load-balancing class map configured in Step 4 • Layer 7 server load-balancing policy map configured in Step 5 • HTTP optimization policy map configured in Step 3	1. Select Config > Devices > context > Expert > Policy Map. 2. Click Add to add a new policy map. 3. In the Type field, select Layer 3/4 Network Traffic. 4. Click Deploy Now. 5. In the Rule table, add the Layer 3/Layer 4 server load-balancing class map configured in Step 4. 6. In the Action table, add the: – Layer 7 server load-balancing policy map created in Step 5 – HTTP optimization policy map created in Step 3 For more information, see: • Configuring Virtual Context Policy Maps, page 11-30 • Setting Policy Map Rules and Actions for Layer 3/Layer 4 Network Traffic, page 11-38

Related Topics

- [Optimization Traffic Policies and Typical Configuration Flow, page 12-2](#)
- [Configuring Action Lists for Application Acceleration and Optimization, page 12-3](#)
- [Optimization Overview, page 12-1](#)

Enabling HTTP Optimization Using Virtual Servers

Use this procedure to configure HTTP optimization using virtual servers.

Procedure

-
- Step 1** Create a virtual server by following the instructions in [Configuring Virtual Servers, page 4-2](#).
- Step 2** Configure HTTP optimization by following the instructions in [Configuring Application Acceleration and Optimization, page 4-37](#).
-

Related Topics

- [Configuring Traffic Policies for HTTP Optimization, page 12-13](#)
- [Optimization Traffic Policies and Typical Configuration Flow, page 12-2](#)

Configuring Global Application Acceleration and Optimization

**Note**

This functionality is available for Admin contexts only and only on ACE appliances.

ANM allows you to configure global application acceleration and optimization options for logging and debugging as performed by the ACE appliance.

Procedure

-
- Step 1** Select **Config > Virtual Contexts > *admin_context* > System > Acceleration and Optimization**. The Application Acceleration and Optimization configuration screen appears.
- Step 2** In the Debug Level field, enter the maximum level of system log messages to be sent to the syslog server, using the values in [Table 3-4](#). The severity level that you specify indicates that you want syslog messages at that level and the more severe levels. For example, if you enter 3 for Error, syslog displays Error, Critical, Alert, and Emergency messages.
- Step 3** Check the AppScope Log check box to indicate that the ACE appliance is to upload optimization statistical log information to the optional AVS 3180A Management station. Clear the check box to indicate that the ACE appliance is not to upload this information.
- Step 4** Click **Deploy Now** to immediately deploy this configuration on the ACE appliance.
-

Related Topics

- [Optimization Overview, page 12-1](#)
- [Optimization Traffic Policies and Typical Configuration Flow, page 12-2](#)



CHAPTER 13

Using Configuration Building Blocks

Revised Date: 3/25/09



Note

In ANM 1.1, configuration building blocks were called *configuration templates*. The name has been changed in ANM 1.2 to more closely reflect the functionality that they provide and how they can be used.

Building blocks allow authorized users to create and design reusable configuration attributes which can then be applied to virtual contexts. The ANM also allows you to extract the configuration of an existing virtual context and tag it as a building block.

In many cases, the same configuration settings can be used in several virtual contexts (for example, it can offer the same service bundle to many customers). To avoid repeating virtual context configuration and testing each time you create a virtual context, you can create a building block of many configuration attributes that can be applied to virtual contexts as appropriate or as needed.

With building blocks, you can also create a variety of configurations that address customers' differing needs. The ability to customize configurations to customer needs also allows you to use network resources most efficiently.

Benefits of configuration building blocks include:

- You can establish baseline versions of working configurations.
- Users can make real-time changes to configurations and roll back to a previously working configuration, if needed.
- Building blocks can be extracted from proven, working configurations.
- Building blocks can be placed under version control, with tagged versions that cannot be modified.

[Table 13-1](#) lists the configuration options that are available for each building block type and provides links to related topics. For descriptive information about the menu options, see [Configuring Virtual Contexts, page 3-5](#).

Table 13-1 Building Block Configuration Options

Menu Option	Building Block Type				Related Topic
	ACE 1.0	ACE 2.0	ACE 4710 Running Image A1(8)	ACE 4710 Running Image A3(1.0)	
System					
Primary Attributes	X	X	X	X	Configuring Building Block Primary Attributes, page 13-7
Static Routes					
Syslog	X	X	X	X	Configuring Virtual Context Syslog Settings, page 3-12
SNMP	X	X	X	X	Configuring SNMP for Virtual Contexts, page 3-19
Global Policy	X	X	X	X	Configuring Virtual Context Global Traffic Policies, page 3-26
Licenses					
Application Acceleration and Optimization					
Resource Classes					
Load Balancing					
Virtual Servers					
Real Servers	X	X	X	X	Configuring Real Servers, page 5-4
Server Farms	X	X	X	X	Configuring Server Farms, page 5-12
Health Monitoring	X	X	X	X	Configuring Health Monitoring for Real Servers, page 5-25
Stickiness	X	X	X	X	Configuring Sticky Groups, page 6-7
HTTP Parameter Map	X	X	X	X	Configuring HTTP Parameter Maps, page 7-8
Connection Parameter Map	X	X	X	X	Configuring Connection Parameter Maps, page 7-2
Optimization Parameter Map			X	X	Configuring Optimization Parameter Maps, page 7-10
Generic Parameter Map		X			Configuring Generic Parameter Maps, page 7-7
RTSP Parameter Map		X			Configuring RTSP Parameter Maps, page 7-17
SIP Parameter Map		X			Configuring SIP Parameter Maps, page 7-18
Skinny Parameter Map		X			Configuring Skinny Parameter Maps, page 7-20
SSL					
Certificates					
Keys	X	X	X	X	Using SSL Keys, page 8-8
Parameter Map	X	X	X	X	Configuring SSL Parameter Maps, page 8-15

Table 13-1 Building Block Configuration Options (continued)

Menu Option	Building Block Type				Related Topic
	ACE 1.0	ACE 2.0	ACE 4710 Running Image A1(8)	ACE 4710 Running Image A3(1.0)	
Chain Group Parameters					
CSR Parameters	X	X	X	X	Configuring SSL CSR Parameters, page 8-19
Proxy Service					
Auth Group Parameters		X		X	Configuring SSL Authentication Groups, page 8-24
Certificate Revocation List		X		X	Configuring CRLs for Client Authentication, page 8-25
Security					
ACLs	X	X	X	X	Creating ACLs, page 3-44
Object Groups		X		X	Configuring Object Groups, page 3-52
Network					
Port Channel					
Gigabit Ethernet Interfaces					
VLAN Interfaces	X	X	X	X	Configuring VLAN Interfaces, page 9-2
BVI Interfaces	X	X	X	X	Configuring Virtual Context BVI Interfaces, page 9-12
Static Routes	X	X	X	X	Configuring Virtual Context Static Routes, page 9-14
Global IP DHCP	X	X	X	X	Configuring Global IP DHCP, page 9-16
Static NAT Overwrite		X			Configuring Static VLANs for Over 8 K Static NAT Configurations, page 9-16
High Availability					
Setup					
HA Tracking and Failure Detection					
Interfaces					
Hosts					
HSRP Groups					
Role-Based Access Control					
Users	X	X	X	X	Configuring Device RBAC Users, page 2-40
Roles	X	X	X	X	Configuring Device RBAC Roles, page 2-43
Domains	X	X	X	X	Configuring Device RBAC Domains, page 2-48
Expert					
Class Map	X	X	X	X	Configuring Virtual Context Class Maps, page 11-6
Policy Map	X	X	X	X	Configuring Virtual Context Policy Maps, page 11-30

Table 13-1 Building Block Configuration Options (continued)

Menu Option	Building Block Type				Related Topic
	ACE 1.0	ACE 2.0	ACE 4710 Running Image A1(8)	ACE 4710 Running Image A3(1.0)	
Action List		X	X	X	Configuring Action Lists for Application Acceleration and Optimization, page 12-3
Building Block Audit					

Related Topics

- [Building Block Versions and Tagging, page 13-4](#)
- [Creating Building Blocks, page 13-5](#)
- [Extracting Building Blocks from Virtual Contexts, page 13-5](#)
- [Applying Building Blocks, page 13-8](#)
- [Tagging Building Blocks, page 13-7](#)
- [Viewing Building Block Use, page 13-9](#)

Building Block Versions and Tagging

The ANM maintains version history for the building blocks that you create, design, and tag. You can tag a working building block version at any point during design or configuration, and reuse any tagged version of a building block.

A building block is not available for deployment until it has been *tagged*. When you tag a building block, the ANM publishes it with a version tag, such as 1.0 or 1.1.

You cannot edit tagged versions of a building block. After a building block is tagged, it is “frozen” and can no longer be modified in any way. When you open a tagged building block for editing, the ANM does not modify the tagged version, but instead creates a new working copy of the building block for you to work in. Any changes you make to the working copy are not available for deployment until you tag the building block under a new version tag.

Related Topics

- [Using Configuration Building Blocks, page 13-1](#)
- [Creating Building Blocks, page 13-5](#)
- [Extracting Building Blocks from Virtual Contexts, page 13-5](#)
- [Applying Building Blocks, page 13-8](#)
- [Tagging Building Blocks, page 13-7](#)
- [Viewing Building Block Use, page 13-9](#)

Creating Building Blocks

Use this procedure to create a building block without using an existing configuration.

To create a building block from an existing virtual context, see [Extracting Building Blocks from Virtual Contexts, page 13-5](#).

Procedure

-
- Step 1** Select **Config > Global > All Building Blocks**. The All Building Blocks table appears.
- Step 2** Click **Add**. The New Building Block screen appears.
- Step 3** In the Name field, enter a unique name for this building block.
- Step 4** In the Type field, select the type of building block to create:
- ACE 1.0—For use with virtual contexts on ACE 1.0 modules.
 - ACE 2.0—For use with virtual contexts on ACE 2.0 modules.
 - ACE 4710—For use with virtual contexts on ACE appliances.
- See [Table 13-1](#) for a list of the available configuration options for each building block type.
- Step 5** In the Description field, enter a brief description for this building block.
- Step 6** Click:
- **Save** to save your entries and to continue with building block configuration. The Primary Attributes configuration screen appears.
 - **Cancel** to exit this procedure without saving your entries and to return to the All Building Blocks table.
 - **Tag** to save your entries and tag the building block. After you tag a building block, the screen refreshes and provides fields for applying the building block. For more information, see [Applying Building Blocks, page 13-8](#).
-

Related Topics

- [Using Configuration Building Blocks, page 13-1](#)
- [Extracting Building Blocks from Virtual Contexts, page 13-5](#)
- [Building Block Versions and Tagging, page 13-4](#)
- [Applying Building Blocks, page 13-8](#)
- [Tagging Building Blocks, page 13-7](#)
- [Viewing Building Block Use, page 13-9](#)

Extracting Building Blocks from Virtual Contexts

An alternative to creating a new configuration building block and configuring each attribute individually is to extract a configuration building block from an existing virtual context. By extracting a building block from a virtual context, you can reduce the time you spend configuring and testing the configuration.

Use this procedure to create a working building block from a virtual context configuration.

Procedure

-
- Step 1** Select **Config > Devices**. The device tree appears.
- Step 2** Select the ACE with the virtual context whose configuration you want to use as a building block. The Virtual Contexts table appears.
- Step 3** Select the context with the configuration you want to extract, then click **Extract Building Block**. A window appears, asking for a building block name.
- Step 4** In the Name field, enter a name for this building block, then click **OK**. The screen refreshes with the Primary Attributes screen for the newly created building block (**Config > Global > *building_block***).
- Step 5** Modify the building block as desired using the information in [Table 13-1](#), or tag and deploy it as described in [Tagging Building Blocks, page 13-7](#) and [Applying Building Blocks, page 13-8](#).
-

Related Topics

- [Applying Building Blocks, page 13-8](#)
- [Tagging Building Blocks, page 13-7](#)
- [Viewing Building Block Use, page 13-9](#)

Configuring Building Blocks

Use this procedure to modify a working version of a configuration building block.



Note

You can modify only working versions of building blocks; you cannot modify tagged versions of building blocks. If you select a tagged building block version, and then select a configuration option (such as **Load Balancing > Health Monitoring**), you can view the entries for that tagged version, but you cannot modify them.

Procedure

-
- Step 1** Select **Config > Global > All Building Blocks**. The All Building Blocks table appears.
- Step 2** Select the working version of the building block that you want to modify, then select the attributes you want to configure. For information on building block configuration options, see [Table 13-1](#).



Note

While it is possible to configure VLAN and BVI interfaces in a building block, we recommend that you do not do so. Applying a building block with these attributes configured to a virtual context with different settings can disrupt network traffic.

- Step 3** To apply this building block, tag it, then deploy it as described in [Tagging Building Blocks, page 13-7](#) and [Applying Building Blocks, page 13-8](#).
-

Related Topics

- [Using Configuration Building Blocks, page 13-1](#)

- [Building Block Versions and Tagging, page 13-4](#)
- [Creating Building Blocks, page 13-5](#)
- [Extracting Building Blocks from Virtual Contexts, page 13-5](#)
- [Tagging Building Blocks, page 13-7](#)
- [Viewing Building Block Use, page 13-9](#)

Configuring Building Block Primary Attributes

Use this procedure to change the description of a configuration building block.

Procedure

-
Step 1	Select Config > Global > All Building Blocks . The All Building Blocks table appears.
Step 2	Select the building block that you want to modify, then select System > Primary Attributes . The Primary Attributes screen appears.
Step 3	In the Description field, modify the description as desired.
Step 4	Click: • Save to save your entries. The screen refreshes with the saved information. • Tag to tag the building block. To deploy the tagged building block, see Applying Building Blocks, page 13-8.
-

Related Topics

- [Creating Building Blocks, page 13-5](#)
- [Configuring Building Blocks, page 13-6](#)
- [Tagging Building Blocks, page 13-7](#)

Tagging Building Blocks

After creating a building block, you must tag it before you can apply it to virtual contexts.

Use this procedure to tag a working copy of a building block.

Procedure

-
Step 1	Select Config > Global > All Building Blocks . The All Building Blocks table appears.
Step 2	Select the working copy of the building block that you want to tag, then click Tag . The All Building Blocks table refreshes with the newly tagged building block identified by its version, such as 1.2 or 1.3. A working copy of the building block remains available so that you can use it for future building block versions.

To apply the tagged building block to virtual contexts on your network, see [Applying Building Blocks, page 13-8](#).

Related Topics

- [Using Configuration Building Blocks, page 13-1](#)
- [Building Block Versions and Tagging, page 13-4](#)
- [Creating Building Blocks, page 13-5](#)
- [Applying Building Blocks, page 13-8](#)
- [Extracting Building Blocks from Virtual Contexts, page 13-5](#)
- [Viewing Building Block Use, page 13-9](#)

Applying Building Blocks

You can apply building blocks in two ways:

- By selecting a virtual context, then applying the building block. See [Applying a Building Block to a Single Virtual Context, page 13-8](#).
- By selecting the tagged building block, then applying it to one or more virtual contexts. See [Applying a Building Block to Multiple Virtual Contexts, page 13-9](#).

Applying a Building Block to a Single Virtual Context

Use this procedure to apply a tagged building block to a virtual context using virtual context configuration screens.



Note

Before applying a building block to a virtual context, confirm that the VLAN and BVI interfaces are defined correctly for the virtual context. If needed, remove VLAN and BVI interface configuration information from the building block and then apply it.

Procedure

- Step 1** Select **Config > Devices > All Devices**. The device tree appears.
- Step 2** Select the virtual context you want to apply a building block to, then select **System > Primary Attributes**. The Primary Attributes screen appears.
- Step 3** In the Tagged Building Block to Apply field, select the building block you want to apply to the virtual context.
- Step 4** Click **Deploy Now**.

Related Topics

- [Applying a Building Block to Multiple Virtual Contexts, page 13-9](#)
- [Using Configuration Building Blocks, page 13-1](#)

- [Building Block Versions and Tagging, page 13-4](#)
- [Extracting Building Blocks from Virtual Contexts, page 13-5](#)
- [Tagging Building Blocks, page 13-7](#)

Applying a Building Block to Multiple Virtual Contexts

Use this procedure to apply a tagged building block to one or more contexts by using the building block configuration screens.



Note

Before applying a building block to a virtual context, confirm that the VLAN and BVI interfaces are defined correctly for the virtual context. If needed, remove VLAN and BVI interface configuration information from the building block and then apply it.

Procedure

- Step 1** Select **Config > Global > All Building Blocks**. The All Building Blocks table appears.
- Step 2** Select the tagged building block that you want to apply to one or more virtual contexts.
- Step 3** Select **System > Primary Attributes**. The Primary Attributes configuration screen appears.
- Step 4** In the Push Building Block to VCs field, select the contexts that you want to apply the building block to in the Available Items list, then click **Add**. They appear in the Selected Items list.

To remove contexts that you do not want to apply the building block to, select them in the Selected Items list, then click **Remove**. They items appear in the Available Items list.
- Step 5** Click **Save**. A progress bar reports status and the screen refreshes when the operation is complete.

Related Topics

- [Applying a Building Block to a Single Virtual Context, page 13-8](#)
- [Using Configuration Building Blocks, page 13-1](#)
- [Building Block Versions and Tagging, page 13-4](#)
- [Creating Building Blocks, page 13-5](#)

Viewing Building Block Use

Use this procedure to identify the virtual contexts using a building block.

Procedure

- Step 1** Select **Config > Devices**. The device tree appears.
- Step 2** Select **All VC**. The Virtual Contexts table appears.

Step 3 View the building blocks being used by one of the following methods:

- For a small number of contexts, scan the Building Block column to see which building blocks are in use on virtual contexts.
 - For a large number of contexts, click **Filter**. The screen refreshes so that you can enter search criteria. In the field beneath the Building Block column heading, enter a building block name or search string, then click **Go**. The table refreshes with entries that match the search criteria.
-

Related Topics

- [Using Configuration Building Blocks, page 13-1](#)
- [Building Block Versions and Tagging, page 13-4](#)
- [Creating Building Blocks, page 13-5](#)
- [Extracting Building Blocks from Virtual Contexts, page 13-5](#)
- [Tagging Building Blocks, page 13-7](#)



CHAPTER 14

Monitoring Your Network

Revised Date: 3/25/09

The ANM Monitor function allows you to monitor key areas of system usage. The following functionality is provided under Monitor:

- **Devices**—Provides statistics about devices including resource usage, traffic information, load balancing, and allows you to enable or disable polling. See [Device Monitoring Features, page 14-2](#).



Note ANM does not support monitoring on chassis.

- **Events**—Lists events originated from devices through syslog, SNMP traps. See [Monitoring Events, page 14-21](#).
- **Device Audit Trail Logging**—Lists device configuration and deployment changes to device, and associated descriptions for viewing and troubleshooting. See [Device Audit Trail Logging, page 14-23](#).
- **Alarm Notifications**—Allows you to define thresholds and view alarms. See [Configuring Alarm Notifications, page 14-25](#).
- **Settings**—Allows you to set global polling and SMTP configurations. See [Setting Polling Parameters, page 14-19](#).
- **Tools**—Allows you to verify connectivity (using the ping command) between a virtual context and an IP address that you specify. See [Testing Connectivity, page 14-33](#).

Before using the Monitoring functions, make sure your devices are properly configured for polling (see [Setting Up Devices for Monitoring, page 14-2](#)).

Setting Up Devices for Monitoring

In order for ANM to successfully monitor your devices, you must configure the devices correctly for polling as show in [Table 14-1](#).

Table 14-1 *Configuring Devices for Monitoring*

Device Type	How to Configure	Parameters to Configure
ACE 1.0 modules	Configure parameters on each virtual context you want ANM to monitor.	- All devices must have a routable IP address from the ANM. - The management policy with the SNMP protocol must be associated to the IP address. - You must enable SNMPv2c with a matching SNMP community string between ANM and the devices to be polled. (See Configuring Virtual Contexts, page 3-1.) - Before using the Monitoring functions, you must enable monitoring on all devices that you want ANM to monitor (see Setting Polling Parameters, page 14-19).
ACE 2.0 modules	Configure parameters on the Admin context only.	
ACE appliances running images A1(8) and A3(1.0)	Configure parameters on each virtual context you want ANM to monitor.	
CSS	Configure parameters on the CSS devices you want ANM to monitor. You cannot use ANM to configure the devices.	- All devices must have a routable IP address from the ANM. - For CSS devices, you must enable SNMPv2c with a matching SNMP community string between ANM and the devices to be polled. (See Configuring CSS Primary Attributes, page 2-24.) - For CSM devices, you must enable SNMPv2c with a matching SNMP community string on the Cat6K chassis in which the CSM resides. (See Configuring CSM Primary Attributes, page 2-23.) - Before using the Monitoring functions, you must enable monitoring on all devices that you want ANM to monitor (see Setting Polling Parameters, page 14-19).
CSM	Configure parameters on the CSM devices you want ANM to monitor. You cannot use ANM to configure the devices.	

Related Topics

- [Device Monitoring Features, page 14-2](#)
- [Monitoring Device Groups, page 14-3](#)
- [Monitoring Devices, page 14-4](#)

Device Monitoring Features

ANM provides several features that allow you to monitor your devices:

- System View—Provides device information and a general overview of your system as a whole, including High Availability (HA) information and licensing information. See [Monitoring the System, page 14-5](#).

- **Resource Usage**—Provides resource usage information on connections and features. See [Monitoring Resource Usage, page 14-5](#). This feature is not available for CSS or CSM devices.
- **Traffic Summary**—Provides traffic information for your devices. See [Monitoring Traffic, page 14-9](#).
- **Load Balancing**—Provides virtual server information and load balancing statistics. See [Monitoring Load Balancing on Virtual Servers, page 14-12](#) and [Monitoring Load Balancing Statistics, page 14-15](#).
- **Application Acceleration**—Displays optimization statistics for ACE appliances on which you have configured application acceleration functions. See [Monitoring Application Acceleration, page 14-17](#). This feature is only available on ACE appliances.
- **Polling Settings**—Allows you to set polling parameters. See [Setting Polling Parameters, page 14-19](#).

Related Topic

- [Monitoring Device Groups, page 14-3](#)

Monitoring Device Groups

You can display monitoring information for device groups that you create in ANM (see [Configuring User-Defined Groups, page 2-54](#)). When you select **Monitor > Devices > Groups > *device_group***, all monitoring features that are supported on any of the devices in the device group are displayed. Because some monitoring features, for example, Application Acceleration, are not supported on all device types, you can click the following buttons at the bottom of the Monitor screens to change what information is displayed:

- **Show Polled Devices**—By default, only the devices in the device group that support the specified feature are displayed.
- **Show All Devices**—All devices in the device group are shown on the Monitoring results screen, whether or not the feature you selected is supported on all the devices.

For example, if you create a device group that contains an ACE appliance and several other different device types, then select **Monitor > Devices > Groups > *device_group* > Application Acceleration**, by default, only the ACE appliance appears in the Application Acceleration screen because the other device types in the device group do not support this feature. If you click **Show Polled Devices**, all devices in the device group are displayed.

When viewing monitoring information, you might see *N/A* or an empty cell in the monitoring results:

- *N/A* indicates that ACE Device Manager was not able to obtain the specified value. In addition, the monitoring screen displays *N/A* in certain fields for which polling has not been executed.
- An empty cell indicates that the value is not applicable.

Related Topics

- [Setting Up Devices for Monitoring, page 14-2](#)
- [Device Monitoring Features, page 14-2](#)
- [Monitoring Devices, page 14-4](#)

Monitoring Devices

ANM monitors activities on ACE, CSS, and CSM devices. When you select **Monitor > Devices**, you can view device information. Using SNMP and CLI commands, ANM gathers information about your devices and displays the information.



Note

ACE devices provide no direct statistics via SNMP MIBs in order to monitor the state of virtual servers. While there are ACE CLIs called by the ANM to give some visibility, these currently cannot be parsed for effective batch monitoring.



Note

If you get a warning message indicating that monitoring is not enabled or functioning, you must enable statistic monitoring on the device. See [Setting Polling Parameters, page 14-19](#).

[Table 14-2](#) lists the features that appear under **Monitor > Devices**, depending on which device type you select in the device tree.

Table 14-2 Supported Monitor > Devices Features According to Device Type

Device Type Selected in the Device Tree		Supported Features Displayed Under Monitor > Devices					
		System View	Resource Usage ¹	Traffic Summary	Load Balancing	Application Acceleration	Polling Settings
ACE module		X	X	X	X		
	Admin context	X	X	X	X		X
	User context		X	X	X		X
ACE appliance		X	X	X	X	X	
	Admin context	X	X	X	X	X	X
	User context		X	X	X	X	X
CSS		X		X	X ²		X
CSM		X			X		X
GSS							X
Groups ³		X	X	X	X	X	

1. See [Monitoring Resource Usage, page 14-5](#) for information about the options available under Resource Usage.
2. CSS devices support Virtual Servers only, so you do not see the **Load Balancing > Statistics** menu option.
3. By default, all monitoring features that are supported on any of the devices in the device group appear when you select a device group. See [Monitoring Device Groups, page 14-3](#) for more information about monitoring various device types within a device group.

Related Topics

- [Monitoring Device Groups, page 14-3](#)
- [Monitoring the System, page 14-5](#)
- [Setting Up Devices for Monitoring, page 14-2](#)
- [Setting Polling Parameters, page 14-19](#)

Monitoring the System

ANM provides a System View that displays device information and a general overview of your system as a whole. If a module has crashed, you can use the System View to find out when and why the crash occurred and display information that affects the module. The System View also displays High Availability (HA) information and licensing information.


Note

For ACEs, the System View is available in the Admin context only.


Note

ANM does not support monitoring of chassis.

Procedure

Step 1 Select **Monitor > Devices > device > System View**. The information that is displayed depends on what device type you select in the device tree.

Step 2 The System View displays the following information:

- Device Information
- High Availability
- License Status
- Module Information (for CSS devices only)


Note

You can sort the information displayed in the table by clicking on a column heading.

Step 3 Click **Poll Now** to have ANM poll the devices and display the current values.

Step 4 Click **OK** when asked if you want to poll the devices for data now.

Related Topics

- [Setting Up Devices for Monitoring, page 14-2](#)
- [Setting Polling Parameters, page 14-19](#)
- [Monitoring Traffic, page 14-9](#)

Monitoring Resource Usage

ANM provides resource usage so that you can easily determine if you need to reallocate resources to a particular virtual context, view traffic usage in your contexts, or determine available usage for your contexts. There are two modes in which ANM provides resource usage for ACEs:

- Virtual-context based resource usage—You must select a virtual context from the device tree to view resource usage specific to the context (see [Monitoring Virtual Context Resource Usage, page 14-6](#)).
- System-wide resource usage—You must select an ACE module or appliance from the device tree to view system-wide information and to display the following options:

- Connections—Displays traffic resource usage information. See [Monitoring System Traffic Resource Usage, page 14-7](#).
- Features—Displays non-connection based resource usage information. See [Monitoring System Non-Connection Based Resource Usage, page 14-8](#).

See the “Configuring Virtualization” chapter of the *Application Control Engine Module Virtualization Configuration Guide* for the maximum resource usage value for each attribute.

Monitoring Virtual Context Resource Usage

ANM displays resource usage for virtual contexts as explained in the following steps.

See the “Configuring Virtualization” chapter of the *Application Control Engine Module Virtualization Configuration Guide* for the maximum resource usage value for each attribute.

Procedure

- Step 1** Select **Monitor > Devices > virtual_context > Resource Usage**. The information in [Table 14-3](#) is displayed.

Table 14-3 Virtual Context Resource Usage Field Descriptions

Field	Description
ACL Memory (Bytes)	ACL memory usage
Bandwidth (Bytes/Sec)	Bandwidth in bytes per second
Concurrent Connections (Connections)	Number of simultaneous connections
Connection Rate (Connections/Sec)	Connections per second
Inspect Connection Rate (Connections/Sec)	RTSP/FTP inspection connections per second
Application Acceleration Connections (conn)	Note This field displays if you selected an ACE appliance in the device tree.
MAC Miss Rate (Connections/Sec)	MAC miss traffic punted to CP packets per second
Management Connection Rate (Connection)	Number of management connections
Management Traffic Rate (Connections/Sec)	Management traffic bytes per second
Proxy Connection Rate (Connections)	Proxy connections
Regular Expression Memory (Bytes)	Regular expressions usage in bytes
SSL Connection Rate (Transactions/Sec)	SSL (Secure Sockets Layer) connections per second
Syslog Buffer Size (Bytes)	Syslog message buffer size in bytes
Throughput	Displays through-the-ACE traffic. This is a derived value (you cannot configure it directly) and it is equal to the bandwidth rate minus the mgmt-traffic rate for the 1-Gbps and 2-Gbps licenses.
Translation Entries	Current number of network and port address translations

- Step 2** Click **Poll Now** to have ANM poll the devices and display the current values.

- Step 3** Click **OK** when asked if you want to poll the devices for data now.

Related Topics

- [Monitoring System Traffic Resource Usage, page 14-7](#)
- [Monitoring System Traffic Resource Usage, page 14-7](#)

Monitoring System Traffic Resource Usage

ANM displays system-wide traffic resource usage as explained in the following steps. See the “Configuring Virtualization” chapter of the *Application Control Engine Module Virtualization Configuration Guide* for the maximum resource usage value for each attribute.

**Note**

You must select an ACE module or appliance from the device tree to view system-wide traffic resource usage information as shown in the following steps.

Procedure

Step 1 Select **Monitor > Devices > ACE > Resource Usage > Connections**.

The current resource usage information is displayed as shown in [Table 14-4](#).

**Note**

There might be a slight delay because the resource usage information is gathered real-time.

Table 14-4 *Resource Usage Connections Field Descriptions*

Field	Description
Context	Name of the virtual context
Conc. Conn.	Number of simultaneous connections
Mgmt. Conn.	Number of management connections
Proxy Conn.	Proxy connections
Application Acceleration Connections (conn)	Note This field displays if you selected an ACE appliance in the device tree.
Bandwidth (bytes/s)	Bandwidth in bytes per second
Throughput (bytes/s)	Note This field displays if you selected an ACE 2.0 device in the device tree. Throughput in bytes per second
Conn. Rate (conn./s)	Connections per second
SSL Conn. Rate (trans./s)	SSL (Secure Sockets Layer) connections per second
Mgmt. Traffic Rate (conn./s)	Management traffic connections per second
MAC Miss Rate (conn./s)	MAC miss traffic punted to CP packets per second
Insp. Conn. Rate (conn./s)	RTSP/FTP inspection connections per second

Step 2 Click **Poll Now** to have ANM poll the devices and display the current values.

Step 3 Click **OK** when asked if you want to poll the devices for data now.

Related Topics

- [Monitoring Resource Usage, page 14-5](#)
- [Monitoring System Non-Connection Based Resource Usage, page 14-8](#)

Monitoring System Non-Connection Based Resource Usage

ANM displays system-wide, non-connection-based resource usage as explained in the following steps.



Note

You must select an ACE module or appliance from the device tree to view the non-connection based resource usage information as shown in the following steps.

Step 1 Select **Monitor > Devices > ACE > Resource Usage > Features**.

The current resource usage information is displayed shown in [Table 14-5](#).



Note

There might be a slight delay because the resource usage information is gathered real-time.

Table 14-5 *Resource Usage Features Field Descriptions*

Field	Description
Context	Name of the virtual context
Translation Entries	Current number of network and port address translations
ACL Memory (bytes)	ACL memory usage in bytes
RegEx Memory (bytes)	Regular expressions memory usage in bytes
Syslog Buffer Size (bytes)	Syslog message buffer size in bytes
Syslog Message Rate (messages/s)	Syslog messages per second

Step 2 Click **Poll Now** to have ANM poll the devices and display the current values.

Step 3 Click **OK** when asked if you want to poll the devices for data now.

