Cisco Application Control Engine
Module Administration Guide

Software Version A2(1.0)
March 2008

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

Text Part Number: OL-11865-01
CONTENTS

Preface xv
   Audience xvi
   How to Use This Guide xvi
   Related Documentation xviii
   Symbols and Conventions xx
   Obtaining Documentation, Obtaining Support, and Security Guidelines xxii
   Open Source License Acknowledgements 1-xxii
      OpenSSL/Open SSL Project 1-xxii
      License Issues 1-xxii

Chapter 1 1-1
   Setting Up the ACE 1-2
      Establishing a Console Connection on the ACE 1-2
      Sessioning and Logging In to the ACE 1-3
      Changing the Administrative Password 1-5
         Resetting the Administrator Account Password 1-7
      Assigning a Name to the ACE 1-8
      Configuring an ACE Inactivity Timeout 1-9
      Configuring a Message-of-the-Day Banner 1-10
      Configuring the Date and Time 1-12
         Configuring the Time Zone 1-12
         Adjusting for Daylight Saving Time 1-15
         Viewing the System Clock Settings 1-17
Cisco Application Control Engine Module Administration Guide

Contents

Configuring Terminal Settings 1-17
  Configuring Terminal Display Attributes 1-18
  Configuring Terminal Line Settings 1-20
    Configuring Console Line Settings 1-20
    Configuring Virtual Terminal Line Settings 1-21
Modifying the Boot Configuration 1-22
  Setting the Boot Method from the Configuration Register 1-23
    Booting the ACE from the rommon Prompt 1-24
  Setting the BOOT Environment Variable 1-25
  Displaying the ACE Boot Configuration 1-26
Restarting the ACE 1-27
  Restarting the ACE from the CLI 1-27
  Restarting the ACE from the Catalyst CLI 1-28
Shutting Down the ACE 1-28

CHAPTER 2
Enabling Remote Access to the ACE 2-1
  Remote Access Configuration Quick Start 2-2
  Configuring Remote Network Management Traffic Services 2-4
    Creating and Configuring a Remote Management Class Map 2-5
      Defining a Class Map Description 2-6
      Defining Remote Network Management Protocol Match Criteria 2-7
    Creating a Layer 3 and Layer 4 Remote Access Policy Map 2-9
      Creating a Layer 3 and Layer 4 Policy Map for Network Management Traffic Received by the ACE 2-9
      Defining a Layer 3 and Layer 4 Policy Map Description 2-10
      Specifying a Layer 3 and Layer 4 Traffic Class With the Traffic Policy 2-11
      Defining Layer 3 and Layer 4 Management Traffic Policy Actions 2-12
    Applying a Service Policy 2-13
  Configuring Telnet Management Sessions 2-15
Configuring SSH Management Sessions 2-16
  Configuring Maximum Number of SSH Sessions 2-16
  Generating SSH Host Key Pairs 2-17
Terminating an Active User Session 2-19
Enabling ICMP Messages to the ACE 2-19
Directly Accessing a User Context Through SSH 2-21
Example of a Remote Access Configuration 2-23
Viewing Session Information 2-24
  Showing Telnet Session Information 2-24
  Showing SSH Session Information 2-25
  Showing SSH Key Details 2-26

CHAPTER 3
Managing ACE Software Licenses 3-1
  Available ACE Licenses 3-2
  Ordering an Upgrade License and Generating a Key 3-3
  Copying a License File to the ACE 3-4
  Installing a New or Upgrade License File 3-5
  Replacing a Demo License with a Permanent License 3-7
  Removing a License 3-8
    Removing a Module Bandwidth License 3-9
    Removing an SSL TPS License 3-9
    Removing a User Context License 3-10
  Backing Up a License File 3-13
  Displaying License Configurations and Statistics 3-14

CHAPTER 5
Managing the ACE Software 5-1
  Saving Configuration Files 5-1
    Saving the Configuration File in Flash Memory 5-2
Contents

- Saving Configuration Files to a Remote Server 5-3
- Copying the Configuration File to the disk0: File System 5-5
- Merging the Startup-Configuration File with the Running-Configuration File 5-6
- Viewing Configuration Files 5-6
- Viewing User Context Running-Config Files from the Admin Context 5-9
- Clearing the Startup-Configuration File 5-10

Loading Configuration Files from a Remote Server 5-11

Using the File System on the ACE 5-12
- Listing the Files in a Directory 5-13
- Copying Files 5-15
  - Copying Files to Another Directory on the ACE 5-15
  - Copying Licenses 5-16
  - Copying a Packet Capture Buffer 5-16
  - Copying Files to a Remote Server 5-17
  - Copying Files from a Remote Server 5-19
  - Copying an ACE Software System Image to a Remote Server 5-20

Uncompressing Files in the disk0: File System 5-21
- Untarring Files in the disk0: File System 5-21
- Creating a New Directory 5-22
- Deleting an Existing Directory 5-23
- Moving Files 5-23
- Deleting Files 5-24
- Displaying File Contents 5-25
- Saving show Command Output to a File 5-25

Viewing and Copying Core Dumps 5-27
- Copying Core Dumps 5-27
- Clearing the Core Directory 5-29
- Deleting a Core Dump File 5-29
Capturing and Copying Packet Information 5-30
  Capturing Packet Information 5-31
  Copying Capture Buffer Information 5-34
  Viewing Packet Capture Information 5-35

Using the Configuration Checkpoint and Rollback Service 5-39
  Overview 5-39
  Creating a Configuration Checkpoint 5-40
  Deleting a Configuration Checkpoint 5-41
  Rolling Back a Running Configuration 5-41
  Displaying Checkpoint Information 5-42

Reformatting the Flash Memory 5-43

CHAPTER 6

Viewing ACE Hardware and Software Configuration Information 6-1
  Displaying Software Version Information 6-2
  Displaying Software Copyright Information 6-3
  Displaying Hardware Information 6-4
  Displaying the Hardware Inventory 6-5
  Displaying System Processes 6-6
  Displaying Process Status Information and Memory Resource Limits 6-11
  Displaying System Information 6-14
  Displaying ICMP Statistics 6-18
  Displaying Technical Support Information 6-19

CHAPTER 7

Configuring Redundant ACE Modules 7-1
  Overview of Redundancy 7-1
    Redundancy Protocol 7-2
    Stateful Failover 7-5
    FT VLAN 7-6
Contents

Configuration Synchronization  7-7
Configuration Requirements and Restrictions  7-8
Redundancy Configuration Quick Start  7-8
Configuring Redundancy  7-11
  Configuring an FT VLAN  7-11
    Creating an FT VLAN  7-12
    Configuring an FT VLAN IP Address  7-12
    Configuring the Peer IP Address  7-13
    Enabling the FT VLAN  7-13
  Configuring an Alias IP Address  7-14
  Configuring an FT Peer  7-14
    Associating the FT VLAN with the Local Peer  7-15
    Configuring the Heartbeat Interval and Count  7-15
    Configuring a Query Interface  7-16
  Configuring an FT Group  7-17
    Associating a Context with an FT Group  7-18
    Associating a Peer with an FT Group  7-19
    Assigning a Priority to the Active FT Group Member  7-19
    Assigning a Priority to the Standby FT Group Member  7-20
    Configuring Preemption  7-21
    Placing an FT Group in Service  7-21
    Modifying an FT Group  7-22
  Specifying the Peer Hostname  7-22
  Specifying the MAC Address Banks for a Shared VLAN  7-22
  Forcing a Failover  7-23
  Synchronizing Redundant Configurations  7-24
Configuring Tracking and Failure Detection  7-27
  Overview of Tracking and Failure Detection  7-27
  Configuring Tracking and Failure Detection for a Host or Gateway  7-29
Creating a Tracking and Failure Detection Process for a Host or Gateway 7-29
Configuring the Gateway or Host IP Address Tracked by the Active Member 7-30
Configuring a Probe on the Active Member for Host Tracking 7-30
Configuring a Priority on the Active Member for Multiple Probes 7-31
Configuring the Gateway or Host IP Address Tracked by the Standby Member 7-32
Configuring a Probe on the Standby Member for Host Tracking 7-32
Configuring a Priority on the Standby Member for Multiple Probes 7-33
Example of a Tracking Configuration for a Gateway 7-33
Configuring Tracking and Failure Detection for an Interface 7-34
Creating a Tracking and Failure Detection Process for an Interface 7-34
Configuring the Interface Tracked by the Active Member 7-35
Configuring a Priority for a Tracked Interface on the Active Member 7-35
Configuring the Interface Tracked by the Standby Member 7-36
Configuring a Priority for a Tracked Interface on the Standby Member 7-36
Example of a Tracking Configuration for an Interface 7-37
Configuring Tracking and Failure Detection for an HSRP Group 7-38
Before You Begin 7-38
Creating a Tracking and Failure Detection Process for an HSRP Group 7-39
Configuring the HSRP Group to Track on the Active Member 7-40
Configuring a Priority for the HSRP Group Tracked by the Active Member 7-41
Configuring the HSRP Group to Track on the Standby Member 7-41
Configuring a Priority for a Tracked HSRP Group on the Standby Member 7-42
Example of a Tracking Configuration for an HSRP Group 7-42
Example of a Redundancy Configuration 7-43
Displaying Redundancy Information 7-45
  Displaying Redundancy Configurations 7-45
  Displaying FT Group Information 7-45
  Displaying the Redundancy Internal Software History 7-50
  Displaying the IDMAP Table 7-51
  Displaying Memory Statistics 7-52
  Displaying Peer Information 7-52
  Displaying FT Statistics 7-57
  Displaying FT Tracking Information 7-59

Clearing Redundancy Statistics 7-63
  Clearing Transport-Layer Statistics 7-63
  Clearing Heartbeat Statistics 7-64
  Clearing Tracking-Related Statistics 7-64
  Clearing All Redundancy Statistics 7-65
  Clearing the Redundancy History 7-65

CHAPTER 8 Configuring SNMP 8-1
  SNMP Overview 8-2
    Managers and Agents 8-3
    SNMP Manager and Agent Communication 8-4
    SNMP Traps and Informs 8-5
    SNMPv3 CLI User Management and AAA Integration 8-6
      CLI and SNMP User Synchronization 8-6
    Supported MIBs and Notifications 8-7
    SNMP Limitations 8-22
  SNMP Configuration Quick Start 8-24
  Configuring SNMP Users 8-26
    Defining SNMP Communities 8-29
    Configuring an SNMP Contact 8-30
Configuring an SNMP Location 8-31
Configuring SNMP Notifications 8-31
  Configuring SNMP Notification Hosts 8-32
  Enabling SNMP Notifications 8-34
  Enabling the IETF Standard for SNMP linkUp and linkDown Traps 8-36
Assigning a VLAN Interface as the Trap-Source Address in SNMPv1 Traps 8-37
Accessing ACE User Context Data Through the Admin Context IP Address 8-37
  Accessing User Context Data When Using SNMPv1/v2 8-38
  Accessing User Context Data When Using SNMPv3 8-38
Configuring an SNMPv3 Engine ID for an ACE Context 8-39
Configuring SNMP Management Traffic Services 8-40
  Creating and Configuring a Layer 3 and Layer 4 Class Map 8-41
    Defining a Class Map Description 8-42
    Defining SNMP Protocol Match Criteria 8-43
  Creating a Layer 3 and Layer 4 Policy Map 8-44
    Creating a Layer 3 and Layer 4 Policy Map for SNMP Network Management Traffic Received by the ACE 8-44
    Specifying a Layer 3 and Layer 4 Traffic Class with the Traffic Policy 8-45
    Specifying Layer 3 and Layer 4 Policy Actions 8-46
  Applying a Service Policy 8-47
Example of an SNMP Configuration 8-50
Displaying SNMP Statistics 8-51

CHAPTER 9
Configuring the XML Interface 9-1
XML Overview 9-2
  XML Usage with the ACE 9-2
  HTTP and HTTPS Support with the ACE 9-3
  HTTP Return Codes 9-5
  Document Type Definition 9-7
Sample XML Configuration 9-9
XML Configuration Quick Start 9-11
Configuring HTTP and HTTPS Management Traffic Services 9-12
Creating and Configuring a Class Map 9-13
Defining a Class Map Description 9-15
Defining HTTP and HTTPS Protocol Match Criteria 9-15
Creating a Layer 3 and Layer 4 Policy Map 9-17
Creating a Layer 3 and Layer 4 Policy Map for Network Management Traffic Received by the ACE 9-17
Specifying a Layer 3 and Layer 4 Traffic Class with the Traffic Policy 9-18
Specifying Layer 3 and Layer 4 Policy Actions 9-19
Applying a Service Policy 9-19
Enabling the Display of Raw XML Request show Command Output in XML Format 9-23
Accessing the ACE DTD File 9-26

APPENDIX A

Upgrading Your ACE Software A-1
Overview of Upgrading ACE Software A-1
Before You Begin A-2
Changing the Admin Password A-2
Changing the www User Password A-3
Checking Your Configuration for FT Priority and Preempt A-3
Creating a Checkpoint A-3
Updating Your Application Protocol Inspection Configurations A-4
ACE Software Upgrade Quick Start A-5
Copying the Software Upgrade Image to the ACE A-9
Configuring the ACE to Autoboot the Software Image A-10
Setting the Boot Variable A-10
Configuring the Configuration Register to Autoboot the Boot Variable A-11
Verifying the Boot Variable and Configuration Register  A-11
Reloading the ACE Module  A-11
Recovering the ACE from the ROMMON Utility  A-12
  Booting the ACE from ROMMON with the Correct Image Name  A-12
  Copying the ACE Image to the Supervisor Engine  A-14
Displaying Software Image Information  A-16
Preface

This guide provides instructions for the administration of the Cisco Application Control Engine (ACE) module in a Catalyst 6500 series switch or a Cisco 7600 series router, hereinafter referred to as the switch or router, respectively.

It describes how to perform administration tasks on the ACE, including doing the initial setup, establishing remote access, managing software licenses, configuring class maps and policy maps, managing the ACE software, configuring Simple Network Management Protocol (SNMP), configuring redundancy, configuring the Extensible Markup Language (XML) interface, and upgrading your ACE software.

This preface contains the following major sections:

- Audience
- How to Use This Guide
- Related Documentation
- Symbols and Conventions
- Obtaining Documentation, Obtaining Support, and Security Guidelines
- Open Source License Acknowledgements
Audience

This guide is intended for the following trained and qualified service personnel who are responsible for configuring the ACE:

- System administrator
- System operator

How to Use This Guide

This guide is organized as follows:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1, Setting Up the ACE</td>
<td>Describes how to configure basic settings on the ACE, including topics such as how to session and log in to the ACE, change the administrative username and password, assign a name to the ACE, configure a message-of-the-day banner, configure the date and time, configure terminal settings, modify the boot configuration, and restart the ACE.</td>
</tr>
<tr>
<td>Chapter 1, Enabling Remote Access to the ACE</td>
<td>Describes how to configure remote access to the Cisco Application Control Engine (ACE) module by establishing a remote connection using the Secure Shell (SSH) or Telnet protocols. It also describes how to configure the ACE to provide direct access to a user context from SSH. This chapter also covers how to configure the ACE to receive ICMP messages from a host.</td>
</tr>
<tr>
<td>Chapter 1, Managing ACE Software Licenses</td>
<td>Describes how to manage the software licenses for your ACE.</td>
</tr>
<tr>
<td>Chapter</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>Chapter 1, Managing the ACE Software</td>
<td>Describes how to save and download configuration files, use the file system, view and copy core dumps, capture and copy packet information, use the configuration checkpoint and rollback service, display configuration information, and display technical support information.</td>
</tr>
<tr>
<td>Chapter 1, Viewing ACE Hardware and Software Configuration Information</td>
<td>Describes how to display ACE hardware and software configuration and technical support information.</td>
</tr>
<tr>
<td>Chapter 1, Configuring Redundant ACE Modules</td>
<td>Describes how to configure the ACE for redundancy, which provides fault tolerance for the stateful failover of flows.</td>
</tr>
<tr>
<td>Chapter 1, Configuring SNMP</td>
<td>Describes how to configure SNMP to query the ACE for Cisco Management Information Bases (MIBs) and to send event notifications to a network management system (NMS).</td>
</tr>
<tr>
<td>Chapter 1, Configuring the XML Interface</td>
<td>Describes how to provide a mechanism using XML to transfer, configure, and monitor objects in the ACE. This XML capability allows you to easily shape or extend the CLI query and reply data in XML format to meet different specific business needs.</td>
</tr>
<tr>
<td>Appendix A, “Upgrading Your ACE Software”</td>
<td>Describes how to upgrade the software on your ACE.</td>
</tr>
</tbody>
</table>
## Related Documentation

In addition to this document, the ACE documentation set includes the following:

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Release Note for the Cisco Application Control Engine Module</em></td>
<td>Provides information about operating considerations, caveats, and command-line interface (CLI) commands for the ACE.</td>
</tr>
<tr>
<td><em>Cisco Application Control Engine Module Hardware Installation Note</em></td>
<td>Provides information for installing the ACE into the Catalyst 6500 series switch or a Cisco 7600 series router.</td>
</tr>
<tr>
<td><em>Cisco Application Control Engine Module Getting Started Guide</em></td>
<td>Describes how to perform the initial setup and configuration tasks for the ACE.</td>
</tr>
<tr>
<td><em>Cisco Application Control Engine Module Virtualization Configuration Guide</em></td>
<td>Describes how to operate your ACE in a single context or in multiple contexts.</td>
</tr>
</tbody>
</table>
| *Cisco Application Control Engine Module Routing and Bridging Configuration Guide* | Describes how to configure the following routing and bridging tasks on the ACE:  
  - VLAN interfaces  
  - Routing  
  - Bridging  
  - Dynamic Host Configuration Protocol (DHCP) |
| *Cisco Application Control Engine Module Server Load-Balancing Configuration Guide* | Describes how to configure the following server load-balancing tasks on the ACE:  
  - Real servers and server farms  
  - Class maps and policy maps to load balance traffic to real servers in server farms  
  - Server health monitoring (probes)  
  - Stickiness  
  - Firewall load balancing  
  - TCL scripts |
<table>
<thead>
<tr>
<th>Document Title</th>
<th>Description</th>
</tr>
</thead>
</table>
| *Cisco Application Control Engine Module Security Configuration Guide* | Describes how to perform the following ACE security configuration tasks:  
- Security access control lists (ACLs)  
- User authentication and accounting using a Terminal Access Controller Access Control System Plus (TACACS+), Remote Authentication Dial-In User Service (RADIUS), or Lightweight Directory Access Protocol (LDAP) server  
- Application protocol and HTTP deep packet inspection  
- TCP/IP normalization and termination parameters  
- Network address translation (NAT) |
| *Cisco Application Control Engine Module SSL Configuration Guide* | Describes how to configure the following Secure Sockets Layer (SSL) tasks on the ACE:  
- SSL certificates and keys  
- SSL initiation  
- SSL termination  
- End-to-end SSL |
| *Cisco Application Control Engine Module System Message Guide* | Describes how to configure system message logging on the ACE. This guide also lists and describes the system log (syslog) messages generated by the ACE. |
| *Cisco Application Control Engine Module Command Reference* | Provides an alphabetical list and descriptions of all CLI commands by mode, including syntax, options, and related commands. |
Symbols and Conventions

This publication uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong> font</td>
<td>Commands, command options, and keywords are in <strong>boldface</strong>. Bold text also indicates a command in a paragraph.</td>
</tr>
<tr>
<td><em>italic</em> font</td>
<td>Arguments for which you supply values are in <em>italics</em>. Italic text also indicates the first occurrence of a new term, book title, emphasized text.</td>
</tr>
<tr>
<td><code>{ }</code></td>
<td>Encloses required arguments and keywords.</td>
</tr>
<tr>
<td><code>[ ]</code></td>
<td>Encloses optional arguments and keywords.</td>
</tr>
<tr>
<td>`{x</td>
<td>y</td>
</tr>
<tr>
<td>`[x</td>
<td>y</td>
</tr>
<tr>
<td><strong>string</strong></td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td><strong>screen</strong> font</td>
<td>Terminal sessions and information the system displays are in <strong>screen</strong> font.</td>
</tr>
</tbody>
</table>
1. A numbered list indicates that the order of the list items is important.
   a. An alphabetical list indicates that the order of the secondary list items is important.
   • A bulleted list indicates that the order of the list topics is unimportant.
     – An indented list indicates that the order of the list subtopics is unimportant.

Notes use the following conventions:

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

Cautions use the following conventions:

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

For additional information about CLI syntax formatting, refer to the Cisco Application Control Engine Module Command Reference.
Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What’s New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:


Open Source License Acknowledgements

The following acknowledgements pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:
© 1998-1999 The OpenSSL Project. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:
   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL Project OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

**Original SSLeay License:**

© 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscape’s SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   “This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”.

The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].
CHAPTER 1

Setting Up the ACE

This chapter describes how to initially configure basic settings on the Cisco Application Control Engine (ACE) module in the Catalyst 6500 series switches. It contains the following major sections:

- Establishing a Console Connection on the ACE
- Sessioning and Logging In to the ACE
- Changing the Administrative Password
- Assigning a Name to the ACE
- Configuring an ACE Inactivity Timeout
- Configuring a Message-of-the-Day Banner
- Configuring the Date and Time
- Configuring Terminal Settings
- Modifying the Boot Configuration
- Restarting the ACE
- Shutting Down the ACE

For details on assigning VLANs to the ACE, configuring VLAN interfaces on the ACE, and configuring a default or static route on the ACE, see the Cisco Application Control Engine Module Routing and Bridging Configuration Guide.
Establishing a Console Connection on the ACE

You can establish a direct serial connection between your terminal and the ACE by making a serial connection to the console port on the front of the ACE. The console port is an asynchronous RS-232 serial port with an RJ-45 connector. Any device connected to this port must be capable of asynchronous transmission. Connection requires a terminal configured as 9600 baud, 8 data bits, 1 stop bit, no parity.

**Note**

Only the Admin context is accessible through the console port; all other contexts can be reached through Telnet or SSH sessions.

Once connected, use any terminal communications application to access the ACE CLI. The following procedure uses HyperTerminal for Windows.

To access the ACE by using a direct serial connection, perform the following steps:

**Step 1**
Launch HyperTerminal. The Connection Description window appears.

**Step 2**
Enter a name for your session in the Name field.

**Step 3**
Click **OK**. The Connect To window appears.

**Step 4**
From the drop-down list, choose the COM port to which the device is connected.

**Step 5**
Click **OK**. The Port Properties window appears.

**Step 6**
Set the following port properties:
- Baud Rate = 9600
- Data Bits = 8
- Flow Control = none
- Parity = none
- Stop Bits = 1

**Step 7**
Click **OK** to connect.

**Step 8**
Press **Enter** to access the CLI prompt.

```
switch login:
```
See the “Sessioning and Logging In to the ACE” section for details on logging in and entering the configuration mode to configure the ACE.

Once a session is created, choose **Save As** from the File menu to save the connection description. Saving the connection description has the following two advantages:

- The next time that you launch HyperTerminal, the session is listed as an option under **Start > Programs > Accessories > HyperTerminal > Name_of_session**. This option lets you reach the CLI prompt directly without going through the configuration steps.

- You can connect your cable to a different device without configuring a new HyperTerminal session. If you use this option, make sure that you connect to the same port on the new device as was configured in the saved HyperTerminal session. Otherwise, a blank screen appears without a prompt.

### Sessioning and Logging In to the ACE

This section describes how to connect (session) to the ACE as the default user from either the ACE console port or from the Catalyst 6500 series CLI. Once you connect to the ACE as the default user, you can then log in and enter the configuration mode to configure the ACE.

The ACE creates two default user accounts at startup: admin and www. The admin user is the global administrator and cannot be deleted. The ACE uses the www user account for the XML interface.

> **Note**
> Only the Admin context is accessible through the console port; all other contexts can be reached through a Telnet or SSH remote access session.

Later, when you configure interfaces and IP addresses on the ACE itself, you can remotely access the ACE CLI through an ACE interface by using the Catalyst console port or by a Telnet or SSH session. To configure remote access to the ACE CLI, see Chapter 2, Enabling Remote Access to the ACE. For details on configuring interfaces on the ACE, see the *Cisco Application Control Engine Module Routing and Bridging Configuration Guide*. 
You can configure the ACE to provide a higher level of security for users accessing the ACE. For information about configuring user authentication for login access, see the Cisco Application Control Engine Module Security Configuration Guide.

To session into the ACE and access configuration mode to perform initial configuration, perform the following steps:

### Step 1
Access the ACE through one of the following methods:

- If you choose to access the ACE directly by its console port, attach a terminal to the asynchronous RS-232 serial port on the front of the ACE. Any device connected to this port must be capable of asynchronous transmission. The connection requires a terminal configured as 9600 baud, 8 data bits, 1 stop bit, no parity. See the “Establishing a Console Connection on the ACE” section.

- If you choose to session into ACE, after the ACE successfully boots, enter the `session` command from the Catalyst CLI to Telnet to the ACE:

  ```
  Cat6k-switch# session slot mod_num processor 0
  ```

  The `mod_num` argument identifies the slot number in the Catalyst 6500 series chassis where the ACE is installed.

### Note
The default escape character sequence is Ctrl-~, and then x. You can also enter `exit` at the remote prompt to end the session.

### Step 2
Log into the ACE by entering the login username and password at the following prompt:

```
switch login: admin
Password: admin
```

By default, both the username and password are admin.

The prompt changes to the following:

```
switch/Admin#
```

To change the default login username and password, see the “Changing the Administrative Password” section for details.
Caution

For software version A2(1.1) and higher, you must change the default Admin password if you have not already done so. Otherwise, you will be able to log in to the ACE only through the console port or through the supervisor engine of the Catalyst 6500 series switch or the Cisco 7600 series router. You will not be able to access the ACE using Telnet or SSH until you change the default Admin password.

Step 3

To access configuration mode, enter:

```
switch/Admin# configure
```

Enter configuration commands, one per line. End with CNTL/Z

The prompt changes to the following:

```
switch/Admin(config)#
```

Changing the Administrative Password

During the initial login process to the ACE, you enter the default user name `admin` and the default password `admin` in lowercase text. You cannot modify or delete the default administrative username; however, for security reasons, you must change the default administrative password. If you do not change the password, then security on your ACE can be compromised because the administrative username and password are configured to be the same for every ACE shipped from Cisco Systems.

Caution

For software version A2(1.1) and higher, you must change the default Admin password if you have not already done so. Otherwise, you can log in to the ACE only through the console port or through the supervisor engine of the Catalyst 6500 series switch or the Cisco 7600 series router.

The administrative username and password are stored in Flash memory. Each time that you reboot the ACE, it reads the username and password from Flash memory. Global administrative status is assigned to the administrative username by default.
Changing the Administrative Password

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 user 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. To verify the account and permission for each user, use the `show user-account` Exec command. For details on contexts, user roles, and domains, see the Cisco Application Control Engine Module Virtualization Configuration Guide.

To change the default Admin username and password, use the `username` command in configuration mode. The syntax of this command is as follows:

```
username name1 [password [0 | 5] {password}]
```

The keywords, arguments, and options are as follows:

- `name1`—Sets the username that you want to assign or change. Enter `Admin`.
- `password`—(Optional) Keyword that indicates that a password follows.
- `0`—(Optional) Specifies a clear text password.
- `5`—(Optional) Specifies an MD5-hashed strong encryption password.
- `password`—The password in clear text, encrypted text, or MD5 strong encryption, depending on the numbered option (0 or 5) that you enter. If you do not enter a numbered option, the password is in clear text by default. Enter a password as an unquoted text string with a maximum of 64 characters.

If you specify an MD5-hashed strong encryption password, the ACE considers a password to be weak if it less than eight characters in length.

The ACE supports the following special characters in a password:

```
, . / = + ^ @ ! % ~ # $ ( )
```

Note that the ACE encrypts clear text passwords in the running-config.

For example, to change the Admin password to `mysecret_801`, enter:

```
switch/Admin(config)# username Admin password 0 mysecret_801
```
Resetting the Administrator Account Password

If you forget the password for the ACE administrator account and cannot access the ACE, you can recover the admin password during the initial bootup sequence of the ACE. You must have access to the ACE through the console port to be able to reset the password for the Admin user back to the factory default value of admin.

Note

Only the Admin context is accessible through the console port.

To reset the password that allows the Admin user access to the ACE, perform the following steps:

**Step 1**
Connect to the console port on the Catalyst 6500 series switch.

**Step 2**
Session in to the ACE through the console port on the front panel.

**Step 3**
Reboot the ACE from the Catalyst 6500 series CLI. See the “Restarting the ACE” section for details.

**Step 4**
During the bootup process, output appears on the console terminal. Press ESC when the “Waiting for 3 seconds to enter setup mode...” message appears on the terminal (see the example below). The setup mode appears. If you miss the time window, wait for the ACE to properly complete booting, reboot the ACE from the Catalyst 6500 series CLI, and try again to access the setup mode by pressing ESC.

```
IXP polling timeout interval: 120
map_pci_xram_to_uspace[149] :: mapping 4096 bytes from 0x58800000
map_pci_xram_to_uspace[149] :: mapping 4096 bytes from 0x5a800000
................................................
IXP's are up... <Sec 48 :Status of IXP1 7, IXP2 7>
map_pci_xram_to_uspace[149] :: mapping 102400 bytes from 0x4fd68000
map_pci_xram_to_uspace[149] :: mapping 102400 bytes from 0x57d68000
Starting lcpfw process...
inserting IPCP klm
Warning: loading /itasca/klm/klm_session.klm will taint the kernel: no license
See http://www.tux.org/lkml/#export-tainted for information about tainted modu les
```
Module klm_session.klm loaded, with warnings
inserting cpu_util klm
create dev node as 'mknod /dev/cpu_util c 236 0'
getting cpu_util dev major num
making new cpu_util dev node

Session Agent waiting for packets.
Waiting for 3 seconds to enter setup mode...
Entering setup sequence...
Reset Admin password [y/n] (default: n): y
Resetting admin password to factory default...
XR Serial driver version 1.0 (2004-11-08) with no serial options enabled
ttyXR major device number: 235
Create a dev file with 'mknod /dev/ttyXR c 235 [0-1]'
cux major device number: 234
Create a dev file with 'mknod /dev/cux c 234 [0-1]'
ttyXR0 at 0x10c00000 (irq = 59) is a 16550A
ttyXR1 at 0x10c00008 (irq = 59) is a 16550A
No licenses installed...

Loading.. Please wait...Done!!!

Step 5 The setup mode prompts if you want to reset the admin password. Enter y. The
“Resetting admin password to factory default” message appears. The ACE deletes
the admin user password configuration from the startup configuration and resets
the password back to the factory default value of admin.
The boot process continues as normal and you are able to enter the admin
password at the login prompt.

Assigning a Name to the ACE

The hostname is used to identify the ACE and for the command-line prompts. If
you establish sessions to multiple devices, the hostname helps you track where
you enter commands. By default, the hostname for the ACE is “switch.” To
specify a hostname for the ACE, use the hostname configuration mode command.
To specify a hostname for the peer ACE in a redundant configuration, use the peer
hostname command.
The syntaxes of these commands are as follows:

```
hostname name

peer hostname name
```

The `name` argument specifies a new hostname for the ACE. Enter a case-sensitive text string that contains from 1 to 32 alphanumeric characters.

For example, to change the hostname of the ACE from switch to ACE_1, enter:

```
switch/Admin(config)# hostname ACE_1
ACE_1/Admin(config)#
```

## Configuring an ACE Inactivity Timeout

By default, the inactivity timeout value is 5 minutes. You can modify the length of time that can occur before the ACE automatically logs off an inactive user by using the `login timeout` command in configuration mode. This command specifies the length of time that a user session can be idle before the ACE terminates the console, Telnet, or SSH session.

The `login timeout` command setting overrides the `terminal session-timeout` setting (see the “Configuring Terminal Display Attributes” section).