Related Topics

- [Monitoring Resource Usage, page 14-5](#)
- [Monitoring System Traffic Resource Usage, page 14-7](#)

Monitoring Traffic

ANM determines traffic information for your ACE and CSS devices by calculating the delta traffic values since the last polling cycle and displays the resulting values. You can view traffic summary information as shown in the steps below.


Note

To get traffic data polled directly from a device, click on an interface name that is displayed in the Interface column. See [Viewing Device-Specific Traffic Data, page 14-11](#).

Procedure

- Step 1** Select **Monitor > Devices > device > Traffic Summary**. The information shown in [Table 14-6](#) is displayed.


Note

You can click on any column heading to sort the table by that column.

Table 14-6 Traffic Summary Fields

Field	Description
Device	Fully-qualified device name. This field does not appear for CSS devices.
Interface	Name of the interface. Click on the interface hyperlink to get traffic data polled directly from the device as shown in Table 14-7 .
Admin Status	User-specified status of the device, which can be • Up • Down • Testing, which indicates that no operational packets can be passed.
Operational Status	Current operational status of the device, which can be • Up • Down • Testing, which indicates that no operational packets can be passed • Unknown • Dormant, which indicates the interface is waiting for external actions (such as a serial line waiting for an incoming connection) • Not present, which indicates the interface has missing components
Packets In / Sec	This field appears for ACEs only. Per second, the number of packets delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer.
Packets Out / Sec	This field appears for ACEs only. Per second, the total number of packets that higher-level protocol requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.

Table 14-6 **Traffic Summary Fields (continued)**

Field	Description
Bytes In / Sec	Number of octets received, including framing characters, per second.
Bytes Out / Sec	Number of octets per second transmitted out of the interface, including framing characters.
Errors In / Sec	Number of inbound packets discarded per second because they contained errors or because of an unknown or unsupported protocol
Errors Out / Sec	Number of outbound packets discarded per second because they contained errors or because of an unknown or unsupported protocol

- Step 2** Click **Poll Now** to have ANM poll the devices and display the current values.
- Step 3** Click **OK** when asked if you want to poll the devices for data now.
- Step 4** Select a device, then click **Details** to see specific traffic information for the selected device. See [Viewing Device-Specific Traffic Data, page 14-11](#)

Related Topic

[Viewing Device-Specific Traffic Data, page 14-11](#)

Viewing Device-Specific Traffic Data

Procedure

- Step 1** Select **Monitor > Devices > device > Traffic Summary**.
- Step 2** Select a device, then click Details. The information shown in [Table 14-7](#) is displayed.



Note You can click on a column heading to sort the table by that column.

Table 14-7 Traffic Summary Details Window Description

Device Type	Field	Description
ACEs and CSS	Bytes In	Total number of octets received on the interface, including framing characters
	Bytes Out	Total number of octets transmitted out of the interface, including framing characters
	Discarded Inbound Packets	Number of inbound packets which were discarded even though no errors were detected to prevent their being delivered to a higher-layer protocol
	Discarded Outbound Packets	Number of outbound packets which were discarded even though no errors were detected to prevent their being transmitted
	Inbound Packet Errors	Total number of inbound packet errors
	Inbound Packets with Unknown Protocol	Total number of packets received via the interface which were discarded because of an unknown or unsupported protocol
	Outbound Packet Errors	Total number of outbound packet errors
	Packets In	Number of packets delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer.
	Packets Out	Number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.
CSS only	Active TCP	Current number of active TCP flows on the interface
	Active UDP	Current number of active UDP flows on the interface
	FCB Count	Number of unused fastpath flow control blocks for the interface
	TCP Average	Five second moving average of TCP flows per second on the interface
	TCP Current	Number of new TCP flows within last second on the interface
	TCP High	Maximum number of TCP flows in any one second interval on the interface
	TCP Total	Total TCP flows on the interface
	UDP Average	Five second moving average of UCP flows per second on the interface
	UDP Current	Number of new UDP flows within last second on the interface
	UDP High	Maximum number of UDP flows in any one second interval on the interface
	UDP Total	Total UDP flows on the interface

- Step 3** Click **OK** to close the window and return to the Traffic Summary screen.

Related Topic

[Monitoring Traffic, page 14-9](#)

Monitoring Load Balancing on Virtual Servers

ANM monitors load balancing and allows you to view the information as shown in the following steps.

You can view additional information about real servers, such as the number of servers that are functioning properly, and probes, such as viewing if an excessing number of probes are failing, by clicking the hyperlink in the respective columns in [Table 14-8](#).

- Step 1** Select **Monitor > Devices > *device* > Load Balancing > Virtual Servers**. Depending on the device type you selected in the device tree, the information described in [Table 14-8](#) is displayed.

**Note**

If you select a CSS device from the device tree, the navigation path does not include Load Balancing; the path is **Monitor > Devices > *CSS_device* > Virtual Servers**.

Table 14-8 Load Balancing Monitoring Information

Device Type	Field	Description
All	Device	Fully-qualified device name
	Virtual Server	Name of the virtual server Note If a virtual server is associated with primary and backup server farms, two entries appear in the table: One for the primary server farm and one for the backup server farm.
	IP Address	IP address of the virtual server
	Protocol	Protocol the virtual server supports, which can be: - Any—Indicates the virtual server is to accept connections using any IP protocol. - TCP—Indicates that the virtual server is to accept connections that use TCP. - UDP—Indicates that the virtual server is to accept connections that use UDP.
	Port	Port to be used for the specified protocol
ACEs, CSS, CSM	Service Policy	Policy map applied to the device
	Serverfarm	Name of the server farm associated with the virtual server.

Table 14-8 Load Balancing Monitoring Information

Device Type	Field	Description
ACEs only	Algorithm	Type of predictor algorithm specified on the load balancer, which can be: • Roundrobin • Leastconn • Hash_url • Hash_addres • Hash_cookie • Hash_header
ACEs, CSS	Admin Status	User-specified status of the virtual server, which can be: • In Service—Indicates the server is in service. • Out of Service—Indicates the server is out of service.
All	# Rservers Up	Number of servers up/Number of total servers configured Note You can click on the hyperlink in this column to view statistics for the real servers configured for the specified virtual server. See Viewing Real Server Statistics, page 14-13 .
ACEs, CSSs, CSM	# Probes Failed	Number of probes failed/Number of probes configured Note You can click on the number displayed to view the statistics for the probes configured for the specified virtual server. See Viewing Probes Statistics, page 14-15 .
ACE 4710 running image A3(1.0) only	Operational Status	Whether appliance is activated or suspended.
	Current Connections	Current number of connections.
CSM	No. of Connections	Current number of connections
CSM	Total Connections	Total number of connections

Step 2 Click on a virtual server, then click **Poll Now** to have ANM poll the devices and display the current values.

Step 3 Click **OK** when asked if you want to poll the devices for data now.

Related Topics

- [Viewing Real Server Statistics, page 14-13](#)
- [Viewing Probes Statistics, page 14-15](#)

Viewing Real Server Statistics

Step 1 Select **Monitor > Devices > device > Load Balancing > Virtual Servers**. The Statistic Viewer displays information about the virtual servers.

- Step 2** In the # Rservers Up column, click on the number displayed. The Real Servers window displays the information shown in table [Table 14-9](#).

Table 14-9 Real Server Statistics Details

Device Type	Field	Description
All	Real Server	Name of the real server.
	IP Address	IP address of the real server. This field appears only for real servers specified as hosts.
	Port	Port number used for the server port address translation (PAT).
	Total Connections	Number of total connections, including current, failed, and dropped connections.
ACE 4710 Running Image A3(1.0)	Current Connections	Number of current connections to this server. If this field indicates <i>N/A</i> , the database does not have any information about current connections. If this field is 0, the database received an SNMP response of 0.
	Current Connections Rate	Current connections per second.
	Dropped Connections	Number of dropped connections.
	Dropped Connections Rate	Dropped connections per second.
	Weight	Weight assigned to the real server.
	Admin Status	The specified state of the server, which can be: • In Service—Indicates the server is in service. • Out of Service—Indicates the server is out of service. • In Service Standby—Indicates the server is a backup server and remains inactive unless the primary server fails. If the primary server fails, the backup server becomes active and starts accepting connections.
	Operational Status	The state of the server, which can be: • In Service—Indicates the server is in service. • Out of Service—Indicates the server is out of service. • In Service Standby—Indicates the server is a backup server and remains inactive unless the primary server fails. If the primary server fails, the backup server becomes active and starts accepting connections.

- Step 3** Click **Poll Now** to have ANM poll the devices and display the current values.

- Step 4** Click **OK** when asked if you want to poll the devices for data now.

Related Topics

- [Monitoring Load Balancing on Virtual Servers, page 14-12](#)
- [Viewing Probes Statistics, page 14-15](#)

Viewing Probes Statistics

To check the health and availability of a real server, the ACE periodically sends a probe to the real server. If you notice an excessive number of probes failing, you can view the monitoring information as shown in the following steps.

Procedure

- Step 1** Select **Monitor > Devices > ACE > Load Balancing > Virtual Servers**. The Statistic Viewer displays information about the virtual servers.
- Step 2** In the # Probes Failed column, click on the number displayed. The Monitoring Probe Details window displays the information shown in table [Table 14-10](#).

Table 14-10 *Monitoring Probe Details Window*

Field	Description
Name	Name of the probe
Type	Type of probe. For a complete list of probe types and their descriptions, see Table 5-9 .
IP Address	IP address the probe is polling
State	State of the probe, which can active or inactive
Passed	Number of passed probes
Passed Rate	Rate of passed probes
Failed	Number of failed probes
Failed Rate	Rate of failed probes

- Step 3** Click **Poll Now** to have ANM poll the devices and display the current values.
- Step 4** Click **OK** when asked if you want to poll the devices for data now.

Related Topics

- [Monitoring Load Balancing on Virtual Servers, page 14-12](#)
- [Monitoring Load Balancing Statistics, page 14-15](#)

Monitoring Load Balancing Statistics

You can monitor load balancing on your ACE and CSM devices as shown in the following procedure.

Procedure

- Step 1** Select **Monitor > Devices > device > Load Balancing > Statistics**. The Statistic Viewer displays the information described in [Table 14-11](#).

Table 14-11 Load Balancing Statistic Viewer Information

Device Type	Field	Description
All	Device	Name of the device
CSM only	Current Connections	Number of current connections
ACEs only	L4 Policy Conn.	Number of Layer 4 policy connections
	L7 Policy Conn.	Number of Layer 7 policy connections
All	Failed Conn.	Number of failed connections
	Dropped L4 Policy Conn.	Number of dropped Layer 4 policy connections
	Dropped L7 Policy Conn.	Number of dropped Layer 7 policy connections
	Rejected Conn. Due To No Policy Match	Number of connections rejected because they did not match policies
	Rejected Conn. Due To ACL deny	Number of connections rejected due to ACL parameters
	Rejected Conn. Due To L7 Config Changes	Number of rejected connections due to Layer 7 configuration changes
ACEs only	Conn. Timed Out	Number of connections that timed out
CSM only	Created Conn.	Number of created connections
	Established Conn.	Number of established connections
	Destroyed Conn.	Number of destroyed connections
	Server Initiated Conn.	Number of server initiated connections
	Failed Server Initiated Conn.	Number of failed server initiated connections
	Bad SSL Format Rejects	Number of connections rejected due to bad SSL form
	No Active Server Rejects	Number of connections rejected because there was no active server
	MaxParseLen Rejects	Number of connections rejected because they exceeded the maximum parse length.
	L7 ParserError Rejects	Number of connections rejected because of Layer 7 errors
	OutOfMemory Rejects	Number of connections rejected because of memory

Table 14-11 Load Balancing Statistic Viewer Information (continued)

Device Type	Field	Description
CSM only	Created Connections	Number of TCP and UDP connections created since SLB was configured
	Established Connections	Number of connections established through SLB (reached the ESTAB state)
	Destroyed Connections	Number of TCP and UDP connections destroyed by SLB, either by TCP/IP teardown or timeout. UDP connections can only be timed out
	Server Initiated Connections	Total number of connections initiated by the servers
	Failed Server Initiated Connections	Number of server initiated connections that failed
	Bad SSL Format Rejects	Number of connections rejected because some invalid or unrecognized SSL format was detected
	No Active Server Rejects	Number of connections rejected because the chosen server farm did not have any active servers
	MaxParseLen Rejects	Number of connections rejected because the length of an HTTP request or response header exceeded the maximum L7 parse length configured for the matching virtual server
	L7 Parser Error Rejects	number of connections rejected because an error occurred while parsing the connection data at Layer 7
	Out of Memory Rejects	number of connections rejected because the SLB module could not allocate the required memory

Step 2 Click **Poll Now** to have ANM poll the devices and display the current values.

Step 3 Click **OK** when asked if you want to poll the devices for data now.

Related Topic

[Testing Connectivity, page 14-33](#)

Monitoring Application Acceleration

If you have configured application acceleration functions on the ACE, you can monitor the optimization statistics as shown in the following steps.

Step 1 Select **Monitor > Devices > device > Application Acceleration**. The Application Accelerator information is displayed as shown in [Table 14-12](#).



Note

For connection-based syslogs, the following additional parameters are displayed: Source IP, Source Port, Destination IP, Destination Port, and Protocol Information. This allows you to sort and filter on these fields if desired.

Table 14-12 **Application Acceleration Monitoring View**

Field	Statistic	Description
Condenser Information	Total HTTP unoptimized requests received	Total number of end-user HTTP request the condenser has received that cannot be optimized
	Accumulated bytes received	Accumulated size (in bytes) of each end-user requested object
	Total responses in bytes	Accumulated size (in bytes) of responses, both for condensable and non-condensable end-user HTTP requests
	Total abandons of delta optimization	Total number of abandons of delta optimization requests
Cacheable Objects Statistics	Total objects served from cache	Total number of cacheable objects served from the cache, excluding the not-modified replies
	Accumulated bytes served	Accumulated size (in bytes) of the cacheable objects served from the cache, excluding not-modified replies
	Total objects not found in cache	Total number of cacheable objects not found in the cache
	Accumulated bytes not found	Accumulated size (in bytes) of the cacheable objects not found in the cache
	Total IMS requests for valid cache	Total number of IMS requests for valid copies of objects in the cache
	Total missed IMS Requests	Total number of IMS request for objects that either do not exist or are stale in the cache
	Total non-cacheable object requests	Total number of non-cacheable object requests
	Total requests with non modified responses	Total number of requests for stale objects that have the response from the origin server as not modified
Flash Forward Objects Statistics	Successful transformations	Total number of successful transformations for FlashForward objects
	Unsuccessful transformations	Total number of unsuccessful transformations for FlashForward objects
	Total HTTP requests	Total number of HTTP requests (excluding the IMS requests) for the transformed FlashForward objects
	Total IMS requests	Total number of IMS requests for transformed FlashForward objects

Step 2 Click **Poll Now** to have ANM poll the devices and display the current values.

Step 3 Click **OK** when asked if you want to poll the devices for data now.

Related Topic

[Configuring Application Acceleration and Optimization, page 12-1](#)

Setting Polling Parameters

You set polling parameters differently depending on the device type:

- ACE devices—You set polling on specific virtual contexts or configure global polling.
- CSM devices—You specify a single polling setting used by ANM.
- CSS devices—You specify a single polling setting used by ANM.
- GSS devices—You specify a single polling setting used by ANM for VIP Answers operation and configuration states and DNS Rules configuration states.

When you select **Monitoring**, the monitoring data for your devices is extracted from cache. The Monitoring screen refreshes every two minutes as new monitoring data is gathered.

When you import a context or device into ANM, the polling interval is set to 5 minutes by default. You can modify the polling parameter on each device (see [Enabling Polling on Specific Devices, page 14-19](#)) or you can modify the global parameter polling setting to change the polling parameters for all devices (see [Enabling Polling on All Devices, page 14-20](#)).

Related Topics

- [Enabling Polling on All Devices, page 14-20](#)
- [Enabling Polling on Specific Devices, page 14-19](#)

Enabling Polling on Specific Devices

Procedure

-
Step 1	Select Monitor > Devices > <i>context</i> > Polling Settings .
Step 2	In the Polling Stats field, click Enable .
Step 3	From the Background Polling Interval field, select a polling interval.
Step 4	Click Deploy Now to save and apply the polling parameters.
-

Related Topics

- [Enabling Polling on All Devices, page 14-20](#)
- [Disabling Polling on Specific Devices, page 14-19](#)

Disabling Polling on Specific Devices

Procedure

-
Step 1	Select Monitor > Devices > <i>context</i> > Polling Settings .
Step 2	In the Polling Stats field, click Disable .

Step 3 Click **Deploy Now** to disable polling.

Related Topics

- [Enabling Polling on Specific Devices, page 14-19](#)
- [Enabling Polling on All Devices, page 14-20](#)

Enabling Polling on All Devices

You can enable polling and set the polling interval for all devices as shown in the following steps.



Note

Currently this feature is available for any user under the ANM Inventory role task. When a user is assigned this task, global polling configuration changes made will apply to all devices, irrespective of the domains that are assigned for this user.

Procedure

- Step 1** Select **Monitor > Settings > Global Polling Configuration**.
- Step 2** In the Polling Stats field, click **Enable**.
- Step 3** From the Background Polling Interval field, select a polling interval.
- Step 4** Click **OK** to save and apply the polling parameters.
-

Related Topics

- [Enabling Polling on Specific Devices, page 14-19](#)
- [Disabling Polling on All Devices, page 14-20](#)

Disabling Polling on All Devices

You can disable polling all devices as shown in the following steps.

Procedure

- Step 1** Select **Monitor > Settings > Global Polling Configuration**.
- Step 2** In the Polling Stats field, click **Disable**.
- Step 3** Click **OK**. Polling is disabled.
-

Related Topics

- [Enabling Polling on All Devices, page 14-20](#)
- [Enabling Polling on Specific Devices, page 14-19](#)

Monitoring Events

The events captured in the Events table include both ACE syslog events and SNMP trap events. A procedure for viewing both types of events and details of information extracted from the syslog are shown below. Fields providing traffic-oriented sorting capability, specifically the information signified by the column heads in the Events Fields screen, shown in [Table 14-13](#) (Source IP, Source Port, Destination IP, Destination Port, and Protocol) are only available for the ACE syslogs.

**Note**

To receive events from devices, the devices must have syslog and SNMP traps configured correctly. See [Configuring Virtual Context Syslog Settings, page 3-12](#) and [Configuring SNMP for Virtual Contexts, page 3-19](#).

Procedure**Step 1**

Select **Monitor > Events**. ANM displays all events received from ACE for Syslog and SNMP traps for all virtual contexts. See [Table 14-13](#) for a description of the displayed information, which is extracted from the syslog.

You can sort information in the table by clicking on a column heading. This allows you to group events and help troubleshooting traffic information.

Table 14-13 **Monitor > Events Fields**

Field	Description
Source ID	Displays the Source ID.
Syslog ID	Displays the Syslog ID. If the event is a trap, this field is empty.
Severity	Indicates the syslog severity level as described in Table 3-4 .
Origination Time	Date and time that the event was last changed in the database.
Source IP	Displays the source name that is reporting the event, for example, <code><chassis/slot>:virtual_context</code> .
Source Port	Displays the source port.
Destination IP	Displays the IP address of the destination if available.
Destination Port	Displays the destination port if available.
Protocol	Protocol used in the syslog.
Detail	Provides additional detail about the event.

Table 14-14 displays the complete list of published ACE syslogs where source and destination IP, ports and protocols are parsed so that the designated table fields populate.

**Note**

Only the ACE syslog messages shown in this table will populate the Events screen fields explained in Table 14-13. Syslogs and traps not in this table will populate fields with a 0.

Table 14-14 ACE Syslogs Fields with Parseable Traffic Oriented Sorting Information

Syslog	Message Contents
ACE-1-106021	<i>Deny protocol reverse path check from source_address to dest_address on interface interface_name</i>
ACE-4-106023	<i>Deny protocol number name src incoming-interface:src-ip dst outgoing-interface:dst-ip by access-group "acl-name" (hash 1, hash 2)</i>
ACE-6-302022	<i>Built TCP connection id for interface:real-address/real-port (mapped-address/mapped-port) to interface:real-address/real-port (mapped-address/mapped-port)</i>
ACE-6-302023	<i>Teardown TCP connection id for interface:real-address/real-port to interface:real-address/real-port duration hh:mm:ss bytes bytes [reason]</i>
ACE-6-302024	<i>Built UDP connection id for interface:real-address/real-port (mapped-address/mapped-port) to interface:real-address/real-port (mapped-address/mapped-port)</i>
ACE-6-302025	<i>Teardown UDP connection id for interface:real-address/real-port to interface:real-address/real-port duration hh:mm:ss bytes bytes</i>
ACE-6-302026	<i>Built ICMP connection for faddr/NATed_ID gaddr/icmp_type laddr/icmpID</i>
ACE-6-302027	<i>Teardown ICMP connection for faddr/NATed ID gaddr/icmp_type laddr/icmpID</i>
ACE-6-302028	<i>Built TCP connection id for interface: real-address/real-port (mapped-address/mapped-port) to interface: real-address/real-port (mapped-address/mapped-port)</i>
ACE-6-302029	<i>Teardown TCP connection id for interface: real-address/real-port to interface: real-address/real-port duration hh:mm:ss bytes bytes [reason]</i>
ACE-6-302030	<i>Built UDP connection id for interface: real-address/real-port (mapped-address/mapped-port) to interface: real-address/real-port (mapped-address/mapped-port)</i>
ACE-6-302031	<i>Teardown UDP connection id for interface: real-address/real-port to interface: real-address/real-port duration hh:mm:ss bytes bytes</i>
ACE-4-313004	<i>Denied ICMP type=icmp_type, from source_address on interface interface_name to dest_address:no matching session</i>
ACE-4-410001	<i>Dropped UDP DNS packet_type from source_interface:source_address/source_port to dest_interface:dest_address/dest_port; error_length_type length bytes exceeds max_length_type limit of maximum_length bytes.</i>

Related Topics

- [Device Audit Trail Logging, page 14-23](#)
- [Monitoring Devices, page 14-4](#)

Device Audit Trail Logging

Certain configuration and deployment changes will be logged in the ANM database, and available for viewing according to your role restricted by device VC as established by RBAC. Log files are located `/var/lib/anm/events/date/audit`, where *date* is in YYYYMMDD format (for example, 20081109 for November 9, 2008).

The following changes will be logged in ANM:

- configuration deployments to devices
- device or VC sync operations
- device or VC import and deletions
- creation/updates/deletion of the to-be-deployed later by the virtual server

Procedure

-
- Step 1** Select **Config > device(s) to view > Device Audit**. ANM displays all operations described above on the specified devices. See [Table 14-15](#) for a description of the displayed information, some of which is extracted from the syslog.

You can sort information in the table by clicking on a column heading, adjust the viewable time range using the pulldown menu, and export the table for reporting and troubleshooting purposes.

Table 14-15 **Config > Device Audit Fields**

Field	Description
Time	ANM server timestamp when the action is complete.
Client IP	Source IP address initiating action.
User	Email address in the following format: <i>username@organization name</i> for example, <i>admin@cisco.com</i> .
Device	Device or VC target of user action.
Action	The action name of the operation, including the following: • add staging object • allocate vlan • change credential • create • create vc • create vc-template • create-vip • delete • delete-vip • deploy staging object • disable polling • enable polling • export-certificate-key • generate-csr • import device • import-certificate-key • import module • remove device • remove vc • restart monitoring • syncup config • syslog-setup • unmanage module • update • update staging object • update-vip
Target	Name of the target configuration object (for example, Serverfarm sf1).

Table 14-15 Config > Device Audit Fields

Field	Description
Status	Indicates whether operation succeeded or not.
Detail	CLI commands sent to the device and/or error messages. ¹

1. If the detail column contains more than approximately 4KB of CLI commands, the data will appear truncated, and not display properly.

Related Topics

- [Configuring Audit Log Settings, page 15-63](#)
- [Monitoring Devices, page 14-4](#)
- [Monitoring Events, page 14-21](#)
- [Viewing Change Audit Logs, page 15-64](#)

Configuring Alarm Notifications

To set up Monitoring alarm notifications, you define a threshold group and specify the statistics to be monitored by ANM for the threshold group. When the value for a specific statistic rises above the setting you specify, an alarm is issued to alert you.

**Note**

CISCO-EPM-NOTIFICATION-MIB is used for ANM alarms notification.

You can specify how you are notified when thresholds are crossed:

- Alarm notification, which you view at **Monitor > Alarm Notifications > Alarm**
- E-mail notification
- Traps

**Note**

Threshold crossing is detected via periodic polling. If a threshold is crossed *between* polling cycles, it is possible that ANM might not issue an alert if the condition recovers before the next polling cycle.

**Note**

ANM performs certificate expiration computations every 24 hours. The computation begins each time ANM is started. Every subsequent computation occurs 24 hours thereafter.

Assumption

For e-mail notification, you have configured SMTP. See [Configuring SMTP for E-mail Notifications, page 14-32](#) for more information.

Procedure

Step 1 Select **Monitor > Alarm Notifications > Threshold Groups**, then click **Add**.

- Step 2** In the Properties section, enter the name and description for the threshold group.
- Step 3** In the Threshold Settings section, click **Add** and then enter the following information shown in [Table 14-16](#).

Table 14-16 Threshold Settings Fields

Field	Description
Device Type	Select the device type to include in the threshold group. VC indicates virtual context.
Category	Select a statistic to include in the threshold group. Table 14-17 identifies and describes the types of statistics available for each device type.
Assert on Value	Enter a value to define the threshold. When the statistic exceeds this value, an alarm is issued. Some values are displayed as percentages as indicated by the percent sign (%). In the case of SSL certificate expiration, assert on value indicates the number of days before certificate expiration. Alarms will be updated daily to indicate the number of days remaining until certificate expiration. If the email is configured, you will be sent email daily alerting you to the number of days left before expiration.
Clear Value	Enter a value on which to clear the alarm. In the case of SSL certificate expiration, the setting has no relevance. When an expired certificate is deleted, the alarm is removed from ANM on the subsequent certificate evaluation. This happens every 24 hours.
Notify on Clear	Click the Notify on Clear box to receive E-mail notification to the specified address when the alarm is cleared.
Severity	Select a severity level for this threshold, which can be Critical, Info, Major, or Minor.

Table 14-17 **Monitoring Thresholds by Device Type**

Category	Threshold	Description
ACE 4710 Running Images A1(8) or A3(1.0)		
	ACL Memory	Percentage of memory allocated for ACLs.
	Bandwidth	Percentage of throughput.
	Concurrent Connections	Percentage of simultaneous connections.
	Current Application Acceleration Connections	Percentage of application acceleration connections.
	Current Connection Rate	Percentage of connections of any kind.
	Inspect Connection Rate	Percentage of application protocol inspection connections.
	MAC Miss Rate	Percentage of messages destined for the ACE that are sent to the control plane when the encapsulation is not correct in packets.
	Management Connections	Percentage of management connections.
	Management Traffic Rate	Percentage of management traffic connections.
	Proxy Connections Rate	Percentage of proxy connections.
	Regular Expression Memory	Percentage of regular expression memory.
	SSL Connection Rate	Percentage of SSL connections.
	Syslog Buffer Size	Percentage of the syslog buffer.
	Syslog Message Rate	Percentage of syslog messages per second.
	Translation Entries	Percentage of network and port address translations.
ACE 4710 VC		
Application Acceleration	Condenser State	State of the condenser.
Interface	Interface Operational State	Operational state of the interface.
Real Server	Real Server Current Connections	Number of current connections on a real server.
	Real Server Operational State	Operational state of a real server.
SLB Stat	Layer 4 Policy Connections	Number of Layer 4 policy connections.
	Layer 7 Policy Connections	Number of Layer 7 policy connections.
SSL Certificate Management	SSL certificate expiration (in days)	Number of days left before SLL certificate expires whose value minus one will send a warning email with the specified severity. ANM updates this field daily.

Table 14-17 **Monitoring Thresholds by Device Type**

Category	Threshold	Description
ACE Module		
	ACL Memory	Percentage of memory allocated for ACLs.
	Bandwidth	Percentage of bandwidth.
	Concurrent Connections	Percentage of simultaneous connections.
	Current Connection Rate	Percentage of connections of any kind.
	Inspect Connection Rate	Percentage of application protocol inspection connections.
	MAC Miss Rate	Percentage of messages destined for the ACE that are sent to the control plane when the encapsulation is not correct in packets.
	Management Connections	Percentage of management connections.
	Management Traffic Rate	Percentage of management traffic connections.
	Proxy Connections Rate	Percentage of proxy connections.
	Regular Expression Memory	Percentage of regular expression memory.
	SSL Connection Rate	Percentage of SSL connections.
	Syslog Buffer Size	Percentage of the syslog buffer.
	Syslog Message Rate	Percentage of syslog messages per second.
	Throughput	Percentage of throughput.
	Translation Entries	Percentage of network and port address translations.
ACE VC		
Interface	Interface Operational State	Operational state of the interface.
Real Server	Real Server Current Connections	Number of current connections on a real server.
	Real Server Operational State	Operational state of a real server.
SLB Stat	Layer 4 Policy Connections	Number of Layer 4 policy connections.
	Layer 7 Policy Connections	Number of Layer 7 policy connections.
SSL Certificate Management	SSL certificate expiration (in days)	Number of days left before SLL certificate expires whose value minus one will send a warning email with the specified severity. ANM updates this field daily.
CSM Module		
Real Server	Real Server Connections	Number of real server connections.
	Real Server Current State	Operational state of a real server.
SLB Stat	Current Opened Connections	Number of open connections.
	Layer 4 Policy Connections	Number of Layer 4 policy connections.
	Layer 7 Policy Connections	Number of Layer 7 policy connections.
SLB Virtual Server	Virtual Server Connections	Number of virtual server connections.
	Virtual Server State	Operational state of a virtual server.
System	CSM Fault Tolerance State	Fault tolerance state of the CSM.

Table 14-17 *Monitoring Thresholds by Device Type*

Category	Threshold	Description
CSS		
Interface	Average TCP Packets	Average number of TCP packets.
	Interface Operational State	Operational state of the interface.
	Max TCP Packets	Maximum number of TCP packets.
Real Server	Active Service Connections	Number of active real server connections.
	Real Server State	State of a real server.
System	CSS Fault Tolerance State	Fault tolerance state of the CSS.
	CSS Module State	State of a CSS module.
Virtual Server	Virtual Server State	Current state of a virtual server.

Step 4 Click **OK**.

Step 5 In Device Selection, select the device type to include in the threshold group. The available devices appear in the Available Items field.



Note Make sure that the device type you select in this field is supported by the threshold that you selected in the Category field in Step 3. If the device type you select is not supported by the threshold you selected, you will not receive alarm notifications.

Step 6 Click on a device in the Available Items field, then the arrow (>) to move the device to the Selected Items field.

Step 7 In the Notify By section, in the E-mail field, enter the E-mail address you want to receive notification E-mail. See [Viewing E-mail Notifications, page 14-31](#) for information contained in the E-mail notifications. If you do not select this field, you must view alarm notifications by selecting **Monitor > Alarm Notifications > Alarm**.



Note You must configure the required host parameters, IP address and port, to send e-mail notifications. See [Configuring SMTP for E-mail Notifications, page 14-32](#).

Step 8 In the Traps field, enter the host IP Address and port number of the machine to which the traps are sent. See [Viewing Traps, page 14-32](#) for information contained in the traps.

Step 9 Click:

- **Save** to save the threshold group settings.
- **Cancel** to cancel the threshold group settings and return to the Threshold Groups page.

Related Topics

- [Configuring SMTP for E-mail Notifications, page 14-32](#)
- [Viewing Alarm Notifications, page 14-30](#)

Viewing Alarm Notifications

After you configure alarm notifications (see [Configuring Alarm Notifications, page 14-25](#)), when the value for a specific statistic rises above the setting you specified, an alarm is issued to alert you.