The syntax of this command is as follows:

```
login timeout minutes
```

The `minutes` argument specifies the length of time that a user can be idle before the ACE terminates the session. Valid entries are from 0 to 60 minutes. A value of 0 instructs the ACE never to timeout. The default is 5 minutes.

For example, to specify a timeout period of 10 minutes, enter:

```
host1/Admin(config)# login timeout 10
```

To restore the default timeout value of 5 minutes, enter the following command:

```
host1/Admin(config)# no login timeout
```
To display the configured login time value, use the `show login timeout` command in Exec mode. For example, enter:

```
host1/Admin# show login timeout
Login Timeout 10 minutes.
```

### Configuring a Message-of-the-Day Banner

You can configure a message in configuration mode to display as the message-of-the-day banner when a user connects to the ACE. Once connected to the ACE, the message-of-the-day banner appears, followed by the login banner and Exec mode prompt.

The syntax of this command is as follows:

```
banner motd text
```

The `text` argument is a line of message text to be displayed as the message-of-the-day banner. The `text` string consists of all characters that follow the first space until the end of the line (carriage return or line feed).

The pound (#) character functions as the delimiting character for each line. For the banner text, spaces are allowed but tabs cannot be entered at the CLI. To instruct the ACE to display multiple lines in a message-of-the-day banner, enter a new `banner motd` command for each line that you want to appear.

The banner message is a maximum of 80 characters per line, up to a maximum of 3000 characters (3000 bytes) for a message-of-the-day banner. This maximum value includes all line feeds and the last delimiting character in the message.

To add multiple lines to an existing a message-of-the-day banner, precede each line by using the `banner motd` command. The ACE appends each line to the end of the existing banner. If the text is empty, the ACE adds a carriage return (CR) to the banner.

You can include tokens in the form `$(token)` in the message text. Tokens will be replaced with the corresponding configuration variable. For example, enter:

- `$(hostname)`—Displays the hostname for the ACE during run time.
- `$(line)`—Displays the tty (teletypewriter) line or name (for example, "/dev/console", "/dev/pts/0", or "1").
To use the $(hostname) in a single line banner motd input, you must include double quotes (") around the $(hostname) so that the $ is interpreted as a special character at the beginning of a variable in the single line. For example, enter:

```
switch/Admin(config)# banner motd #Welcome to "$(hostname)"...#
```

Do not use the double quote character (") or the percent sign character (%) as a delimiting character in a single line message string.

For multi-line input, double quotes (") are not required for the token because the input mode is different from signal-line mode. When you operate in multi-line mode, the ACE interprets the double quote character (") literally. The following example shows how to span multiple lines and use tokens to configure the banner message:

```
switch/Admin(config)# banner motd #
Enter TEXT message. End with the character '#'.
================================
Welcome to Admin Context
--------------------------------
Hostname: $(hostname)
Tty Line: $(line)
================================#
```

To replace a banner or a line in a multi-line banner, use the `no banner motd` command before adding the new lines.

To display the configured banner message, use the `show banner motd` command in Exec mode. For example, enter:

```
host1/Admin# show banner motd
```
Configuring the Date and Time

The ACE time and date are synchronized with the clock from the Catalyst 6500 series supervisor engine. You may configure the time zone and daylight saving time of the ACE for display purposes. See the Cisco 6500 Series Switch Cisco IOS Software Configuration Guide for details on setting the system clock on the switch.

This section contains the following topics:
- Configuring the Time Zone
- Adjusting for Daylight Saving Time
- Viewing the System Clock Settings

Configuring the Time Zone

To set the time zone of the ACE, use the `clock timezone` command in configuration mode. The ACE keeps time internally in Universal Time Coordinated (UTC) offset.

The syntax of this command is as follows:

```
    clock timezone {zone_name{+|-}hours minutes} | {standard timezone}
```

The keywords, arguments, and options are as follows:
- `zone_name`—The 8-character name of the time zone (for example, PDT) to be displayed when the time zone is in effect. Table 1-1 lists the common time zone acronyms that you can use for the `zone_name` argument.
- `hours`—Hours offset from UTC. The range is from –23 to 23.
- `minutes`—Minutes offset from UTC. The range is from 0 to 59 minutes.
- `standard timezone`—Displays a list of well known time zones that include an applicable UTC hours offset. Available choices are as follows:
  - AKST—Alaska Standard Time, as UTC –9 hours
  - AST—Atlantic Standard Time, as UTC –4 hours
  - BST—British Summer Time, as UTC + 1 hour
  - CEST—Central Europe Summer Time, as UTC + 2 hours
- **CET**—Central Europe Time, as UTC + 1 hour
- **CST**—Central Standard Time, as UTC –6 hours
- **CST**—Central Standard Time, as UTC + 9.5 hours
- **EEST**—Eastern Europe Summer Time, as UTC + 3 hours
- **EET**—Eastern Europe Time, as UTC + 2 hours
- **EST**—Eastern Standard Time, as UTC -5 hours
- **GMT**—Greenwich Mean Time, as UTC
- **HST**—Hawaiian Standard Time, as UTC –10 hours
- **IST**—Irish Summer Time, as UTC + 1 hour
- **MSD**—Moscow Summer Time, as UTC + 4 hours
- **MSK**—Moscow Time, as UTC + 3 hours
- **MST**—Mountain Standard Time, as UTC –7 hours
- **PST**—Pacific Standard Time, as UTC –8 hours
- **WEST**—Western Europe Summer Time, as UTC + 1 hour
- **WST**—Western Standard Time, as UTC + 8 hours

Table 1-1 lists common time zone acronyms that you can specify for the `zone_name` argument.

**Table 1-1  Common Time Zone Acronyms**

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Time Zone Name and UTC Offset</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Europe</strong></td>
<td></td>
</tr>
<tr>
<td>BST</td>
<td>British Summer Time, as UTC + 1 hour</td>
</tr>
<tr>
<td>CET</td>
<td>Central Europe Time, as UTC + 1 hour</td>
</tr>
<tr>
<td>CEST</td>
<td>Central Europe Summer Time, as UTC + 2 hours</td>
</tr>
<tr>
<td>EET</td>
<td>Eastern Europe Time, as UTC + 2 hours</td>
</tr>
<tr>
<td>EEST</td>
<td>Eastern Europe Summer Time, as UTC + 3 hours</td>
</tr>
<tr>
<td>GMT</td>
<td>Greenwich Mean Time, as UTC</td>
</tr>
<tr>
<td>IST</td>
<td>Irish Summer Time, as UTC + 1 hour</td>
</tr>
<tr>
<td>MSK</td>
<td>Moscow Time, as UTC + 3 hours</td>
</tr>
</tbody>
</table>
### Table 1-1  Common Time Zone Acronyms (continued)

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Time Zone Name and UTC Offset</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSD</td>
<td>Moscow Summer Time, as UTC + 4 hours</td>
</tr>
<tr>
<td>WET</td>
<td>Western Europe Time, as UTC</td>
</tr>
<tr>
<td>WEST</td>
<td>Western Europe Summer Time, as UTC + 1 hour</td>
</tr>
<tr>
<td><strong>United States and Canada</strong></td>
<td></td>
</tr>
<tr>
<td>AST</td>
<td>Atlantic Standard Time, as UTC – 4 hours</td>
</tr>
<tr>
<td>ADT</td>
<td>Atlantic Daylight Time, as UTC – 3 hours</td>
</tr>
<tr>
<td>CT</td>
<td>Central Time, either as CST or CDT, depending on the place and time of the year</td>
</tr>
<tr>
<td>CST</td>
<td>Central Standard Time, as UTC – 6 hours</td>
</tr>
<tr>
<td>CDT</td>
<td>Central Daylight Saving Time, as UTC – 5 hours</td>
</tr>
<tr>
<td>ET</td>
<td>Eastern Time, either as EST or EDT, depending on the place and time of the year</td>
</tr>
<tr>
<td>EST</td>
<td>Eastern Standard Time, as UTC – 5 hours</td>
</tr>
<tr>
<td>EDT</td>
<td>Eastern Daylight Saving Time, as UTC – 4 hours</td>
</tr>
<tr>
<td>MT</td>
<td>Mountain Time, either as MST or MDT, depending on the place and time of the year</td>
</tr>
<tr>
<td>MDT</td>
<td>Mountain Daylight Saving Time, as UTC – 6 hours</td>
</tr>
<tr>
<td>MST</td>
<td>Mountain Standard Time, as UTC – 7 hours</td>
</tr>
<tr>
<td>PT</td>
<td>Pacific Time, either as PST or PDT, depending on the place and time of the year</td>
</tr>
<tr>
<td>PDT</td>
<td>Pacific Daylight Saving Time, as UTC – 7 hours</td>
</tr>
<tr>
<td>PST</td>
<td>Pacific Standard Time, as UTC – 8 hours</td>
</tr>
<tr>
<td>AKST</td>
<td>Alaska Standard Time, as UTC – 9 hours</td>
</tr>
<tr>
<td>AKDT</td>
<td>Alaska Standard Daylight Saving Time, as UTC – 8 hours</td>
</tr>
<tr>
<td>HST</td>
<td>Hawaiian Standard Time, as UTC – 10 hours</td>
</tr>
<tr>
<td><strong>Australia</strong></td>
<td></td>
</tr>
<tr>
<td>CST</td>
<td>Central Standard Time, as UTC + 9.5 hours</td>
</tr>
</tbody>
</table>
Chapter 1      Setting Up the ACE

Configuring the Date and Time

For example, to set the time zone to PST and to set an UTC offset of –8 hours, enter:

```text
host1/Admin(config)# clock timezone PST -8 0
```

To remove the clock timezone setting, use the `no` form of this command. For example, enter:

```text
host1/Admin(config)# no clock timezone
```

Adjusting for Daylight Saving Time

To configure the ACE to change the time automatically to summer time (daylight saving time), use the `clock summer-time` command in configuration mode.

The first part of the command specifies when summer time begins, and the second part of the command specifies when summer time ends. All times are relative to the local time zone; the start time is relative to standard time and the end time is relative to summer time. If the starting month is after the ending month, the ACE assumes that you are located in the Southern Hemisphere.

The syntax of this command is as follows:

```text
clock summer-time {daylight_timezone_name start_week start_day start_month start_time end_week end_day end_month end_time daylight_offset | standard timezone}
```

The keywords, arguments, and options are as follows:

- `daylight_timezone_name`—The eight-character name of the time zone (for example, PDT) to be displayed when summer time is in effect. See Table 1-1 for the list the common time zone acronyms used for the `daylight_timezone_name` argument.
- `start_week end_week`—The week, ranging from 1 through 5.

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Time Zone Name and UTC Offset</th>
</tr>
</thead>
<tbody>
<tr>
<td>EST</td>
<td>Eastern Standard/Summer Time, as UTC + 10 hours (+11 hours during summer time)</td>
</tr>
<tr>
<td>WST</td>
<td>Western Standard Time, as UTC + 8 hours</td>
</tr>
</tbody>
</table>

For example, to set the time zone to EST and to set an UTC offset of –5 hours, enter:

```text
host1/Admin(config)# clock timezone EST -5 0
```

To remove the clock timezone setting, use the `no` form of this command. For example, enter:

```text
host1/Admin(config)# no clock timezone
```
• *start_day end_day*—The day, ranging from Sunday through Saturday.

• *start_month end_month*—The month, ranging from January through December.

• *start_time end_time*—Time, in military format, specified in hours and minutes.

• *daylight_offset*—Number of minutes to add during the summer time. Valid entries are 1 to 1440.

• *standard timezone*—Displays a list of well known time zones that include an applicable daylight time start and end range along with a daylight offset. Available choices are as follows:
  
  – **ADT**—Atlantic Daylight Time: 2 a.m. 1st Sunday April to 2 a.m. last Sunday Oct, + 60 min
  
  – **AKDT**—Alaska Standard Daylight Time: 2 a.m. 1st Sunday April to 2 a.m. last Sunday Oct, + 60 min
  
  – **CDT**—Central Daylight Time: 2 a.m. 1st Sunday April to 2 a.m. last Sunday Oct, + 60 min
  
  – **EDT**—Eastern Daylight Time: 2 a.m. 1st Sunday April to 2 a.m. last Sunday Oct, + 60 min
  
  – **MDT**—Mountain Daylight Time: 2 a.m. 1st Sunday April to 2 a.m. last Sunday Oct, + 60 min
  
  – **PDT**—Pacific Daylight Time: 2 a.m. 1st Sunday April to 2 a.m. last Sunday Oct, + 60 min

For example, to specify that summer time begins on the first Sunday in April at 02:00 and ends on the last Sunday in October at 02:00, with a daylight offset of 60 minutes, enter:

```
host1/Admin(config)# clock summer-time Pacific 1 Sun Apr 02:00 5 Sun Oct 02:00 60
```

To remove the clock summer-time setting, use the `no` form of this command. For example, enter:

```
host1/Admin(config)# no clock summer-time
```
Viewing the System Clock Settings

To display the system clock of the ACE, use the `show clock` command in Exec mode.

The syntax of this command is as follows:

```
show clock
```

The following sample output shows the current clock settings:

```
host1/Admin# show clock
Mon Mar  6 18:26:55 UTC 2006
```

Configuring Terminal Settings

You can access the ACE CLI by using one of the following methods:

- Make a direct connection by using a dedicated terminal attached to the console port on the front of the ACE.
- Establish a remote connection to the ACE through the Catalyst 6500 series switch using the Secure Shell (SSH) or Telnet protocols.

**Note**

Only the Admin context is accessible through the console port; all other contexts can be reached through Telnet or SSH.

This section contains the following topics:

- Configuring Terminal Display Attributes
- Configuring Terminal Line Settings

For details on configuring remote access to the ACE CLI using SSH or Telnet, see Chapter 2, Enabling Remote Access to the ACE.
Configuring Terminal Display Attributes

You can specify the number of lines and the width for displaying information on a terminal during a console session. The maximum number of displayed screen lines is 511 columns. To configure the terminal display settings, use the `terminal` command in Exec mode. The `terminal` command allows you to set the width for displaying command output.

The syntax of the command is as follows:

```
terminal {length lines | monitor | session-timeout minutes | terminal-type
text | width characters}
```

The keywords, arguments, and options are as follows:

- **length lines**—Sets the number of lines displayed on the current terminal screen. This command is specific to only the console port. Telnet and SSH sessions set the length automatically. Valid entries are from 0 to 511. The default is 24 lines. A value of 0 instructs the ACE to scroll continuously (no pausing) and overrides the terminal width value. If you later change the terminal length to any other value, the originally configured terminal width value takes effect.

- **monitor**—Displays syslog output on the terminal for the current terminal and session. To enable the various levels of syslog messages to the terminal, use the `logging monitor` command (see the Cisco Application Control Engine Module System Message Guide for details).

- **session-timeout minutes**—Specifies the inactivity timeout value in minutes to configure the automatic logout time for the current terminal session on the ACE. When inactivity exceeds the time limit configured by this command, the ACE closes the session and exits. The range is from 0 to 525600. The default value is inherited from the value that is configured for the `login timeout` command. If you do not configure a value for the `login timeout` command, the default for both commands is 5 minutes. You can set the `terminal session-timeout` value to 0 to disable this feature so that the terminal remains active until you choose to exit the ACE. The ACE does not save this change in the configuration file.

**Note**

The `login timeout` command setting overrides the `terminal session-timeout` setting (see the “Configuring an ACE Inactivity Timeout” section).
• terminal-type text—Specifies the name and type of the terminal used to access the ACE. If a Telnet or SSH session specifies an unknown terminal type, the ACE uses the VT100 terminal by default. Specify a text string from 1 to 80 alphanumeric characters.

• width characters—Sets the number of characters displayed on the current terminal screen. This command is specific to only the console port. Telnet and SSH sessions set the width automatically. Valid entries are from 24 to 512. The default is 80 columns.

For example, to specify the VT200 terminal, set the number of screen lines to 35, and set the number of characters to 250, enter:

```
host1/Admin# terminal terminal-type vt200
host1/Admin# terminal length 35
host1/Admin# terminal width 250
```

For example, to specify a terminal timeout of 600 minutes for the current session, enter:

```
host1/Admin# terminal session-timeout 600
```

To reset a terminal setting to its default value, such as the screen line length, use the no form of the command:

```
host1/Admin# terminal no width
```

For example, to start the current terminal monitoring session, enter:

```
host1/Admin# terminal monitor
host1/Admin# %ACE-7-111009: User ‘admin’ executed cmd: terminal monitor
%ACE-7-111009: User ‘admin’ executed cmd: terminal monitor......
```

To stop the current terminal monitoring session, enter:

```
host1/Admin# terminal no monitor
```

To display the console terminal settings, use the show terminal Exec mode command. For example, enter:

```
host1/Admin# show terminal
TTY: /dev/pts/0 Type: “vt100”
Length: 25 lines, Width: 80 columns
Session Timeout: 60 minutes
```
Configuring Terminal Line Settings

This section describes how to configure the terminal line settings for accessing the ACE by a console or a virtual terminal and contains the following topics:

- Configuring Console Line Settings
- Configuring Virtual Terminal Line Settings

Configuring Console Line Settings

The console port is an asynchronous serial port on the ACE that allows you to directly access the module to perform an initial configuration through a standard RS-232 port with an RJ-45 connector. Any device connected to this port must be capable of asynchronous transmission. Connection requires a terminal configured as 9600 baud, 8 data bits, 1 stop bit, no parity.

Use the `line console` configuration mode command to configure the console interface settings. The CLI displays the console configuration mode.

To configure the line console settings from the console configuration mode, specify one or more of the following commands:

- **databits number**—Specifies the number of data bits per character. The range is from 5 to 8. The default is 8 data bits.
- **parity**—Sets the parity for the console connection. The supported choices are: **even** (even parity), **none** (no parity), or **odd** (odd parity). The default is **none**.
- **speed speed**—Sets the transmit and receive speeds for the serial console. The range is between 110 and 115200 baud (110, 150, 300, 600, 1200, 2400, 4800, 9600, 19200, 28800, 38400, 57600, or 115200). The default is 9600 baud.
- **stopbits**—Sets the stop bits for the console connection. Valid values are 1 or 2 stop bits. The default is 1 stop bit.
For example, to configure the console line settings for the ACE, enter:

```
host1/Admin# config
Enter configuration commands, one per line. End with CNTL/Z
host1/Admin(config)#
```

```
host1/Admin(config)# line console
```

```
host1/Admin(config-console)# databits 6
host1/Admin(config-console)# parity even
host1/Admin(config-console)# speed 19200
host1/Admin(config-console)# stopbits 1
```

To disable a setting for the configured console line, use the **no** form of the command. For example, enter:

```
host1/Admin(config-console)# no stopbits 1
```

Use the **show line console** Exec mode command to verify the configured console settings for the ACE.

The syntax of this command is as follows:

```
show line console [connected]
```

The optional **connected** keyword displays the physical connection status.

For example, to display the configured console settings, enter:

```
host1/Admin# show line console
```

```
line Console:
  Speed:        9600 bauds
  Databits:     8 bits per byte
  Stopbits:     1 bit(s)
  Parity:       none
```

**Configuring Virtual Terminal Line Settings**

Virtual terminal lines allow remote access to the ACE. A virtual terminal line is not associated with the console port; instead, it is a virtual port on the Catalyst 6500 series switch that allows you to access the ACE.

Use the **line vty** configuration mode command to configure the virtual terminal line settings. The CLI displays the line configuration mode. Use the **session-limit** command to configure the maximum number of terminal sessions per line.

The syntax of this command is as follows:

```
session-limit number
```
The number argument configures the maximum number of terminal sessions per line. The range is from 1 to 251.

For example, to configure a virtual terminal line, enter:

```
host1/Admin# config
Enter configuration commands, one per line. End with CNTL/Z
host1/Admin(config)# line vty
host1/Admin(config-line)# session-limit 23
```

To disable a setting for the configured virtual terminal line, use the no form of the command. For example, enter:

```
host1/Admin(config-line)# no session-limit 23
```

Use the clear line command in Exec mode to close a specified vty session. The syntax of this command is as follows:

```
clear line vty_name
```

The vty_name argument specifies the name of the VTY session. Enter a maximum of 64 characters for the name of the virtual terminal.

For example, to close a specified vty session, enter:

```
host1/Admin# clear line vty vty1
```

## Modifying the Boot Configuration

You can control how the ACE performs its boot process through ROMMON mode. ROMMON is the ROM-resident code that starts executing as soon as you power up or reset the ACE. Two user-configurable parameters determine how the ACE boots: the boot field in the configuration register and the BOOT environment variable.

This section describes how to modify the boot configuration of the ACE and contains the following topics:

- Setting the Boot Method from the Configuration Register
- Setting the BOOT Environment Variable
- Displaying the ACE Boot Configuration
Setting the Boot Method from the Configuration Register

The ROMMON code executes upon power up, reset, or when a fatal exception occurs. The ACE enters ROMMON mode if it does not find a valid system image, if the Flash memory configuration is corrupted, or if the configuration register is set to enter ROMMON mode.

You can manually enter ROMMON mode by restarting the ACE and then pressing the **Break** key during the first 60 seconds of startup. If you are connected to the ACE through a terminal server, you can escape to the Telnet prompt and then enter the **send break** command to enter the ROMMON mode.

You can modify the boot method that the ACE uses at the next startup by setting the boot field in the software configuration register. The configuration register identifies how the ACE should boot and where the system image is stored. You can modify the boot field to force the ACE to boot a particular system image at startup instead of using the default system image.

To change the configuration register settings, use the **config-register** configuration command. This command affects only the configuration register bits that control the boot field and leaves the remaining bits unaltered.

The syntax of this command is as follows:

```
config-register value
```

The **value** argument represents the configuration register value that you want to use the next time that you restart the ACE. The supported **value** entries are as follows:

- **0**—Upon reboot, the ACE boots to the rommon prompt. The ACE remains in ROMMON mode at startup.

- **1**—Upon reboot, the ACE boots the system image identified in the **BOOT** environment variable (see the “Setting the **BOOT** Environment Variable” section). The **BOOT** environment variable specifies a list of image files on various devices from which the ACE can boot at startup. If the ACE encounters an error or if the image is not valid, it will try the second image (if one is specified). If the second image also fails to boot, the ACE returns to ROMMON mode.

See the “**Booting the ACE from the rommon Prompt**” section for details on booting the ACE from the rommon prompt.
For example, to set the boot field in the configuration register to boot the system image identified in the BOOT environment variable upon reboot, enter:

```
host1/Admin(config)# config-register 1
```

**Booting the ACE from the rommon Prompt**

If you specify a value of 0 for the `config-register` command, this configuration register setting forces the ACE to enter the ROMMON mode upon a reload or power cycle of the ACE. The ACE remains in ROMMON mode until you identify the location of an image file to boot.

The ACE supports two methods of booting the module from the rommon prompt:

- To manually change the configuration register setting in ROMMON mode, use the `confreg` command followed by a value of 0 or 1.
- To change the boot characteristics using onscreen prompts, use the `confreg` command without a value.

To instruct the ACE to manually boot from a particular system image, use the `confreg` command and specify a configuration register value of 1. Identify the name of the system image file that the ACE uses to boot.

A `confreg` value of 0 instructs the ACE to boot to the rommon prompt.

For example, to use the `confreg` command at the rommon prompt to instruct the ACE to boot from the `c6ace-t1k9-mzg.3.0.0_A0_2.48.bin` system image, enter:

```
rommon 11 > confreg 1
rommon 12 > BOOT=disk0:c6ace-t1k9-mzg.3.0.0_A0_2.48.bin
rommon 13 > sync
```

To instruct the ACE to automatically boot from the image specified in the BOOT variable (see the “Setting the BOOT Environment Variable” section), use the `confreg` command without specifying a configuration register value to launch the Configuration Summary menu-based utility. You can then instruct the ACE to boot from the system image identified in the BOOT environment variable (see the “Setting the BOOT Environment Variable” section).
For example, to use the `confreg` command to display the onscreen prompts for changing the boot characteristics of the ACE, enter:

```
rommon 11 > confreg
Configuration Summary
(Virtual Configuration Register: 0x1)
enabled are:
break/abort has effect
console baud: 9600
boot: the ROM monitor
do you wish to change the configuration? y/n [n]: y
disable “break/abort has effect”? y/n [n]:
enable “ignore system config info”? y/n [n]:
change the boot characteristics? y/n [n]: y
enter to boot:
0 = ROM Monitor
1 = boot file specified in BOOT variable
[1]: 1
```

For example, to use the `confreg` command to instruct the ACE to boot from the c6ace-t1k9-mzg.3.0.0_A0_2.48.bin system image, enter:

```
rommon 11 > confreg
Configuration Summary
(Virtual Configuration Register: 0x1)
enabled are:
break/abort has effect
console baud: 9600
boot: the ROM monitor
do you wish to change the configuration? y/n [n]: n
rommon 12 > BOOT=disk0:c6ace-t1k9-mzg.3.0.0_A0_2.48.bin
rommon 13 > sync
```

### Setting the BOOT Environment Variable

The BOOT environment variable specifies a list of image files on various devices from which the ACE can boot at startup. You can add several images to the BOOT environment variable to provide a fail-safe boot configuration. If the first file fails to boot the ACE, subsequent images that are specified in the BOOT environment variable are tried until the ACE boots or there are no additional images to attempt to boot. If there is no valid image to boot, the ACE enters ROMMON mode where you can manually specify an image to boot.
The ACE stores and executes images in the order in which you added them to the
BOOT environment variable. If you want to change the order in which images are
tried at startup, you can either prepend and clear images from the BOOT
environment variable to attain the desired order or you can clear the entire BOOT
environment variable and then redefine the list in the desired order.

To set the BOOT environment variable, use the **boot system image:** command.
The syntax of this command is as follows:

```
boot system image:image_name
```

The `image_name` argument specifies the name of the system image file. If the file
does not exist (for example, if you entered the wrong filename), then the filename
is appended to the bootstrap string, and this message displays, “Warning: File not found
but still added in the bootstring.” If the file does exist, but is not a valid image, the
file is not added to the bootstring, and this message displays, “Warning: file found
but it is not a valid boot image.”

For example, to set the BOOT environment variable, enter:

```
host1/Admin(config)# boot system
image:c6ace-t1k9-mzg.3.0.0_A0_2.48.bin
```

### Displaying the ACE Boot Configuration

To display the current BOOT environment variable and configuration register
setting, use the **show bootvar** command in Exec mode.

For example, to display the BOOT environment variable settings, enter:

```
host1/Admin# show bootvar
BOOT variable = “disk0:c6ace-t1k9-mzg.3.0.0_A0_2.48.bin”
Configuration register is 0x1
```
Chapter 1  Setting Up the ACE

Restarting the ACE

You can reload the ACE directly from its CLI or reboot it by using the Catalyst 6500 series CLI. You may need to reboot the ACE from the Catalyst CLI if you cannot reach the ACE through its CLI or by using an external Telnet session.

This section contains the following topics:

- Restarting the ACE from the CLI
- Restarting the ACE from the Catalyst CLI

Restarting the ACE from the CLI

To reboot the ACE directly from its CLI and reload the configuration, use the `reload` command in Exec mode. The `reload` command reboots the ACE and performs a full power cycle of both the hardware and software. The reset process can take several minutes. Any open connections with the ACE are dropped after you enter the `reload` command.

⚠️ Configuration changes that are not written to the Flash partition are lost after a reload. Before rebooting, enter the `copy running-conf startup-config` command in Exec mode to store the current configuration in Flash memory. If you fail to save your configuration changes, the ACE reverts to its previous settings upon restart.

When you specify `reload`, the ACE prompts you for confirmation and performs a cold restart of the ACE:

```
host1/Admin# reload
This command will reboot the system
Save configurations for all the contexts. Save? [yes/no]: [yes]
```
Restarting the ACE from the Catalyst CLI

To restart the ACE from the Catalyst 6500 series CLI, use the `hw-module` command. The syntax of this command is as follows:

```
hw-module module mod_num reset
```

The arguments and keywords are as follows:
- **module mod_num**—Applies the command to the module in the specified slot number in the Catalyst 6500 series chassis where the ACE is installed
- **reset**—Resets the specified module

For example, to use the Catalyst 6500 series CLI to reset the ACE located in slot 3 of the chassis, enter:

```
Cat6k-switch# hw-module module 3 reset
Proceed with reload of module?[confirm]
% reset issued for module 3
```

Press **Enter** to confirm the restart operation.

Shutting Down the ACE

⚠️ **Caution**

Do not remove the ACE from the Catalyst 6500 series switch until the module has shut down completely and the Status LED is orange. You can damage the ACE if you remove it from the switch before it completely shuts down.

To avoid corrupting the ACE, you must correctly shut down the module before you disconnect the power or remove it from the Catalyst 6500 series chassis. To properly shut down the ACE, enter the `no power enable module` command in configuration mode at the Catalyst 6500 series CLI.

If the ACE fails to respond to this command, shut down the module by using a small, pointed object (such as a paper clip) to access the recessed Shutdown button on the front panel of the ACE. The shutdown procedure may take several minutes. The Status LED turns off when the ACE shuts down.
Enabling Remote Access to the ACE

This chapter describes how to configure remote access to the Cisco Application Control Engine (ACE) module by establishing a remote connection by using the Secure Shell (SSH) or Telnet protocols. It also describes how to configure the ACE to provide direct access to a user context from SSH. This chapter also covers how to configure the ACE to receive ICMP messages from a host.

This chapter contains the following major sections:

- Remote Access Configuration Quick Start
- Configuring Remote Network Management Traffic Services
- Configuring Telnet Management Sessions
- Configuring SSH Management Sessions
- Terminating an Active User Session
- Enabling ICMP Messages to the ACE
- Directly Accessing a User Context Through SSH
- Example of a Remote Access Configuration
- Viewing Session Information

Note

For information about how to make a direct connection using a dedicated terminal attached to the Console port on the front of the ACE, configure terminal display attributes, and configure terminal line settings for accessing the ACE by console or virtual terminal connection, see Chapter 1, Setting Up the ACE.
Remote Access Configuration Quick Start

Table 2-1 provides a quick overview of the steps required to configure remote network management access for the ACE. Each step includes the CLI command required to complete the task.

Table 2-1  Remote Network Management Configuration Quick Start

<table>
<thead>
<tr>
<th>Task and Command Example</th>
<th>Command Details</th>
</tr>
</thead>
</table>
| 1. If you are operating in multiple contexts, observe the CLI prompt to verify that you are operating in the desired context. If necessary, log directly in to, or change to, the correct context. | host1/Admin#  changeto C1  
host1/C1# |
| The rest of the examples in this table use the Admin context, unless otherwise specified. For details on creating contexts, see the Cisco Application Control Engine Module Virtualization Configuration Guide. | |
| 2. Enter configuration mode. | host1/Admin#  config  
Enter configuration commands, one per line. End with CNTL/Z  
host1/Admin(config)# |
| 3. Create a class map that permits network management traffic to be received by the ACE based on the network management protocol (SSH or Telnet) and client source IP address. | host1/Admin(config)#  class-map type management match-all  
SSH-ALLOW_CLASS  
host1/Admin(config-cmap-mgmt)#  match protocol ssh source-address  
172.16.10.0 255.255.255.254  
host1/Admin(config-cmap-mgmt)#  exit  
host1/Admin(config)#  
host1/Admin(config)#  class-map type management match-all  
TELNET-ALLOW_CLASS  
host1/Admin(config-cmap-mgmt)#  match protocol telnet source-address 172.16.10.0 255.255.255.254  
host1/Admin(config-cmap-mgmt)#  exit  
host1/Admin(config)# |
Table 2-1 Remote Network Management Configuration
Quick Start (continued)

Task and Command Example

4. Configure a policy map that activates the SSH and Telnet management protocol classifications.

```
host1/Admin(config)# policy-map type management first-match REMOTE_MGMT_ALLOW_POLICY
host1/Admin(config-pmap-mgmt)# class SSH-ALLOW_CLASS
host1/Admin(config-pmap-mgmt-c)# permit
host1/Admin(config-pmap-mgmt-c)# exit
host1/Admin(config-pmap-mgmt)# class TELNET-ALLOW_CLASS
host1/Admin(config-pmap-mgmt-c)# permit
host1/Admin(config-pmap-mgmt-c)# exit
host1/Admin(config-pmap-mgmt)# exit
host1/Admin(config)#
```

5. Attach the traffic policy to a single VLAN interface or globally to all VLAN interfaces in the same context. For example, to specify an interface VLAN and apply the remote management policy map to the VLAN, enter:

```
host1/Admin(config)# interface vlan 50
host1/Admin(config-if)# ip address 172.16.1.100 255.255.0.0
host1/Admin(config-if)# service-policy input REMOTE_MGMT_ALLOW_POLICY
host1/Admin(config-if)# exit
```

6. (Optional) Configure the maximum number of Telnet sessions allowed for each context.

```
host1/Admin(config)# telnet maxsessions 3
```

7. (Optional) Configure the maximum number of SSH sessions allowed for each context.

```
host1/Admin(config)# ssh maxsessions 3
```
You configure rules for remote access to the ACE through the use of class maps, policy maps, and service policies. The following items summarize the role of each function in configuring remote network management access to the ACE:

- **Class map**—Provides the remote network traffic match criteria to permit traffic based on:
  - Remote access network management protocols (SSH, Telnet, or ICMP)
  - Client source IP address
- **Policy map**—Enables remote network management access for a traffic classification that matches the criteria listed in the class map.
- **Service policy**—Activates the policy map and attaches the traffic policy to an interface or globally on all interfaces.