Depending on how you specified to be notified when a threshold is crossed, you can view the alarms

- By selecting **Monitor > Alarm Notifications > Alarm**. See [Viewing Alarms in ANM, page 14-30](#).
- By viewing an E-mail notification. See [Viewing E-mail Notifications, page 14-31](#).
- By viewing traps. See [Viewing Traps, page 14-32](#).



Note

Threshold crossing is detected via periodic polling. If a threshold is crossed *between* polling cycles, it is possible that ANM might not issue an alert if the condition recovers before the next polling cycle.

Related Topics

- [Configuring Alarm Notifications, page 14-25](#)
- [Viewing Alarms in ANM, page 14-30](#)
- [Viewing E-mail Notifications, page 14-31](#)
- [Viewing Traps, page 14-32](#)

Viewing Alarms in ANM

After you configure alarm notifications (see [Configuring Alarm Notifications, page 14-25](#)), when the value for a specific statistic rises above the setting you specified, an alarm is issued to alert you.

You can view alarms issued by selecting **Monitor > Alarm Notifications > Alarms**. Alarms issued by ANM are displayed with the following information shown in [Table 14-18](#).



Note

If an alarm has been cleared, it does not appear on the **Monitor > Alarm Notifications > Alarms** page. This page displays active alarms only.

Table 14-18 ANM Alarm Notification Content

Field	Description
Source ID	ANM server IP address that issued the alarm
Severity	Specified severity level of the threshold, which can be • Info • Critical • Major • Minor
Origination Time	Time the alarm was issued
Threshold Group	Specified threshold group name
Category	Alarm name
Component	Component name, for example, VLAN20

Table 14-18 ANM Alarm Notification Content

Field	Description
State/Value	Specified state or value of the alarm
Detail	Displays additional information about the alarm.
Notes	Click the Notes icon to add notes to the alarm. See Adding Notes to Alarms , page 14-31

Related Topics

- [Configuring SMTP for E-mail Notifications](#), page 14-32
- [Configuring Alarm Notifications](#), page 14-25
- [Adding Notes to Alarms](#), page 14-31
- [Viewing E-mail Notifications](#), page 14-31

Adding Notes to Alarms

ANM allows you to add notes to alarms. If you are working on resolving an alarm, you can add a note to the alarm to let others know you are looking into the problem. The notes you enter appear in the Notes column of the Alarm Management table (**Monitor > Alarm Notifications > Alarms**).

Procedure

-
- Step 1** Select **Monitor > Alarm Notifications > Alarms**.
- Step 2** Click the icon in the Notes column for the alarm for which you want to add a note.
- Step 3** In the Notes screen, type the information you want to include in the note.
- Step 4** Click:
- **Save**—to save the note and add another note.
 - **Clear**—to clear the note without saving it and return to the Alarm screen.
 - **OK**—to save the note and return to the Alarm screen.
-

Related Topics

- [Configuring Alarm Notifications](#), page 14-25
- [Viewing Alarm Notifications](#), page 14-30

Viewing E-mail Notifications

After you configure alarm notifications (see [Configuring Alarm Notifications](#), page 14-25) and specify to receive notification E-mail, when the value for a specific statistic rises above the setting you specify, ACE Device Manager sends an E-mail to alert you.

[Table 14-19](#) describes the information contained in the E-mail alarm notification.

Table 14-19 E-mail Alarm Notification Content

Field	Description
ANM Server Host Name	ANM server host name
ANM Server IP Address	ANM server IP address
Device ID	Device name
Component Name	Component name, for example, VLAN20
Severity	Specified severity level of the threshold, which can be • Info • Critical • Major • Minor
Time	Time the alarm was issued
Alarm Name	Specified name of the alarm
Alarm Value	Specified value of the alarm
Threshold Assert Value	Specified value on when to issue the alarm
Threshold Group Name	Specified threshold group name
Alarm State	State of the alarm which can be • Active • Clear

Related Topics

- [Configuring Alarm Notifications, page 14-25](#)
- [Viewing Alarm Notifications, page 14-30](#)

Viewing Traps

After you configure alarm notifications (see [Configuring Alarm Notifications, page 14-25](#)) and specify to send traps to a trap receiver, when the value for a specific statistic rises above the setting you specify, ANM issues a trap to alert you.

Related Topics

- [Configuring Alarm Notifications, page 14-25](#)
- [Viewing Alarm Notifications, page 14-30](#)

Configuring SMTP for E-mail Notifications

You can specify that e-mail notifications be sent each time a monitoring threshold is crossed.

**Note**

You must configure your SMTP server in order to receive e-mail notifications.

Assumption

You have configured threshold crossing alerts. See [Configuring Alarm Notifications, page 14-25](#) for more information.

Procedure

-
- Step 1** Select **Monitor > Settings > SMTP Configuration**.
- Step 2** In the SMTP Server to Send E-mail Notifications field, enter your SMTP server.
- Step 3** Click **Deploy Now** to apply the SMTP configuration.
-

Related Topics

- [Monitoring Events, page 14-21](#)
- [Configuring Alarm Notifications, page 14-25](#)
- [Viewing E-mail Notifications, page 14-31](#)

Testing Connectivity

Use the following steps to verify the connectivity (using the ping command) between ANM and the IP address you specify.

**Note**

The Ping feature is disabled if you have not imported any devices into the ANM server.

Procedure

-
- Step 1** Select **Monitor > Tools > Ping**.
- Step 2** From the object selector field, select the device you want to test.
- Step 3** Enter the information shown in [Table 14-20](#).

Table 14-20 *Ping Fields*

Field	Description
IP Address	Enter the IP address of the real server to which you want to ping.
Elapsed Time	Elapsed time before the ping request is declared a failure.
Repeat	Enter how many times to repeat the test.
Datagram Size	Enter a value for the argument size (size of the packet) of the ping command.

- Step 4** Click **Start** to run the connectivity test.

- Step 5** After the test completes, the results are displayed. Click:
- **New** to enter new parameters and create a new ping test.
 - **Restart** to rerun the connectivity test.
-

Related Topic

[Setting Up Devices for Monitoring, page 14-2](#)



CHAPTER 15

Administering the Cisco Application Networking Manager

Revised: 3/25/09

The following topics describe how to administer, maintain, and manage the ANM management system. Previous topics described how to manage your network devices on ANM, while this topic describes how to perform procedures on the system itself.

- [Overview of the Admin Function, page 15-2](#)
- [Controlling Access to the Cisco ANM, page 15-2](#)
- [How ANM Handles Role-Based Access Control, page 15-7](#)
- [Configuring User Authentication, page 15-31](#)
- [Managing User Accounts, page 15-38](#)
- [Displaying or Terminating Current User Sessions, page 15-42](#)
- [Managing User Roles, page 15-43](#)
- [Managing Domains, page 15-49](#)
- [Managing ANM, page 15-54](#)
- [Lifeline Management, page 15-65](#)

Overview of the Admin Function


Note

Some of the Admin options might not be visible to some users; the roles assigned to your login determine which options are available.

[Table 15-1](#) describes the options that are displayed when you click **Admin**.

Table 15-1 Admin Menu Options

Menu	Option	Description	Reference
Role-Based Access Control	Organizations	Manage organizations, configure external authentication mechanisms	See Configuring User Authentication , page 15-31
	Users	Manage users	See Managing User Accounts , page 15-38
	Active Users	Display active users	See Displaying or Terminating Current User Sessions , page 15-42
	Roles	Manage user roles	See Managing User Roles , page 15-43
	Domains	Manage domains	See Managing Domains , page 15-49
ANM Management	ANM	Checks the status of the ANM server.	See Checking the Status of the ANM Server , page 15-54
	License Management	Views ANM license state, add more licenses, and tracks license information on your ACE	See Managing ANM Licenses , page 15-56
	Statistics	Displays ACE statistics (for example, CPU, disk, and memory usage).	See Viewing ANM Server Statistics , page 15-62
	Statistics Collection	Enables ACE server statistics polling.	See Configuring ANM Statistics Collection , page 15-63
Lifeline Management		Use this tool to report a problem to the Cisco support line and generate a diagnostic package	See Lifeline Management , page 15-65

Controlling Access to the Cisco ANM

Access to ANM is based on usernames and passwords, which can be authenticated to a local database on the ANM system or to an external RADIUS, Active Directory/Lightweight Directory Access Protocol (AD/LDAPS), or TACACS+ server. For detailed procedures on remote authentication, see the “Configuring Authentication and Accounting Services” chapter of the Cisco ACE 4700 Series Appliance

Security Configuration Guide on cisco.com at http://www.cisco.com/en/US/products/ps7027/products_installation_and_configuration_guides_list.html.

**Note**

ANM supports LDAPS is only through Active Directory (AD).

When a user logs into the system, the specific tasks they can perform and areas of the system they can use are controlled by *organizations*, *roles*, and *domains*.

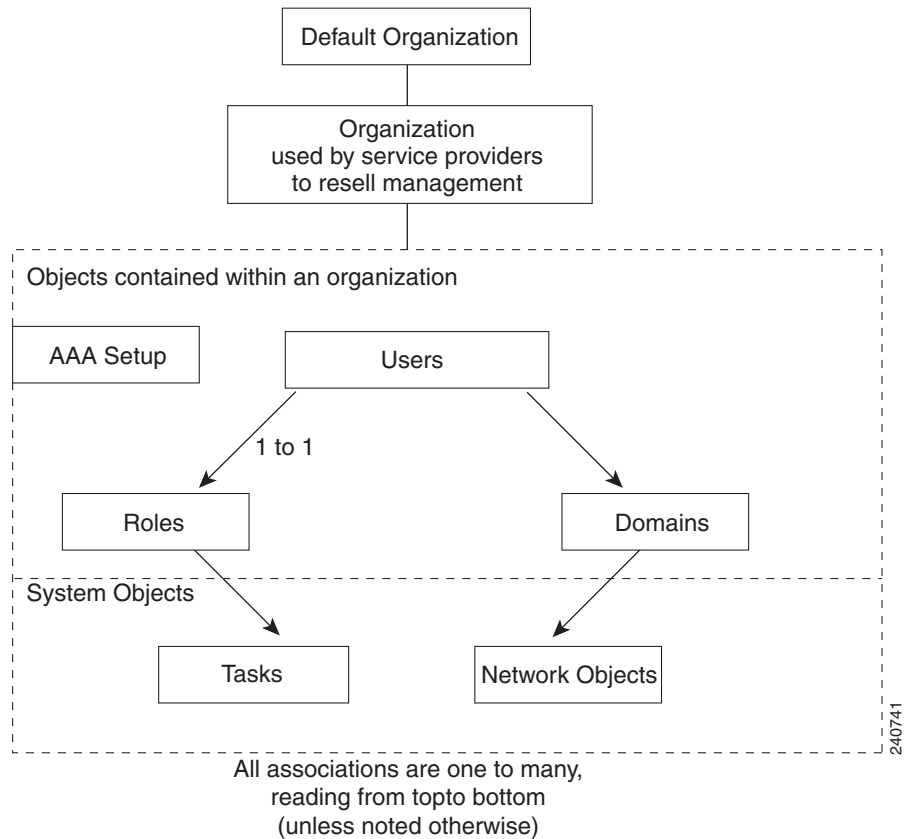
An organization is a virtual group of users, their roles, and domains managed by a specific server that provides authentication to its users. Each organization has its own set of users. See [Understanding Organizations, page 15-7](#) for information on organizations.

The role assigned to a user defines the tasks a user can perform and the items in the hierarchy that they can see. Roles are either pre-defined or set up by the system administrator. See [Understanding Roles, page 15-5](#) for more information.

A domain is a collection of managed objects. When a user is given access to a domain, this acts as a filter for a sub-set of objects on the network which are displayed as a virtual context. The types of objects in the system that are domain controlled are:

- Chassis (with VLANs)
- Virtual contexts
- Building Blocks
- Resource classes
- Real servers
- Virtual servers

Thus, role-based access control ensures that a user or organization can view only the devices or services or perform the actions that are included in the domains to which they have been given access.

Figure 15-1 Role-Based Access Control Containment Overview

The following is an example of RBAC containment.

Organization		
Webmasters		
Domains		
East Coast servers	Central servers	West Coast servers
Role		
Web server administrator		
Users		
User A	User B	User C
Note Each association is one-to-many. Because the organization itself is a collection, it is possible for a role to be used in many organizations.		

All other user interfaces, such as configuration and monitoring, respect this role-based access control policy:

- Roles limit the screens (or functions on those screens) that a user can see.
- Domains limit the objects that are listed on any screen that the roles allow.

- Users (other than the system administrator) can only create subdomains of the domains to which they are assigned.
- The system administrator user can see and modify all objects. All other users are subject to the role-based access controls illustrated in [Figure 15-1](#).

Related Topics

- [Types of Users, page 15-5](#)
- [Understanding Roles, page 15-5](#)
- [Understanding Operations Privileges, page 15-6](#)
- [Understanding Domains, page 15-7](#)
- [Understanding Organizations, page 15-7](#)
- [Managing User Accounts, page 15-38](#)

Types of Users

Two types of users configure and monitor the ANM system:

- Default users—individuals associated with the data center or IT department where the ANM system is installed. The default administrative account (user ID **admin**) is a system user account that is preconfigured on the system. The default administrative password (**admin**) is also set on the system. You can change the password for the admin user account in the same manner as any user password (see [Managing User Accounts, page 15-38](#)).

System roles are defined by the system administrator when the system is first set up. System roles are specified in terms of resource types and operations privileges. For each system role, the system administrator specifies which resource types a role can work with and what operations a role can perform on each resource type.

- Organization users—users who work for the customer of a service provider or AAA server that segments your users and to whom you want to grant access to ANM. Organization users automatically have their access limited to the organization to which they belong.

Related Topics

- [Configuring User Authentication, page 15-31](#)
- [Managing User Accounts, page 15-38](#)

Understanding Roles

Roles in the Cisco ANM system are defined by the system administrator. Roles are specified in terms of resource types and operations privileges. For each role, the system administrator specifies which resource types a role can work with and what operations a role can perform on each resource type.

When users are created, they are assigned at least one system role and inherit the operations privileges specified for each of the resource types assigned to that role.

The options a user sees in the menu are filtered according to that user's role. See [Table 15-2 on page 15-9](#).

Roles can be applied to both default and organization users. All users are strictly limited by the combination of their operations privileges and user access. For example, a user cannot create another user who has greater privileges or access.

Related Topics

- [Configuring User Authentication, page 15-31](#)
- [Managing User Accounts, page 15-38](#)
- [Managing User Roles, page 15-43](#)

Understanding Operations Privileges

Operations privileges define what users can do in the designated resource types. For example, each command and function on ANM has an assigned privilege. If a user's privileges are not sufficient, the command or function will not be available to them. The following operations privileges can be granted:

- No Access—The user has no access to this command or function.

**Note**

If a user is configured with no access to virtual contexts, it means absolutely no access to them. The most a user with this access can do is activate or suspend real servers.

- View—Allows the user to view statistics and specify parameter collection and threshold settings. Gives the user read-only or view access to system objects and information.
- Modify—Allows the user to change the persistent information associated with system objects, such as an organization record, or configuration.
- Debug—Gives the user read-only or view access to system objects and information.
- Create—Allows the user to control system objects, for example, creating them, enabling them, or powering up. Also allows the user to control system objects, for example, deleting them, disabling them, or powering down.

Privileges are hierarchical. If a user has Modify privileges, they have View privileges as well. If a user has Create or Debug privileges, they have View privileges as well.

**Note**

The ability to create automatically contains the modify function, but the reverse is not true (a user with modify privileges cannot automatically create items).

Related Topics

- [How ANM Handles Role-Based Access Control, page 15-7](#)
- [Managing User Roles, page 15-43](#)
- [Guidelines for Managing User Roles, page 15-43](#)
- [Understanding Predefined Roles, page 15-44](#)

Understanding Domains

Domains in the Cisco ANM system are defined by the system administrator. A domain is a collection of managed objects to which a user is given access. By setting up a domain, you are filtering for a subset of objects on the network. The user is then given access to this virtual context.

The rows a user sees in any table are filtered according to the domain to which that user has access.

Understanding Organizations

An organization allows you to configure AAA server lookup for your users or set up users who work for a service provider customer. Organizations in the Cisco ANM system are defined by the system administrator.

When you use a ACE device as a AAA Server you may want to segment them for customer, business, or security reasons. If you use more than one authentication server, then you can use organizations to configure them to authenticate your users.

For example, if your company has four servers, one each for local, RADIUS, TACACS+, and LDAP authentication, then organizations could reflect that. The Default organization in ANM is set up to act as the local server.

ANM supports different device types that have unique ways of configuring authentication access (which helps with future device support). ANM can configure which users are authenticated by which authentication servers, but does not act as a AAA server itself since this would be in conflict of its role as a RBAC administrator. This allows for the separation of authority that is needed to perform RBAC successfully.

How ANM Handles Role-Based Access Control

This section describes how and why a system administrator might want to use the ANM role-based access control (RBAC) features.

ANM supports two distinct, but related RBAC capabilities:

1. Where ANM acts as a system and network device overseer allowing it to implement its use of RBAC, referred to as ANM RBAC.
2. That which the device enforces, referred to as device RBAC.

Understanding ANM RBAC

ANM is a central place where you can globally set the RBAC for users, roles, and domains (as well as for virtual contexts or device types using device RBAC).

As an system administrator you may need to delegate authority to allow another administrators to perform specific tasks on specific devices; such as activating, suspending, and monitoring traffic flow to specific real servers, but disabling any other capabilities. ANM interface enables you to accomplish this delegation with more control. For a description of how the roles map to the functions, see [Table 15-2 on page 15-9](#).

Understanding Device RBAC

ANM's device RBAC allows you to set up device permission levels of a more granular nature. You no longer have to provide "all-or-nothing" roles-based access of devices and device modules. Without ANM, some devices may be open to users who can perform every task on that device or module,

regardless of their authorization due to permission level requirements on modules and or switches. ANM provides a central place to grant special access to users you specify. Device users, roles, and domain data are not part of, nor can they be used by ANM. Device RBAC is only for CLI access directly to the context.

For example, there may be a small number of users that need level 3 access when direct troubleshooting of ACE hardware is required. You can set up these users with or without ANM, but ANM centralizes the capability to do so. If you want to configure a network engineer with a special role, for example either ACE-Admin or Network-Admin, to provide the level 3 access. ANM accesses the ACE as a level 15 user and an admin supervisor and uses the RBAC to determine the level of access (to device types, segments, elements, subelements, and so on).

Some Cisco devices have the ability to configure RBAC directly on the device, for example the ACE. An example of a device that does not have the capability to have its own RBAC is the CSS or a CSM.

When you configure remote authentication (AAA, RADIUS, LDAP, or TACACs+) for the ACE via ANM, users no longer have to log out to access their device via Telnet. When you manually log into a CSS, the CSS performs user authentication in a Telnet session. Telnet does not provide any domain enforcement so is less secure.

If you are an admin using a CSS module outside of the ANM program, then you might have permission to do anything on this switch. If you are using ANM, you can set up better authorization for your administrators for specific devices. Better authorization controls are one of the advantages of using the ANM versus using only the CLI on the ACE hardware. You can now configure separate access for one function for this user in this domain only. ANM allows this high level of granularity and with it, more control over who does what to your devices.

You can access device RBAC using **Config > Devices** or **Config > Global > All Building Blocks**.



Note

When configuring device RBAC via Config > Devices, an message displays reminding you that you are configuring RBAC outside of ANM for direct access. Be aware that this may contradict your ANM settings.

For more information on centralizing direct access to devices through RBAC on individual devices, see [Configuring Device Role-Based Access Controls, page 2-40](#).

Case Example

In this example, a CSM device must have a level 15 access which by default makes the admin a supervisor on everything in the switch (and everything in the module). Another way of looking at this is providing read-only access to everything or configuration access to everything.

ACE hardware can be configured on a virtual context to perform that task on a subset domain for every individual module, on every context, but this type of configuration must be configured individually.

A system administrator might need to configure a network admin to manage two CSM modules, one out of six virtual contexts, and all East Coast web servers. With ANM, the admin could create one configuration set that includes a user account with a Network-Admin role and a domain that includes these objects. ANM then becomes the security window through which this user passes to get to their destination for that domain and for that virtual context.

If there were six users, nine domains, and three virtual contexts, there would be 54 entries required into a AAA Server and ACE module. In ANM there is one entry completed for each of the six users.

Table 15-2 **Role Mapping in ANM**

Role Tasks/Permissions	Resulting Menus Available
ACE-Admin Predefined Role	
Threshold/View	Monitor / Alarm Notifications / Alarms Monitor / Alarm Notifications / Threshold Groups Monitor / Alarm Notifications / Threshold Groups /Edit Monitor / Settings / SMTP Configuration
Device Events/Create	Monitor / Events / Events
Virtual Contexts/Create	Config / Deploy Config / Deploy / Deploy Now Config / Deploy / Edit Config / Devices / Device RBAC / Domains Config / Devices / Device RBAC / Roles Config / Devices / Device RBAC / Users Config / Devices / Expert / Action List Config / Devices / Expert / Building Block Audit Config / Devices / Expert / Class Map Config / Devices / Expert / Policy Map Config / Devices / HA Tracking and Failure Detection / Hosts Config / Devices / HA Tracking and Failure Detection / HSRP Groups Config / Devices / HA Tracking and Failure Detection / Interfaces Config / Devices / High Availability (HA) / Setup Config / Devices / Load Balancing / Health Monitoring Config / Devices / Load Balancing / Parameter Maps / Connection Parameter Map Config / Devices / Load Balancing / Parameter Maps / Generic Parameter Map Config / Devices / Load Balancing / Parameter Maps / HTTP Parameter Map Config / Devices / Load Balancing / Parameter Maps / Optimization Parameter Map Config / Devices / Load Balancing / Parameter Maps / RTSP Parameter Map

Table 15-2 Role Mapping in ANM

Role Tasks/Permissions (continued)	Resulting Menus Available (continued)
ACE-Admin Predefined Role (continued)	
Virtual Contexts/Create (continued)	Config / Devices / Load Balancing / Parameter Maps / SIP Parameter Map Config / Devices / Load Balancing / Parameter Maps / Skinny Parameter Map Config / Devices / Load Balancing / Real Servers Config / Devices / Load Balancing / Server Farms Config / Devices / Load Balancing / Stickiness Config / Devices / Load Balancing / Virtual Servers Config / Devices / Load Balancing / Virtual Servers / Add Config / Devices / Load Balancing / Virtual Servers / Edit Config / Devices / Network / BVI Interfaces Config / Devices / Network / GigabitEthernet Interfaces Config / Devices / Network / Global IP DHCP Config / Devices / Network / Port Channel Interfaces Config / Devices / Network / Static Routes Config / Devices / Network / Static VLAN Config / Devices / Network / VLAN Interfaces Config / Devices / Security / ACLs Config / Devices / Security / Object Groups Config / Devices / SSL / Auth Group Parameters Config / Devices / SSL / Certificate Revocation List Config / Devices / SSL / Certificates Config / Devices / SSL / Chain Group Parameters Config / Devices / SSL / CSR Parameters Config / Devices / SSL / Keys Config / Devices / SSL / Parameter Map Config / Devices / SSL / Proxy Service Config / Devices / System / Application Acceleration and Optimization Config / Devices / System / Global Policy Config / Devices / System / Licenses Config / Devices / System / Primary Attributes Config / Devices / System / Resource Classes Config / Devices / System / Resource Classes / Add Config / Devices / System / Resource Classes / Edit

Table 15-2 **Role Mapping in ANM**

Role Tasks/Permissions (continued)	Resulting Menus Available (continued)
ACE-Admin Predefined Role (continued)	
Virtual Contexts/Create (continued)	Config / Devices / System / SNMP Config / Devices / System / Syslog Config / Devices / Virtual Context Management Config / Devices / Virtual Context Management / Add Config / Devices / Virtual Context Management / Edit Config / Devices / Virtual Context Management / Extract building block Config / Devices / Virtual Context Management / Restart Polling Config / Devices / Virtual Context Management / Sync Config / Global / Building Blocks Config / Global / Building Blocks / Add Config / Global / Building Blocks / Tag Config / Global / Expert / Action List Config / Global / Expert / Class Map Config / Global / Expert / Policy Map Config / Global / Load Balancing / Health Monitoring Config / Global / Load Balancing / Parameter Maps / Connection Parameter Map Config / Global / Load Balancing / Parameter Maps / Generic Parameter Map Config / Global / Load Balancing / Parameter Maps / HTTP Parameter Map Config / Global / Load Balancing / Parameter Maps / Optimization Parameter Map Config / Global / Load Balancing / Parameter Maps / RTSP Parameter Map Config / Global / Load Balancing / Parameter Maps / SIP Parameter Map Config / Global / Load Balancing / Parameter Maps / Skinny Parameter Map Config / Global / Load Balancing / Real Servers Config / Global / Load Balancing / Server Farms Config / Global / Load Balancing / Stickiness

Table 15-2 Role Mapping in ANM

Role Tasks/Permissions (continued)	Resulting Menus Available (continued)
ACE-Admin Predefined Role (continued)	
Virtual Contexts/Create (continued)	Config / Global / Network / BVI Interfaces Config / Global / Network / Global IP DHCP Config / Global / Network / Static Routes Config / Global / Network / Static VLAN Config / Global / Network / VLAN Interfaces Config / Global / Resource Classes Config / Global / Resource Classes / Add Config / Global / Resource Classes / Audit Config / Global / Resource Classes / Edit Config / Global / Role-Based Access Control / Domains Config / Global / Role-Based Access Control / Roles Config / Global / Role-Based Access Control / Users Config / Global / Security / ACLs Config / Global / Security / Object Groups Config / Global / SSL / Auth Group Parameters Config / Global / SSL / Certificate Revocation List Config / Global / SSL / CSR Parameters Config / Global / SSL / Keys Config / Global / SSL / Parameter Map Config / Global / System / Global Policy Config / Global / System / Primary Attributes Config / Global / System / SNMP Config / Global / System / Syslog Config / Operations / Real Servers Config / Operations / Virtual Servers Config / Operations / Virtual Servers / Activate Config / Operations / Virtual Servers / Details Config / Operations / Virtual Servers / Suspend Monitor / Devices / Application Acceleration Monitor / Devices / Load Balancing Monitor / Devices / Load Balancing / Statistics Monitor / Devices / Load Balancing / Virtual Servers

Table 15-2 *Role Mapping in ANM*

Role Tasks/Permissions (continued)	Resulting Menus Available (continued)
ACE-Admin Predefined Role (continued)	
Virtual Contexts/Create (continued)	Monitor / Devices / Polling Settings Monitor / Devices / Resource Usage Monitor / Devices / Resource Usage Monitor / Devices / Resource Usage / Connections Monitor / Devices / Resource Usage / Features Monitor / Devices / System View Monitor / Devices / Traffic Summary Monitor / Devices / Virtual Context Management Monitor / Devices / Virtual Servers Monitor / Events /Virtual Context Management Monitor / Tools / Ping Change Password Copy License Export Generate CSR Import Install Resequence Status Uninstall Update
ANM-Admin Predefined Role	
All Options	All menus (ANM System, ANM User Access, and ANM Inventory)
Network-Admin Predefined Role	
Threshold/View	Monitor / Alarm Notifications / Alarms Monitor / Alarm Notifications / Threshold Groups Monitor / Alarm Notifications / Threshold Groups / Edit Monitor / Settings / SMTP Configuration

Table 15-2 Role Mapping in ANM

Role Tasks/Permissions (continued)	Resulting Menus Available (continued)
Network-Admin Predefined Role (continued)	
Switch/Create	Config / Devices / Device Management / Change Password Config / Devices / Device Management / Edit Config / Devices / Device Management / Sync Config / Devices / Interfaces / Access Ports Config / Devices / Interfaces / Routed Ports Config / Devices / Interfaces / Summary Config / Devices / Interfaces / Switched Virtual Interfaces Config / Devices / Interfaces / Trunk Ports Config / Devices / System / Primary Attributes Config / Devices / System / Static Routes Config / Devices / VLANs / Groups Config / Devices / VLANs / Layer 2 Config / Devices / VLANs / Layer 2 / Add Config / Devices / VLANs / Layer 2 / Edit Config / Devices / VLANs / Layer 3 Config / Devices / VLANs / Layer 3 / Add Config / Devices / VLANs / Layer 3 / Edit Config / Devices / VLANs / Summary Monitor / Events / Modules
Routing/Create	Config / Devices / Network / GigabitEthernet Interfaces Config / Devices / Network / Global IP DHCP Config / Devices / Network / Port Channel Interfaces Config / Devices / Network / Static Routes Config / Devices / Network / Static VLAN
Interface/Create	Config / Devices / Network / BVI Interfaces Config / Devices / Network / VLAN Interfaces Monitor / Devices / Traffic Summary Monitor / Tools / Ping
NAT/Create	No specific menus

Table 15-2 **Role Mapping in ANM**

Role Tasks/Permissions (continued)	Resulting Menus Available (continued)
Network-Admin Predefined Role (continued)	
Connection/Create	Config / Devices / Load Balancing / Parameter Maps / Connection Parameter Map Config / Devices / Load Balancing / Parameter Maps / Generic Parameter Map Config / Devices / Load Balancing / Parameter Maps / HTTP Parameter Map Config / Devices / Load Balancing / Parameter Maps / Optimization Parameter Map Config / Devices / Load Balancing / Parameter Maps / RTSP Parameter Map Config / Devices / Load Balancing / Parameter Maps / SIP Parameter Map Config / Devices / Load Balancing / Parameter Maps / Skinny Parameter Map
Network-Monitor Predefined Role	
Inventory (which includes Threshold, UDG, Device Events, Switch, and all Virtual Context tasks)/View	Config / Deploy Config / Deploy / Edit Config / Devices / Device Management Config / Devices / Device Management / Edit Config / Devices / Device Management / Modules Config / Devices / Device RBAC / Domains Config / Devices / Device RBAC / Roles Config / Devices / Device RBAC / Users Config / Devices / Expert / Action List Config / Devices / Expert / Action List Config / Devices / Expert / Building Block Audit Config / Devices / Expert / Class Map Config / Devices / Expert / Policy Map Config / Devices / Groups Config / Devices / Groups / Edit Config / Devices / HA Tracking and Failure Detection / Hosts Config / Devices / HA Tracking and Failure Detection / HSRP Groups

Table 15-2 Role Mapping in ANM

Role Tasks/Permissions (continued)	Resulting Menus Available (continued)
Network-Monitor Predefined Role	
Inventory/View (continued)	Config / Devices / HA Tracking and Failure Detection / Interfaces Config / Devices / High Availability (HA) / Setup Config / Devices / Interfaces / Access Ports Config / Devices / Interfaces / Routed Ports Config / Devices / Interfaces / Summary Config / Devices / Interfaces / Switched Virtual Interfaces Config / Devices / Interfaces / Trunk Ports Config / Devices / Load Balancing / Health Monitoring Config / Devices / Load Balancing / Parameter Maps / Connection Parameter Map Config / Devices / Load Balancing / Parameter Maps / Generic Parameter Map Config / Devices / Load Balancing / Parameter Maps / HTTP Parameter Map Config / Devices / Load Balancing / Parameter Maps / Optimization Parameter Map Config / Devices / Load Balancing / Parameter Maps / RTSP Parameter Map Config / Devices / Load Balancing / Parameter Maps / SIP Parameter Map Config / Devices / Load Balancing / Parameter Maps / Skinny Parameter Map Config / Devices / Load Balancing / Real Servers Config / Devices / Load Balancing / Server Farms Config / Devices / Load Balancing / Stickiness Config / Devices / Load Balancing / Virtual Servers Config / Devices / Load Balancing / Virtual Servers / Edit Config / Devices / Network / BVI Interfaces Config / Devices / Network / GigabitEthernet Interfaces Config / Devices / Network / Global IP DHCP Config / Devices / Network / Port Channel Interfaces Config / Devices / Network / Static Routes Config / Devices / Network / Static VLAN

Table 15-2 *Role Mapping in ANM*

Role Tasks/Permissions (continued)	Resulting Menus Available (continued)
Network-Monitor Predefined Role (continued)	
Inventory/View (continued)	Config / Devices / Network / VLAN Interfaces Config / Devices / Security / ACLs Config / Devices / Security / Object Groups Config / Devices / SSL / Auth Group Parameters Config / Devices / SSL / Certificate Revocation List Config / Devices / SSL / Certificates Config / Devices / SSL / Chain Group Parameters Config / Devices / SSL / CSR Parameters Config / Devices / SSL / Keys Config / Devices / SSL / Parameter Map Config / Devices / SSL / Proxy Service Config / Devices / System / Application Acceleration and Optimization Config / Devices / System / Global Policy Config / Devices / System / Licenses Config / Devices / System / Primary Attributes Config / Devices / System / Primary Attributes Config / Devices / System / Resource Classes Config / Devices / System / Resource Classes / Edit Config / Devices / System / SNMP Config / Devices / System / Static Routes Config / Devices / System / Syslog Config / Devices / Virtual Context Management Config / Devices / Virtual Context Management / Edit Config / Devices / VLANs / Groups Config / Devices / VLANs / Layer 2 Config / Devices / VLANs / Layer 2 / Edit Config / Devices / VLANs / Layer 3 Config / Devices / VLANs / Layer 3 / Edit Config / Devices / VLANs / Summary Config / Global / Building Blocks Config / Global / Expert / Action List Config / Global / Expert / Class Map

Table 15-2 Role Mapping in ANM

Role Tasks/Permissions (continued)	Resulting Menus Available (continued)
Network-Monitor Predefined Role (continued)	
Inventory/View (continued)	Config / Global / Expert / Policy Map Config / Global / Load Balancing / Health Monitoring Config / Global / Load Balancing / Parameter Maps / Connection Parameter Map Config / Global / Load Balancing / Parameter Maps / Generic Parameter Map Config / Global / Load Balancing / Parameter Maps / HTTP Parameter Map Config / Global / Load Balancing / Parameter Maps / Optimization Parameter Map Config / Global / Load Balancing / Parameter Maps / RTSP Parameter Map Config / Global / Load Balancing / Parameter Maps / SIP Parameter Map Config / Global / Load Balancing / Parameter Maps / Skinny Parameter Map Config / Global / Load Balancing / Real Servers Config / Global / Load Balancing / Server Farms Config / Global / Load Balancing / Stickiness Config / Global / Network / BVI Interfaces Config / Global / Network / Global IP DHCP Config / Global / Network / Static Routes Config / Global / Network / Static VLAN Config / Global / Network / VLAN Interfaces Config / Global / Resource Classes Config / Global / Resource Classes / Audit Config / Global / Resource Classes / Edit Config / Global / Role-Based Access Control / Domains Config / Global / Role-Based Access Control / Roles Config / Global / Role-Based Access Control / Users Config / Global / Security / ACLs Config / Global / Security / Object Groups Config / Global / SSL / Auth Group Parameters Config / Global / SSL / Certificate Revocation List

Table 15-2 **Role Mapping in ANM**

Role Tasks/Permissions (continued)	Resulting Menus Available (continued)
Network-Monitor Predefined Role (continued)	
Inventory/View (continued)	Config / Global / SSL / CSR Parameters Config / Global / SSL / Keys Config / Global / SSL / Parameter Map Config / Global / System / Global Policy Config / Global / System / Primary Attributes Config / Global / System / SNMP Config / Global / System / Syslog Config / Operations / Real Servers Config / Operations / Virtual Servers Config / Operations / Virtual Servers / Details Config / Tools / Credential Pool Management Config / Tools / IP Discovery Monitor / Alarm Notifications / Alarms Monitor / Alarm Notifications / Threshold Groups Monitor / Alarm Notifications / Threshold Groups / Edit Monitor / Devices / Application Acceleration Monitor / Devices / Device Management Monitor / Devices / Load Balancing Monitor / Devices / Load Balancing / Statistics Monitor / Devices / Load Balancing / Statistics Monitor / Devices / Load Balancing / Virtual Servers Monitor / Devices / Polling Settings Monitor / Devices / Resource Usage Monitor / Devices / Resource Usage Monitor / Devices / Resource Usage / Connections Monitor / Devices / Resource Usage / Features Monitor / Devices / System View Monitor / Devices / Traffic Summary Monitor / Devices / Virtual Context Management Monitor / Devices / Virtual Servers Monitor / Events / Events Monitor / Events / Modules Monitor / Events / Virtual Context Management Monitor / Settings / Global Polling Configuration

Table 15-2 Role Mapping in ANM

Role Tasks/Permissions (continued)	Resulting Menus Available (continued)
Network-Monitor Predefined Role (continued)	
Inventory/View (continued)	Monitor / Settings / SMTP Configuration Monitor / Tools / Ping Export Status
Org-Admin Predefined Role	
ANM User Access/Create	Admin / Role-Based Access Control / Domains Admin / Role-Based Access Control / Domains / Add Admin / Role-Based Access Control / Domains / Edit Admin / Role-Based Access Control / Roles Admin / Role-Based Access Control / Roles / Add Admin / Role-Based Access Control / Roles / Edit Admin / Role-Based Access Control / Roles / Users Admin / Role-Based Access Control / Users Admin / Role-Based Access Control / Users / Add Admin / Role-Based Access Control / Users / Edit
ANM Inventory/Create	Config / Deploy Config / Deploy / Deploy Now Config / Deploy / Edit Config / Devices / Device Management Config / Devices / Device Management / Add Config / Devices / Device Management / Change Password Config / Devices / Device Management / Edit Config / Devices / Device Management / Modules Config / Devices / Device Management / Modules / Sync Config / Devices / Device Management / Restart Polling Config / Devices / Device Management / Sync Config / Devices / Device RBAC / Domains Config / Devices / Device RBAC / Roles Config / Devices / Device RBAC / Users Config / Devices / Expert / Action List Config / Devices / Expert / Building Block Audit Config / Devices / Expert / Class Map

Table 15-2 **Role Mapping in ANM**

Role Tasks/Permissions (continued)	Resulting Menus Available (continued)
Org-Admin Predefined Role (continued)	
ANM Inventory/Create (continued)	Config / Devices / Expert / Policy Map Config / Devices / Groups Config / Devices / Groups / Add Config / Devices / Groups / Edit Config / Devices / HA Tracking and Failure Detection / Hosts Config / Devices / HA Tracking and Failure Detection / HSRP Groups Config / Devices / HA Tracking and Failure Detection / Interfaces Config / Devices / High Availability (HA) / Setup Config / Devices / Interfaces / Access Ports Config / Devices / Interfaces / Routed Ports Config / Devices / Interfaces / Summary Config / Devices / Interfaces / Switched Virtual Interfaces Config / Devices / Interfaces / Trunk Ports Config / Devices / Load Balancing / Health Monitoring Config / Devices / Load Balancing / Parameter Maps / Connection Parameter Map Config / Devices / Load Balancing / Parameter Maps / Generic Parameter Map Config / Devices / Load Balancing / Parameter Maps / HTTP Parameter Map Config / Devices / Load Balancing / Parameter Maps / Optimization Parameter Map Config / Devices / Load Balancing / Parameter Maps / RTSP Parameter Map Config / Devices / Load Balancing / Parameter Maps / SIP Parameter Map Config / Devices / Load Balancing / Parameter Maps / Skinny Parameter Map Config / Devices / Load Balancing / Real Servers Config / Devices / Load Balancing / Server Farms Config / Devices / Load Balancing / Stickiness Config / Devices / Load Balancing / Virtual Servers

Table 15-2 Role Mapping in ANM

Role Tasks/Permissions (continued)	Resulting Menus Available (continued)
Org-Admin Predefined Role (continued)	
ANM Inventory/Create (continued)	Config / Devices / Load Balancing / Virtual Servers / Add Config / Devices / Load Balancing / Virtual Servers / Edit Config / Devices / Network / BVI Interfaces Config / Devices / Network / GigabitEthernet Interfaces Config / Devices / Network / Global IP DHCP Config / Devices / Network / Port Channel Interfaces Config / Devices / Network / Static Routes Config / Devices / Network / Static VLAN Config / Devices / Network / VLAN Interfaces Config / Devices / Security / ACLs Config / Devices / Security / Object Groups Config / Devices / SSL / Auth Group Parameters Config / Devices / SSL / Certificate Revocation List Config / Devices / SSL / Certificates Config / Devices / SSL / Chain Group Parameters Config / Devices / SSL / CSR Parameters Config / Devices / SSL / Keys Config / Devices / SSL / Parameter Map Config / Devices / SSL / Proxy Service Config / Devices / System / Application Acceleration and Optimization Config / Devices / System / Global Policy Config / Devices / System / Licenses Config / Devices / System / Primary Attributes Config / Devices / System / Primary Attributes Config / Devices / System / Resource Classes Config / Devices / System / Resource Classes / Add Config / Devices / System / Resource Classes / Edit Config / Devices / System / SNMP Config / Devices / System / Static Routes Config / Devices / System / Syslog Config / Devices / Virtual Context Management Config / Devices / Virtual Context Management / Add Config / Devices / Virtual Context Management / Edit

Table 15-2 **Role Mapping in ANM**

Role Tasks/Permissions (continued)	Resulting Menus Available (continued)
Org-Admin Predefined Role (continued)	
ANM Inventory/Create (continued)	Config / Devices / Virtual Context Management / Extract building block Config / Devices / Virtual Context Management / Restart Polling Config / Devices / Virtual Context Management / Sync Config / Devices / VLANs / Groups Config / Devices / VLANs / Layer 2 Config / Devices / VLANs / Layer 2 / Add Config / Devices / VLANs / Layer 2 / Edit Config / Devices / VLANs / Layer 3 Config / Devices / VLANs / Layer 3 / Add Config / Devices / VLANs / Layer 3 / Edit Config / Devices / VLANs / Summary Config / Global / Building Blocks Config / Global / Building Blocks / Add Config / Global / Building Blocks / Tag Config / Global / Expert / Action List Config / Global / Expert / Action List Config / Global / Expert / Class Map Config / Global / Expert / Policy Map Config / Global / Load Balancing / Health Monitoring Config / Global / Load Balancing / Parameter Maps / Connection Parameter Map Config / Global / Load Balancing / Parameter Maps / Generic Parameter Map Config / Global / Load Balancing / Parameter Maps / HTTP Parameter Map Config / Global / Load Balancing / Parameter Maps / Optimization Parameter Map Config / Global / Load Balancing / Parameter Maps / RTSP Parameter Map Config / Global / Load Balancing / Parameter Maps / SIP Parameter Map Config / Global / Load Balancing / Parameter Maps / Skinny Parameter Map

Table 15-2 Role Mapping in ANM

Role Tasks/Permissions (continued)	Resulting Menus Available (continued)
Org-Admin Predefined Role (continued)	
ANM Inventory/Create (continued)	Config / Global / Load Balancing / Real Servers Config / Global / Load Balancing / Server Farms Config / Global / Load Balancing / Stickiness Config / Global / Network / BVI Interfaces Config / Global / Network / Global IP DHCP Config / Global / Network / Static Routes Config / Global / Network / Static VLAN Config / Global / Network / VLAN Interfaces Config / Global / Resource Classes Config / Global / Resource Classes / Add Config / Global / Resource Classes / Audit Config / Global / Resource Classes / Edit Config / Global / Role-Based Access Control / Domains Config / Global / Role-Based Access Control / Roles Config / Global / Role-Based Access Control / Users Config / Global / Security / ACLs Config / Global / Security / Object Groups Config / Global / SSL / Auth Group Parameters Config / Global / SSL / Certificate Revocation List Config / Global / SSL / CSR Parameters Config / Global / SSL / Keys Config / Global / SSL / Parameter Map Config / Global / System / Global Policy Config / Global / System / Primary Attributes Config / Global / System / SNMP Config / Global / System / Syslog Config / Operations / Real Servers Config / Operations / Virtual Servers Config / Operations / Virtual Servers / Activate Config / Operations / Virtual Servers / Details Config / Operations / Virtual Servers / Suspend Config / Tools / Credential Pool Management Config / Tools / IP Discovery

Table 15-2 **Role Mapping in ANM**

Role Tasks/Permissions (continued)	Resulting Menus Available (continued)
Org-Admin Predefined Role (continued)	
ANM Inventory/Create (continued)	Monitor / Alarm Notifications / Alarms Monitor / Alarm Notifications / Threshold Groups Monitor / Alarm Notifications / Threshold Groups / Add Monitor / Alarm Notifications / Threshold Groups / Edit Monitor / Devices / Application Acceleration Monitor / Devices / Device Management Monitor / Devices / Load Balancing Monitor / Devices / Load Balancing / Statistics Monitor / Devices / Load Balancing / Virtual Servers Monitor / Devices / Polling Settings Monitor / Devices / Resource Usage Monitor / Devices / Resource Usage / Connections Monitor / Devices / Resource Usage / Features Monitor / Devices / System View Monitor / Devices / Traffic Summary Monitor / Devices / Virtual Context Management Monitor / Devices / Virtual Servers Monitor / Events / Events Monitor / Events / Modules Monitor / Events / Virtual Context Management Monitor / Settings / Global Polling Configuration Monitor / Settings / SMTP Configuration Monitor / Tools / Ping Change Password Copy License Export Generate CSR Import Install Resequencing
Org-Admin Predefined Role (continued)	
ANM Inventory/Create (continued)	Status Uninstall Update

Table 15-2 **Role Mapping in ANM**

Role Tasks/Permissions (continued)	Resulting Menus Available (continued)
Security-Admin Predefined Role	
AAA/Create	No specific menu items
Access List/	Config / Devices / Security / ACLs Config / Devices / Security / Object Groups Resequene
Interface/Modify	Config / Devices / Network / BVI Interfaces Config / Devices / Network / VLAN Interfaces Monitor / Devices / Traffic Summary Monitor / Tools / Ping
NAT/Create	No specific menu items
Inspect/Create	No specific menu items
Connection/Create	Config / Devices / Load Balancing / Parameter Maps / Connection Parameter Map Config / Devices / Load Balancing / Parameter Maps / Generic Parameter Map Config / Devices / Load Balancing / Parameter Maps / HTTP Parameter Map Config / Devices / Load Balancing / Parameter Maps / Optimization Parameter Map Config / Devices / Load Balancing / Parameter Maps / RTSP Parameter Map Config / Devices / Load Balancing / Parameter Maps / SIP Parameter Map Config / Devices / Load Balancing / Parameter Maps / Skinny Parameter Map
Server-Appln Maintenance Predefined Role	
Threshold/View	Monitor / Alarm Notifications / Alarms Monitor / Alarm Notifications / Threshold Groups Monitor / Alarm Notifications / Threshold Groups/ Edit Monitor / Settings / SMTP Configuration

Table 15-2 **Role Mapping in ANM**

Role Tasks/Permissions (continued)	Resulting Menus Available (continued)
Security-Admin Predefined Role (continued)	
VIP/View	Config / Deploy Config / Deploy / Edit Config / Devices / Load Balancing / Health Monitoring Config / Devices / Load Balancing / Real Servers Config / Devices / Load Balancing / Server Farms Config / Devices / Load Balancing / Stickiness Config / Devices / Load Balancing / Virtual Servers Config / Devices / Load Balancing / Virtual Servers / Edit Config / Operations / Real Servers Config / Operations / Virtual Servers Config / Operations / Virtual Servers / Details Monitor / Devices / Load Balancing Monitor / Devices / Load Balancing / Statistics Monitor / Devices / Load Balancing / Virtual Servers Monitor / Devices / Virtual Servers
Server-Maintenance Predefined Role	
Threshold/View	Monitor / Alarm Notifications / Alarms Monitor / Alarm Notifications / Threshold Groups Monitor / Alarm Notifications / Threshold Groups /Edit Monitor / Settings / SMTP Configuration
VIP/View	Config / Deploy Config / Deploy / Edit Config / Devices / Load Balancing / Health Monitoring Config / Devices / Load Balancing / Real Servers Config / Devices / Load Balancing / Server Farms Config / Devices / Load Balancing / Stickiness Config / Devices / Load Balancing / Virtual Servers Config / Devices / Load Balancing / Virtual Servers / Edit Config / Operations / Real Servers Config / Operations / Virtual Servers Config / Operations / Virtual Servers / Details Monitor / Devices / Load Balancing Monitor / Devices / Load Balancing / Statistics

Table 15-2 Role Mapping in ANM

Role Tasks/Permissions (continued)	Resulting Menus Available (continued)
Security-Admin Predefined Role (continued)	
VIP/View	Monitor / Devices / Load Balancing / Virtual Servers Monitor / Devices / Virtual Servers
SLB-Admin Predefined Role	
Threshold/View	Monitor / Alarm Notifications / Alarms Monitor / Alarm Notifications / Threshold Groups Monitor / Alarm Notifications / Threshold Groups /Edit Monitor / Settings / SMTP Configuration
Building Block/Create	Config / Global / Building Blocks Config / Global / Building Blocks / Add Config / Global / Building Blocks / Tag Config / Global / Expert / Action List Config / Global / Expert / Action List Config / Global / Expert / Class Map Config / Global / Expert / Policy Map Config / Global / Load Balancing / Health Monitoring Config / Global / Load Balancing / Parameter Maps / Connection Parameter Map Config / Global / Load Balancing / Parameter Maps / Generic Parameter Map Config / Global / Load Balancing / Parameter Maps / HTTP Parameter Map Config / Global / Load Balancing / Parameter Maps / Optimization Parameter Map Config / Global / Load Balancing / Parameter Maps / RTSP Parameter Map Config / Global / Load Balancing / Parameter Maps / SIP Parameter Map Config / Global / Load Balancing / Parameter Maps / Skinny Parameter Map Config / Global / Load Balancing / Real Servers Config / Global / Load Balancing / Server Farms Config / Global / Load Balancing / Stickiness Config / Global / Network / BVI Interfaces Config / Global / Network / Global IP DHCP Config / Global / Network / Static Routes

Table 15-2 **Role Mapping in ANM**

Role Tasks/Permissions (continued)	Resulting Menus Available (continued)
SLB-Admin Predefined Role (continued)	
Building Block/Create (continued)	Config / Global / Network / Static VLAN Config / Global / Network / VLAN Interfaces Config / Global / Role-Based Access Control / Domains Config / Global / Role-Based Access Control / Roles Config / Global / Role-Based Access Control / Users Config / Global / Security / ACLs Config / Global / Security / Object Groups Config / Global / SSL / Auth Group Parameters Config / Global / SSL / Certificate Revocation List Config / Global / SSL / CSR Parameters Config / Global / SSL / Keys Config / Global / SSL / Parameter Map Config / Global / System / Global Policy Config / Global / System / Primary Attributes Config / Global / System / SNMP Config / Global / System / Syslog
Interface/Modify	Config / Devices / Network / BVI Interfaces Config / Devices / Network / VLAN Interfaces Monitor / Devices / Traffic Summary Monitor / Tools / Ping
Expert/Create	Config / Deploy Config / Deploy / Deploy Now Config / Deploy / Edit Config / Devices / Expert / Action List Config / Devices / Expert / Action List Config / Devices / Expert / Class Map Config / Devices / Expert / Policy Map Config / Devices / Load Balancing / Health Monitoring Config / Devices / Load Balancing / Parameter Maps / Connection Parameter Map Config / Devices / Load Balancing / Parameter Maps / Generic Parameter Map

Table 15-2 Role Mapping in ANM

Role Tasks/Permissions (continued)	Resulting Menus Available (continued)
Expert/Create (continued)	Config / Devices / Load Balancing / Parameter Maps / HTTP Parameter Map Config / Devices / Load Balancing / Parameter Maps / Optimization Parameter Map Config / Devices / Load Balancing / Parameter Maps / RTSP Parameter Map Config / Devices / Load Balancing / Parameter Maps / SIP Parameter Map Config / Devices / Load Balancing / Parameter Maps / Skinny Parameter Map Config / Devices / Load Balancing / Real Servers Config / Devices / Load Balancing / Server Farms Config / Devices / Load Balancing / Stickiness Config / Devices / Load Balancing / Virtual Servers Config / Devices / Load Balancing / Virtual Servers / Add Config / Devices / Load Balancing / Virtual Servers / Edit Config / Operations / Real Servers Config / Operations / Virtual Servers Config / Operations / Virtual Servers / Activate Config / Operations / Virtual Servers / Details Config / Operations / Virtual Servers / Suspend Monitor / Devices / Load Balancing Monitor / Devices / Load Balancing / Statistics Monitor / Devices / Load Balancing / Statistics Monitor / Devices / Load Balancing / Virtual Servers Monitor / Devices / Virtual Servers
SSL-Admin	
SSL/Create	Config / Devices / SSL / Auth Group Parameters Config / Devices / SSL / Certificate Revocation List Config / Devices / SSL / Certificates Config / Devices / SSL / Chain Group Parameters Config / Devices / SSL / CSR Parameters Config / Devices / SSL / Keys Config / Devices / SSL / Parameter Map

Table 15-2 **Role Mapping in ANM**

Role Tasks/Permissions (continued)	Resulting Menus Available (continued)
SSL/Create (continued)	Config / Devices / SSL / Proxy Service Export Generate CSR Import

Configuring User Authentication

In ANM, you can configure authentication for your users by specifying which AAA servers are used for specific users. You do this through *organizations*. An organization allows you to configure your AAA server lookup for your users, then associate specific users, roles, and domains with those organizations.

The following sections describe the organization authentication tasks you can complete in the ANM interface:

- [Guidelines for Managing Organizations, page 15-32](#)
- Configuring AAA Server lookup for your users—See [Guidelines for Managing Organizations, page 15-32](#)
- Changing server passwords—See [Changing Authentication Server Passwords, page 15-35](#)
- [Modifying Organizations, page 15-35](#)
- [Duplicating an Organization, page 15-36](#)
- [Displaying Authentication Server Organizations, page 15-37](#)
- [Deleting Organizations, page 15-37](#)

The Default organization (in which all users belong), authenticates users through the ANM internal mechanism, which is based on the RBAC security model. This mechanism authenticates users through the local authentication module and a local database of user IDs and passwords. If you choose to use an external authentication method, you must specify the authentication server and port.

Many organizations, however, already have an authentication service. To use your own authentication service instead of the local module, you can select one of the alternate modules:

- TACACS+
- RADIUS
- AD/LDAP



Note

For detailed procedures on remote authentication, see the “Configuring Authentication and Accounting Services” chapter of the Cisco ACE 4700 Series Appliance Security Configuration Guide on [cisco.com](http://www.cisco.com/en/US/products/ps7027/products_installation_and_configuration_guides_list.html) at http://www.cisco.com/en/US/products/ps7027/products_installation_and_configuration_guides_list.html.

After you configure an organization, all authentication transactions are performed by the authentication service associated with that organization. Users log in with the user ID and password associated with the current authentication module.

Related Topics

- [Managing User Accounts, page 15-38](#)
- [Managing User Roles, page 15-43](#)
- [Managing Domains, page 15-49](#)

Guidelines for Managing Organizations

Organizations define the mechanism for authenticating users: RADIUS, TACACS+, AD/LDAP, or Local. When the authentication is remote, users within that organization will have their passwords validated externally.

**Note**

For detailed procedures on remote authentication, see the “Configuring Authentication and Accounting Services” chapter of the Cisco ACE 4700 Series Appliance Security Configuration Guide on cisco.com at http://www.cisco.com/en/US/products/ps7027/products_installation_and_configuration_guides_list.html.

Use this procedure to configure organizations.

**Note**

All users logging into ANM must have a local account.

Procedure

- Step 1** Select **Admin > Role-Based Access Control > All Organizations**.
- Step 2** Click **Add**.
- Step 3** Enter the name of the new organization, and notes if required. Click **Save**.

- Step 4** Enter the attributes described in [Table 15-3](#). Certain attributes will display when specific options are selected.

Table 15-3 **Organization Attributes**

Attribute	Description
Notes	Description of the organization or notes to administrator.
Organization Name	This can be different from the organization name above. Specifies the company, department, or division of the organization that administers the ANM server. Default name entered appears.
Account Number	Specifies an account number for the organization.
Contact Name	Specifies the name of the individual who is the contact in the organization.
E-Mail	Specifies an address for the organization's contact person.
Telephone #	Specifies a telephone number for the organization's contact person. The format is free text with no embedded spaces.
Alternative Telephone #	Specifies an alternative telephone number for the organization's contact person.
Street Address	Specifies the street for the organization.
City	Specifies the city where the organization is located.
Zip Code	Specifies a zip code for the organization's address.
Country	Specifies the country where the organization is located.
Authentication	Specifies how users are to be authenticated by the system. The default authentication mechanism is ANM's internal mechanism, which is based on ANM's security model. If an external authentication method is chosen, the authentication server and port must be specified. Options: • Local—Specifies the use of the local database. • RADIUS • TACACS+ • AD/LDAP (ANM requires that a Domain Controller Server certificate be installed on the Active Directory Server. For a document containing the detailed instructions, see the “Configuring an LDAP Server” section in the “Configuring Authentication and Accounting Services” chapter of the <i>Cisco ACE 4700 Series Appliance Security Configuration Guide</i> on cisco.com at http://www.cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/ace_appliances/vA3_1_0/configuration/security/guide/aaa.html#wp1537851.)  Note ANM itself does not perform authorization. ANM only provides authentication for users who are logging in to ANM.

Table 15-3 **Organization Attributes (continued)**

Attribute	Description
authentication-port	(Optional) Specifies the UDP destination port for communicating authentication requests to the authentication server. Depending on your server, the following may be true: • By default, the RADIUS authentication port is 1812 (as defined in RFC 2138 and RFC 2139). The port_number argument specifies the RADIUS port number. Valid values are from 1 to 65535. • TACACS+ • LDAP
secondary-authentication-port	(Optional) Specifies another UDP destination port for communicating authentication requests to the RADIUS server if the initial port is busy.
Note You will see the following fields if external authentication is used in the organization.	
Authentication Server	Specifies the IP address of a RADIUS, TACACS+, or LDAP server for user authentication. Specifies an external server when RADIUS, TACACS+, or LDAP is to be used to authenticate users. Note Setting the server with this command is mandatory if the authentication mechanism is anything other than default. If you select an external authentication method, you might need to specify a separate user ID for the authentication server. For AD/LDAPS, you must provide the FQDN of the server (which must be in the users authenticating domain).  Note ANM supports LDAPS is only through Active Directory (AD).
Secondary Authentication Server	(Optional) Specifies a secondary external server when Radius or TACACS+ is to be used to authenticate users. If you specify a secondary authentication server, ANM uses this server to authenticate users if the primary authentication server is unavailable.
Authentication Secret	Encrypts the traffic between the Cisco ANM and the AAA server. This string needs to be identical on both.

Step 5 Click **Save**.**Related Topics**

- [Managing User Accounts, page 15-38](#)
- [Changing the Admin Password, page 15-35](#)

Changing Authentication Server Passwords

**Note**

Your user role determines whether you can use this option.

Procedure

-
- Step 1** Select **Admin > Role-Based Access Control > Organization**.
- Step 2** Select the organization you want to modify, then click **Edit**.
- Step 3** Change the password attribute in the attributes table (see [Table 15-4](#)).
- Step 4** Click **Save**.
- Step 5** The Edit User Details screen appears. Make any changes and click **Save**. When all the details are correct, click **Cancel**. The User Management table is displayed.
-

Related Topics

- [Managing User Accounts, page 15-38](#)
- [Changing the Admin Password, page 15-35](#)

Changing the Admin Password

Each ANM has an admin user account built into the device. The root user ID is **admin**, and the password is set when the system is installed. For information about changing the Admin password, see [Changing Your Account Password, page 1-4](#).

Modifying Organizations

Assumptions

- ANM is installed and running.
- The organization exists in the ANM database.
- You have reviewed the guidelines for managing customer organizations (see [Guidelines for Managing Organizations, page 15-32](#)).

**Note**

Your user role determines whether you can use this option.

Procedure

-
- Step 1** Select **Admin > Role-Based Access Control > Organizations**.
- Step 2** Select the organization you want to modify.
- Step 3** Click **Edit**.

- Step 4** Modify any of the attributes in the attributes table (see [Table 15-3](#)).
- Step 5** Click **Save**.
-

Related Topics

[Configuring User Authentication, page 15-31](#)

Duplicating an Organization

Use this option to create a new organization from an existing one.

Assumptions

- ANM is installed and running.
- The organization exists in the ANM database.
- You have reviewed the guidelines for managing customer organizations (see [Guidelines for Managing Organizations, page 15-32](#)).

**Note**

Your user role determines whether you can use this option.

Procedure

-
- Step 1** Select **Admin > Role-Based Access Control > Organizations**.
- Step 2** Select the organization you want to copy.
- Step 3** Click **Duplicate**.
- Step 4** At the prompt, enter a name for the new organization.
- Step 5** Click **OK**.
- Step 6** Make any changes to the organization settings (see [Table 15-3](#)).
- Step 7** Click **Save**.
-

Related Topics

[Configuring User Authentication, page 15-31](#)

Displaying Authentication Server Organizations

**Note**

Your user role determines whether you can use this option.

Procedure

-
- Step 1** Select **Admin > Role-Based Access Control > All Organizations**.
- The list of customer organizations appears in the All Organizations table.
- Step 2** From this screen you can create a users, roles, and domains that are associated with this specific organization. You can also access organizations by selecting the organization from the object selector that displays in the top right portion of the content area.
-

Related Topics

- [Understanding Organizations, page 15-7](#)
- [Configuring User Authentication, page 15-31](#)

Deleting Organizations

Assumptions

- ANM is installed and running.
- The organization exists in the ANM database.
- You have reviewed the guidelines for managing customer organizations (see [Guidelines for Managing Organizations, page 15-32](#)).

**Note**

Your user role determines whether you can use this option.

Procedure

-
- Step 1** Select **Admin > Role-Based Access Control > Organizations**.
- The Organizations list contains a list of the existing organizations.
- Step 2** Select the organization to be deleted.
- Step 3** Click **Delete**. All users, domains, and roles within that organization are removed.
-

Related Topics

[Configuring User Authentication, page 15-31](#)

Managing User Accounts

Use the User Management feature to specify the people that are allowed to log onto the system. The following sections describe how to manage user accounts:

- [Guidelines for Managing User Accounts, page 15-38](#)
- [Displaying a List of Users, page 15-38](#)
- [Creating User Accounts, page 15-39](#)
- [Duplicating a User Account, page 15-40](#)
- [Modifying User Accounts, page 15-41](#)
- [Deleting User Accounts, page 15-42](#)



Note

You can create users in the organization in which you are a member. You will see users only in the organizations in which you are a member.

Guidelines for Managing User Accounts

- User cannot log in until they have one domain and one user role associated via an organization. This can be the Default domain but a role must be specified.
- Users cannot be moved from one organization to another. Organizations are designed to be separate and distinct.

Displaying a List of Users

Procedure

Step 1	Select Admin > Role-Based Access Control > Organization > Users . A table of users, their role, and their domain appears.
Step 2	From this screen you can create a new user, duplicate, modify or delete any existing user to which you have access.

Related Topics

[Managing User Accounts, page 15-38](#)

Creating User Accounts


Note

Your user role determines whether you can use this option.