This section provides an overview on creating a class map, policy map, and service policy for remote network access.

### Table 2-1 Remote Network Management Configuration

#### Quick Start (continued)

**Task and Command Example**

8. If you have global administrator privileges, use the `ssh key` command to generate the SSH private key and the corresponding public key for use by the SSH server. There is only one host-key pair. For example, to generate an RSA1 key pair in the Admin context, enter:

```plaintext
host1/Admin(config)# ssh key rsa1 1024
generating rsa1 key
.....
generated rsa1 key
```

9. (Optional) Save your configuration changes to Flash memory.

```plaintext
host1/Admin(config)# exit
host1/Admin# copy running-config startup-config
```
Configuring Remote Network Management Traffic Services

Telnet and SSH remote access sessions are established to the ACE on a per context basis. For details on creating users and contexts, see the Cisco Application Control Engine Module Virtualization Configuration Guide.

This section contains the following topics:

- Creating and Configuring a Remote Management Class Map
- Creating a Layer 3 and Layer 4 Remote Access Policy Map
- Applying a Service Policy

Creating and Configuring a Remote Management Class Map

To create a Layer 3 and Layer 4 class map to classify the remote network management traffic received by the ACE, use the `class-map type management` configuration-mode command. This command permits network management traffic to be received by the ACE by identifying the incoming IP protocols that the ACE can receive as well as the client source IP address and subnet mask as the matching criteria. The `type management` keywords define the allowed network traffic to manage security for protocols such as SSH, Telnet, and ICMP.

A class map can have multiple match commands. You can configure class maps to define multiple management protocol and source IP address match commands in a group that you then associate with a traffic policy. The `match-all` and `match-any` keywords determine how the ACE evaluates multiple match statements operations when multiple match criteria exist in a class map.

The syntax of this command is as follows:

```
class-map type management [match-all | match-any] map_name
```

The keywords, arguments, and options are as follows:

- `match-all` | `match-any`—(Optional) Determines how the ACE evaluates Layer 3 and Layer 4 network management traffic when multiple match criteria exist in a class map. The class map is considered a match if the match commands meet one of the following conditions.
  - `match-all`—(Default) All of the match criteria listed in the class map are satisfied to match the network traffic class in the class map, typically match commands of the same type.
--- match-any --- Any one of the match criteria listed in the class map is satisfied to match the network traffic class in the class map, typically match commands of different types.

- map_name — Specifies the name assigned to the class map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

The CLI enters the class map management configuration mode. To classify the remote network management traffic received by the ACE, include one or more of the match protocol commands to configure the match criteria for the class map:

For example, to allow SSH and Telnet access to the ACE from IP address 172.16.10.0, enter:

```plaintext
host1/Admin(config)# class-map type management match-all SSH-TELNET_ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# match protocol ssh source-address 172.16.10.0 255.255.255.254
host1/Admin(config-cmap-mgmt)# match protocol telnet source-address 172.16.10.0 255.255.255.254
host1/Admin(config-cmap-mgmt)# exit
host1/Admin(config)#
```

To remove a Layer 3 and Layer 4 network management class map from the ACE, enter:

```plaintext
host1/Admin(config)# no class-map type management match-all SSH-TELNET_ALLOW_CLASS
```

This section contains the following topics:

- Defining a Class Map Description
- Defining Remote Network Management Protocol Match Criteria

### Defining a Class Map Description

To provide a brief summary about the Layer 3 and Layer 4 remote management class map, use the `description` command in class map configuration mode.

The syntax of this command is as follows:

```
description text
```

Use the `text` argument to enter an unquoted text string with a maximum of 240 alphanumeric characters.
For example, to specify a description that the class map is to allow remote Telnet access, enter:

```bash
host1/Admin(config)# class-map type management TELNET-ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# description Allow Telnet access to the ACE
```

To remove the description from the class map, enter:

```bash
host1/Admin(config-cmap-mgmt)# no description
```

### Defining Remote Network Management Protocol Match Criteria

To configure the class map to identify the remote network access management protocols that can be received by the ACE, use the `match protocol` command in class map management configuration mode. You configure the associated policy map to permit access to the ACE for the specified management protocols. As part of the network management access traffic classification, you also specify either a client source host IP address and subnet mask as the matching criteria or instruct the ACE to allow any client source address for the management traffic classification.

The syntax of this command is as follows:

```
[line_number] match protocol {http | https | icmp | kalap-udp | snmp | ssh | telnet} {any | source-address ip_address mask}
```

- `line_number`—(Optional) Assists you in editing or deleting individual `match` commands. Enter an integer from 2 to 255 as the line number. You can enter `no line_number` to delete long `match` commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the `match` statements.

- `http`—Specifies the Hypertext Transfer Protocol (HTTP). The configuration of the HTTP management protocol is described in Chapter 8, Configuring the XML Interface.

- `https`—Specifies the secure (SSL) Hypertext Transfer Protocol (HTTP). The configuration of the HTTPS management protocol is described in Chapter 8, Configuring the XML Interface.

- `icmp`—Specifies Internet Control Message Protocol messages to the ACE. The configuration of the ICMP management protocol is described in the “Enabling ICMP Messages to the ACE” section.
• **kalap-udp**—Specifies management access using KAL-AP over UDP. The configuration of the KAL-AP management access is described in the “Configuring Health Monitoring” chapter of the *Cisco Application Control Engine Module Server Load-Balancing Configuration Guide*.

• **snmp**—Specifies the Simple Network Management Protocol (SNMP). The configuration of the SNMP management protocol is described in Chapter 7, Configuring SNMP.

• **ssh**—Specifies a Secure Shell (SSH) remote connection to the ACE. The ACE supports the SSH remote shell functionality provided in SSH Version 1 and supports DES and 3DES ciphers. The configuration of the SSH management protocol is described in the “Configuring SSH Management Sessions” section.

  **Note**  
  SSH v1.x and v2 are entirely different protocols and are not compatible. Make sure that you use an SSH v1.x client when accessing the ACE.

• **telnet**—Specifies a Telnet remote connection to the ACE. The configuration of the Telnet management protocol is described in the “Configuring Telnet Management Sessions” section.

• **any**—Specifies any client source address for the management traffic classification.

• **source-address**—Specifies a client source host IP address and subnet mask as the network traffic matching criteria. As part of the classification, the ACE implicitly obtains the destination IP address from the interface on which you apply the policy map.

• **ip_address**—Source IP address of the client. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).

• **mask**—Subnet mask of the client in dotted-decimal notation (for example, 255.255.255.0).

For example, to specify that the class map allows SSH access to the ACE from source IP address 192.168.10.1 255.255.255.0, enter:

```
host1/Admin(config)# class-map type management SSH-ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# match protocol ssh source-address 192.168.10.1 255.255.255.0
```
To deselect the specified network management protocol match criteria from the class map, enter:

```
host1/Admin(config-cmap-mgmt)# no match protocol ssh source-address 192.168.10.1 255.255.255.0
```

### Creating a Layer 3 and Layer 4 Remote Access Policy Map

For a Layer 3 and Layer 4 traffic classification, you create a Layer 3 and Layer 4 policy map with actions to configure the network management traffic received by the ACE. This section outlines the general steps to configure a Layer 3 and Layer 4 network traffic policy and contains the following topics:

- Creating a Layer 3 and Layer 4 Policy Map for Network Management Traffic Received by the ACE
- Defining a Layer 3 and Layer 4 Policy Map Description
- Specifying a Layer 3 and Layer 4 Traffic Class With the Traffic Policy
- Defining Layer 3 and Layer 4 Management Traffic Policy Actions

### Creating a Layer 3 and Layer 4 Policy Map for Network Management Traffic Received by the ACE

To configure a Layer 3 and Layer 4 policy map that defines the different actions that are applied to the IP management traffic received by the ACE, use the `policy-map type management first-match` configuration command. The ACE executes the specified action only for traffic that meets the first matching classification with a policy map. The ACE does not execute any additional actions.

The syntax of this command is as follows:

```
policy-map type management first-match map_name
```

The `map_name` argument specifies the name assigned to the Layer 3 and Layer 4 network management policy map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

When you use this command, you will access policy map management configuration mode.
For example, to create a Layer 3 and Layer 4 network traffic management policy map, enter:

```
host1/Admin(config) # policy-map type management first-match REMOTE_MGMT_ALLOW_POLICY
host1/Admin(config-pmap-mgmt) #
```

To remove a policy map from the ACE, enter:

```
host1/Admin(config) # no policy-map type management first-match REMOTE_MGMT_ALLOW_POLICY
```

**Defining a Layer 3 and Layer 4 Policy Map Description**

To provide a brief summary about the Layer 3 and Layer 4 remote management policy map, use the `description` command in policy map configuration mode.

The syntax of this command is as follows:

```
description text
```

The `text` argument specifies the description that you want to provide. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

For example, to specify a description that the policy map is to allow remote Telnet access, enter:

```
host1/Admin(config-pmap-mgmt)# description Allow Telnet access to the ACE
```

To remove a description from the policy map, enter:

```
host1/Admin(config-pmap-mgmt)# no description
```
Specifying a Layer 3 and Layer 4 Traffic Class With the Traffic Policy

To specify a Layer 3 and Layer 4 traffic class created with the class-map command to associate network traffic with the traffic policy, use the class command in policy map configuration mode. This command enters the policy map management class configuration mode.

The syntax of this command is as follows:

```
class {name1 [insert-before name2] | class-default}
```

The arguments, keywords, and options are as follows:

- **name1** — Name of a previously defined Layer 3 and Layer 4 traffic class, configured with the class-map command, to associate traffic to the traffic policy. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

- **insert-before name2** — (Optional) Places the current class map ahead of an existing class map or inline match condition specified by the name2 argument in the policy map configuration. The ACE does not save the sequence reordering as part of the configuration. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

- **class-default** — Specifies the class-default class map for the Layer 3 and Layer 4 traffic policy. This class map is a reserved class map created by the ACE. You cannot delete or modify this class. All network 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 match, the ACE then matches the action specified under the class class-default command. The class-default class map has an implicit match any statement in it and is used to match any traffic classification. The class-default class map has an implicit match any statement that matches all traffic.

For example, to specify an existing class map within the Layer 3 and Layer 4 remote access policy map, enter:

```
host1/Admin(config-pmap-mgmt)# class L4_REMOTE_ACCESS_CLASS
host1/Admin(config-pmap-mgmt-c)#
```

To use the insert-before command to define the sequential order of two class maps in the policy map, enter:

```
host1/Admin(config-pmap-mgmt)# class L4_SSH_CLASS insert-before L4_REMOTE_ACCESS_CLASS
```
To specify the class-default class map for the Layer 3 and Layer 4 traffic policy, enter:

```
host1/Admin(config-pmap-mgmt)# class class-default
```

To remove a class map from a Layer 3 and Layer 4 policy map, enter:

```
host1/Admin(config-pmap-mgmt)# no class L4_REMOTE_ACCESS_CLASS
```

### Defining Layer 3 and Layer 4 Management Traffic Policy Actions

To allow the network management traffic listed in the Layer 3 and Layer 4 class map to be received or rejected by the ACE, specify either the `permit` or `deny` command in policy map class configuration mode as follows:

- Use the `permit` command in policy map class configuration mode to allow the remote management protocols listed in the class map to be received by the ACE.
- Use the `deny` command in policy map class configuration mode to refuse the remote management protocols listed in the class map to be received by the ACE.

For example, to create a Layer 3 and Layer 4 remote network traffic management policy map that permits SSH, Telnet, and ICMP connections to be received by the ACE, enter:

```
host1/Admin(config)# policy-map type management first-match REMOTE_MGMT_ALLOW_POLICY
host1/Admin(config-pmap-mgmt)# class SSH-ALLOW_CLASS
host1/Admin(config-pmap-mgmt-c)# permit
host1/Admin(config-pmap-mgmt-c)# exit
host1/Admin(config-pmap-mgmt)# class TELNET-ALLOW_CLASS
host1/Admin(config-pmap-mgmt-c)# permit
host1/Admin(config-pmap-mgmt-c)# exit
host1/Admin(config-pmap-mgmt)# class ICMP-ALLOW_CLASS
host1/Admin(config-pmap-mgmt-c)# permit
host1/Admin(config-pmap-mgmt-c)# exit
```

For example, to create a policy map that restricts an ICMP connection by the ACE, enter:

```
host1/Admin(config)# policy-map type management first-action ICMP.Restrict_POLICY
host1/Admin(config-pmap-mgmt)# class ICMP-ALLOW_CLASS
host1/Admin(config-pmap-mgmt-c)# deny
```
Applying a Service Policy

Use the `service-policy` command to perform the following tasks:

- Apply a previously created policy map.
- Attach the traffic policy to a specific VLAN interface or globally to all VLAN interfaces in the same context.
- Specify that the traffic policy is to be attached to the input direction of an interface.

The `service-policy` command is available at both the interface configuration mode and at the configuration mode. Specifying a policy map in the interface configuration mode applies the policy map to a specific VLAN interface. Specifying a policy map in the configuration mode applies the policy to all of the VLAN interfaces associated with a context.

The syntax of this command is as follows:

```
service-policy input policy_name
```

The keywords, arguments, and options are as follows:

- `input`—Specifies that the traffic policy is to be attached to the input direction of an interface. The traffic policy evaluates all traffic received by that interface.
- `policy_name`—Name of a previously defined policy map, configured with a previously created `policy-map` command. The name can be a maximum of 40 alphanumeric characters.

For example, to specify an interface VLAN and apply the remote access policy map to a VLAN, enter:

```
host1/Admin(config)# interface vlan 50
host1/Admin(config-if)# ip address 172.16.1.100 255.255.0.0
host1/Admin(config-if)# service-policy input REMOTE_MGMT_ALLOW_POLICY
```

For example, to globally apply the remote access policy map to all of the VLANs associated with a context, enter:

```
host1/Admin(config)# service-policy input REMOTE_MGMT_ALLOW_POLICY
```

To detach the remote access traffic policy from an interface, enter:

```
host1/Admin(config-if)# no service-policy input REMOTE_MGMT_ALLOW_POLICY
```
To globally detach the remote access traffic policy from all VLANs associated with a context, enter:

```
host1/Admin(config)# no service-policy input REMOTE_MGMT.Allow_POLICY
```

You can detach a traffic policy by either of the following methods:

- Individually from the last VLAN interface on which you applied the service policy
- Globally from all VLAN interfaces in the same context

The ACE automatically resets the associated service policy statistics to provide a new starting point for the service policy statistics the next time that you attach a traffic policy to a specific VLAN interface or globally to all VLAN interfaces in the same context.