Procedure

- Step 1** Select **Admin > Role-Based Access Control > Organization > Users**. A list of users appears.
- Step 2** Click **Add**.
- Step 3** Complete the following required fields:

Table 15-4 **User Attributes**

Field	Description
Login Name	Specifies the name by which the user is to be identified in the system (up to 24 characters). Only letters, numbers, and underscore can be used. The field is case sensitive.
Name	Specifies the full name of the user. The format is free text.
Password	Allows you to specify a password for this user account.
Confirm	Renter the password for this account.
E-Mail	Specifies an e-mail address for this user.
Telephone#	Specifies a telephone number for this user. The format is free text with no embedded spaces.
Role	Specifies a predefined role from the list.
Domains	Allows you to use the Add and Remove buttons to select domains to which this user belongs.
Allowed login IP	Defines an IP address or a subnetwork from which the user is allowed to log in. You can define up to ten different addresses for a single user. Unless you specifically define IP addresses or subnetworks using this option, the user can log in from any IP address. When you enter an allowed single IP address or an allowed subnet, then the user is only allowed to log in from the specified addresses. To restrict access to a specific subnetwork, enter the IP address and the mask, for example, 10.1.200.60/255.255.255.0.
	 Note IP addresses 1.1.1.1 and 0.0.0.0 cannot be entered in this field.
Description	Enter any notes about the user.
firstmenu	Menu that displays when this user first logs in. Choose one from the pulldown menu.
Last login	Last time (local time) this user logged in.

- Step 4** Click **Save**. The Users table is displayed.

Related Topics[Managing User Accounts, page 15-38](#)

Duplicating a User Account

Use this option to create a new user account using settings from an existing user.

**Note**

Your user role determines whether you can use this option.

Procedure

- Step 1** Select **Admin > Role-Based Access Control > Organization > Users**. A table of users, their role and domain appears.
- Step 2** Select the user account you want to copy.
- Step 3** Click **Duplicate**.
- Step 4** At the prompt, enter a name for the new user account.
- Step 5** Click **OK**.
- The Users table appears with the new user account.
- Step 6** To make changes to the user account settings as shown in [Table 15-5](#).

Table 15-5 Duplicate User Attributes

Field	Description
Login Name	Name you specified when you created the user you want to duplicate. This is the name by which the user is to be identified in the system (up to 24 characters). Only letters, numbers, and underscore can be used. The field is case sensitive.
Name	Specifies the full name of the user. The format is free text.
E-Mail	Specifies an e-mail address for this user.
Telephone#	Specifies a telephone number for this user. The format is free text with no embedded spaces.
Role	Specifies a predefined role from the list.
Domains	Allows you to use the Add and Remove buttons to select domains to which this user belongs.
Allowed login IP	Defines an IP address or a subnetwork from which the user is allowed to log in. You can define up to ten different addresses for a single user. Unless you specifically define IP addresses or subnetworks using this option, the user can log in from any IP address. When you enter an allowed single IP address or an allowed subnet, then the user is only allowed to log in from the specified addresses. To restrict access to a specific subnetwork, enter the IP address and the mask, for example, 10.1.200.60/255.255.255.0.
	 Note IP addresses 1.1.1.1 and 0.0.0.0 cannot be entered in this field.
Description	Enter any notes about the user.

Table 15-5 Duplicate User Attributes

Field	Description
firstmenu	Menu that is displayed when this user first logs in. Choose one from the pulldown menu.
Last login	Last time (local time) this user logged in and the IP address that was used.

Step 7 Click **Save**.

Step 8 The Edit Organization User screen appears. Make any changes and click **Save**. When all the details are correct, click **Cancel**. The table of users is displayed.

Related Topics

[Managing User Accounts, page 15-38](#)

Modifying User Accounts



Note

Your user role determines whether you can use this option.

Procedure

- Step 1** Select **Admin > Role-Based Access Control > Organization > Users**. A table of users, their role, and domain appears.
- Step 2** Select the user account you want to modify.
- Step 3** Click **Edit**.
- Step 4** Modify any of the attributes in the attributes table (see [Table 15-4](#)).
- Step 5** Click **Save**.
- Step 6** The Edit User Details screen appears. Make any changes and click **Save**. When all the details are correct, click **Cancel**, the User Management table is displayed.

Related Topics

[Managing User Accounts, page 15-38](#)

Deleting User Accounts


Note

Your user role determines whether you can use this option.

Procedure

-
- Step 1** Select **Admin > Role-Based Access Control > Organization > Users**. A table of users, their role and domain appears.
- Step 2** Select the user account to be deleted, then click **Delete**.
- Step 3** Confirm deletion of the user by clicking **OK** or **Cancel** to return to the Users table.
The user account is removed from the ANM database.
-

Related Topics

[Managing User Accounts, page 15-38](#)

Displaying or Terminating Current User Sessions

You can view a list of the users currently logged into the system and end their sessions, if required.

You can only see the users in your organization.


Note

Your user role determines whether you can use this option.

Procedure

-
- Step 1** Select **Admin > Role-Based Access Control > Active Users**.
The Active User Sessions screen displays the following information for each active user who is logged in:

Table 15-6 **Active User Session Information**

Column	Description
Name	The name used to log into the Cisco ANM
Type of login	Method used to log in, for example WEB
Login from IP	IP address of host
Time of login	Time user logged in

- Step 2** To terminate an active session, click **Terminate**.
When a user session is terminated, the user is logged out of the interface from which the user session was initiated. If the user was making changes to a configuration, the configuration lock is released and any uncommitted configuration change is discarded.

If a user session is terminated while an operation is in progress, the current operation is not stopped, but any subsequent operation is denied.

For more details on terminating active users, see [Displaying or Terminating Current User Sessions](#), page 15-42.

Related Topics

- [Controlling Access to the Cisco ANM](#), page 15-2
- [Managing User Accounts](#), page 15-38

Managing User Roles

Use the Roles Management feature to add, modify, and delete user-defined roles and to modify predefined roles. You cannot delete predefined roles.

A user's role determines the tasks the user can access. Each role is associated with permissions or rules that define what feature access this role contains. For example, if you design a role that provides access to virtual servers, the role automatically includes access to all real servers that could be included in the virtual server.

The following sections describe how to manage user roles:

- [Guidelines for Managing User Roles](#), page 15-43
- [Displaying User Roles](#), page 15-46
- [Creating User Roles](#), page 15-46
- [Duplicating a User Role](#), page 15-47
- [Modifying User Roles](#), page 15-48
- [Deleting User Roles](#), page 15-48

Guidelines for Managing User Roles

- System Administrators can view and modify all roles.
- Organization administrator users can only see and modify the users, roles, and domains in their organization.
- Other users can only view the user, roles, and domains assigned to them.
- User-defined roles can be created but follow strict rules about which tasks can be selected or deselected. See the user interface for specific dependencies or [Table 15-2 on page 15-9](#) for role to task mapping information.
- You must have the ability to create real servers in your role and at least one virtual context in your domain before you can create real servers.
- 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.
- If you upgrade to ANM 1.2, any custom roles that are migrated retain their associations but have different role definitions. We encourage you to use the ANM 1.2 predefined default roles.

Understanding Predefined Roles

You must have one of the predefined roles in the Admin context in order to use the `changeto` command (which allows users to visit other contexts). Non-admin/user contexts do not have access to the `changeto` command; they can only visit their home context. Context administrators, who have access to multiple contexts, must explicitly log in to other contexts to which they have access.

The predefined roles and their default privileges are defined in [Table 15-7](#). For detailed information on RBAC, see the *Cisco 4700 Series Application Control Engine Appliance Virtualization Configuration Guide*.

Table 15-7 ANM 1.2 Predefined Role Tasks

Predefined Role	Description	Role Tasks/Operation Privileges ¹
ACE-Admin	Access to create virtual contexts and monitor threshold information.	- View Threshold - Create Device Events - Create Virtual Context+
ANM-Admin	Access to create virtual contexts and monitor threshold information. Provides access to all features and functions.	- Create ANM System - Create ANM User Access - Create ANM Inventory+
Network-Admin	Admin for L3 (IP and Routes) and L4 VIPs	- View Threshold - Create Switch - Create Routing - Create Interface - Create NAT - Create Connection
Network-Monitor	Monitoring for all features	View ANM Inventory+
Org-Admin	Access to create role-based access control and import and update device data.	- Create ANM User - Create ANM Inventory+
Security-Admin	Security features	- Create AAA - Modify Interface - Create NAT - Create Inspect - Create Connection

Table 15-7 ANM 1.2 Predefined Role Tasks

Predefined Role	Description	Role Tasks/Operation Privileges ¹
Server-Appln-Maintenance	Server maintenance and L7 policy application	- View Threshold - View VIP - View Virtual Inservice - Create LoadBalancer+
Server-Maintenance	Server maintenance, monitoring, and debugging	- View Threshold - View VIP+ - Modify Real Server - Debug Probe - Create Real Inservice
SLB-Admin	Load-balancing features	- View Threshold - Create Building Block - Modify Interface - Create Expert+
SSL-Admin	SSL feature features	Create SSL+

1. Where the plus sign (+) is indicated, all permissions included in this folder are included at the same privilege level, unless otherwise noted. For example, Virtual Contexts tasks are comprised of tasks such as AAA, Building Blocks, and so on. These tasks are depicted as columns in the Roles table.

Displaying User Role Relationships

Use this procedure to display which users are associated to specific roles.



Note

Your user role determines whether you can use this option.

Procedure

- Step 1** Select **Admin > Role-Based Access Control > Organizations > Roles**. A table of the defined roles and their settings appears.
- Step 2** Select a role and click **Users**. A screen displays a table containing the following:
- Name—User name
 - Role—Role name
 - Domain—Domain access for this user
- From this screen you can delete or duplicate a user.
- Step 3** Click **Close** to return to the Roles table.

Related Topics

- [Duplicating a User Account, page 15-40](#)
- [Managing User Roles, page 15-43](#)

Displaying User Roles

Use this option to display the existing user roles.

**Note**

Your user role determines whether you can use this option.

Procedure

-
- Step 1** Select **Admin > Role-Based Access Control > Organizations > Roles**. A table of the defined roles and their settings appears.
- Step 2** You can use the options in this screen to:
- Create a new role (see [Creating User Roles, page 15-46](#)).
 - View the users assigned to a role (see [Displaying User Role Relationships, page 15-45](#)).
 - Modify any existing role to which you have access (see [Modifying User Roles, page 15-48](#)).
 - Duplicate any existing role to which you have access (see [Duplicating a User Role, page 15-47](#)).
 - Delete any existing role to which you have access (see [Deleting User Roles, page 15-48](#)).
-

Related Topics

- [Understanding Operations Privileges, page 15-6](#)
- [Managing User Roles, page 15-43](#)

Creating User Roles

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

**Note**

Your user role determines whether you can use this option.

Procedure

-
- Step 1** Select **Admin > Role-Based Access Control > Organization > Roles**. A table of the defined roles and their settings appears.
- Step 2** Click **Add**. The New Role form appears.

Step 3 Enter the following attributes:

Table 15-8 *Role Attributes*

Attribute	Description
Name	The name of the role.
Description	A brief description of the role.
Role Tasks	A role tree that defines the operation privileges and features available to this role.
Resulting Menu Items	Displays a synchronized list of features in the form of menus that this role is able to access after setting the role task operation privileges.

Step 4 Click **Save**. The new role is added to the list of user roles.

Step 5 To assign this new role to one or more users, go to **Admin > Organizations > Users**. For detailed steps, see [Modifying User Accounts, page 15-41](#).

Related Topics

- [Understanding Operations Privileges, page 15-6](#)
- [Managing User Roles, page 15-43](#)

Duplicating a User Role

Use this option to create a new user-defined role from an existing one.



Note

Your user role determines whether you can use this option.

Procedure

- Step 1** Select **Admin > Role-Based Access Control > Organization > Roles**. A table of the defined roles and their settings appears.
- Step 2** Select the role you want to copy.
- Step 3** Click **Duplicate**.
- Step 4** At the prompt, enter a name for the new role.
- Step 5** Click **OK**.
- Step 6** Make any changes to the role settings.
- Step 7** Click **Save**.

Related Topics

- [Understanding Operations Privileges, page 15-6](#)
- [Managing User Roles, page 15-43](#)

Modifying User Roles

You can modify any user-defined roles.



Note

Your user role determines whether you can use this option.

Procedure

-
- Step 1** Select **Admin > Role-Based Access Control > Organization > Roles**. A table of the defined roles and their settings appears.
 - Step 2** Select the role you want to modify.
 - Step 3** Click **Edit**.
 - Step 4** Make the changes.
 - Step 5** Click **Save**.
-

Related Topics

- [Understanding Operations Privileges, page 15-6](#)
- [Managing User Roles, page 15-43](#)

Deleting User Roles

You can delete any user-defined roles.



Note

Your user role determines whether you can use this option.

Procedure

-
- Step 1** Select **Admin > Role-Based Access Control > Organization > Roles**. A table of the defined roles and their settings appears.
 - Step 2** Select the role to be deleted.
 - Step 3** Click **Delete**.
 - Step 4** Click **OK** to confirm the deletion. Users that have the deleted role no longer have that access.
-

Related Topics

[Managing User Roles, page 15-43](#)

Managing Domains

Network domains provide a means for organizing the devices and their components (physical and logical) in your network and permitting access according to the way your site is organized. You can allow access to a domain by assigning it to an organization. Examples are specific virtual contexts, or specific servers within a context.

The following sections describe how to manage domains:

- [Guidelines for Managing Domains, page 15-49](#)
- [Displaying Network Domains, page 15-50](#)
- [Creating a Domain, page 15-50](#)
- [Duplicating a Domain, page 15-51](#)
- [Modifying a Domain, page 15-52](#)
- [Deleting a Domain, page 15-52](#)

Guidelines for Managing Domains

- Domains are *logical* concepts. You do *not* delete a member of a domain when you delete the domain.
- Domains can include supported Cisco chassis, ACE modules, ACE appliances, and CSS or CSM devices, as well as their virtual contexts, building blocks, resource classes, and real and virtual servers.
- Select the Allow All setting to include current and future device objects in a domain.
- Objects must already exist in ANM. To add objects, see [Adding Network Devices into ANM, page 2-7](#).
- You must have the ability to create real servers in your role and at least one virtual context in your domain before you can create real servers.
- 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.
- Domains continue to display device information even after you remove that device from ANM. This allows the domain information to be easily reassociated if you reimport the device. The device name must remain the same for this to work properly.



Caution

Domain objects are hierarchical. If you include a parent object in a domain, the child object is also included even though they do not display in the Object selector tree when you add or edit domains.

For example:

- Inclusion of a Catalyst device includes all cards, virtual contexts, real servers and virtual servers
- Inclusion of an ACE 4710 includes all cards, virtual contexts, real servers and virtual servers
- Inclusion of a virtual context, CSM module or CSS device includes all associated objects

Related Topics

- [Creating a Domain, page 15-50](#)
- [Modifying a Domain, page 15-52](#)

- [Displaying Network Domains, page 15-50](#)
- [Duplicating a Domain, page 15-51](#)
- [Deleting a Domain, page 15-52](#)

Displaying Network Domains



Note

Your user role determines whether you can use this option.

Procedure

- Step 1** Select **Admin > Role-Based Access Control > Organization > Domains**. The Domains table appears.
- Step 2** Expand the table until you can see all the network domains.
- Step 3** Select a domain from the Domains table to view the settings for that domain, then click **Edit**.

Related Topics

- [Managing Domains, page 15-49](#)
- [Guidelines for Managing Domains, page 15-49](#)
- [Creating a Domain, page 15-50](#)
- [Duplicating a Domain, page 15-51](#)
- [Modifying a Domain, page 15-52](#)
- [Deleting a Domain, page 15-52](#)

Creating a Domain

Use this option to create a new domain.



Note

Your user role determines whether you can use this option.

Procedure

- Step 1** Select **Admin > Role-Based Access Control > Organization > Domains**. The Domains table appears.
- Step 2** Click **Add**.
- Step 3** For the new domain, enter the following information:

Table 15-9 Domain Attributes

Field	Description
Name	The name of the domain.
Description	The description of the domain.

Table 15-9 Domain Attributes

Field	Description
Allow all check box	Enables all objects within this domain (current and future objects). If left empty, the Objects tree displays.
Objects	The collection of objects which comprise this domain. Select an object name and use the arrows to move it from the available to selected column. For example, selecting a virtual context selects all real servers within that virtual context, or selecting a chassis selects the virtual contexts on that chassis. The interface does not explicitly display this in the table, but the objects are, in fact, selected. See Guidelines for Managing Domains, page 15-49 for domain rules about creating virtual contexts and real servers.

Step 4 Click **Save**.

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

Related Topics

- [Managing Domains, page 15-49](#)
- [Guidelines for Managing Domains, page 15-49](#)
- [Displaying Network Domains, page 15-50](#)
- [Creating a Domain, page 15-50](#)
- [Duplicating a Domain, page 15-51](#)
- [Modifying a Domain, page 15-52](#)
- [Deleting a Domain, page 15-52](#)

Duplicating a Domain

Use this option to create a new domain from an existing one.

**Note**

Your user role determines whether you can use this option.

Procedure

- Step 1** Select **Admin > Role-Based Access Control > Organization > Domains**.
- Step 2** Select the domain you want to copy.
- Step 3** Click **Duplicate**.
- Step 4** At the prompt, enter a name for the new domain, then click **OK**.
- Step 5** Click **Save**.

Related Topics

- [Managing Domains, page 15-49](#)
- [Guidelines for Managing Domains, page 15-49](#)
- [Displaying Network Domains, page 15-50](#)
- [Creating a Domain, page 15-50](#)
- [Modifying a Domain, page 15-52](#)
- [Deleting a Domain, page 15-52](#)

Modifying a Domain

Use this option to change the settings in a domain.

**Note**

Your user role determines whether you can use this option.

Procedure

-
- Step 1** Select **Admin > Role-Based Access Control > Organization > Domains**.
 - Step 2** Select the domain you want to change.
 - Step 3** Click **Edit**.
 - Step 4** Make the changes. For detailed domain attribute descriptions, see [Table 15-9 on page 15-50](#).
 - Step 5** Click **Save**.
-

Related Topics

- [Managing Domains, page 15-49](#)
- [Guidelines for Managing Domains, page 15-49](#)
- [Displaying Network Domains, page 15-50](#)
- [Creating a Domain, page 15-50](#)
- [Duplicating a Domain, page 15-51](#)
- [Deleting a Domain, page 15-52](#)

Deleting a Domain

Use this option to delete a network domain from the systems. You do *not* delete objects associated with that domain when you delete the domain.

**Note**

Your user role determines whether you can use this option.

Procedure

-
- Step 1** Select **Admin > Role-Based Access Control > Organization > Domains**.
The Domains list contains a list of the existing domains.
- Step 2** Select the domain you want to delete.
- Step 3** Click **Delete**. A prompt asks if you to confirm this action.
- Step 4** Click **OK**. The domain is removed from the ANM database.
-

Related Topics

- [Managing Domains, page 15-49](#)
- [Guidelines for Managing Domains, page 15-49](#)
- [Displaying Network Domains, page 15-50](#)
- [Creating a Domain, page 15-50](#)
- [Duplicating a Domain, page 15-51](#)
- [Modifying a Domain, page 15-52](#)

Managing ANM

When you select **Admin > ANM Management**, you can view the following information:

- ANM—Allows you to check the status of your ACE. See [Checking the Status of the ANM Server, page 15-54](#).
- License Management—Displays the license information stored in the ACE hardware. See [Managing ANM Licenses, page 15-56](#).
- Statistics—Displays the ANM server statistics. See [Viewing ANM Server Statistics, page 15-62](#).
- Statistics Collection—Allows you to enable or disable ANM server statistic collection. See [Configuring ANM Statistics Collection, page 15-63](#).
- Audit Log Settings—Allows you to determine how long audit log records are kept. See [Configuring Audit Log Settings, page 15-63](#).
- Change Audit Log—Displays ANM server logs. See [Viewing Change Audit Logs, page 15-64](#).
- Auto Sync Settings—Allows you to allow ANM to automatically sync with CLI when it detects out of band changes between itself and the ACE. See [Configuring Auto Sync Settings, page 15-65](#).

Checking the Status of the ANM Server

The ANM server can be configured either as:

- A non-HA ANM. The non-HA ANM consists of only one host and is referred to as a standalone ANM.
- An HA (high availability or fault-tolerant) ANM, which consists of two hosts: an active ANM and a standby ANM. An HA ANM has a virtual IP address that is always assigned to the active ANM. Users log into this virtual IP address—they never log into the real IP addresses of the hosts. In addition, an HA ANM has a secondary NIC and IP address on each host over which “heartbeat” messages are used to arbitrate which host is active and which is standby.

**Note**

Your user role determines whether you can use this option.

Use this option to check if ANM has a backup server and to view the server status.

Procedure

Step 1 Select **Admin > ANM Management > ANM**.

The ANM Server status screen appears. This screen contains the following information:

Table 15-10 ANM Server Status Information

Field	Description
HA Replication State	Options: - OK—This is an HA ANM and it is running properly. - Standalone—This is a non-HA ANM, and therefore the HA attributes and operations are not meaningful. - Stopped—This is an HA ANM and database replication has stopped. Under normal circumstances this is a transitory state. - Failed—This is an HA ANM and database replication cannot proceed. Most likely this is because the standby ANM is not alive or is unreachable.
Version	The version of the ANM software.
Build Number and Build Timestamp	Build identification information.
Time Server Started	The date and time the ANM server started.
Virtual IP Address	Virtual IP address that associates with the active host. This IP address must be on the same subnet as the primary IP addresses of both Node 1 and Node 2.
Active Name	Name of Node 1, which can be displayed by issuing the uname -n command on the host.
Active IP	IP address used by Node 1 for normal (non-heartbeat related) communication. This IP address must be on the same subnet as the primary address for Node 2.
Active Heartbeat IP	IP address associated with the crossover network interface for Node 1. This IP address must be on the same subnet as the Heartbeat IP address for Node 2.
Standby Name	Name of Node 2, which can be returned by issuing the uname -n command on the host.
Standby IP	IP address used by Node 2 for normal (non-heartbeat related) communication. This IP address must be on the same subnet as the primary IP address for Node 1.
Standby Heartbeat IP	IP address associated with the crossover network interface for Node 2. This IP address must be on the same subnet as the Heartbeat IP address for Node 1.

Table 15-10 ANM Server Status Information (continued)

Field	Description
License Server State	Options: - OK—There is a valid license on the host. - Invalid—The host either contains an invalid license or there is no license present. - Unknown—It is not possible to communicate with the host's license manager, therefore, the license state is unknown. Note The Unknown and Invalid states will not display for the active (local) ANM. If the standby ANM has an Invalid license state, you should install a valid license. If the standby ANM has an Unknown license state, check that the standby ANM has been installed correctly. - DEMO—Used for the demonstration purposes. It lasts for 30, 60, or 90 days from the issue day of the license. It allows you to use all features.
Standby License Server State	

Related Topics

- Managing ANM Licenses, page 15-56
- Viewing ANM Server Statistics, page 15-62
- Configuring ANM Statistics Collection, page 15-63

Managing ANM Licenses

Cisco Application Networking Manager manages software licenses for the ANM server as well as ACE devices. For information about managing ACE licenses, see [Managing ACE Licenses, page 3-27](#). For a complete list of supported devices, see the *Supported Devices Table for the Cisco Application Networking Manager 1.2*.

Since ANM is licensed, it requires a software license key to work properly. You may be required to purchase another server license if you are using a backup server. ANM may also need additional software licenses to run large networks with many ACE devices and modules.

**Note**

ANM uses TCP port 10444 for the ANM License Manager. For other port numbers, see [Appendix A, “ANM Ports Reference.”](#)

Use this feature to view license state, add license files, and track license compliance information on your ANM.

This topic contains the following tasks:

- [Adding Licenses into License Management, page 15-58](#)
- [Viewing Licenses in License Management, page 15-59](#)

- [Checking on License Compliance, page 15-60](#)
- [Ordering ANM Licenses, page 15-61](#)
- [Removing Licenses Files, page 15-61](#)

For more details on ANM licenses, see [Understanding ANM License Information, page 15-57](#) or the *Installation Guide for the Cisco Application Networking Manager 1.2*.

Related Topics

- [Understanding ANM License Information, page 15-57](#)
- [Preparing Devices for Import, page 2-4](#)
- [Managing ACE Licenses, page 3-27](#)

Understanding ANM License Information

When you install ANM 1.2 for the first time you need to add a license from the command line before you can access ANM. See the *Installation Guide for the Cisco Application Networking Manager 1.2* for instructions.

ANM requires licenses to manage virtual devices and to run the ANM server or servers.

[Table 15-11](#) describes the various licenses and their purpose.

Table 15-11 ANM License Descriptions

License Name	Description
ANM-AD-<count> ANM-AD-20	Where A stands for ACE and D stands for devices. This product ID allows <count> number of ACE devices/modules to be managed by ANM. If you have purchased two ANM-AD-10, it means that ANM is allowed to manager 20 ACE devices. The maximum number of ACE devices can be managed by one ANM server is no more than 50.
ANM-CD-<count> ANM-CD-10	Where A stands for ACE and C stands for CSS or CSM devices/modules supported.
ANM-AV-<supported # of virtual contexts> ANM-AV-100	Where A stands for ACE and V stands for virtual contexts. This license allows ANM to manage one ACE module/device which has an ACE license supporting <number of virtual context>. If you have three ACE modules with two supporting 50 virtual contexts each (ACE-VIRT-050) and one ACE supporting 250 contexts (ACE-VIRT-250), then you are required to have either two ANM-AV-50 licenses or one ANM-AV-50 licenses with count of two and one ANM-AV-250. The interpretation of <supported number of virtual contexts> in ANM-AV is different from <count> in ANM-AD.
ANM-DEMO or DEMO	Used for the demonstration purposes. It lasts for 30, 60, or 90 days from the issue day of the license. It allows you to use all features.
ANM-SERVER-XX or ANM-SERVER-XX-H	Used to allow access to the ANM server. Use ANM-SERVER-XX for standalone or primary servers and ANM-SERVER-XX-H for your backup server when running HA.

Related Topics

- [Managing ACE Licenses, page 3-27](#)
- [Managing ANM Licenses, page 15-56](#)
- [Viewing Licenses in License Management, page 15-59](#)
- [Adding Licenses into License Management, page 15-58](#)
- [Ordering ANM Licenses, page 15-61](#)
- [Removing Licenses Files, page 15-61](#)

Adding Licenses into License Management

Use this procedure to add new ANM licenses to expand the number of network devices you can manage.

**Note**

Your user role determines whether you can use this option.

Procedure

- Step 1** Select **Admin > ANM Management > License Management > Licenses**. The Licenses table appears.
- Step 2** Click **Install**. The New License screen appears.
- Step 3** Click **Browse** to locate the new license name. Use the browser to select the license file.
- Step 4** Click **Upload** to copy the license you entered onto the ANM Server or **Cancel** to exit.

The license file appears in the Licenses table as well as in the License Files table. From the Licenses table you can also filter, add more licenses, or alter table views. See [Table 1-3 on page 1-9](#) for a description of the table buttons.

From the License Files table you can see the Install Status of the license file and if there are any errors. See [Viewing Licenses in License Management, page 15-59](#) for details on what steps to do next.

Related Topics

- [Managing ACE Licenses, page 3-27](#)
- [Managing ANM Licenses, page 15-56](#)
- [Viewing Licenses in License Management, page 15-59](#)
- [Understanding ANM License Information, page 15-57](#)
- [Ordering ANM Licenses, page 15-61](#)
- [Removing Licenses Files, page 15-61](#)

Viewing Licenses in License Management

Use this procedure to view ANM licenses that allow you to expand the number of network devices you can manage.

Procedure

Step 1 Select **Admin > ANM Management > License Management > Licenses**.

The License table appears. If there are license files, the License Files table also appears on the same page. This screen contains the following information (see [Table 15-12](#) and [Table 15-13](#)):

Table 15-12 ANM License Information

Field	Description
Name	Contains the license type name information about how many virtual contexts can be allocated on an ACE, as well as ANM license information. - ANM_DEMO—Temporary 30, 60, or 90 day licenses; three free demos allowed. - ANM_SERVER—Enables management of one ANM and two ACE devices; neither can have an ACE VIRT license (ACE_VIRT_100). Licenses contained a -H correspond to a standby ANM-SERVER node. - ANM_AD—Management of devices 5, 10, 20, 50 (ANM-AD-20). - ANM_CD—Enables management of CSS or CSM devices/modules. - ANM_AV_xxx—Enables management of 20, 50, 100, or 250 virtual contexts. For details on how to understand license name acronyms, see Understanding ANM License Information, page 15-57.
Installed Server	Indicates whether the license is installed on an active or standby ANM server. This field displays only when ANM is in HA mode.
File Name	The name of the license file you installed on the ACE appliance.
Vendor	Name of vendor that supplied the license.
Expiry Date	Date license expires. If no expiration, permanent displays.
Maximum Count	Number of licenses available (purchased).

Table 15-13 License Files

Field	Description
File Name	The name of the license file you installed on the ANM host.
Install Status	Status of the license file. Any licensing errors display here. If errors display, see Removing Licenses Files, page 15-61 for details on how to remove this file and import a working file.

From this table you can also filter, add, or alter table views. See [Table 1-3 on page 1-9](#) for a description of the table buttons.

Related Topics

- Managing ACE Appliance Licenses in *Installation Guide for the Cisco Application Networking Manager 1.2*
- [Understanding ANM License Information, page 15-57](#)
- [Adding Licenses into License Management, page 15-58](#)
- [Ordering ANM Licenses, page 15-61](#)
- [Managing ANM Licenses, page 15-56](#)
- [Removing Licenses Files, page 15-61](#)
- [Managing ACE Licenses, page 3-27](#)

Checking on License Compliance

Use this procedure to verify that the ANM licenses in your network are compliant with your ACE licenses.

Procedure

Step 1 Select **Admin > ANM Management > License Management > Compliance**.

The License Compliance table displays (see [Table 15-14](#)).

Table 15-14 License Compliance

Field	Description
License Type	Lists types of licenses found. See Understanding ANM License Information, page 15-57 .
HA	Displays Active when in HA mode or non-HA mode. Disregard this column if you are running a standalone server.
Total	Number of licenses present. Corresponds to maximum count on the Licenses table.
Used	Number of licenses in use.
Remaining	Number of licenses available for use. A negative number displays in red if there are not enough licenses for the network devices you are managing. A number displays highlighted in yellow if the number of licenses used is equal to the total licenses you have purchased.
Expiration	Expiration date (if temporary license).

Step 2 Click **Refresh** to update the licenses in this window.

Related Topics

- [Understanding ANM License Information, page 15-57](#)
- [Adding Licenses into License Management, page 15-58](#)
- [Ordering ANM Licenses, page 15-61](#)
- [Updating ACE Licenses, page 3-31](#)
- [Managing ACE Licenses, page 3-27](#)

Ordering ANM Licenses

If you need to purchase additional ANM licenses in order to be compliant with the number of ACE licenses you are managing, contact your sales team or use Cisco.com to place your order. After you receive your PAK information, you can then access the Cisco Product License Registration web site page at <http://www.cisco.com/go/license>. The Cisco Product License Registration web site provides you with license key/files that you can upload to ANM and ensure your compliance with software requirements.

If you already have your Product Activation Key (PAK), you can manually use the Cisco web site to obtain licenses or you can use the Cisco License Manager. Cisco License Manager performs license fulfillment for you and also deploys the licenses to network devices using a wizard-based GUI.

Related Topics

- [Managing ANM Licenses, page 15-56](#)
- [Understanding ANM License Information, page 15-57](#)
- [Adding Licenses into License Management, page 15-58](#)
- [Viewing Licenses in License Management, page 15-59](#)
- [Checking on License Compliance, page 15-60](#)
- [Managing ACE Licenses, page 3-27](#)

Removing Licenses Files

If your license files will not work in the ANM due to file errors, you need to remove them from the ANM host and request another license file from Cisco. There is no remove license command. You can remove the license from the operating system by deleting the file.

Procedure

-
Step 1	Log in as the root user.
Step 2	To remove the license file, enter: rm /opt/CSCOanm/etc/license/<ANM_LICENSE_FILE> The license file is removed from the ANM host only. The license on your managed device is still valid.
Step 3	Restart ANM to allow it to update the licenses table data. To restart ANM, see instructions in the <i>Installation Guide for the Cisco Application Networking Manager 1.2</i> . To request another license from Cisco to replace the one that had errors, open a service request using the TAC Service Request Tool or call the Technical Assistance Center. Then add the license into ANM.
-

Related Topics

- [Managing ANM Licenses, page 15-56](#)
- [Understanding ANM License Information, page 15-57](#)
- [Adding Licenses into License Management, page 15-58](#)
- [Viewing Licenses in License Management, page 15-59](#)
- [Ordering ANM Licenses, page 15-61](#)

Viewing ANM Server Statistics

Use this procedure to display ANM statistics (for example, CPU, disk, and memory usage on the ACE).

Procedure

- Step 1** Select **Admin > ANM Management > Statistics**. The statistics viewer displays the fields in [Table 15-15](#).

Table 15-15 *ACE Server Statistics*

Name	Description
Owner	Process where statistics are collected.
Statistic	Includes the following statistics: • CPU Usage—Overall ACE CPU busy percentage in the last 5-minute period. • Disk Usage—Amount of disk space being used by the ANM server or ACE appliance. • Memory Usage—Amount of memory being used by the ANM server or ACE hardware. • Process Uptime—Amount of time since this system was last initialized, or the amount of time since the network management portion of the system was last reinitialized.
Value	Value of the statistic.
Description	Information the statistic gathered.

Related Topics

- [Checking the Status of the ANM Server, page 15-54](#)
- [Configuring ANM Statistics Collection, page 15-63](#)

Configuring ANM Statistics Collection

Use this procedure to enable ACE server statistics polling.

Procedure

-
Step 1	Select Admin > ANM Management > Statistics Collection . The Primary Attributes configuration screen appears.
Step 2	In the Polling Stats field, select Enable to start background polling or Disable to stop background polling.
Step 3	In the Background Polling Interval field, select the polling interval appropriate for your networking environment.
Step 4	Click Deploy Now to save your entries.
-

Related Topics

- [Viewing ANM Server Statistics, page 15-62](#)
- [Checking the Status of the ANM Server, page 15-54](#)

Configuring Audit Log Settings

Audit Log Purge Settings allow you to specify the following:

- How many days the log records in the database will be kept (default is 31).
- The maximum of log records that will be stored in the ANM database (default 100,000).

Audit Log File Purge Settings allows you to specify the following:

- The number of days worth of log record files that will be stored in the ANM database (default 31 days).
- The number of daily rolling files that will be stored in the ANM database (default 10 files each day, allowable file size is 2 Megabytes and is not configurable).

Use this procedure to determine how long audit logs are kept in the database.

Procedure

-
Step 1	Select Admin > ANM Management > Audit Log Settings . The Audit Log Settings configuration screen appears. Audit Log Purge Settings fields let you determine whether audit log table entries will be deleted after a certain number of days (default is 31 days) or after the table entries reach a certain size (default is 100 entries).
Step 2	Enter the greatest number of days you would like entries to be retained in the Number of Days field.
Step 3	Enter the maximum amount of log records to be stored in the ANM database in the audit log tables in the Number of Entries (Thousand) field (default 100,000). Audit Log File Purge Settings fields let you determine whether to retain log files according by age (default is 31 days) or by amount saved in a given day (default is 10 entries).

- Step 4** Enter the greatest number of days you would like entries to be retained in **Number of Days** field.
- Step 5** Enter the greatest number of log files you would like retained in **Number of Daily Rolling Log Files** field.
- Step 6** Click:
- **Reset to Default** to erase changes and restore the default values.
- or
- **Save Now** to save your entries.
-

Related Topics

- [Configuring Audit Log Settings, page 15-63](#)
- [Viewing Change Audit Logs, page 15-64](#)

Viewing Change Audit Logs

Any key or change related activities to the ANM server will be logged and viewed according to your role. Use this procedure to display ANM change audit logs for example, user login attempts, create/update/delete objects such as RBAC, Global Resource Class, Credential, device group, and threshold setting.

Procedure

- Step 1** Select **Admin > ANM Management > ANM Change Audit Log**. The audit log displays the fields in [Table 15-16](#).

Table 15-16 Server Audit Log

Name	Description
Time	Server time stamp when user action is complete.
Client IP	IP address where action originated.
User	Email address in the following format: <i>username@organization name</i> for example, <i>admin@cisco.com</i> .
Message	Boilerplate text descriptive of action taken, usually self-explanatory (for example “User authentication succeeded.”)

Related Topics

- [Device Audit Trail Logging, page 14-23](#)
- [Checking the Status of the ANM Server, page 15-54](#)
- [Configuring Audit Log Settings, page 15-63](#)

Configuring Auto Sync Settings

Use this procedure to configure ANM server auto sync settings.

Procedure

-
Step 1	Select Admin > ANM Management > ANM Auto Sync Settings . The Setup ANM auto-sync settings screen appears.
Step 2	In the ANM Auto sync field, select one of the following: Enable to have the ANM server automatically sync with ACE CLI when it detects out of band changes. or Disable to have the ANM server warn but not take independent action when it detects out of band changes between the server and ACE CLI.
Step 3	In the Polling Interval field, select the polling interval you would like the ANM server to employ.
Step 4	Click OK to save your entries.
-

Related Topic

[Synchronizing Virtual Context Configurations, page 3-66](#)

Lifeline Management

Use the troubleshooting and diagnostics tools provided by the Lifeline feature to report a critical problem to the Cisco support line and generate a diagnostic package. For more information about this feature, see [Using Lifeline, page 16-3](#).



CHAPTER 16

Troubleshooting Cisco Application Networking Manager Problems

Revised Date: 3/25/09

Topics in the section include:

- [Changing Configuration Property Values, page 16-1](#)
- [Discovering and Adding a Device Does Not Work, page 16-3](#)
- [Using Lifeline, page 16-3](#)
- [Backing Up and Restoring Data, page 16-7](#)

For additional troubleshooting information, see the *Installation Guide for the Cisco Application Networking Manager 1.2*.

Changing Configuration Property Values

After you have installed the ANM, you can reconfigure ANM ports and some other ANM configuration properties.



Caution

Remember if you enable HTTP, you are making your connection to the ANM less secure.

To reconfigure ports or other ANM configuration properties, complete the following steps:

-
- Step 1** Log in as the root user.
- Step 2** Enter one of the following:
- For a standard configuration change: `/opt/CSCOanm/bin/anm-tool configure`
 - To switch from a HA to a non-HA system configuration: `/opt/CSCOanm/bin/anm-tool --ha=0 configure`
 - To switch from a non-HA to a HA system configuration: `/opt/CSCOanm/bin/anm-tool --ha=1 configure`
- Step 3** When prompted **Keep existing ANM configuration? [y/n]:** enter **n**.
You are prompted for the same configuration information as was presented during installation.
- Step 4** For each configuration property, the current value is displayed in square brackets.

Do one of the following:

- To accept the value for a configuration property, press **Enter**.
- To change a configuration property, enter the appropriate information.

Step 5 When you have accepted or changed all of the configuration property values, a list of all the properties is displayed and you are prompted:

Commit these values? [y/n/q]:

Do one of the following:

- To accept the value and restart the ANM, enter **y**.
- To go through the list of configuration properties again, enter **n**.
- To retain the original property values and exit the configuration session, enter **q**.



Tip

If you receive errors when attempting to change the HA properties configuration values after installing ANM, check the node ID to be sure they are not switched.

The following is an example of a configuration session for an HA system. Non-HA systems will not contain any HA properties, but will include some limited property value configuration. The values shown in the brackets are the currently configured values.

```
/opt/CSCOanm/bin/anm-tool configure
Configuring ANM

Checking ANM configuration files
Keep existing ANM configuration? [y/n]: n
Creating config file (/opt/CSCOanm/etc/cs-config.properties)

Data directory [/var/lib/anm]:
HTTP Port of Web Server [10080]:
Enable HTTP for Web Server [false]:
HTTPS Port of Web Server [10443]:
Enable HTTPS for Web Server [true]:
HA Node 1 UName [rh23.cisco.com]:
HA Node 2 UName [rh25.cisco.com]:
HA Node 1 Primary IP [192.168.65.23]:
HA Node 2 Primary IP [192.168.65.25]:
HA Node 1 HeartBeat IP [12.12.12.2]:
HA Node 2 HeartBeat IP [12.12.12.1]:
HA Virtual IP [192.168.65.126]:
HA Node ID [2]:

These are the values:
Data directory: /var/lib/anm
HTTP Port of Web Server: 10080
Enable HTTP for Web Server: false
HTTPS Port of Web Server: 10443
Enable HTTPS for Web Server: true
HA Node 1 UName: rh23.cisco.com
HA Node 2 UName: rh25.cisco.com
HA Node 1 Primary IP: 192.168.65.23
HA Node 2 Primary IP: 192.168.65.25
HA Node 1 HeartBeat IP: 12.12.12.2
HA Node 2 HeartBeat IP: 12.12.12.1
HA Virtual IP: 192.168.65.126
```



```
HA Node ID: 2

Commit these values? [y/n/q]: y
Committing values ... done
Keeping existing configuration: /opt/CSCOanm/lib/java/thirdparty/ctm_config.txt

Stopping services
Stopping monit services (/etc/monit.conf) ... (0)
Stopping monit ... Stopped
Stopping heartbeat ... Stopped
Stopping mysql ... Stopped

Installing system configuration files

Setting service attributes
Enabling mysql for SELinux
setsebool: SELinux is disabled.
Service monit is started by OS at boot time

Starting mysql ... Started

Configuring mysql
Checking mysql user/password
Setting mysql privileges
Disabling mysql replication
Setting up database
extracting anmdb.sql ... done
executing anmdb.sql ... done

Starting services
Starting monit ... Started
```

Discovering and Adding a Device Does Not Work

After IP discovery checked the network and made a list of devices of each type, the device import may have failed when you tried to import the device. The device import may not have worked because IP discovery uses Telnet and SNMP to discover potential devices, while ANM requires SSH to import a device. So it is likely that IP discovery may have found some devices that cannot be imported or may not have found devices that could be imported.

To update the device so that it can be imported by ANM, see [Preparing Devices for Import, page 2-4](#).

To add the device, use the Config > Devices > Add method. For detailed procedures, [Adding Network Devices into ANM, page 2-7](#).

Using Lifeline

Diagnosing network or system-related problems that happen in real time can consume a considerable amount of time and lead to frustration even for a system expert. When a critical problem occurs within the ANM system or the network components managed by the ANM, you can use the troubleshooting and diagnostics tools provided by the Lifeline feature to report to the Cisco support line and generate a diagnostic package. Support engineers and developers can subsequently reconstruct your system and debug the problem using the comprehensive information captured in the lifeline.

Lifeline takes a snapshot of the running system configuration, status, buffers, logs, thread dumps, messages, CLI device configuration commands, device **showrun** commands, and so on. It gathers a period of historical network and system events that have been recorded directly preceding the event. If required, Lifeline can back up and package the ANM database or a file subdirectory or trace and package a period of traffic flow packets for a specified virtual context.

The following sections describe how to use the Lifeline feature:

- [Guidelines for Using Lifeline, page 16-4](#)
- [Creating a Lifeline Package, page 16-4](#)
- [Downloading a Lifeline Package, page 16-5](#)
- [Adding a Lifeline Package, page 16-6](#)
- [Deleting a Lifeline Package, page 16-7](#)

Guidelines for Using Lifeline

Lifelines can be created when unwanted events occur. Under such circumstances, available resources could be extremely low (CPU and memory could be nearly drained). You should be aware of the following:

- Create a Lifeline package after you encounter a problem that might require customer support assistance. The package is meant to be viewed by customer support.
- Lifeline collects debug data from diagnostic generators based on priority – most important to least important. When the total data size reaches 200MB, the collector stops collecting, and data from generators with lower priorities can be lost. For details on content, size, time, state, and any dropped data, see the Readme file included in each Lifeline package.
- Lifeline collects the last 25 MB of data from the file and truncates the beginning content.
- Lifelines are automatically packaged by the system in zip files. The naming convention for a lifeline package is “lifeline-yyMMdd-hhmmss.zip”. For example, lifeline-07062-152140.zip is a Lifeline package created at 3:21:40 PM, June 22, 2007.
- Only one Lifeline package is created at a time. The system will reject a second request made before the first Lifeline has been packaged.
- Lifeline times out in 60 minutes.
- A maximum of 20 Lifeline packages are stored at a time.

Creating a Lifeline Package

Use this procedure to create a package.

Assumptions

- ANM is installed and running.
- You have reviewed the guidelines for managing lifelines (see [Guidelines for Using Lifeline, page 16-4](#)).
- You have opened a case with Cisco technical support.

Procedure

**Note**

Your user role determines whether you can use this option.

- Step 1** Select **Admin > Lifeline Management**.
- Step 2** Enter a description for the package (required). This can include information about why the package is being created, who requested the package, and so forth.
- Step 3** Click **Save**. The package is created in the following format: lifeline-yyMMdd-hhmmss.zip, and displays in the Lifelines pane. The package size, name, and generation date display in the New Lifeline window.

**Note**

Do not perform any module maintenance until the package is created.

After the package is created, you can:

- Click **Download** to save the package to a directory on your computer or to view the package contents—See [Downloading a Lifeline Package, page 16-5](#).
- Click **Add** to add the package to the ANM database—See [Adding a Lifeline Package, page 16-6](#).
- Click **Delete** to delete the package—See [Deleting a Lifeline Package, page 16-7](#).

Related Topics

- [Using Lifeline, page 16-3](#)
- [Creating a Lifeline Package, page 16-4](#)
- [Adding a Lifeline Package, page 16-6](#)
- [Downloading a Lifeline Package, page 16-5](#)

Downloading a Lifeline Package

Use this procedure to download a package for viewing or saving to your local drive.

Assumption

You have created a package (see [Creating a Lifeline Package, page 16-4](#)).

Procedure

**Note**

Your user role determines whether you can use this option.

- Step 1** Select **Admin > Lifeline Management**.
- Step 2** Select the package from the list.
- Step 3** Click **Download**. The package is sent to your web browser, with which you can save or view the package.

**Note**

Do not perform any module maintenance until the package download to your web browser has completed.

Related Topics

- [Using Lifeline, page 16-3](#)
- [Creating a Lifeline Package, page 16-4](#)
- [Adding a Lifeline Package, page 16-6](#)
- [Deleting a Lifeline Package, page 16-7](#)

Adding a Lifeline Package

Use this procedure to add a package to the ANM database.

Assumption

You have created a package (see [Creating a Lifeline Package, page 16-4](#)).

Procedure**Note**

Your user role determines whether you can use this option.

Step 1 Select **Admin > Lifeline Management**.

Step 2 Click **Add**. The package is added to the Lifelines list, and the screen refreshes.

**Note**

Do not perform any module maintenance until the package is added to the list.

Related Topics

- [Using Lifeline, page 16-3](#)
- [Creating a Lifeline Package, page 16-4](#)
- [Downloading a Lifeline Package, page 16-5](#)
- [Deleting a Lifeline Package, page 16-7](#)

Deleting a Lifeline Package

Use this procedure to delete a package.

Procedure



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

-
- Step 1** Select **Admin > Others > Lifeline Management**.
- Step 2** Select the package from the list, then click **Delete**.
A message requests you confirm the deletion.
- Step 3** Click **OK** to delete the package.
-

Related Topics

- [Using Lifeline, page 16-3](#)
- [Creating a Lifeline Package, page 16-4](#)
- [Adding a Lifeline Package, page 16-6](#)
- [Downloading a Lifeline Package, page 16-5](#)

Backing Up and Restoring Data

These procedures enable you to backup ANM's configuration and restore it if necessary. This section contains the following topics:

- [Backing Up Data, page 16-7](#)
- [Restoring Data, page 16-8](#)

Backing Up Data

Assumptions

MySQL must be running to perform the backup.

Procedure

-
- Step 1** Log in as the root user as follows:



Caution

As the root user, you can adversely affect your operating environment if you are unaware of the effects of the commands you use. If you are a relatively inexperienced Linux user, limit your activities as the root user to the tasks described in this procedure.

- If you are not logged in, log in as the root user:
>login: root

>Password: root-password

- If you are already logged in, but not as the root user, use the **su** command to change your login to root:

su

Password: root-password

Step 2 Verify ANM servers are running by entering the following command:

/opt/CSCOanm/bin/anm-tool info-services

Step 3 Back up the ANM configuration by entering the following command:

/opt/CSCOanm/bin/anm-tool backup *backup-file*

where *backup-file* is the name of the file that you want to back up.

Related Topics

[Restoring Data, page 16-8](#)

Restoring Data

Use this procedure to restore ANM configuration data.



Note

You must restore the data on the same version of ANM on which you performed the back up. Restoring data to a different version of ANM is not supported in this release.

Procedure

Step 1 Log in as the root user as follows:



Caution

As the root user, you can adversely affect your operating environment if you are unaware of the effects of the commands you use. If you are a relatively inexperienced Linux user, limit your activities as the root user to the tasks described in this procedure.

- If you are not logged in, log in as the root user:

>login: root

>Password: root-password

- If you are already logged in, but not as the root user, use the **su** command to change your login to root:

su

Password: root-password

Step 2 Verify the ANM servers are running by entering the following command:

/opt/CSCOanm/bin/anm-tool info-services

Step 3 Restore the data by entering the following command:

```
/opt/CSCOanm/bin/anm-tool restore backup-file
```

where *backup-file* is the name of the file you want to restore.

ANM automatically restarts.

Related Topics

[Backing Up Data, page 16-7](#)



Draft - CISCO CONFIDENTIAL

APPENDIX A

ANM Ports Reference

Revised Date: 3/25/09

ANM uses specific ports for its processes. For more details on the ports and key words, see the following sections:

- [TCP Ports Used by ANM](#)
- [UDP Ports Used by ANM](#)

TCP Ports Used by ANM Processes

[Table A-1](#) lists the TCP ports that are used by ANM 2.0 for its processes.

Table A-1 TCP Ports Used by ANM

Port	Keyword	Description
80		ANM HTTP (default port used in ANM 1.2 and 2.0)
443		ANM HTTPS (default port used in ANM 1.2 and 2.0)
3306	mysql	MySQL Database system
8083		HTTP WME HTTP
9082		DAL JMX
10003		ANM DOE (Distributed Object Environment)
10004		ANM DOE
10023		ANM CLI
10080		ANM HTTP (default port used in ANM 1.1)
10443		ANM HTTPS (default port used in ANM 1.1)  Note If you do not have port 10443 open for communication between the ANM host server and an ACE 4710 you will receive an error message. ANM uses port 10443 to communicate to the ACE 4710 device because the appliance uses 443 for the embedded ACE Device Manager.
10444	lm	ANM License Manager

Table A-1 TCP Ports Used by ANM (continued)

Port	Keyword	Description
10445	lm	ANM License Manager
40000		DAL CSTM Registry
40001		DAL Inter-process between remote managed objects (RMO) and device access layer (DAL)
40002		ANM CSTM
40003		IP Discovery

UDP Ports Used by ANM

[Table A-2](#) lists the UDP ports that are used by ANM for backend processes.

Table A-2 UDP Ports Used by ANM

Port	Keyword	Description
161		SNMP trap
162	SNMPTRAP	SNMP trap
514		SYSLOG
10003		ANM DOE

For more information on ports, and a detailed listing of well known ports used by ANM, see “Application Networking Manager Ports Reference” in Appendix A in the online help or the *User Guide for Cisco Application Networking Manager 2.0*.



GLOSSARY

Revised: 3/25/09

A

- ACE** Cisco Application Control Engine, available as a module that resides in a Cisco Catalyst 6500 series chassis, Cisco 7600 series router, or as a standalone appliance. The ACE offers high-performance server load balancing (SLB), routing and bridging configuration, traffic policies, redundancy (high availability), virtualization for resource management, SSL, security features, and application acceleration and optimization.
- ACL** Access Control List. A mechanism in computer security used to enforce privilege separation. An ACL identifies the privileges and access rights a user or client has to a particular object, such as a server, file system, or application.
- activate** Places an entity into the resource pool for load balancing content requests or connections and starts the keepalive function. *See also* [suspend](#).
- administrative distance** The first criterion a router uses to determine which routing protocol to use if two protocols provide route information for the same destination. Administrative distance is a measure of the trustworthiness of the source of the routing information. Administrative distance has only local significance, and is not advertised in routing updates.
- The smaller the administrative distance value, the more reliable the protocol. The values range from 0 (zero) for a connected interface and 1 for a static route, to 255 for an unknown protocol.
- AES** Advanced Encryption Standard. One of the possible encryption algorithms available for use in SNMP communications.
- ARP** Address Resolution Protocol. Internet protocol used to map an IP address to a MAC address. Defined in RFC 826.

B

- building block** Reusable configuration attributes which can be applied to virtual contexts for consistent, standardized implementation.
- BVI** Bridge-Group Virtual Interface. Logical Layer 3-only interface associated with a bridge group when integrated routing and bridging (IRB) is configured.

C

CCM	Cisco CallManager. A Cisco product that provides the software-based, call-processing component of the Cisco IP Telephony Solutions for the Enterprise, part of Cisco AVVID (Architecture for Voice, Video, and Integrated Data). CallManager acts as a signaling proxy for call events initiated over other common protocols such as SIP , ISDN (Integrated Services Digital Network), or MGCP (Media Gateway Control Protocol).
certificate chain	A certificate chain is a hierarchal list of certificates used in SSL that includes the subject's certificate, the root CA certificate, and any intermediate CA certificates.
certificate signing request	See CSR .
Cisco.com	Replaces the Cisco Connection Online Web site. Use this site to access customer service and support.
class map	A mechanism for classifying types of network traffic. The ANM uses class maps to classify the network traffic that is received and transmitted by the ACE. Types of traffic include Layer 3/Layer 4 traffic that can pass through the ACE, network management traffic that can be received by the ACE, and Layer 7 HTTP load-balancing traffic.
CSR	Certificate Signing Request. A message sent to a certificate authority, such as VeriSign and Thawte to apply for a digital identity certificate for use with SSL. The request includes information that identifies the SSL site, such as location and serial number, and a public key that you choose. The request may also provide any additional proof of identity required by the certificate authority.
Cisco IOS Software	The Cisco system software that allows centralized, integrated, and automated installation and management of internetworks, while ensuring support for a wide variety of protocols, media, services, and platforms.
context	See virtual context .

D

DES	Data Encryption Standard. One of the possible encryption algorithms available for use in SNMP communications.
DFP	Dynamic Feedback Protocol. A protocol that allows load-balanced servers (both local and remote) to dynamically report changes in their status and their ability to provide services.
distinguished name	Used for SSL, a set of attributes that provides the certificate authority with the information it needs to authenticate your site.

E

event	A message from the ANM that informs you of activities on parts of the system, including each virtual context, the management system, and hardware components.

event type Alarm, Log, Audit, Attack Log

exception A group of related faults.

F

fault An abnormal condition that occurs when a system component exceeds a performance threshold or is not functioning properly.

File Transfer Protocol See [FTP](#).

FTP File Transfer Protocol. Application protocol, part of the TCP/IP protocol stack, used for transferring files between network nodes. FTP is defined in RFC 959.

H

H.323 An umbrella recommendation from the ITU Telecommunication Standardization Sector (ITU-T) that defines the protocols that provide audio-visual communication sessions on any packet network. It is a part of the H.32x series of protocols which also address communications over Integrated Services Digital Network (ISDN), Public switched telephone network (PSTN) or Signaling System 7 (SS7). H.323 is commonly used in Voice over IP (VoIP, Internet Telephony, or IP Telephony) and Internet Protocol (IP)-based videoconferencing. H.323 defines a common set of CODECs, call setup and negotiating procedures, and basic data transport methods.

HSRP Hot Standby Router Protocol. A networking protocol that provides network redundancy for IP networks, ensuring that user traffic immediately and transparently recovers from first hop failures in network edge devices or access circuits.

I

ICMP Internet Control Message Protocol. Network layer Internet protocol that reports errors and provides other information relevant to IP packet processing. Documented in RFC 792.

Internet Control Message Protocol See [ICMP](#).

interface

1. A network connection.
2. A connection between two systems or devices.
3. In telephony, a shared boundary defined by common physical interconnection characteristics, signal characteristics, and meanings of interchanged signals.

L

load balancing An action that spreads network requests among available servers within a cluster of servers, based on a variety of algorithms.

M

MD5 Message Digest 5 or Message-Digest Algorithm. One of the possible encryption algorithms available for use in SNMP communications.

MIB Database of network management information that is used and maintained by a network management protocol, such as SNMP or CMIP. The value of a MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a GUI network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

N

NAT Name Address Translation. A method of connecting multiple computers to the Internet (or any other IP network) using one IP address.

O

object group A logical grouping of similar objects, such as servers, clients, services, or networks. Creating an object group allows you to apply common attributes to a number of objects without specifying each object individually.

P

PAT Port Address Translation. A mechanism that allows many devices on a LAN to share one IP address by allocating a unique port address at Layer 4.

ping	A common method for troubleshooting the accessibility of devices. A ping tests an ICMP echo message and its reply. Because ping is the simplest test for a device, it is the first to be used. If ping fails, try using traceroute. Run ping to view the packets transmitted, packets received, percentage of packet loss, and round-trip time in milliseconds.
port	1. An interface on an internetworking device (such as a router); a physical entity. 2. In IP terminology, an upper-layer process that receives information from lower layers. Ports are numbered, and each numbered port is associated with a specific process. For example, SMTP is associated with port 25. A port number is also called a well-known address. 3. To rewrite software or microcode so that it will run on a different hardware platform or in a different software environment than that for which it was originally designed.

R

RAS	Registration, Admission, and Status Protocol. Protocol that is used between endpoints and the gatekeeper to perform management functions. RAS signalling function performs registration, admissions, bandwidth changes, status, and disengage procedures between the VoIP gateway and the gatekeeper.
RBAC	Role-Based Access Control. A mechanism that allows privileges to be assigned to defined roles. The roles are then assigned to real users, allowing or limiting access to specific features as appropriate for each role.
real server	A real server is a physical device assigned to a server farm.
redundancy	In internetworking, the duplication of devices, services, or connections so that, in the event of a failure, the redundant devices, services, or connections can perform the work of those that failed.
resource class	A defined set of resources and allocations available for use by a device (such as an ACE). Using resource classes prevents a single device from using all available resources.
role	See user role .
RSA	Rivest, Shamir, and Adelman Signatures. A public-key cryptographic system used for authentication.
RTSP	Real Time Streaming Protocol. A client-server multimedia presentation control protocol, designed to address the needs for efficient delivery of streamed multimedia over IP networks.

S

SCCP	Skinny Client Control Protocol. A proprietary terminal control protocol owned and defined by Cisco as a messaging set between a skinny client and the Cisco CallManager (CCM). Examples of skinny clients include the Cisco 7900 series of IP phone such as the Cisco 7960, Cisco 7940 and the 802.11b wireless Cisco 7920, along with Cisco Unity voicemail server. See also Skinny.

server farm	A collection of servers that contain the same content.
Server Load Balancer	See SLB .
service	A destination location where a piece of content resides physically. Also referred to in general terms for this release as including content rules, owners, virtual servers, real servers, and so on.
Simple Message Transfer Protocol	See SMTP .
SIP	Session Initiation Protocol. Protocol developed by the IETF MMUSIC Working Group as an alternative to H.323 . SIP features are compliant with IETF RFC 2543, published in March 1999. SIP equips platforms to signal the setup of voice and multimedia calls over IP networks.
Skinny	Skinny is a lightweight protocol which allows for efficient communication with Cisco CallManager. See also SCCP .
SLB	Server Load Balancer. A device that makes load balancing decisions based on application availability, server capacity, and load distribution algorithms, such as round robin or least connections. Using load balancing and server/application feedback, an SLB device determines a real server for the packet flow and sends this information to the requesting forwarding agent. After the optimal destination is decided on, all other packets in the packet flow are directed to a real server by the forwarding agent, increasing packet throughput.
special configuration file	Managed file resource on an ACE module, such as a piece of a configuration file or a keep-alive script.
SMTP	Simple Message Transfer Protocol. Internet protocol that provides e-mail services.
sticky	A feature that ensures that the same client gets the same server for multiple connections. It is used when applications require a consistent and constant connection to the same server. If you are connecting to a system that keeps state tables about your connection, sticky allows you to get back to the same real server again and retain the statefulness of the system.
suspend	Removes an entity from the resource pool for future load-balancing content requests or connections. Suspending a service or device does not affect existing content flows, but it prevents additional connections from accessing the suspended entity or content. See also activate .

T

TCP	Transport Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.
template	See building block .
threshold	A range in which you expect your network to perform. If a threshold is exceeded or goes below the expected bounds, you examine the areas for potential problems. You can create thresholds for a specific device.

tracert A diagnostic tool that helps you understand why ping fails or why applications time out. Using it, you can view each hop (or gateway) on the route to your device and how long each took.

Transport Control Protocol See [TCP](#).

U

URI Uniform Resource Identifier. Type of formatted identifier that encapsulates the name of an Internet object, and labels it with an identification of the name space, thus producing a member of the universal set of names in registered name spaces and of addresses referring to registered protocols or name spaces. [RFC 1630]

user role A mechanism for granting access to features and functionality to a user account. The Cisco Application Networking Manager includes four predefined roles: System Administrator, Server Manager, Network Manager, and Service Provider Customer.

V

virtual context A concept that allows users to partition an ACE into multiple virtual devices. Each virtual context contains its own set of policies, interfaces, resources, and administrators, allowing administrators to more efficiently manage system resources and services.

VLAN Virtual LAN. Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

VLAN Trunking Protocol See [VTP](#).

virtual server A virtual server represents groups of real servers and are associated with a real server farm.

VTP VLAN Trunking Protocol. A Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs within a VTP domain. VTP minimizes misconfigurations and configuration inconsistencies that can result in a number of problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.

VTP domain Also called a VLAN management domain, a domain composed of one or more network devices that share the same VTP domain name and that are interconnected with trunks.

W

Web server A machine that contains Web pages that are accessible by others.