Note the following guidelines and restrictions when creating a service policy:

- Policy maps, applied globally in a context, are internally applied on all interfaces existing in the context.
- A policy activated on an interface overwrites any specified global policies for overlapping classification and actions.
- The ACE allows only one policy of a specific feature type to be activated on a given interface.

To display service policy statistics for all policy maps or a specific Layer 3 and Layer 4 remote network traffic management policy map, use the `show service-policy` command in Exec mode.

The syntax of this command is as follows:

```
show service-policy [policy_name [detail]]
```

The keywords, options, and arguments are as follows:

- `policy_name`—(Optional) Existing policy map that is currently in service (applied to an interface) as an unquoted text string with a maximum of 64 alphanumeric characters. If you do not enter the name of an existing policy map, the ACE displays information and statistics for all policy maps.
- `detail`—(Optional) Displays a more detailed listing of policy map statistics and status information.
Note
The ACE updates the counters that the show service-policy command displays after the applicable connections are closed.

For example, to display service policy statistics for the REMOTE_MGMT_ALLOW_POLICY policy map, enter:

```
host1/Admin# show service-policy REMOTE_MGMT_ALLOW_POLICY
```

Status : ACTIVE
Description: Allow mgmt protocols
Context Global Policy:
  service-policy: REMOTE_MGMT_ALLOW_POLICY

To clear the service policy statistics for a policy map, use the clear service-policy command. The syntax of this command is as follows:

```
clear service-policy policy_name
```

For the policy_name argument, enter the identifier of an existing policy map that is currently in service (applied to an interface).

For example, to clear the statistics for the policy map REMOTE_MGMT_ALLOW_POLICY that is currently in service, enter:

```
host1/Admin# clear service-policy REMOTE_MGMT_ALLOW_POLICY
```

## Configuring Telnet Management Sessions

The ACE supports a maximum 16 concurrent Telnet management sessions for the Admin context and 4 concurrent Telnet management sessions for each user context.

To control the maximum number of Telnet sessions allowed for each context, use the telnet maxsessions command in configuration mode. The ACE supports a total maximum of 256 concurrent Telnet sessions.

Telnet remote access sessions are established on the ACE per context. You can create a context, assign an interface and IP address to it, and then log into the ACE by using Telnet to connect to that IP address. This capability allows you to specify a particular context when accessing the ACE. For details on creating users and contexts, see the Cisco Application Control Engine Module Virtualization Configuration Guide.
The syntax of this command is as follows:

```
telnet maxsessions max_sessions
```

The `max_sessions` argument sets the maximum number of concurrent Telnet sessions allowed for the associated context. The range is from 1 to 16 Telnet sessions for the Admin context and from 1 to 4 Telnet sessions for each user context. The defaults are 16 (Admin context) and 4 (user context).

For example, to configure the maximum number of concurrent Telnet sessions to 3 in the Admin context, enter:

```
host1/Admin(config)# telnet maxsessions 3
```

To revert to the default of 16 Telnet sessions for the Admin context, enter:

```
host1/Admin(config)# no telnet maxsessions
```

### Configuring SSH Management Sessions

This section contains the following topics:

- Configuring Maximum Number of SSH Sessions
- Generating SSH Host Key Pairs

SSH remote access sessions are established on the ACE per context. You can create a context, assign an interface and IP address to it, and then log into the ACE by using SSH to connect to that IP address. This capability allows you to specify a particular context when accessing the ACE. For details on creating users and contexts, see the *Cisco Application Control Engine Module Virtualization Configuration Guide*.

### Configuring Maximum Number of SSH Sessions

The ACE supports a maximum of 16 concurrent SSH management sessions for the Admin context and 4 concurrent SSH management sessions for each user context.

To control the maximum number of SSH sessions allowed for each context, use the `ssh maxsessions` command in configuration mode. The ACE supports a total maximum of 256 concurrent SSH sessions.
Chapter 2    Enabling Remote Access to the ACE

Configuring SSH Management Sessions

The syntax of this command is as follows:

```
ssh maxsessions max_sessions
```

The `max_sessions` argument sets the maximum number of concurrent SSH sessions allowed for the associated context. The range is from 1 to 16 SSH sessions for the Admin context and from 1 to 4 SSH sessions for each user context. The defaults are 16 (Admin context) and 4 (user context).

For example, to configure the maximum number of concurrent SSH sessions in the Admin context to 3, enter:

```
host1/Admin(config)# ssh maxsessions 3
```

To revert to the default of 16 Telnet sessions for the Admin context, enter:

```
host1/Admin(config)# no ssh maxsessions
```

Generating SSH Host Key Pairs

The ACE supports remote login over an SSH session that uses private and public key pairs to perform authentication for the context. DSA and RSA keys are generated in pairs—one public key and one private key. With this method of remote connection, use a generated private and public key pair to participate in a secure communication by encrypting and decrypting messages.

The global administrator performs the key generation in the Admin context. All contexts associated with the ACE share the common key. There is only a single host-key pair.

Note

If you are the administrator or another user authorized in the Admin context, use the `changeto` command in Exec mode to move to the Admin context. An administrator can perform all allowable functions within the Admin context.

Ensure that you have an SSH host key pair with the appropriate version before enabling the SSH service. The SSH service accepts three types of key pairs for use by SSH versions 1 and 2. Generate the SSH host key pair according to the SSH client version used. The number of bits specified for each key pair ranges from 768 to 4096.

To generate the SSH private key and the corresponding public key for use by the SSH server, use the `ssh key` command in configuration mode.
The syntax of this command is as follows:

```
ssh key {dsa | rsa | rsa1} [bits [force]]
```

The arguments, keywords, and options are as follows:

- `dsa`—Generates the DSA key pair for the SSH version 2 protocol.
- `rsa`—Generates the RSA key pair for the SSH version 2 protocol.
- `rsa1`—Generates the RSA1 key pair for the SSH version 1 protocol.
- `bits`—(Optional) Number of bits for the key pair. For DSA, the range is from 768 to 2048. For RSA and RSA1, the range is from 768 to 4096. The greater the number of bits that you specify, the longer it takes to generate the key. The default is 768.
- `force`—(Optional) Forces the generation of a DSA or RSA key even when previous keys exist. If the SSH key pair option is already generated for the required version, use the `force` option to overwrite the previously generated key pair.

Before you generate the key, set the hostname. This setting is used in the generation of the key. See Chapter 1, Setting Up the ACE, for details on setting a hostname.

For example, to generate an RSA1 key pair in the Admin context, enter:

```
host1/Admin(config)# ssh key rsa1 1024
generating rsa1 key
.....
generated rsa1 key
```

To remove the SSH host key pair, enter:

```
host1/Admin(config)# no ssh key rsa1
```

To clear the public keys of all trusted hosts, use the `clear ssh hosts` Exec command. These keys are either sent to an SSH client by an SSH server or are entered manually. When a SSH connection is made from the ACE, the SSH client receives the public key and stores it locally. To clear all these keys, use the `clear ssh hosts` command in Exec mode.
Terminating an Active User Session

To terminate an active SSH or Telnet session for the active context, use one of the following commands in Exec mode:

- `clear ssh {session_id | hosts}
- `clear telnet {session_id}

The arguments, keywords, and options are as follows:

- `session_id`—Specifies the identifier of the SSH or Telnet session to disconnect. You can obtain the specific `session_id` value using either the `show ssh session-info` command or the `show telnet` command in Exec mode. See the “Directly Accessing a User Context Through SSH” section for details.

- `hosts`—Clears the list of trusted SSH hosts from the ACE configuration.

For example, to terminate an SSH session, enter:

```
host1/Admin # clear ssh 345
```

Enabling ICMP Messages to the ACE

By default, the ACE does not allow ICMP messages to be received by an ACE interface or to pass through the ACE interface. ICMP is an important tool for testing your network connectivity; however, network hackers can also use ICMP to attack the ACE or your network. We recommend that you allow ICMP during your initial testing, but then disallow it during normal operation.

To permit or deny address(es) to reach an ACE interface with ICMP messages, either from a host to the ACE, or from the ACE to a host which requires the ICMP reply to be allowed back, configure one of the following:

- Class map to provide the ICMP network traffic match criteria for the ACE.
- Policy map to enable ICMP network management access to and from the ACE.
- Service policy to activate the policy map, attach the traffic policy to an interface or globally on all interfaces, and specify the direction in which the policy should be applied.
See the “Configuring Remote Network Management Traffic Services” section for details on configuring a network management class map, policy map, and service policy for the ACE.

To allow ICMP messages to pass through the ACE, configure an ICMP ACL to permit or deny network connections based on the ICMP type (for example, echo, echo-reply, or unreachable). See the Cisco Application Control Engine Module Security Configuration Guide for details.

**Note**

If you want only to allow the ACE to ping a host (and allow the echo reply back to the interface), but not allow hosts to ping the ACE, enable the ICMP application protocol inspection function instead of defining a class map and policy map. See the Cisco Application Control Engine Module Security Configuration Guide for details.

For example, to allow the ACE to receive ICMP pings, enter:

```bash
class-map type management match-all ICMP-ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# description Allow ICMP packets
host1/Admin(config-cmap-mgmt)# match protocol icmp source-address 172.16.10.0 255.255.255.254
host1/Admin(config-cmap-mgmt)# exit
policy-map type management first-action ICMP_ALLOW_POLICY
host1/Admin(config-pmap-mgmt)# class ICMP-ALLOW_CLASS
host1/Admin(config-pmap-mgmt-c)# permit
host1/Admin(config-pmap-mgmt-c)# exit
host1/Admin(config-pmap-mgmt)# exit
interface vlan 50
host1/Admin(config-if)# ip address 172.16.1.100 255.255.0.0
host1/Admin(config-if)# service-policy input ICMP_ALLOW_POLICY
```
Directly Accessing a User Context Through SSH

As the global administrator, from the Admin context, you can configure a user context and enable direct login access to that user context from a remote SSH session. To configure the ACE to provide direct access to a user context from SSH, perform the following steps:

Step 1 Create a user context by entering the following command:

```
host1/Admin(config)# context C1
host1/Admin(config-context)#
```

See the Cisco Application Control Engine Module Virtualization Configuration Guide.

Step 2 Associate an existing VLAN with the user context so that the context can receive traffic classified for it by entering the following command:

```
host1/Admin(config-context)# allocate-interface vlan 100
```

See the Cisco Application Control Engine Module Routing and Bridging Configuration Guide.

Step 3 Generate the SSH host key pair by entering the following command:

```
host1/Admin(config-context)# ssh key rsa1 1024
generating rsa1 key
.....
generated rsa1 key
```

See the “Generating SSH Host Key Pairs” section.

Step 4 Change to the C1 context that you created in Step 1 and enter configuration mode in that context by entering the following commands:

```
host1/Admin(config-context)# do changeto C1
host1/C1(config-context)# exit
host1/C1(config)#
```

Only users authenticated in the Admin context can use the changeto command.
**Step 5** Configure the VLAN interface that you allocated to the user context in Step 2 by entering the following commands:

```
host1/C1(config)# interface vlan 50
host1/C1(config-if)# ip address 192.168.1.1 255.255.255.0
host1/C1(config-if)# no shutdown
host1/C1(config-if)# exit
host1/C1(config)#
```

For example, assign an IP address to the interface and reenable the interface within the context with the `no shutdown` command. See the *Cisco Application Control Engine Module Routing and Bridging Configuration Guide*.

**Step 6** Create an SSH remote management policy and apply the associated service policy to all VLAN interfaces or just to the VLAN interface allocated to the user context by entering the following commands:

```
host1/C1(config)# class-map type management match-all SSH-ALLOW_CLASS
host1/C1(config-cmap-mgmt)# match protocol ssh source-address 172.16.10.0 255.255.255.254
host1/C1(config-cmap-mgmt)# exit
host1/C1(config)#
host1/C1(config)# policy-map type management first-match REMOTE_MGMT_ALLOW_POLICY
host1/C1(config-pmap-mgmt)# class SSH-ALLOW_CLASS
host1/C1(config-pmap-mgmt-c)# permit
host1/C1(config-pmap-mgmt-c)# exit
host1/C1(config)# interface vlan 50
host1/C1(config-if)# ip address 192.168.1.1 255.255.255.0
host1/C1(config-if)# service-policy input REMOTE_MGMT_ALLOW_POLICY
host1/C1(config-if)# exit
host1/C1(config)#
```

See the “Configuring Remote Network Management Traffic Services” section.

**Step 7** Create an IP route by entering the following command:

```
host1/C1(config)# ip route 0.0.0.0 255.255.255.0 192.168.4.8
```

See the *Cisco Application Control Engine Module Security Configuration Guide*.
To directly access the user context from an SSH client, perform the following steps:

**Step 1** From the SSH client, establish a remote SSH session to the IP address of the user context VLAN interface.

**Step 2** Enter the password for the user context VLAN interface. The ACE CLI prompt appears in Exec mode of the user context.

```
host1/C1#
```

---

**Example of a Remote Access Configuration**

The following example illustrates a running-configuration that defines rules for remote access to the ACE through the use of class maps, policy maps, and service policies. The remote access configuration appears in bold in the example.

```
telnet maxsessions 3

ssh maxsessions 3

access-list ACL1 line 10 extended permit ip any any

class-map type management match-any L4_REMOTE-MGT_CLASS
   description Allows Telnet, SSH, and ICMP protocols
   2 match protocol telnet any
   3 match protocol ssh any
   4 match protocol icmp any

policy-map type management first-match L4_REMOTE-MGT_POLICY
   class L4_REMOTE-MGT_CLASS
   permit

interface vlan 50
   ip address 192.168.1.1 255.255.255.0
   access-group input ACL1

   service-policy input L4_REMOTE-MGT_POLICY
   no shutdown

   ssh key rsa1 1024 force
```
Viewing Session Information

This section contains the following topics:

- Showing Telnet Session Information
- Showing SSH Session Information

Showing Telnet Session Information

To display information related to the Telnet session, use the `show telnet` command in Exec mode. Only the context administrator can view Telnet information associated with a particular context.

The syntax of this command is as follows:

```
show telnet [context_name]
```

The optional `context_name` argument specifies the name of the context for which you want to view specific Telnet session information. The `context_name` argument is case sensitive.

For example, enter:

```
host1/Admin# show telnet
```

Table 2-2 describes the fields in the `show telnet` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SessionID</td>
<td>Unique session identifier for the Telnet session.</td>
</tr>
<tr>
<td>Remote Host</td>
<td>IP address and port of the remote Telnet client.</td>
</tr>
<tr>
<td>Active Time</td>
<td>Time since the Telnet connection request was received by the ACE.</td>
</tr>
</tbody>
</table>

To display the maximum number of enabled Telnet sessions, use the `show telnet maxsessions` command in Exec mode. Only context administrators can view Telnet session information associated with a particular context.
The syntax of this command is as follows:

```
show telnet maxsessions [context_name]
```

The optional `context_name` argument specifies the name of the context for which you want to view the maximum number of Telnet sessions. The `context_name` argument is case sensitive.

For example, enter:

```
host1/Admin# show telnet maxsessions
```

Maximum Sessions Allowed is 4

### Showing SSH Session Information

This section contains the following topics:

- Showing SSH Session Information
- Showing SSH Key Details

#### Showing SSH Session Information

To display information related to the SSH session, use the `show ssh session-info` command in Exec mode. Only context administrators can view SSH session information associated with a particular context.

The syntax of this command is as follows:

```
show ssh session-info [context_name]
```

The optional `context_name` argument specifies the name of the context for which you want to view specific SSH session information. The `context_name` argument is case sensitive.

For example, enter:

```
host1/Admin# show ssh session-info
```

Table 2-3 describes the fields in the `show ssh session-info` command output.
To display the maximum number of enabled SSH sessions, use the `show ssh maxsessions` command in Exec mode. Only context administrators can view SSH session information associated with a particular context.

The syntax of this command is as follows:

```
show ssh maxsessions [context_name]
```

The optional `context_name` argument specifies the name of the context for which the context administrator wants to view the maximum number of SSH sessions. The `context_name` argument is case sensitive.

For example, enter:

```
host1/Admin# show ssh maxsessions
Maximum Sessions Allowed is 4 (SSH Server is enabled)
```

### Showing SSH Key Details

Use the `show ssh key` command in Exec mode to display the host key pair details for the specified key or for all keys if you do not specify a key.