INDEX

Numerics

6500 series devices

adding to ANM [2-8](#)

7600 series router

adding to ANM [2-8](#)

adding VLANs [2-35](#)

configuration options [2-23](#)

configuring

access ports [2-29](#)

interfaces [2-28](#)

primary attributes [2-26](#)

routed ports [2-33](#)

switch virtual interfaces [2-32](#)

trunk ports [2-30](#)

license file name [15-57](#)

managing [2-52](#)

synchronizing configurations [2-52](#)

viewing

all modules [2-61](#)

ports [2-34](#)

VLAN

managing [2-35](#)

modifying [2-38](#)

viewing [2-36](#)

A

acceleration

configuring [4-37](#)

configuring globally on ACE appliances [12-16](#)

FlashForward [12-1](#)

traffic policies [12-2](#)

typical configuration flow [12-2](#)

access control, configuring on VLAN interfaces [9-8](#)

access credentials, configuring [2-17](#)

access ports, configuring [2-29](#)

account password [1-4](#)

accounts

user, managing [15-38](#)

ACE

changing passwords [2-58](#)

class map

configuring [11-6](#)

match conditions [11-8](#)

configuration options [3-8](#)

definition [GL-1](#)

license

ANM license requirements [3-27](#)

copying [3-28](#)

details [3-32](#)

installing [3-29](#)

managing [3-27](#)

removing [3-30](#)

updating [3-31](#)

viewing [3-27](#)

notation in device tree [3-2](#)

parameter maps [7-1](#)

policy map

configuring [11-31](#)

rules and actions [11-33](#)

traffic policies [11-2](#)

viewing license details [3-32](#)

virtual server protocols [4-8](#)

ACE 1.0 module

class maps [11-6](#)

- Config Status display [3-66](#)
- configuration building block [13-5](#)
- parameter maps [7-1](#)
- policy maps [11-31](#)
- synchronizing configurations [3-66](#)
- traffic policies [11-2](#)
- virtual server protocols [4-8](#)
- ACE 2.0 module
 - action list configuration options [12-3](#)
 - class map
 - match conditions [11-9](#)
 - types [11-6](#)
 - configuration building block [13-5](#)
 - parameter map
 - generic [7-7](#)
 - RTSP [7-17](#)
 - SIP [7-18](#)
 - Skippy [7-20](#)
 - parameter maps [7-1](#)
 - policy maps [11-31](#)
 - sticky types [6-2](#)
 - traffic policies [11-2](#)
 - virtual server protocols [4-8](#)
- ACE appliance
 - action list
 - configuration options [12-6](#)
 - configuring [12-6](#)
 - class maps [11-6](#)
 - configuration building block [13-5](#)
 - configuring [2-22](#)
 - license file name [15-57](#)
 - licenses
 - configuration [3-32](#)
 - statistics [3-32](#)
 - optimization parameter map [7-10](#)
 - parameter maps [7-1](#)
 - policy maps [11-31](#)
 - synchronizing configurations [2-52](#)
 - traffic policies [11-2](#)
 - virtual server protocols [4-8](#)
- ACE appliances
 - SSH, enabling [2-5](#)
- ACE license
 - and required ANM licenses [3-27](#)
 - copying for importing [3-28](#)
 - details [3-32](#)
 - installing [3-29](#)
 - managing [3-27](#)
 - removing [3-30](#)
 - updating [3-31](#)
 - viewing [3-27](#)
- ACE module
 - configuring [2-22](#)
 - configuring access credentials [2-17](#)
 - discovery
 - enabling SSH access [2-17](#)
 - process [2-20](#)
 - license file name [15-57](#)
 - monitoring discovery status [2-21](#)
 - synchronizing configurations [2-53](#)
 - viewing
 - by 7600 series router [2-61](#)
 - by chassis [2-61](#)
- ACE modules
 - ACE 2.0 SNMP polling [2-7](#)
 - adding to ANM [2-11](#)
 - HTTPS, enabling [2-5](#)
 - OK/Pass state requirement [2-11](#)
 - SSH, enabling [2-5](#)
- ACL
 - configuration overview [3-43](#)
 - configuring
 - EtherType attributes [3-51](#)
 - extended ACL attributes [3-47](#)
 - for VLANs [9-8](#)
 - object groups [3-52](#)
 - creating [3-44](#)
 - deleting [3-61](#)

- managing [3-60](#)
- objects
 - ICMP service parameters [3-58](#)
 - IP addresses [3-53](#)
 - protocols [3-55](#)
 - subnet objects [3-54](#)
 - TCP/UDP service parameters [3-56](#)
- resequencing [3-50](#)
- viewing by context [3-60](#)
- ACL object group
 - configuring [3-52](#)
 - network objects
 - IP addresses [3-53](#)
 - subnet objects [3-54](#)
 - service objects
 - ICMP service parameters [3-58](#)
 - protocols [3-55](#)
 - TCP/UDP service parameters [3-56](#)
- ACLs, creating [3-44](#)
- action, setting for policy maps [11-33](#)
- action list
 - ACE appliance configuration options [12-6](#)
 - configuration options [4-39](#)
 - configuring [12-3](#)
 - for ACE 2.0 modules [12-3](#)
 - for ACE appliances [12-6](#)
 - pattern replacements [12-10](#)
 - pattern replacements [12-10](#)
- activate, definition [GL-1](#)
- activating
 - DNS rules for GSS [4-54](#)
 - real servers [5-7](#)
 - virtual servers [4-51](#)
- adding
 - 6500 series devices [2-8](#)
 - 7600 series routers [2-8](#)
 - ACE appliances [2-8](#)
 - ACE modules [2-11](#)
 - CSM [2-13](#)
 - CSS [2-8](#)
 - devices to ANM [2-7](#)
 - domains [2-49](#)
 - GSS devices [2-14](#)
 - resource classes [3-36](#)
 - SSL
 - CSR parameters [8-20](#)
 - parameter map cipher info [8-17](#)
 - parameter maps [8-16, 8-22](#)
 - user-defined groups [2-54](#)
- Admin context, first virtual context [3-2](#)
- administrative distance, definition [GL-1](#)
- admin password [15-35](#)
- advanced editing mode [1-13](#)
- advanced image type, configuration options [4-46](#)
- AES, definition [GL-1](#)
- alarms
 - configuring for notification [14-25](#)
 - viewing [14-30](#)
- all-match policy map [11-31](#)
- ANM interface
 - features [1-1](#)
 - logging in [1-2](#)
 - overview [1-5](#)
 - password, changing
 - account [1-4](#)
 - login [1-4](#)
 - table
 - conventions [1-11](#)
 - customizing [1-11](#)
 - terminology [1-15](#)
- ANM server
 - auto-sync settings [15-65](#)
 - change audit logs [15-64](#)
 - change audit logs, viewing [15-64](#)
 - configuring
 - attributes [15-63](#)
 - license file name [15-57](#)
 - polling, enabling [15-63](#)

- statistics [15-62](#)
- application acceleration
 - action lists [12-3](#)
 - configuring [4-37](#)
 - action lists [4-39](#)
 - globally on ACE appliances [12-16](#)
 - monitoring [14-17](#)
 - overview [12-1](#)
 - traffic policies [12-2](#)
 - typical configuration flow [12-2](#)
 - virtual server, additional configuration options [4-43](#)
- applying configuration building blocks [13-8](#)
- Appscope, configuration options [4-45](#)
- ARP
 - configuring static ARP [9-9](#)
 - definition [GL-1](#)
- attributes
 - BVI interfaces [9-13](#)
 - DNS probes [5-30](#)
 - Echo-TCP probes [5-30](#)
 - Echo-UDP probes [5-30](#)
 - Finger probes [5-31](#)
 - for sticky group types [6-9](#)
 - FTP probes [5-31](#)
 - health monitoring [5-27](#)
 - high availability [10-5](#)
 - HTTP content sticky group [6-10](#)
 - HTTP cookie sticky group [6-11](#)
 - HTTP header sticky group [6-11](#)
 - HTTP probes [5-31](#)
 - HTTPS probes [5-33](#)
 - IMAP probes [5-35](#)
 - IP netmask sticky group [6-12](#)
 - Layer 4 payload sticky group [6-12](#)
 - new device [2-8](#)
 - parameter map
 - connection [7-2](#)
 - generic [7-7](#)
 - HTTP [7-8](#)
 - optimization [7-11](#)
 - RTSP [7-17](#)
 - SIP [7-18](#)
 - Skinny [7-20](#)
 - POP probes [5-35](#)
 - predictor method [5-17](#)
 - RADIUS
 - sticky groups [6-13](#)
 - RADIUS probes [5-36](#)
 - real servers [5-4, 5-15](#)
 - resource class [3-34](#)
 - resource classes [3-34](#)
 - RTSP
 - header sticky groups [6-14](#)
 - probes [5-36](#)
 - scripted probes [5-37](#)
 - server farms [4-29, 5-13](#)
 - SIP-TCP probes [5-38](#)
 - SIP-UDP probes [5-38](#)
 - SMTP probes [5-39](#)
 - SNMP [3-19](#)
 - SNMP probes [5-39](#)
 - SSL
 - certificate export [8-13](#)
 - certificate import [8-7](#)
 - CSR parameters [8-20](#)
 - for virtual servers [4-13](#)
 - key export [8-14](#)
 - key pair import [8-9](#)
 - parameter map cipher info [8-17](#)
 - parameter maps [8-16, 8-22](#)
 - sticky group [6-8](#)
 - TCP probes [5-39](#)
 - Telnet probes [5-40](#)
 - UDP probes [5-40](#)
 - virtual context [3-3, 3-11](#)
 - virtual servers [4-5](#)
 - VLAN interfaces [9-3](#)
- audience, intended [ix](#)

- auditing
 - building block configuration [3-62](#)
 - resource classes [3-38](#)
- audit log
 - configuring
 - purge settings [15-63](#)
- audit logs
 - ANM server change audit [15-64](#)
- audit sync settings
 - configuring [15-65](#)
- authorization group certificate, configuring for SSL [8-24](#)
- autosync
 - setting up syslog settings for [3-66](#)

B

- backing up data [16-7](#)
- bandwidth optimization, configuring [4-38](#)
- building block
 - applying [13-8](#)
 - configuration
 - audit [3-62](#)
 - changes and version numbers [13-4](#)
 - options [13-2](#)
 - primary attributes [13-7](#)
 - configuring [13-6](#)
 - creating [13-5](#)
 - extracting from virtual contexts [13-5](#)
 - overview [13-1](#)
 - primary attributes [13-7](#)
 - tagging [13-4, 13-7](#)
 - types [13-5](#)
 - using [13-1](#)
 - versions [13-4](#)
 - viewing use [13-9](#)
- buttons
 - descriptions [1-9](#)
- BVI, definition [GL-1](#)
- BVI interfaces

- attributes [9-13](#)
- configuring [9-12](#)
- viewing by context [9-14](#)

C

- caching, dynamic [12-2](#)
- caution, logging in as root user [16-7, 16-8](#)
- certificate
 - exporting for SSL [8-12](#)
 - importing for SSL [8-6](#)
 - SSL [8-5](#)
- certificate chain, definition [GL-2](#)
- certificate signing request, definition [GL-2](#)
- chain group certificate, configuring for SSL [8-19](#)
- chain group parameters, configuring for SSL [8-18](#)
- changing
 - account password [1-4](#)
 - admin password [15-35](#)
 - domain information [2-49](#)
 - login password [1-4](#)
 - role rules [2-47](#)
 - user passwords [15-35](#)
- chassis
 - adding VLANs [2-35](#)
 - changing passwords [2-57](#)
 - configurations options [2-23](#)
 - configuring [2-22](#)
 - access credentials [2-17](#)
 - access ports [2-29](#)
 - interfaces [2-28](#)
 - primary attributes [2-26](#)
 - routed ports [2-33](#)
 - switch virtual interfaces [2-32](#)
 - trunk ports [2-30](#)
 - discovery process [2-20](#)
 - managing [2-52](#)
 - monitoring
 - discovery status [2-21](#)

- running discovery [2-20](#)
- SSH, enabling [2-5](#)
- synchronizing configurations [2-52](#)
- Telnet default [2-5](#)
- viewing
 - all modules [2-61](#)
 - ports [2-34](#)
- VLAN
 - managing [2-35](#)
 - modifying [2-38](#)
 - viewing [2-36](#)
- checking status of the Cisco ANM server [15-54](#)
- Cisco IOS software, definition [GL-2](#)
- class map
 - ACE device support [11-6, 11-8](#)
 - configuring [11-6](#)
 - definition [GL-2](#)
 - deleting [11-6, 11-8](#)
 - match conditions
 - generic server load balancing [11-22](#)
 - Layer 3/4 management traffic [11-12](#)
 - Layer 3/4 network traffic [11-9](#)
 - Layer 7 FTP command inspection [11-21](#)
 - Layer 7 HTTP deep packet inspection [11-15](#)
 - Layer 7 server load balancing [11-13](#)
 - Layer 7 SIP deep packet inspection [11-28](#)
 - RADIUS server load balancing [11-23](#)
 - RTSP server load balancing [11-25](#)
 - SIP server load balancing [11-27](#)
 - overview [11-2, 11-3](#)
 - setting match conditions [11-8](#)
 - use with real servers [5-3](#)
- command inspection, FTP commands [11-21](#)
- configuration attributes
 - advanced image type [4-46](#)
 - Appscope [4-45](#)
 - delta optimization [4-43](#)
 - device VLAN [2-36](#)
 - extended ACL [3-47](#)
 - FlashConnect [4-45](#)
 - health monitoring [5-27](#)
 - high availability [10-5](#)
 - HTTP return code maps [5-22](#)
 - parameter map
 - connection [7-2](#)
 - generic [7-7](#)
 - HTTP [7-8](#)
 - optimization [7-11](#)
 - RTSP [7-17](#)
 - SIP [7-18](#)
 - Skinny [7-20](#)
 - predictor method [5-17](#)
 - probe
 - DNS [5-30](#)
 - Echo-TCP [5-30](#)
 - Echo-UDP [5-30](#)
 - Finger [5-31](#)
 - FTP [5-31](#)
 - HTTP [5-31](#)
 - HTTPS [5-33](#)
 - IMAP [5-35](#)
 - POP [5-35](#)
 - RADIUS [5-36](#)
 - RTSP [5-36](#)
 - scripted [5-37](#)
 - SIP-TCP [5-38](#)
 - SIP-UDP [5-38](#)
 - SMTP [5-39](#)
 - SNMP [5-39](#)
 - TCP [5-39](#)
 - Telnet [5-40](#)
 - UDP [5-40](#)
 - real server [5-4, 5-15](#)
 - resource class [3-34](#)
 - server farm [4-29, 5-13](#)
 - SNMP users [3-22](#)
 - SSL [4-13](#)
 - sticky group [6-8](#)

- sticky type [4-32](#)
- syslog [3-13](#)
- trunk ports [2-31](#)
- virtual context [3-3](#)
- virtual server [4-5](#)
- XSLT merge [4-45](#)
- configuration building block
 - applying [13-8](#)
 - configuring [13-6](#)
 - creating [13-5](#)
 - options [13-2](#)
 - overview [13-1](#)
 - tagging [13-4, 13-7](#)
 - using [13-1](#)
 - versions [13-4](#)
- configuration options
 - 7600 series routers [2-23](#)
 - ACE appliance action lists [12-6](#)
 - building blocks [13-2](#)
 - by ACE device type [3-8](#)
 - chassis [2-23](#)
 - URL mapping [12-9](#)
 - virtual contexts [3-6](#)
- configurations
 - synchronizing
 - for ACE modules [2-53](#)
 - for devices [2-52](#)
 - for high availability [10-19](#)
 - for virtual contexts [3-66](#)
- configuration screen conventions [3-5](#)
- configuration synchronization [10-23](#)
- configuration template. See building block.
- configuration values, changing [16-1](#)
- configuring
 - 7600 series router [2-22, 2-26](#)
 - access ports [2-29](#)
 - interfaces [2-28](#)
 - switch virtual interfaces [2-32](#)
 - trunk ports [2-30](#)
 - acceleration [4-37](#)
 - access credentials [2-17](#)
 - access ports [2-29](#)
 - ACE passwords [2-58](#)
 - ACE SNMP for polling [2-6](#)
 - ACE syslog messages [2-15](#)
 - ACLs [3-44, 9-8](#)
 - EtherType [3-51](#)
 - extended [3-47](#)
 - object groups [3-52](#)
 - resequencing [3-50](#)
 - action list pattern replacements [12-10](#)
 - action lists [4-39, 12-3](#)
 - for ACE 2.0 modules [12-3](#)
 - for ACE appliances [12-6](#)
 - application acceleration action lists [4-39](#)
 - bandwidth optimization [4-38](#)
 - building block primary attributes [13-7](#)
 - building blocks [13-6](#)
 - BVI interfaces [9-12](#)
 - chassis [2-22, 2-26](#)
 - access ports [2-29](#)
 - interfaces [2-28](#)
 - trunk ports [2-30](#)
 - chassis passwords [2-57](#)
 - class map match conditions
 - generic server load balancing [11-22](#)
 - Layer 3/4 management traffic [11-12](#)
 - Layer 3/4 network traffic [11-9](#)
 - Layer 7 FTP command inspection [11-21](#)
 - Layer 7 HTTP deep packet inspection [11-15](#)
 - Layer 7 server load balancing [11-13](#)
 - Layer 7 SIP deep packet inspection [11-28](#)
 - RADIUS server load balancing [11-23](#)
 - RTSP server load balancing [11-25](#)
 - SIP server load balancing [11-27](#)
 - class maps [11-6](#)
 - CSM [2-22, 2-23](#)
 - CSS [2-22, 2-24](#)

- devices [2-22](#)
- DHCP relay [9-12](#)
- DNS probe expect address [5-40](#)
- gigabit Ethernet interfaces [9-17](#)
- global
 - application acceleration on ACE appliances [12-16](#)
 - optimization on ACE appliances [12-16](#)
- GSS [2-25](#)
- health monitoring general attributes [5-27](#)
- high availability
 - groups [10-8, 10-9](#)
 - host tracking [10-14](#)
 - interface tracking [10-13](#)
 - peer host probes [10-17](#)
 - peers [10-5](#)
 - synchronization [10-23](#)
 - tracking and failure detection [10-13](#)
- host probes for high availability [10-15](#)
- HTTP probe headers [5-41](#)
- HTTP retcode maps [5-21](#)
- HTTPS probe headers [5-41](#)
- latency optimization [4-38](#)
- Layer 2 VLANs [2-37](#)
- Layer 3 VLANs [2-38](#)
- Layer 7 default load balancing [4-35](#)
- load balancing
 - real servers [5-4](#)
 - server farms [5-12](#)
 - sticky groups [6-7](#)
 - virtual servers [4-25](#)
- NAT [4-47, 9-10](#)
- object groups
 - ICMP service parameters [3-58](#)
 - IP addresses [3-53](#)
 - protocols [3-55](#)
 - subnet objects [3-54](#)
 - TCP/UDP service parameters [3-56](#)
- OID for SNMP probes [5-43](#)
- optimization [4-37](#)
 - action lists [4-39](#)
 - traffic policies [12-13](#)
- organization passwords [15-32](#)
- parameter maps
 - connection [7-2](#)
 - generic [7-7](#)
 - HTTP [7-8](#)
 - optimization [7-10, 12-12](#)
 - RTSP [7-17](#)
 - SIP [7-18](#)
 - Skinny [7-20](#)
- PAT [9-10](#)
- pattern replacements [12-10](#)
- policy map rules and actions [11-33](#)
 - generic server load balancing [11-34](#)
 - Layer 3/4 management traffic [11-37](#)
 - Layer 3/4 network traffic [11-38](#)
 - Layer 7 FTP command inspection [11-45](#)
 - Layer 7 HTTP deep packet inspection [11-47](#)
 - Layer 7 HTTP optimization [11-53](#)
 - Layer 7 server load balancing [11-56](#)
 - Layer 7 SIP deep packet inspection [11-62](#)
 - Layer 7 Skinny deep packet inspection [11-64](#)
 - RADIUS server load balancing [11-66](#)
 - RDP server load balancing [11-68](#)
 - RTSP server load balancing [11-70](#)
 - SIP server load balancing [11-73](#)
- policy maps [11-30](#)
- port channel interfaces [9-21](#)
- probe attributes [5-29](#)
- probe expect status [5-42](#)
- protocol inspection [4-14](#)
- real servers [5-8](#)
- resource classes
 - global [3-36](#)
 - local [3-41](#)
- routed ports [2-33](#)
- server farm predictor method [5-16](#)

- shared objects [4-7](#)
- SNMP [3-19](#)
 - communities [3-20](#)
 - credentials [2-18](#)
 - notification [3-24](#)
 - on virtual contexts [3-19](#)
 - trap destination hosts [3-23](#)
 - version 3 users [3-21](#)
- SSL
 - chain group parameters [8-18](#)
 - CSR parameters [8-19](#)
 - for virtual servers [4-12](#)
 - parameter map [8-15](#)
 - parameter map cipher [8-17](#)
 - proxy service [8-22](#)
- static ARP for VLANs [9-9](#)
- static routes [2-27, 9-14](#)
- sticky groups [4-32, 6-7](#)
- sticky statics [6-14](#)
- switch virtual interfaces [2-32](#)
- syslog
 - logging [3-12](#)
 - log hosts [3-16](#)
 - log messages [3-17](#)
 - log rate limits [3-18](#)
- Telnet
 - credentials [2-18](#)
- Telnet on chassis [2-5](#)
- traffic policies [11-1](#)
- trunk ports [2-30](#)
- URL mappings [12-9](#)
- virtual context [3-1, 3-5, 3-67](#)
 - class maps [11-6](#)
 - global policies [3-26](#)
 - policy maps [11-30](#)
 - primary attributes [3-11](#)
 - resource classes [3-41](#)
 - system attributes [3-11](#)
- virtual server
 - configuration overview [4-2](#)
 - default load balancing [4-35](#)
 - Layer 7 load balancing [4-25](#)
 - NAT [4-47](#)
 - optimization [12-16](#)
 - properties [4-8](#)
 - protocol inspection [4-14](#)
 - shared objects [4-6](#)
 - SSL termination service [4-12](#)
- VLAN
 - interface access control [9-8](#)
 - interface options [9-7](#)
 - interface policy maps [9-7](#)
 - interfaces [9-2](#)
 - Layer 2 [2-37](#)
 - Layer 3 [2-38](#)
 - VLAN groups [2-39](#)
- connection parameter map
 - attributes [7-2](#)
 - configuring [7-2](#)
 - TCP options [7-6](#)
- connectivity, testing between devices [14-33](#)
- Content Switching Module devices
 - adding to ANM [2-8](#)
- context
 - configuration options [3-6](#)
 - configuring [3-5](#)
 - application acceleration [12-1](#)
 - BVI interfaces [9-12](#)
 - global policies [3-26](#)
 - load balancing [4-1](#)
 - optimization [12-1](#)
 - primary attributes [3-11](#)
 - resource classes [3-41](#)
 - static routes [9-14](#)
 - traffic policies [11-1](#)
 - virtual servers [4-1](#)
 - VLAN interfaces [9-2](#)
 - creating [3-2](#)

- definition [GL-7](#)
- deleting [3-68](#)
- editing [3-67](#)
- extracting configurations for building blocks [13-5](#)
- modifying [3-67](#)
- polling
 - restarting [3-69](#)
 - viewing status [3-65](#)
- protocols [3-4](#)
- synchronizing configurations [3-66](#)
- sync status [3-64](#)
- upgrading [3-68](#)
- using for configuration building blocks [13-5](#)

controlling access to Cisco ANM [15-2](#)

conventions in ANM

- dropdown lists [3-5](#)
- for configuration screens [3-5](#)
- radio buttons [3-3](#)
- table [1-11](#)

conventions in this guide [x](#)

cookie

- client [6-3](#)
- sticky client identification [6-3](#)

creating

- ACLs [3-44](#)
- building blocks [13-5](#)
- domains [15-50](#)
- user accounts [15-39](#)
- user roles [15-46](#)
- virtual contexts [3-2](#)

creating ACLs [3-44](#)

credentials

- modifying [2-19](#)
- SNMP [2-18](#)
- Telnet [2-18](#)

CSM

- adding to ANM [2-13](#)
- configuring [2-22](#)
- license file name [15-57](#)

- primary attributes [2-23](#)
- viewing by chassis [2-61](#)

CSR

- configuring parameters [8-19](#)
- definition [GL-2](#)
- generating for SSL [8-21](#)

CSS

- configuring [2-22](#)
- license file name [15-57](#)
- primary attributes [2-24](#)
- synchronizing configurations [2-52](#)

customizing

- tables [1-11](#)

D

data

- backing up [16-7](#)
- restoring [16-8](#)

deep packet inspection

HTTP

- class map match conditions [11-15](#)
- policy map rules and actions [11-47](#)

SIP

- class map match conditions [11-28](#)
- policy map rules and actions [11-62](#)
- Skinny policy map rules and actions [11-64](#)

default distance values [2-28](#)

deleting

- ACLs [3-61](#)
- class map in use [11-6](#)
- device RBAC user accounts [2-43](#)
- domains [2-51, 15-52](#)
- high availability groups [10-12](#)
- host probes for high availability [10-16](#)
- organizations [15-37](#)
- peer host probes [10-18](#)
- resource classes [3-40, 3-42](#)
- role rules [2-47](#)

- roles or domains [2-40](#)
 - SSL objects [8-2](#)
 - user accounts [15-42](#)
 - user-defined groups [2-56](#)
 - user roles [2-47, 15-48](#)
 - virtual contexts [3-68](#)
 - delta optimization
 - configuration options [4-43](#)
 - description [12-1](#)
 - deploying
 - configuration building blocks [13-8](#)
 - staged virtual servers [4-49](#)
 - DES, definition [GL-2](#)
 - device
 - adding to ANM [2-7](#)
 - configuring [2-22](#)
 - management overview [2-2](#)
 - managing [2-1](#)
 - monitoring [14-4](#)
 - polling
 - restarting [2-59](#)
 - status [2-60](#)
 - viewing
 - All Devices table [2-60](#)
 - device audit trail logs
 - monitoring [14-23](#)
 - device groups, monitoring [14-3](#)
 - devices
 - adding to ANM [2-8](#)
 - device tree
 - ACE version notation [3-2](#)
 - overview [1-8](#)
 - DHCP relay, configuring [9-12](#)
 - discovery
 - enabling
 - SSH on ACE modules [2-17](#)
 - monitoring progress [2-20, 2-21](#)
 - process [2-20](#)
 - running [2-20](#)
 - displaying
 - current user sessions [15-42](#)
 - list of users [15-38](#)
 - network domains [15-50](#)
 - organizations [15-37](#)
 - user roles [15-46](#)
 - users who have a selected role [15-46](#)
 - distinguished name, definition [GL-2](#)
 - DNS
 - configuring protocol inspection [4-15](#)
 - probe
 - attributes [5-30](#)
 - expect address [5-40](#)
 - DNS rules, and GSS [4-54](#)
 - domains
 - deleting [2-40](#)
 - duplicating
 - domains [15-51](#)
 - organizations [15-36](#)
 - user accounts [15-40](#)
 - user-defined groups [2-56](#)
 - user roles [15-47](#)
 - dynamic caching [12-2](#)
-
- ## E
- Echo-TCP probe attributes [5-30](#)
 - Echo-UDP probe attributes [5-30](#)
 - e-commerce
 - applications, sticky requirements [6-1](#)
 - using stickiness [6-4](#)
 - editing
 - role rules [2-47](#)
 - enabling
 - ACE syslog messages [2-15](#)
 - SNMP polling from ANM [2-6](#)
 - Ethernet interfaces, configuring [9-17](#)
 - EtherType ACL, configuring [3-51](#)
 - event

- definition [GL-2](#)
- monitoring [14-21](#)
- event type, definition [GL-3](#)
- exception, definition [GL-3](#)
- expert options, for virtual contexts [3-62](#)
- exporting
 - SSL
 - certificates [8-12](#)
 - key [8-14](#)
 - key pair [8-14](#)
- extended ACL
 - configuration options [3-47](#)
 - resequencing entries [3-50](#)

F

- failover [10-22](#)
- fault, definition [GL-3](#)
- fault tolerance
 - groups [10-21](#)
 - task overview [10-4](#)
- features of ANM [1-1](#)
- filtering tables [1-11](#)
- Finger probe attributes [5-31](#)
- first-match policy map [11-31](#)
- FlashConnect, configuration options [4-45](#)
- FlashForward object acceleration [12-1](#)
- FTP, configuring protocol inspection [4-15](#)
- FTP command inspection
 - available commands [11-21](#)
 - class map match conditions [11-21](#)
 - policy map rules and actions [11-45](#)
- FTP probe attributes [5-31](#)
- FTP strict, and RFP standards [11-45](#)
- FT VLAN [10-23](#)

G

- generating
 - ANM licenses
 - overview [1-4](#)
- generic parameter map
 - attributes [7-7](#)
 - configuring [7-7](#)
- generic server load balancing
 - class map match conditions [11-22](#)
 - policy map rules and actions [11-34](#)
- global acceleration and optimization, ACE appliances [12-16](#)
- global policies, configuring for virtual contexts [3-26](#)
- global resource class [3-33](#)
 - applying to contexts [3-37](#)
 - auditing [3-38](#)
 - configuring [3-36](#)
 - deleting [3-40](#)
 - deploying [3-37](#)
 - modifying [3-39](#)
 - using [3-35](#)

GSS

- devices
 - adding to ANM [2-14](#)
 - DNS rules, activating suspending [4-54](#)
 - primary attributes [2-25](#)
 - VIP Answer table, managing [4-53](#)
- guidelines for managing
 - domains [15-49](#)
 - user accounts [15-38](#)
 - user roles [15-43](#)

H

- hash load-balancing methods
 - address [5-2](#)
 - cookie [5-2](#)
 - header [5-2](#)

- url [5-2](#)
 - health monitoring
 - configuring [5-24](#)
 - for real servers [5-25](#)
 - general attributes [5-27](#)
 - overview [5-23](#)
 - probe types [5-26](#)
 - TCL scripts [5-24](#)
 - heartbeat packets [10-21](#)
 - high availability
 - clearing
 - links between ACE appliances [10-7](#)
 - pairs [10-7](#)
 - configuration attributes [10-5](#)
 - configuring
 - groups [10-8](#)
 - host probes [10-15](#)
 - host tracking process [10-14](#)
 - interface tracking process [10-13](#)
 - overview [10-20](#)
 - peer host probes [10-17](#)
 - peers [10-5](#)
 - deleting
 - groups [10-12](#)
 - host probes [10-16](#)
 - peer host probes [10-18](#)
 - failover detection [10-13](#)
 - importance of synchronizing configurations [10-19](#)
 - modifying groups [10-9](#)
 - protocol [10-21](#)
 - switching over a group [10-11](#)
 - task overview [10-4](#)
 - tracking status [10-13](#)
 - HSRP, definition [GL-3](#)
 - HTTP
 - configuring protocol inspection [4-15](#)
 - content
 - sticky group attributes [6-10](#)
 - sticky type [6-3](#)
 - cookie
 - sticky group attributes [6-11](#)
 - sticky type [6-3](#)
 - deep packet inspection
 - class map match conditions [11-15](#)
 - policy map rules and actions [11-47](#)
 - header
 - sticky client identification [6-4](#)
 - sticky group attributes [6-11](#)
 - sticky type [6-4](#)
 - load balancing conditions and options [4-27](#)
 - optimization policy map rules and actions [11-53](#)
 - parameter map
 - attributes [7-8](#)
 - configuring [7-8](#)
 - probe
 - attributes [5-31](#)
 - configuring headers [5-41](#)
 - retcode maps [5-21](#)
 - return code map configuration options [5-22](#)
 - protocol inspection conditions and options [4-18](#)
 - HTTPS
 - ACE modules, enabling [2-5](#)
 - configuring protocol inspection [4-15](#)
 - load balancing conditions and options [4-27](#)
 - probe
 - attributes [5-33](#)
 - configuring headers [5-41](#)
 - protocol inspection conditions and options [4-18](#)
-
- ICMP service parameters, for object groups [3-58](#)
 - image optimization [12-2](#)
 - IMAP probe attributes [5-35](#)
 - Import Failed, configuration status [3-64, 3-66](#)
 - importing
 - ACE modules [2-11](#)
 - CSM [2-13](#)

- device failures [16-3](#)
- GSS devices [2-14](#)
- overview [2-7](#)
- SSL
 - certificates [8-6](#)
 - keys [8-9](#)
- installing ACE licenses [3-29](#)
- intended audience [ix](#)
- interface
 - ANM [1-5](#)
 - buttons [1-9](#)
 - configuring
 - on 7600 series routers [2-28](#)
 - on chassis [2-28](#)
 - definition [GL-3](#)
 - gigabit Ethernet, configuring [9-17](#)
 - table conventions [1-11](#)
 - VLAN options, configuring [9-7](#)
- IP addresses, for object groups [3-53](#)
- IP discovery
 - failure [16-3](#)
- IP netmask
 - for sticky client identification [6-4](#)
 - sticky group attributes [6-12](#)
 - sticky type [6-4](#)

K

- key
 - exporting for SSL [8-14](#)
 - importing for SSL [8-9](#)
 - SSL [8-8](#)
- key pair, generating [8-11](#)

L

- latency optimization, configuring [4-38](#)
- Layer 2 VLANs, configuring [2-37](#)

Layer 3/4

- management traffic
 - class map match conditions [11-12](#)
 - policy map rules and actions [11-37](#)
- network traffic
 - class map match conditions [11-9](#)
 - policy map rules and actions [11-38](#)

Layer 3 VLANs, configuring [2-38](#)