The syntax of this command is as follows:

```
show ssh key [dsa | rsa | rsa1]
```

The arguments, keywords, and options are as follows:

- `dsa`—Specifies the DSA key pair for the SSH version 2 protocol.
- `rsa`—Specifies the RSA key pair for the SSH version 2 protocol.
- `rsa1`—Specifies the RSA1 key pair for the SSH version 1 protocol.

#### Table 2-3  Field Descriptions for the `show ssh session-info` Command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SessionID</td>
<td>Unique session identifier for the SSH session.</td>
</tr>
<tr>
<td>Remote Host</td>
<td>IP address and port of the remote SSH client.</td>
</tr>
<tr>
<td>Active Time</td>
<td>Time since the SSH connection request was received by the ACE.</td>
</tr>
</tbody>
</table>
For example, enter:

host1/Admin # show ssh key
*******************************
could not retrieve rsa1 key information
*******************************
rsa Keys generated:Tue Mar 7 19:37:17 2006

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEA4v4DQ8aNl482qDTRJu9G07hEIXcGTwAnPm+WOCUlki
hz
QND5zwA50CBAJSfIIIIB41Ed61qhhOkbXSNeCvTp9SmVoish2wvJrETpIDIEGxXh/jjWVsUM/e
eBQA/7o6tv
gCeT6p7jGSP50UNYFP0CeZ9Bi1Wdc4j8mYEQLEqJHPrMhSFE=

bitcount:1024
fingerprint:
*******************************

da Keys generated:Tue Dec 20 19:37:17 2005

ssh-das
AAAAB3NzaC1dk3MAAACBAPqDDRqU+0qNLbKRMq+DQAAXnvcB+H8Nq8jA4WgJ7uQcuDCLaG7
Lq
tKlTtJJa6aZyvwsQW4n4Kt1xvZy3cJ6PUbSyqmCtsaYYo4UQ6cKr9V+NsfgzTSLW
TH8iDvVJl
ct32tQ1Eka7mpseQeX3Jy1Mrlh8qRkhbKxKkc49XAAAAAFCPM0QJrg6+kkaqJpeNxeXhU
H9HwAAAE
keZ12JM6sfKQJDLH7ktrO+jpBV9Ur4VyY0zMoeh/LmSaZDq+Mc8UN1LM+15vkQgnKce
arD91M+hR
z2QYx5hO1YCKj/ny2a5p/8Hk152cnmQAg6ebkITTWAPrChHDS/1mca159zLrZcdlXW5
gB/7MTG
sICmYwJiweAwAAECAjQ66zdZQqY1CwzRmkridEGDTLV6ixDjBNGb8Aqj1+y1XmZqLL0
D4oMsb7i1dE
L3m4hQQY7hKTK0o5cKvaxILVtnk2vrgoQnLNQRMViaJUX7WKk1Ln6vWPGZe8koALv0G
XxsOv2ugz/T
TDk01oCatTvW/bxKjtoVROgILXtLIP

bitcount:1024
fingerprint:
*******************************
Managing ACE Software Licenses

This chapter describes how to manage the software licenses for your Cisco Application Control Engine (ACE) module. It contains the following major sections:

- Available ACE Licenses
- Ordering an Upgrade License and Generating a Key
- Copying a License File to the ACE
- Installing a New or Upgrade License File
- Replacing a Demo License with a Permanent License
- Removing a License
- Backing Up a License File
- Displaying License Configurations and Statistics

Note

You can access the license and show license commands only in the Admin context. You must have the Admin role in the Admin context to install, remove, and update the license file.
Available ACE Licenses

By default, the ACE supports the following features and capabilities:

- Virtualization with one Admin context and five user contexts
- Module bandwidth of 4 gigabits per second (Gbps)
- Secure Sockets Layer (SSL) with 1000 transactions per second (TPS)

You can increase the number of default user contexts, module bandwidth, and SSL TPS by purchasing upgrade licenses. Table 3-1 lists the available ACE licenses, product IDs (PIDs), and descriptions.

Table 3-1  ACE Licenses

<table>
<thead>
<tr>
<th>Feature (Default)</th>
<th>License PID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtualization (default, one Admin context and five user contexts)</td>
<td>ACE-VIRT-020</td>
<td>20 virtual contexts</td>
</tr>
<tr>
<td></td>
<td>ACE-VIRT-050</td>
<td>50 virtual contexts</td>
</tr>
<tr>
<td></td>
<td>ACE-VIRT-100</td>
<td>100 virtual contexts</td>
</tr>
<tr>
<td></td>
<td>ACE-VIRT-250</td>
<td>250 virtual contexts</td>
</tr>
<tr>
<td></td>
<td>ACE-VIRT-UP1</td>
<td>Upgrades 20 to 50 contexts</td>
</tr>
<tr>
<td></td>
<td>ACE-VIRT-UP2</td>
<td>Upgrades 50 to 100 contexts</td>
</tr>
<tr>
<td></td>
<td>ACE-VIRT-UP3</td>
<td>Upgrades 100 to 250 contexts</td>
</tr>
<tr>
<td>Module bandwidth (default, 4 Gbps)</td>
<td>ACE-04G-LIC</td>
<td>Default 4-Gbps bandwidth</td>
</tr>
<tr>
<td></td>
<td>ACE-08G-LIC</td>
<td>8-Gbps bandwidth</td>
</tr>
<tr>
<td></td>
<td>ACE-16G-LIC</td>
<td>16-Gbps bandwidth (ACE20-MOD-K9 module only)</td>
</tr>
<tr>
<td></td>
<td>ACE-UPG1-LIC</td>
<td>Upgrades 4-Gbps bandwidth to 8-Gbps bandwidth</td>
</tr>
<tr>
<td></td>
<td>ACE-UPG2-LIC</td>
<td>Upgrades 8-Gbps bandwidth to 16-Gbps bandwidth (ACE20-MOD-K9 module only)</td>
</tr>
</tbody>
</table>
Ordering an Upgrade License and Generating a Key

You can upgrade virtualization in increments if you do not exceed the limits of the ACE (a maximum of 250 contexts).

For information on ACE demo licenses, contact your Cisco account representative.

Note: If you need to replace the ACE, you can copy and install the license file for the license onto the replacement module.

### Table 3-1  ACE Licenses (continued)

<table>
<thead>
<tr>
<th>Feature (Default)</th>
<th>License PID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL TPS (default, 1000 TPS)</td>
<td>ACE-SSL-05K-K9</td>
<td>SSL with 5000 TPS</td>
</tr>
<tr>
<td></td>
<td>ACE-SSL-10K-K9</td>
<td>SSL with 10,000 TPS</td>
</tr>
<tr>
<td></td>
<td>ACE-SSL-15K-K9</td>
<td>SSL with 15,000 TPS</td>
</tr>
</tbody>
</table>

Ordering an Upgrade License and Generating a Key

This section describes the process that you use to order an upgrade license and to generate a license key for your ACE. To order an upgrade license, perform the following steps:

**Step 1** Order one of the licenses from the list in the “Available ACE Licenses” section using any of the available Cisco ordering tools on cisco.com.

**Step 2** When you receive the Software License Claim Certificate from Cisco, follow the instructions that direct you to the Cisco.com website. As a registered user of Cisco.com, go to this URL:

   http://www.cisco.com/go/license

**Step 3** Enter the Product Authorization Key (PAK) number found on the Software License Claim Certificate as your proof of purchase.

**Step 4** Provide all the requested information to generate a license key.
Step 5  After the system generates the license key, you will receive a license key e-mail with an attached license file and installation instructions. Save the license key e-mail in a safe place in case you need it in the future (for example, to transfer the license to another ACE).

Copying a License File to the ACE

When you receive the software license key e-mail from Cisco Systems, you must copy the attached license file to a network server. Use the copy command in Exec mode from the Admin context to copy the file to disk0: on the ACE. For detailed information on copying files from a remote server, see Chapter 4, Managing the ACE Software.

For example, the syntax of the copy tftp command is as follows:

```
copy tftp:////server//path//filename disk0:path//filename
```

The arguments and keywords are as follows:

- `//server//path//filename`—The path to the network server. This path is optional because the ACE prompts you for this information if you omit it.
- `disk0:path//filename`—Specifies that the file destination is the disk0: directory of the current context and the filename. If you do not provide the optional path, the ACE copies the file to the root directory on the disk0: file system.

For example, to copy the ACE-VIRT-020.lic license file from the license directory on the track network server to the root directory on disk0:, enter:

```
host1/Admin# copy tftp://track/license/ACE-VIRT-020.lic disk0:
```

If the license is a demo or permanent license for a new or upgrade installation, see the “Installing a New or Upgrade License File” section.

If the license is a permanent license replacing a demo license, see the “Replacing a Demo License with a Permanent License” section.
Installing a New or Upgrade License File

After you copy a demo or permanent license file to the ACE for a new or upgrade installation, you can install the license. All license installations except two have no adverse impact to an operating ACE as follows:

- A reboot is required when you upgrade the bandwidth license from 8 Gbps to 16 Gbps in an ACE10 module.
- In a redundant configuration, mismatched context licenses between the active and the standby ACEs cause the active ACE to generate a syslog message (if logging is enabled) and to disable configuration synchronization. After you install the correct matching license on the standby ACE, the software automatically detects the new license and restores normal operation.

After you install the correct matching license on the standby ACE, the software automatically detects the license and restores normal operation. For information on replacing a demo license with a permanent one, see the “Replacing a Demo License with a Permanent License” section.

Caution

If you install a context demo license, make sure that you save the Admin running configuration and all user context running configurations to a remote server. If you allow a context license to expire, the ACE automatically removes all user contexts from the Admin running configuration and all configurations for the user contexts.

To install or upgrade a license on your ACE, use the `license install disk0:` command in Exec mode from the Admin context. The syntax of this command is as follows:

```
license install disk0:[path]/filename [target_filename]
```

The arguments are as follows:

- `[path]/filename`—License stored on the disk0: file system. If you do not specify the optional path, the ACE looks for the file in the root directory.
- `target_filename`—(Optional) Target filename for the license file.

For example, to upgrade the module bandwidth license from 4 Gbps to 8 Gbps, enter:

```
host1/Admin# license install disk0:ACE-UPG1-LIC.lic
```
To install a license file for an SSL 5000 TPS license, enter:

```bash
host1/Admin# license install disk0:ACE-SSL-05K-K9.lic
```
To install a license file for a 20 context license, enter:

```
host1/Admin# license install disk0:ACE-VIRT-020.lic
```

There are multiple virtual context licenses including upgrade licenses. The number of contexts currently installed on the ACE determines which additional license you can install, as shown in Table 3-2.

### Table 3-2 Allowable Virtual User Context Installation

<table>
<thead>
<tr>
<th>Current Number of Contexts</th>
<th>Allowable License Installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 (default)</td>
<td>ACE-VIRT-020</td>
</tr>
<tr>
<td></td>
<td>ACE-VIRT-050</td>
</tr>
<tr>
<td></td>
<td>ACE-VIRT-100</td>
</tr>
<tr>
<td></td>
<td>ACE-VIRT-250</td>
</tr>
<tr>
<td>20</td>
<td>ACE-VIRT-UP1 (to upgrade to 50 contexts)</td>
</tr>
<tr>
<td>50</td>
<td>ACE-VIRT-UP2 (to upgrade to 100 contexts)</td>
</tr>
<tr>
<td>100</td>
<td>ACE-VIRT-UP3 (to upgrade to 250 contexts)</td>
</tr>
<tr>
<td>250</td>
<td>No additional licenses</td>
</tr>
</tbody>
</table>

**Replacing a Demo License with a Permanent License**

If you installed an ACE demo license, four weeks before the license expires, the ACE generates warning syslog messages once a day. During the final week, a warning syslog message occurs once an hour. Before this period ends, you must update the demo license with a permanent license. Otherwise, the ACE will revert to its previous bandwidth, SSL TPS, or number of contexts.

**Caution**

If you replace the context demo license with a permanent license, you can continue to use the configured user contexts on the ACE. However, if you allow a context license to expire, the ACE automatically removes all user contexts from


the Admin running configuration and all configurations for the user contexts. Before a context license expires, save the Admin running configuration and the user context running configurations to a remote server.

To view the expiration of the demo license, use the `show license usage` command in Exec mode from the Admin context.

After you copy the permanent license file to the ACE, you can install it. To replace a demo license with a permanent license, use the `license update disk0:` command in Exec mode from the Admin context. The syntax of this command is as follows:

```
license update disk0:[path/]permanent_filename demo_filename
```

The arguments are as follows:
- `[path/]permanent_filename`—Filename for the permanent license file that you copied onto the ACE.
- `demo_filename`—Filename for the demo license file that the permanent license file is replacing.

For example, enter:

```
host1/Admin# license update disk0:ACE-VIRT-250.lic
ACE-VIRT-250-DEMO.lic
```

### Removing a License

To remove a module bandwidth, SSL TPS, or user context license, use the `license uninstall` command in Exec mode from the Admin context. The syntax of this command is as follows:

```
license uninstall license_filename
```

The `license_filename` argument specifies the filename of the license file that you want to remove. Enter the license filename as an unquoted text string with no spaces.
Chapter 3  Managing ACE Software Licenses

Removing a License

Note
When you enter the `clear startup-config` or the `write erase` command, the ACE does not remove license files from the startup-configuration file. You must use the `license uninstall` command to remove license files from the ACE.

This section contains the following topics:

- Removing a Module Bandwidth License
- Removing an SSL TPS License
- Removing a User Context License

Caution
When you remove a demo or permanent virtual context license, the ACE removes all user contexts from the Admin running configuration. By removing the user contexts, their running and startup configurations are also removed from the ACE. Before removing any virtual context license, save the Admin running configuration and the user context running configurations to a remote server. For more information, see the “Removing a User Context License” section.

Removing a Module Bandwidth License

To remove a bandwidth license, use the `license uninstall` command in Exec mode from the Admin context. When you uninstall an ACE-08G-LIC or ACE-UPG1-LIC bandwidth license, it reduces the module bandwidth to the default of 4 Gbps on the ACE. When you install an ACE-UPG2-LIC bandwidth license, it reduces the module bandwidth to 8 Gbps on the ACE.

For example, to remove an ACE-08G-LIC bandwidth license, enter:

```
host1/Admin# license uninstall ACE-08G-LIC.lic
```

Removing an SSL TPS License

To remove an SSL TPS license, use the `license uninstall` command in Exec mode from the Admin context. When you uninstall an SSL license, it reduces SSL TPS performance to 1000 TPS on the ACE.

For example, to remove an ACE-SSL-05K-K9 SSL TPS license, enter:
Removing a License

3-10

host1/Admin# license uninstall ACE-SSL-05K-K9.lic

Removing a User Context License

The number of virtual contexts and type of licenses currently installed on the ACE determines which license you can remove. Table 3-3 lists the currently installed contexts, the type of license on the ACE, and the remaining number of context after the license is removed.

Table 3-3 Virtual Context License Removal

<table>
<thead>
<tr>
<th>Current Number of Contexts</th>
<th>Applicable Licenses</th>
<th>Results of License Removal</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 (default)</td>
<td>Not applicable</td>
<td>—</td>
</tr>
<tr>
<td>20</td>
<td>ACE-VIRT-020</td>
<td>5 contexts</td>
</tr>
<tr>
<td>50</td>
<td>ACE-VIRT-050</td>
<td>5 contexts</td>
</tr>
<tr>
<td></td>
<td>ACE-VIRT-UP1</td>
<td>20 contexts</td>
</tr>
<tr>
<td>100</td>
<td>ACE-VIRT-100</td>
<td>5 contexts</td>
</tr>
<tr>
<td></td>
<td>ACE-VIRT-UP2</td>
<td>50 contexts</td>
</tr>
<tr>
<td></td>
<td>ACE-VIRT-250</td>
<td>5 contexts</td>
</tr>
<tr>
<td></td>
<td>ACE-VIRT-UP3</td>
<td>100 contexts</td>
</tr>
</tbody>
</table>

Caution

When you remove a demo or permanent virtual context license, the ACE removes all user contexts from the Admin running configuration. By removing the user contexts, their running and startup configurations are also removed from the ACE. Before removing any virtual context license, save the Admin running configuration and the user context running configurations to a remote server.