Layer 4 payload

- sticky group attributes [6-12](#)
- sticky type [6-4](#)

Layer 7

- configuring load balancing [4-25](#)
- default load balancing on virtual servers [4-35](#)
- FTP command inspection
 - class map match conditions [11-21](#)
 - policy map rules and actions [11-45](#)
- HTTP deep packet inspection
 - class map match conditions [11-15](#)
 - policy map rules and actions [11-47](#)
- HTTP optimization policy map rules and actions [11-53](#)
- load balancing
 - HTTP/HTTPS conditions and options [4-27](#)
 - setting match conditions [4-26](#)
- server load balancing
 - class map match conditions [11-13](#)
 - policy map rules and actions [11-56](#)
- SIP deep packet inspection
 - class map match conditions [11-28](#)
 - policy map rules and actions [11-62](#)
- Skinny deep packet inspection policy map rules and actions [11-64](#)
- least bandwidth, load-balancing method [5-2](#)
- leastconns, load-balancing method [5-2](#)
- least loaded, load-balancing method [5-2](#)
- license
 - compliance [15-60](#)
 - errors, removing [15-61](#)

- installing ACE licenses [3-29](#)
- managing for ACE devices [3-27](#)
- relationship between ANM and ACE licenses [3-27](#)
- removing ACE licenses [3-30](#)
- updating ACE licenses [3-31](#)
- viewing ACE license details [3-32](#)
- licenses
 - ANM, removing [15-61](#)
 - overview of ANM [1-4](#)
- lifeline
 - guidelines for use [16-4](#)
 - overview [16-3](#)
- lifeline management [15-65](#)
- load balancing
 - configuration overview [4-1](#)
 - configuring
 - real servers [5-1, 5-4](#)
 - server farms [5-1, 5-12](#)
 - sticky groups [6-7](#)
 - virtual servers [4-25](#)
 - definition [GL-4](#)
 - hash address [5-2](#)
 - hash cookie [5-2](#)
 - hash header [5-2](#)
 - hash url [5-2](#)
 - least bandwidth [5-2](#)
 - leastconns [5-2](#)
 - least loaded [5-2](#)
 - monitoring [14-12, 14-15](#)
 - overview [4-1, 5-1](#)
 - predictors [5-2](#)
 - response [5-2](#)
 - roundrobin [5-2](#)
- local resource class [3-33](#)
 - auditing [3-38](#)
 - configuring [3-41](#)
 - deleting [3-42](#)
 - using [3-41](#)
- logging, syslog levels [3-12](#)

- logging in
 - to ANM [1-2](#)

M

- managing
 - 7600 series routers [2-52](#)
 - ACLs [3-60](#)
 - ANM [15-54](#)
 - chassis [2-52](#)
 - devices [2-1](#)
 - domains [15-49](#)
 - organizations [15-31](#)
 - real servers [5-6](#)
 - resource classes [3-32](#)
 - user accounts [15-38](#)
 - user roles [15-43](#)
 - virtual contexts [3-63](#)
 - virtual servers [4-48](#)
 - VLANs [2-35](#)
- match condition
 - class map
 - generic server load balancing [11-22](#)
 - Layer 3/4 management traffic [11-12](#)
 - Layer 3/4 network traffic [11-9](#)
 - Layer 7 FTP command inspection [11-21](#)
 - Layer 7 HTTP deep packet inspection [11-15](#)
 - Layer 7 server load balancing [11-13](#)
 - Layer 7 SIP deep packet inspection [11-28](#)
 - RADIUS server load balancing [11-23](#)
 - RTSP server load balancing [11-25](#)
 - SIP server load balancing [11-27](#)
 - setting for
 - class maps [11-8](#)
 - Layer 7 load balancing [4-26](#)
 - optimization [4-39](#)
 - SIP protocol inspection [4-22](#)
- MD5, definition [GL-4](#)
- menus, understanding [1-6](#)

MIB, definition [GL-4](#)

MIME types, supported [7-21](#)

modifying

deployed virtual servers [4-50](#)

domains [2-51, 15-52](#)

global resource class [3-39](#)

high availability groups [10-9](#)

organizations [15-35](#)

real servers [5-8](#)

staged virtual servers [4-50](#)

user accounts [2-42, 15-41](#)

user-defined groups [2-55](#)

user roles [2-46, 15-48](#)

virtual contexts [3-67](#)

module

configuring access credentials [2-17](#)

discovery process [2-20](#)

monitoring discovery progress [2-20](#)

running discovery [2-20](#)

viewing

by chassis [2-61](#)

by router [2-61](#)

monitoring

alarms [14-30](#)

device audit trail logs [14-23](#)

devices [14-2](#)

events [14-21](#)

load balancing [14-12, 14-15](#)

probes [14-15](#)

traffic [14-9](#)

multi-match policy map [11-31](#)

configuring for virtual servers [4-47](#)

definition [GL-4](#)

network object group

configuring [3-52](#)

IP addresses [3-53](#)

subnet objects [3-54](#)

O

object, configuring for virtual servers [4-6](#)

object group

configuring [3-52](#)

ICMP service parameters [3-58](#)

IP addresses [3-53](#)

protocols [3-55](#)

subnet objects [3-54](#)

TCP/UDP service parameters [3-56](#)

operational states, real servers [5-9](#)

optimization

action list [12-3](#)

additional configuration options [4-43](#)

configuration overview [12-13](#)

configuring [4-37](#)

action lists [4-39](#)

globally on ACE appliances [12-16](#)

match conditions [4-39](#)

parameter maps [12-12](#)

traffic policies [12-13](#)

delta optimization [12-1](#)

enabling on virtual servers [12-16](#)

image [12-2](#)

match criteria [4-39](#)

overview [12-1](#)

redirect [12-2](#)

traffic policies [12-2](#)

typical configuration flow [12-2](#)

virtual server, additional configuration options [4-43](#)

optimization parameter map

attributes [7-11](#)

N

Name Address Translation

configuring [9-10](#)

definition [GL-4](#)

NAT

configuring [9-10](#)

- configuring [7-10](#)
- organizations
 - definition [1-15](#)
- Out of Sync, configuration status [3-64, 3-66](#)
- overview
 - ACL configuration [3-43](#)
 - adding supported devices [2-7](#)
 - admin icon [15-2](#)
 - application acceleration [12-1](#)
 - building blocks [13-1](#)
 - class maps [11-2, 11-3](#)
 - configuration building blocks [13-1](#)
 - global and local resource classes [3-33](#)
 - health monitoring [5-23](#)
 - importing devices [2-7](#)
 - load balancing [4-1, 5-1](#)
 - load-balancing predictors [5-2](#)
 - managing devices [2-2](#)
 - optimization [12-1](#)
 - optimization traffic policies [12-13](#)
 - parameter maps [7-1](#)
 - policy maps [11-2, 11-4](#)
 - protocol inspection [11-5](#)
 - real server [5-3](#)
 - resource classes [3-32](#)
 - server farm [5-3](#)
 - server health monitoring [5-23](#)
 - server load balancing [5-1](#)
 - SSL [8-1](#)
 - stickiness [6-1](#)
 - sticky group [6-6](#)
 - sticky table [6-6](#)
 - traffic policies [11-1](#)
 - user-defined groups [2-54](#)
 - using SSL keys and certificates [8-3](#)
 - virtual server [4-2](#)

P

- parameter expander functions [12-11](#)
- parameter map
 - ACE device support [7-1](#)
 - attributes
 - connection [7-2](#)
 - generic [7-7](#)
 - HTTP [7-8](#)
 - optimization [7-11](#)
 - RTSP [7-17](#)
 - SIP [7-18](#)
 - Skinny [7-20](#)
 - configuring
 - connection [7-2](#)
 - for SSL [8-15](#)
 - generic [7-7](#)
 - HTTP [7-8](#)
 - optimization [7-10, 12-12](#)
 - RTSP [7-17](#)
 - SIP [7-18](#)
 - Skinny [7-20](#)
 - overview [7-1](#)
 - types of [7-1](#)
 - using with
 - Layer 3/Layer 4 policy maps [11-5](#)
 - policy maps [7-1](#)
- parameter map cipher, configuring for SSL [8-17](#)
- passwords, changing
 - admin [15-35](#)
 - for accounts [1-4](#)
 - for chassis [2-57](#)
 - for the ACE [2-58](#)
 - in login screen [1-4](#)
- PAT
 - configuring [9-10](#)
 - definition [6L-4](#)
- peers, high availability [10-5](#)
- ping

- between devices [14-33](#)
- definition [GL-5](#)
- policy map [11-33](#)
 - ACE device support [11-31](#)
 - associating with VLAN interface [9-7](#)
 - configuring [11-30](#)
 - match type
 - all-match [11-31](#)
 - first-match [11-31](#)
 - multi-match [11-31](#)
 - overview [11-2, 11-4](#)
 - rule and action topic reference [11-33](#)
 - rules and actions
 - generic server load balancing [11-34](#)
 - Layer 3/4 management traffic [11-37](#)
 - Layer 3/4 network traffic [11-38](#)
 - Layer 7 FTP command inspection [11-45](#)
 - Layer 7 HTTP deep packet inspection [11-47](#)
 - Layer 7 HTTP optimization [11-53](#)
 - Layer 7 server load balancing [11-56](#)
 - Layer 7 SIP deep packet inspection [11-62](#)
 - Layer 7 Skinny deep packet inspection [11-64](#)
 - RADIUS server load balancing [11-66](#)
 - RDP server load balancing [11-68](#)
 - RTSP server load balancing [11-70](#)
 - SIP server load balancing [11-73](#)
 - setting rules and actions [11-33](#)
- polling
 - enabling [15-63](#)
 - parameters, setting [14-19](#)
 - restarting
 - for devices [2-59](#)
 - for virtual contexts [3-69](#)
 - status
 - for devices [2-60](#)
 - for virtual contexts [3-65](#)
- POP probe attributes [5-35](#)
- Port Address Translation
 - configuring [9-10](#)
 - definition [GL-4](#)
- port channel interfaces
 - attributes [9-21](#)
 - configuring [9-21](#)
- ports
 - ANM, used by [A-1](#)
 - definition [GL-5](#)
 - reference [A-1](#)
 - TCP [A-1](#)
 - UDP [A-2](#)
- predictor
 - hash address [5-2](#)
 - hash cookie [5-2](#)
 - hash header [5-2](#)
 - hash url [5-2](#)
 - least bandwidth [5-2](#)
 - leastconns [5-2](#)
 - least loaded [5-2](#)
 - response [5-2](#)
 - roundrobin [5-2](#)
- predictor method
 - attributes [5-17](#)
 - configuring for server farms [5-16](#)
- primary attributes
 - 7600 series routers [2-26](#)
 - chassis [2-26](#)
 - configuration building blocks [13-7](#)
 - CSM [2-23](#)
 - CSS [2-24](#)
 - GSS [2-25](#)
 - virtual contexts [3-11](#)
- probe
 - attribute tables [5-29](#)
 - configuring expect status [5-42](#)
 - configuring for health monitoring [5-25](#)
 - configuring SNMP OIDs [5-43](#)
 - DNS [5-30](#)
 - Echo-TCP [5-30](#)
 - Echo-UDP [5-30](#)

- Finger [5-31](#)
- FTP [5-31](#)
- HTTP [5-31](#)
- HTTPS [5-33](#)
- IMAP [5-35](#)
- POP [5-35](#)
- RADIUS [5-36](#)
- RTSP [5-36](#)
- scripted [5-37](#)
- scripting using TCL [5-24](#)
- SIP-TCP [5-38](#)
- SIP-UDP [5-38](#)
- SMTP [5-39](#)
- SNMP [5-39](#)
- TCP [5-39](#)
- Telnet [5-40](#)
- types for real server monitoring [5-26](#)
- UDP [5-40](#)
- probes
 - monitoring [14-15](#)
- process, for traffic classification [11-3](#)
- protocol inspection
 - configuring for virtual servers [4-14](#)
 - configuring match criteria
 - HTTP and HTTPS [4-17](#)
 - SIP [4-22](#)
 - HTTP/HTTPS conditions and options [4-18](#)
 - overview [11-5](#)
 - SIP conditions and options [4-23](#)
 - virtual server options [4-15](#)
- protocol names and numbers [3-49](#)
- protocols
 - for object groups [3-55](#)
 - for virtual contexts [3-4](#)
 - for virtual servers [4-8](#)
- proxy service, configuring for SSL [8-22](#)

R

RADIUS

- probe attributes [5-36](#)
- server load balancing
 - class map match conditions [11-23](#)
 - policy map rules and actions [11-66](#)
- sticky group attributes [6-13](#)
- sticky type [6-5](#)

RBAC, definition [GL-5](#)

RDP server load balancing policy map rules and actions [11-68](#)

real server

- activating [5-7](#)
- adding to server farm [5-14](#)
- configuration attributes [5-4, 5-15](#)
- configuring [5-4](#)
 - load balancing service [5-1](#)
- definition [GL-5](#)
- health monitoring [5-23, 5-25](#)
- modifying [5-8](#)
- operational states [5-9](#)
- overview [5-3](#)
- suspending [5-7](#)
- viewing all [5-9](#)

redirect optimization [12-2](#)

redundancy

- configuration requirements [10-24](#)
- configuration synchronization [10-23](#)
- definition [GL-5](#)
- FT VLAN [10-23](#)
- protocol [10-21](#)
- task overview [10-4](#)

removing

- ACE license [3-30](#)
- ANM license files [15-61](#)
- rules from roles [2-47](#)

resource, required for sticky groups [6-7](#)

resource class

- adding [3-36](#)
 - allocation constraints [3-34](#)
 - applying global resource classes [3-37](#)
 - attributes [3-34](#)
 - auditing local and global resource classes [3-38](#)
 - configuring
 - globally [3-36](#)
 - locally [3-41](#)
 - definition [GL-5](#)
 - deleting
 - global resource class [3-40](#)
 - local resource class [3-42](#)
 - deploying global resource class [3-37](#)
 - global [3-33](#)
 - local [3-33](#)
 - managing [3-32](#)
 - modifying [3-39](#)
 - overview [3-32](#)
 - using
 - global classes [3-35](#)
 - local classes [3-41](#)
 - viewing use by contexts [3-43](#)
 - resources, allocation constraints [3-34](#)
 - resource usage, viewing [14-5](#)
 - response load-balancing method [5-2](#)
 - restarting
 - ANM (see the Installation Guide) [15-61](#)
 - restarting device polling [2-59](#)
 - restoring data [16-8](#)
 - reverting to old data [16-8](#)
 - role
 - definition [GL-7](#)
 - deleting [2-40](#)
 - role-based access control
 - containment overview [15-4](#)
 - definition [GL-5](#)
 - roundrobin, load-balancing predictor [5-2](#)
 - routed ports, configuring [2-33](#)
 - routes, configuring static routes [2-27](#)
 - RSA, definition [GL-5](#)
 - RTSP
 - header
 - sticky group attributes [6-14](#)
 - sticky type [6-5](#)
 - parameter map
 - attributes [7-17](#)
 - configuring [7-17](#)
 - probe attributes [5-36](#)
 - server load balancing
 - class map match conditions [11-25](#)
 - policy map rules and actions [11-70](#)
 - rule
 - changing for roles [2-47](#)
 - setting for policy maps [11-33](#)
-
- ## S
- screens, understanding [1-6](#)
 - scripted probe
 - attributes [5-37](#)
 - overview [5-24](#)
 - server
 - activating
 - real [5-7](#)
 - virtual [4-51](#)
 - managing [5-6](#)
 - suspending
 - real [5-7](#)
 - virtual [4-52](#)
 - server farm
 - adding real servers [5-14](#)
 - configuration attributes [4-29, 5-13](#)
 - configuring
 - HTTP return error-code checking [5-21](#)
 - load balancing [5-1, 5-12](#)
 - predictor method [5-16](#)
 - definition [GL-6](#)
 - health monitoring [5-23](#)

- overview [5-3](#)
- predictor method attributes [5-17](#)
- viewing list of [5-23](#)
- Server Load Balancer (SLB), definition [GL-6](#)
- server load balancing
 - generic class map match conditions [11-22](#)
 - generic policy map rules and actions [11-34](#)
 - Layer 7 class map match conditions [11-13](#)
 - Layer 7 policy map rules and actions [11-56](#)
 - overview [4-1, 5-1](#)
 - RADIUS class map match conditions [11-23](#)
 - RADIUS policy map rules and actions [11-66](#)
 - RDP policy map rules and actions [11-68](#)
 - RTSP class map match conditions [11-25](#)
 - RTSP policy map rules and actions [11-70](#)
 - SIP class map match conditions [11-27](#)
 - SIP policy map rules and actions [11-73](#)
- service, definition [GL-6](#)
- service object group
 - configuring [3-52](#)
 - ICMP service parameters [3-58](#)
 - protocols [3-55](#)
 - TCP/UDP service parameters [3-56](#)
- setup sequence
 - SSL [8-4](#)
- shared object
 - and deleting virtual servers [4-7](#)
 - configuring [4-7](#)
 - configuring for virtual servers [4-6](#)
- SIP
 - configuring protocol inspection [4-16](#)
 - deep packet inspection
 - class map match conditions [11-28](#)
 - policy map rules and actions [11-62](#)
 - header sticky type [6-5](#)
 - parameter map
 - attributes [7-18](#)
 - configuring [7-18](#)
 - protocol inspection conditions and options [4-23](#)
 - server load balancing
 - class map match conditions [11-27](#)
 - policy map rules and actions [11-73](#)
- SIP-TCP probe attributes [5-38](#)
- SIP-UDP probe attributes [5-38](#)
- Skinny
 - deep packet inspection policy map rules and actions [11-64](#)
 - parameter map
 - attributes [7-20](#)
 - configuring [7-20](#)
- SMTP
 - configuring for e-mail notifications [14-32](#)
 - probe attributes [5-39](#)
- SNM, enabling polling [2-6](#)
- SNMP
 - configuration attributes [3-19](#)
 - configuring
 - communities [3-20](#)
 - for virtual contexts [3-19](#)
 - notification [3-24](#)
 - trap destination hosts [3-23](#)
 - version 3 users [3-21](#)
 - credentials [2-18](#)
 - enabling collection [3-69](#)
 - probe attributes [5-39](#)
 - trap destination host configuration [3-23](#)
 - user configuration attributes [3-22](#)
- special characters for matching string expressions [11-76](#)
- special configuration file, definition [GL-6](#)
- SSH
 - ACE appliance, enabling [2-5](#)
 - ACE modules, enabling [2-5](#)
 - chassis, enabling [2-5](#)
 - enabling on ACE modules for discovery [2-17](#)
- SSH2, chassis requirement in ANM [2-5](#)
- SSL
 - certificate
 - exporting [8-12](#)

- exporting attributes [8-13](#)
- importing [8-6](#)
- importing attributes [8-7](#)
- overview [8-3](#)
- using [8-5](#)
- configuring
 - authorization group certificates [8-24](#)
 - chain group certificates [8-19](#)
 - chain group parameters [8-18](#)
 - CSR parameters [8-19](#)
 - for virtual servers [4-12](#)
 - parameter map [8-15](#)
 - parameter map cipher [8-17](#)
 - proxy service [8-22](#)
- CSR parameters [8-20](#)
- editing
 - CSR parameters [8-20](#)
 - parameter map cipher info [8-17](#)
 - parameter maps [8-16, 8-22](#)
- exporting
 - certificates [8-12](#)
 - key pairs [8-14](#)
 - keys [8-14](#)
- generating
 - CSR [8-21](#)
 - key pair [8-11](#)
- importing
 - certificates [8-6](#)
 - keys [8-9](#)
- key
 - exporting [8-14](#)
 - importing [8-9](#)
 - overview [8-3](#)
 - using [8-8](#)
- key pair
 - exporting [8-14](#)
 - generating [8-11](#)
 - importing attributes [8-9](#)
- objects, deleting [8-2](#)
- overview [8-1](#)
- parameter map cipher table [8-17](#)
- parameter maps [8-16, 8-22](#)
- procedure overview [8-3](#)
- setup sequence
 - using [8-4](#)
- SSL certificate, using [8-5](#)
- SSL key, using [8-8](#)
- SSL setup sequence, using [8-4](#)
- staged virtual server
 - deploying [4-49](#)
 - viewing all [4-49](#)
- static ARP, configuring [9-9](#)
- static route
 - configuring [2-27, 9-14](#)
 - viewing by context [9-15](#)
- statistics
 - ANM server [15-62](#)
- status, Cisco ANM server [15-54](#)
- stickiness
 - cookie-based [6-3](#)
 - HTTP content [6-3](#)
 - HTTP cookie [6-3](#)
 - HTTP header [6-4](#)
 - IP netmask [6-4](#)
 - Layer 4 payload [6-4](#)
 - overview [6-1](#)
 - RADIUS [6-5](#)
 - RTSP header [6-5](#)
 - SIP header [6-5](#)
 - sticky group [6-6](#)
 - sticky table [6-6](#)
 - types [6-2](#)
- sticky
 - cookies for client identification [6-3](#)
 - definition [GL-6](#)
 - e-commerce application requirements [6-1](#)
 - groups [6-6](#)
 - HTTP header for client identification [6-4](#)

- IP netmask for client identification [6-4](#)
- overview [6-1](#)
- table, overview [6-6](#)
- types [6-2](#)
- sticky group
 - attributes
 - HTTP content [6-10](#)
 - HTTP cookie [6-11](#)
 - HTTP header [6-11](#)
 - IP netmask [6-12](#)
 - Layer 4 payload [6-12](#)
 - RADIUS [6-13](#)
 - RTSP header [6-14](#)
 - configuration options [4-32, 6-8](#)
 - configuring
 - load balancing [6-7](#)
 - sticky statics [6-14](#)
 - overview [6-6](#)
 - required resource allocation [6-7](#)
 - type-specific attributes [6-9](#)
 - viewing [6-14](#)
- sticky statics, configuring for sticky groups [6-14](#)
- sticky table overview [6-6](#)
- sticky type
 - HTTP content [6-3](#)
 - HTTP cookie [6-3](#)
 - HTTP header [6-4](#)
 - IP netmask [6-4](#)
 - Layer 4 payload [6-4](#)
 - RADIUS [6-5](#)
 - RTSP header [6-5](#)
 - SIP header [6-5](#)
- string expression, special characters [11-76](#)
- subnet objects, for object groups [3-54](#)
- supervisor module, viewing by chassis [2-61](#)
- suspend, definition [GL-6](#)
- suspending
 - DNS rules for GSS [4-54](#)
 - real servers [5-7](#)

- virtual servers [4-52](#)
- switchover [10-22](#)
- switch virtual interfaces, configuring [2-32](#)
- synchronization of configuration [10-23](#)
- synchronizing
 - ACE module configurations [2-53](#)
 - configurations for high availability [10-19](#)
 - contexts created in CLI [4-2, 4-4](#)
 - device configurations [2-52](#)
 - virtual context configurations [3-66](#)
- sync status, virtual contexts [3-64](#)
- syslog
 - configuration attributes [3-13](#)
 - configuring
 - logging [3-12](#)
 - logging levels [3-12](#)
 - log hosts [3-16](#)
 - log messages [3-17](#)
 - log rate limits [3-18](#)
 - settings for synchronizing with ACE CLI
 - autosync [3-66](#)
- syslog logging, configuring [3-12](#)
- syslog messages
 - enabling ACE [2-15](#)

T

- table
 - conventions [1-11](#)
 - customizing [1-11](#)
 - default distance values [2-28](#)
 - filtering information in [1-11](#)
 - ICMP type numbers and names [3-59](#)
 - protocol names and numbers [3-49](#)
 - topic reference for policy map rules and actions [11-33](#)
- table conventions [1-11](#)
- tables
 - for probe attributes [5-29](#)
 - for sticky group attributes [6-9](#)

tagging building blocks [13-4, 13-7](#)
 takeover, forcing in high availability [10-11](#)
 task overview, redundancy [10-4](#)
 TCL script
 health monitoring [5-24](#)
 overview [5-24](#)
 TCP
 options for connection parameter maps [7-6](#)
 probe attributes [5-39](#)
 service parameters for object groups [3-56](#)
 TCP ports
 ANM, used by [A-1](#)
 Telnet
 configuring credentials [2-18](#)
 import method for chassis [2-5](#)
 probe attributes [5-40](#)
 template. See building block.
 terminating
 current user sessions [15-42](#)
 terminology used in ANM [1-15](#)
 threshold, definition [GL-6](#)
 topic reference for configuring rules and actions [11-33](#)
 traceroute, definition [GL-7](#)
 traffic, monitoring [14-9](#)
 traffic class components [11-3, 11-6](#)
 traffic classification process [11-3](#)
 traffic policy
 ACE device support [11-2](#)
 components [11-4](#)
 configuring [11-1](#)
 for application acceleration [12-2](#)
 for optimization [12-2](#)
 lookup order [11-4](#)
 overview [11-1](#)
 troubleshooting
 importing, ACE module state [2-11](#)
 IP discovery [16-3](#)
 troubleshooting, using lifeline [16-3](#)
 trunk ports, configuring [2-30](#)

types of user [15-5](#)

U

UDP ports
 ANM, used by [A-2](#)
 UDP probe attributes [5-40](#)
 UDP service parameters, for object groups [3-56](#)
 understanding
 domains [15-7](#)
 operations privileges [15-6](#)
 roles [15-5](#)
 user groups [15-7](#)
 Unprovisioned, configuration status [3-64, 3-66](#)
 updating, configuration values [16-1](#)
 updating ACE licenses [3-31](#)
 upgrading virtual contexts [3-68](#)
 URL mapping, configuration options [12-9](#)
 user-defined groups
 adding [2-54](#)
 deleting [2-56](#)
 duplicating [2-56](#)
 modifying [2-55](#)
 overview [2-54](#)
 user roles, definition [GL-7](#)
 using
 ACLs [3-43](#)
 building blocks [13-1](#)
 virtual contexts [3-1](#)

V

versions of building blocks [13-4](#)
 viewing [15-65](#)
 7600 series router VLANs [2-36](#)
 ACE license details [3-27](#)
 ACLs by context [3-60](#)
 all devices [2-60](#)

- all real servers [5-9](#)
- all server farms [5-23](#)
- all sticky groups [6-14](#)
- all virtual servers [4-55](#)
- building block use [13-9](#)
- BVI interfaces by context [9-14](#)
- chassis VLANs [2-36](#)
- configuration building block use [13-9](#)
- current user sessions [15-42](#)
- license compliance [15-60](#)
- license information [3-32](#)
- ports [2-34](#)
- resource class use on contexts [3-43](#)
- staged virtual servers [4-49](#)
- static routes by context [9-15](#)
- virtual server details [4-54](#)
- virtual servers by context [4-51](#)
- VLAN interfaces by context [9-6](#)
- VIP Answer table, and GSS [4-53](#)
- virtual context
 - comparing configuration with building block [3-62](#)
 - configuration
 - attributes [3-3](#)
 - audit [3-62](#)
 - options [3-5, 3-6](#)
 - configuring [3-1](#)
 - BVI interfaces [9-12](#)
 - class map match conditions [11-8](#)
 - class maps [11-6](#)
 - global policies [3-26](#)
 - load balancing services [4-1](#)
 - policy map rules and actions [11-33](#)
 - policy maps [11-30](#)
 - primary attributes [3-11](#)
 - resource classes [3-41](#)
 - SNMP [3-19](#)
 - static routes [9-14](#)
 - syslog [3-12](#)
 - system attributes [3-11](#)
 - VLAN interfaces [9-2](#)
 - creating [3-2](#)
 - definition [GL-7](#)
 - deleting [3-68](#)
 - description [3-1](#)
 - expert options [3-62](#)
 - license file name [15-57](#)
 - managing [3-63](#)
 - modifying [3-67](#)
 - monitoring resource usage [14-6](#)
 - polling
 - restarting [3-69](#)
 - viewing status [3-65](#)
 - protocols [3-4](#)
 - synchronizing configurations [3-66](#)
 - sync status [3-64](#)
 - syslog setup for autosync [3-66](#)
 - upgrading [3-68](#)
 - using
 - for configuration building blocks [13-5](#)
 - overview [3-1](#)
 - viewing
 - all contexts [3-64](#)
 - BVI interfaces [9-14](#)
 - polling status [3-65](#)
 - resource class use [3-43](#)
 - static routes [9-15](#)
 - sync status [3-64](#)
 - VLANs [9-6](#)
- Virtual Local Area Network (VLAN), definition [GL-7](#)
- virtual server [4-25, 4-43](#)
 - activating [4-51](#)
 - additional options [4-3](#)
 - advanced view properties [4-9](#)
 - and user roles [4-3](#)
 - application acceleration [4-37](#)
 - application acceleration, additional configuration options [4-43](#)
 - basic view properties [4-11](#)

- configuration
 - methods [4-4](#)
 - recommendations [4-4](#)
 - configuration subsets [4-5](#)
 - configuring [4-1, 4-2, 4-4](#)
 - application acceleration [4-37](#)
 - default Layer 7 load balancing [4-35](#)
 - in ANM [4-2](#)
 - in CLI [4-2, 4-4](#)
 - Layer 7 load balancing [4-25](#)
 - NAT [4-47](#)
 - optimization [4-37, 12-16](#)
 - properties [4-8](#)
 - protocol inspection [4-14](#)
 - shared objects [4-6](#)
 - SSL [4-12](#)
 - definition [GL-7](#)
 - deleting and shared objects [4-7](#)
 - deployed servers, modifying [4-50](#)
 - deploying staged servers [4-49](#)
 - load balancing
 - default [4-35](#)
 - Layer 7 [4-25](#)
 - managing [4-48](#)
 - minimum configuration [4-2](#)
 - modifying
 - deployed servers [4-50](#)
 - staged servers [4-50](#)
 - optimization [4-37](#)
 - overview [4-2](#)
 - properties
 - advanced view [4-9](#)
 - basic view [4-11](#)
 - protocols [4-8](#)
 - recommendations for configuring [4-4](#)
 - shared objects [4-4, 4-6](#)
 - SSL attributes [4-13](#)
 - staged servers
 - deploying [4-49](#)
 - modifying [4-50](#)
 - viewing [4-49](#)
 - suspending [4-52](#)
 - viewing
 - all [4-55](#)
 - by context [4-51](#)
 - details [4-54](#)
 - servers [4-51](#)
 - staged servers [4-49](#)
- VLAN
- adding to 7600 series router [2-35](#)
 - adding to chassis [2-35](#)
 - configuring
 - access control [9-8](#)
 - ACLs [9-8](#)
 - DHCP relay [9-12](#)
 - Layer 2 VLANs [2-37](#)
 - Layer 3 VLANs [2-38](#)
 - NAT [9-10](#)
 - policy maps [9-7](#)
 - static ARP [9-9](#)
 - creating VLAN groups [2-39](#)
 - definition [GL-7](#)
 - FT VLAN for redundancy [10-23](#)
 - interface
 - access control [9-8](#)
 - attributes [9-3](#)
 - configuring [9-2](#)
 - DHCP relay [9-12](#)
 - NAT pools [9-10](#)
 - options [9-7](#)
 - policy maps [9-7](#)
 - static ARP [9-9](#)
 - viewing [9-6](#)
 - managing [2-35](#)
 - modifying
 - on 7600 series router [2-38](#)
 - on chassis [2-38](#)
 - viewing

by 7600 series router [2-36](#)

by chassis [2-36](#)

VLAN group, creating [2-39](#)

VLAN interfaces

attributes [9-3](#)

configuring [9-2](#)

access control [9-8](#)

for virtual contexts [9-2](#)

options [9-7](#)

policy maps [9-7](#)

viewing by context [9-6](#)

VLAN Trunking Protocol, definition [GL-7](#)

VTP, definition [GL-7](#)

VTP domain, definition [GL-7](#)

W

Web server, definition [GL-7](#)

weighted roundrobin. See roundrobin

X

XSLT merge, configuration options [4-45](#)