To remove a context license, perform the following steps:

Step 1
Save the Admin and user context running configurations to a remote server by entering the `copy running-config` command in Exec mode in each context. For more information on this command, see Chapter 4, Managing the ACE Software.
For example, to copy the Admin running configuration to an TFTP server as R-CONFIG-ADM, enter:

```
host1/Admin# copy running-config tftp://192.168.1.2/R-CONFIG-ADM
```

To copy the C1 user context running configuration to an TFTP server, access the C1 context and enter:

```
host1/C1# copy running-config tftp://192.168.1.2/R-CONFIG-C1
```

**Step 2**

Remove the license with the `license uninstall` command. For example, to remove the ACE-VIRT-250.LIC license, enter:

```
host1/Admin# license uninstall ACE-VIRT-250.lic
```

The ACE displays the following messages and prompt:

```
Clearing license ACE-VIRT-250.lic:
SERVER this_host ANY
VENDOR cisco
INCREMENT ACE-VIRT-250 cisco 1.0 permanent 1 \
  VENDOR_STRING=<count>1</count> HOSTID=ANY \
NOTICE="<LicFileID>200511031515824</LicFileID><LicLineID>1</LicLineID> \
  <PAK></PAK>" SIGN=86A13B1EA2F2
_INCREMENT ACE-VIRT-250 cisco 1.0 permanent 1 \
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!! WARNING: Uninstalling virtual context license will automatically!!
!!! cleanup all the user context configurations, please backup the 
!!! configurations before proceeding further with uninstallation  !!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Do you want to continue? (y/n)
```

**Step 3**

If you have not saved the running configurations for the Admin and user contexts to a remote server, enter `n`. Go to Step 1

If you saved the running configurations for the Admin and user contexts to a remote server, enter `y`.

During the license removal, the ACE removes the user context configurations from the Admin running configuration, causing the deletion of all user contexts including their running and startup configurations.

**Step 4**

Display the current number of supported contexts on the ACE by entering the `show license status` command in Exec mode of the Admin context.
Removing a License

Step 5  Determine which contexts you want to keep in the Admin running configuration. Using a text editor, manually remove the extra context configurations from the Admin running configuration on the remote server.

If the Admin running configuration contains more contexts than what the ACE supports and you copy this configuration to the ACE, the ACE rejects contexts that exceed the supported limit. For example, if the running configuration contains 20 contexts, when you remove the license, the ACE supports five contexts. If you attempt to copy the configuration with all 20 contexts, the ACE allows the first five contexts, fails the remaining contexts, and displays error messages on the console.

Note  You can also manually recreate the user contexts in the running configuration that is currently on the ACE. If you do, go to Step 7.

Step 6  Retrieve the modified Admin running configuration from the remote server. For example, to copy the R-CONFIG-ADM Admin running configuration from the TFTP server, enter:

```
host1/Admin# copy tftp://192.168.1.2/R-CONFIG-ADM running-config
```

Step 7  Copy the Admin running configuration to the startup-configuration file. For example, enter:

```
host1/Admin# copy running-config startup-config
```

Note  If you do not update the startup configuration with the latest running configuration, when the ACE restarts, it uses the startup configuration with the extra contexts. The ACE allows the number of contexts that the license supports, but fails the remaining contexts.

Step 8  Access the user context, and copy its running configurations from the remote server. For example, to copy the C1 user context running configuration from the TFTP server, access the C1 context and enter:

```
host1/C1# tftp://192.168.1.2/R-CONFIG-C1 copy running-config
```

Step 9  Copy the user context running configuration to the startup-configuration file. For example, enter:

```
host1/Admin# copy running-config startup-config
```
Chapter 3      Managing ACE Software Licenses

Step 10  Repeat Steps 8 and 9 until you retrieve the running configurations for all user contexts configured in the Admin configuration.

Back Up a License File

To protect your license files, we recommend that you back up your license files to the ACE Flash disk as tar files. To back up license files in .tar format, use the copy licenses command in Exec mode from the Admin context. The syntax of this command is as follows:

```
copy licenses disk0:[path/]
```

The keyword and argument are as follows:

- **disk0:**—Specifies that the backup license file is copied to the disk0: file system.
- **[path/]filename.tar**—Destination filename for the backup licenses. The destination filename must have a .tar file extension.

For example, enter:

```
host1/Admin# copy licenses disk0:mylicenses.tar
```

If you accidently remove or lose the license on the ACE, you can untar the backup file and reinstall it. To untar the license, use the untar command in Exec mode. The syntax of this command is as follows:

```
untar disk0:[path/]
```

The [path/]filename.tar argument is the filename of the .tar backup license file. For example, to untar the mylicense.tar file on disk0:, enter:

```
host1/Admin# untar disk0:mylicenses.tar
```

For information on installing the license, see the “Installing a New or Upgrade License File” section.
Displaying License Configurations and Statistics

This section describes the `show` commands that you can use to display license information about your ACE. To display license information, use the `show license` command in Exec mode from the Admin context. The syntax of this command is:

```
show license brief | file filename | internal event-history | status | usage
```

The options and arguments for this command are as follows:

- `brief`—Displays a list of the currently installed licenses
- `file filename`—Displays the file contents of the specified license
- `internal event-history`—Displays a history of licensing-related events
- `status`—Displays the status of licensed features
- `usage`—Displays the usage table for all licenses

**Note**

Entering the `show license` command without any options and arguments displays all installed ACE license files and their contents.

Table 3-4 describes the fields in the `show license status` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licensed Feature</td>
<td>List including the ACE virtualized contexts, the SSL transactions per second, and the module bandwidth feature.</td>
</tr>
<tr>
<td>Count</td>
<td>Number of ACE-supported contexts, SSL transactions per second (TPS), and bandwidth in gigabits per second (Gbps). This information also provides the default number of contexts, SSL TPS, and module bandwidth that the ACE supports when a license is not installed.</td>
</tr>
</tbody>
</table>
Table 3-5 describes the fields in the show license usage command output.

Table 3-5  Field Descriptions for the show license usage Command Output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>License</td>
<td>Name of the license.</td>
</tr>
<tr>
<td>Ins</td>
<td>Whether the license is installed (Yes or No).</td>
</tr>
<tr>
<td>Lic Count</td>
<td>Number of licenses for this feature.</td>
</tr>
<tr>
<td>Status</td>
<td>Current state of the feature (In use or Unused).</td>
</tr>
<tr>
<td>Expiry Date</td>
<td>Date when the demo license expires, as defined in the license file. If the license is permanent, this field displays Never.</td>
</tr>
<tr>
<td>Comments</td>
<td>Licensing errors, if any.</td>
</tr>
</tbody>
</table>

You can also view the ACE license by entering the following commands:

- The show version command in Exec mode on the ACE.
- The show module services command on the supervisor engine. See the license information under the Services field.
CHAPTER 4

Managing the ACE Software

This chapter describes how to manage the software running on the Cisco Application Control Engine (ACE) module and contains the following major sections:

- Saving Configuration Files
- Loading Configuration Files from a Remote Server
- Using the File System on the ACE
- Viewing and Copying Core Dumps
- Capturing and Copying Packet Information
- Using the Configuration Checkpoint and Rollback Service
- Reformatting the Flash Memory

Saving Configuration Files

Upon startup, the ACE loads the startup-configuration file stored in Flash memory (nonvolatile memory) to the running-configuration file stored in RAM (volatile memory). When you partition your ACE into multiple contexts, each context contains its own startup-configuration file.

Flash memory stores the startup-configuration files for each existing context. When you create a new context, the ACE creates a new context directory in Flash memory to store the context-specific startup-configuration files. When you copy a configuration file from the ACE, you create a copy of the configuration information of the context from where you executed the command.
To display the contents of the startup-configuration file associated with the current context, use the `show startup-config` command in Exec mode (see the “Viewing Configuration Files” section).

When you make configuration changes, the ACE places those changes in a virtual running-configuration file called the running-config, which is associated with the context that you are working in. When you enter a CLI command, the change is made only to the running-configuration file in volatile memory. Before you log out or reboot the ACE, copy the contents of the running-configuration file to the startup-configuration file (startup-config) to save configuration changes for the current context to Flash memory. The ACE uses the startup-configuration file on subsequent reboots.

This section contains the following topics:

- Saving the Configuration File in Flash Memory
- Saving Configuration Files to a Remote Server
- Copying the Configuration File to the disk0: File System
- Merging the Startup-Configuration File with the Running-Configuration File
- Viewing Configuration Files
- Viewing User Context Running-Config Files from the Admin Context
- Clearing the Startup-Configuration File

### Saving the Configuration File in Flash Memory

After you create or update the running-configuration file in RAM (volatile memory), save the contents to the startup-configuration file for the current context in Flash memory (nonvolatile memory) on the ACE. To copy the contents of the running-configuration file to the startup-configuration file, use the `copy running-config startup-config` command from Exec mode.

The syntax for the command is as follows:

```
copy running-config startup-config
```

For example, to save the running-configuration file to the startup-configuration file in Flash memory on the ACE, enter:

```
host1/Admin# copy running-config startup-config
```
You can also use the write memory command to copy the contents of the running-configuration file for the current context to the startup-configuration file. The write memory command is equivalent to the copy running-config startup-config command.

The syntax for the command is as follows:

```
write memory [all]
```

The optional write memory all keyword saves configurations for all existing contexts. This keyword is available only in the Admin context.

If you intend to use the write memory command to save the contents of the running-configuration file for the current context to the startup-configuration file, be sure to also specify this command in the Admin context. You should save changes to the Admin context startup-configuration file; the Admin context startup-configuration file contains all configurations that are used to create each user context.

### Saving Configuration Files to a Remote Server

To save the running-configuration file or startup-configuration file to a remote server using File Transfer Protocol (FTP), Secure File Transfer Protocol (SFTP), or Trivial Transfer Protocol (TFTP), use the copy running-config or copy startup-config command in Exec mode. The copy serves as a backup file for the running-configuration file or startup-configuration file for the current context.

Before installing or migrating to a new software version, back up the ACE startup-configuration file to a remote server using FTP, SFTP, or TFTP. When you name the backup file, we recommend that you name it in such a way that you can easily tell the context source of the file (for example, running-config-ctx1, startup-config-ctx1).

The syntax for the command is as follows:

```
copy {running-config | startup-config} {ftp://server/path/[filename] | sftp://[username@]server/path/[filename] | tftp://server[:port]/path/[filename]}
```
The keywords, arguments, and options are as follows:

- **running-config**—Specifies the running-configuration file currently residing on the ACE in volatile memory.
- **startup-config**—Specifies the startup-configuration file currently residing on the ACE in Flash memory.
- **ftp://server/path[/filename]**—Specifies the FTP network server and, optionally, the renamed configuration file.
- **sftp://username@server/path[/filename]**—Specifies the SFTP network server and, optionally, the renamed configuration file.
- **tftp://server:[port]/path[/filename]**—Specifies the TFTP network server and, optionally, the renamed configuration file.

When you select a destination file system using `ftp:`, `sftp:`, or `tftp:`, the ACE performs the following tasks:

- Prompts you for your username and password if the destination file system requires user authentication.
- Prompts you for the server information if you do not provide the information with the command.
- Copies the file to the root directory of the destination file system if you do not provide the path information.

For example, to save a startup-configuration file to a remote FTP server, enter:

```
host1/Admin# copy running-config ftp://192.168.1.2/running-config_Adminctx
Enter username[]? user1
Enter the file transfer mode[bin/ascii]: [bin]
Password: password1
Passive mode on.
Hash mark printing on (1024 bytes/hash mark).
####
```

**Note**
The **bin** (binary) file transfer mode is intended for transferring compiled files (executables). The **ascii** file transfer mode is intended for transferring text files, such as config files. The default selection of **bin** should be sufficient in all cases when copying files to a remote FTP server.
Saving Configuration Files

Copying the Configuration File to the disk0: File System

After you create or update the running-configuration file or the startup-configuration file, you can copy the file to the disk0: file system in Flash memory on the ACE by using the following commands:

- To save the contents of the running-configuration file to the disk0: file system, use the `copy running-config disk0:` command in Exec mode.
- To save the contents of the startup-configuration file to the disk0: file system, use the `copy startup-config disk0:` command in Exec mode.

The syntax for the command is as follows:

```
copy {running-config | startup-config} disk0:[path[/]filename
```

The keywords, arguments, and options are as follows:

- `running-config`—Specifies the running-configuration file currently residing on the ACE in RAM (volatile memory).
- `startup-config`—Specifies the startup-configuration file currently residing on the ACE in Flash memory (nonvolatile memory).
- `disk0:`—Specifies that the running-configuration file or startup-configuration file is copied to the disk0: file system.
- `[path[/]filename`—(Optional) The path in the disk0: file system. If you do not provide the optional path, the ACE copies the file to the root directory on the disk0: file system.

For example, to save the running-configuration file to the disk0: file system as running-config_copy, enter:

```
host1/Admin# copy running-config disk0:running-config_copy
```
Merging the Startup-Configuration File with the Running-Configuration File

To merge the contents of the startup-configuration file into the running-configuration file, use the `copy startup-config running-config` command in Exec mode. This command copies any additional configurations from the startup-configuration file into the running-configuration file. If any common commands exist in both files, the startup-configuration file overwrites the attributes in the running-configuration file.

The syntax for the command is as follows:

```
   copy startup-config running-config
```

For example, enter:

```
host1/Admin# copy startup-config running-config
```

Viewing Configuration Files

To display the ACE running-configuration file associated with the current context, use the `show running-config` command in Exec mode. Configuration entries within each mode in the running-configuration file appear in chronological order, based on the order in which you configure the ACE. The ACE does not display default configurations in the ACE running-configuration file.

The `write terminal` command can also be used to display the ACE running-configuration file. The `write terminal` command is equivalent to the `copy running-config` command.

To view the content of the running- and startup-configuration files, use the following commands:

- To view the running-configuration file, use the `show running-config` command.
- To view the startup-configuration file, use the `show startup-config` command.
Saving Configuration Files

The syntax for the `show startup-config` command is as follows:

```
show startup-config
```

The syntax for the `show running-config` command is as follows:

```
show running-config [aaa | access-list | action-list | class-map | context | dhcp | domain | ft | interface | object-group | parameter-map | policy-map | probe | resource-class | role | rsrv | serverfarm | sticky]
```

The keywords and options are as follows:

- `aaa`—(Optional) Displays AAA information.
- `access-list`—(Optional) Displays access control list (ACL) information.
- `action-list`—(Optional) Displays action-list information. You use action lists to group together certain Layer 7 policy-map actions.
- `class-map`—(Optional) Displays the list of all class maps configured for the current context. The ACE also displays configuration information for each class map listed.
- `context`—(Optional) Displays the list of contexts configured on the ACE. The ACE also displays the resource class (member) assigned to each context. The `context` keyword works only from within the Admin context.
- `dhcp`—(Optional) Displays Dynamic Host Configuration Protocol (DHCP) information.
- `domain`—(Optional) Displays the list of domains configured for the current context. The ACE also displays configuration information for each domain listed.
- `ft`—(Optional) Displays the list of redundancy or fault-tolerance (FT) configurations configured for the current context. The ACE also displays configuration information for each ft configuration listed.
- `interface`—(Optional) Displays interface information.
- `object-group`—(Optional) Displays ACL object-group information.
- `parameter-map`—(Optional) Displays parameter map information.
- `policy-map`—(Optional) Displays policy map information.
- `probe`—(Optional) Displays probe information.
• **resource-class**—(Optional) Displays resource class information.
• **role**—(Optional) Displays the list of roles configured for the current context.
  The ACE also displays configuration information for each role on the list.
• **rserver**—(Optional) Displays real server information.
• **serverfarm**—(Optional) Displays serverfarm information.
• **sticky**—(Optional) Displays sticky information.

For details on the `show running-config` output associated with the optional
keywords, see the chapters in the ACE documentation set related to the specific
software functions.

For example, to view the entire contents of the running-configuration file on the
ACE, enter:

```
host1/Admin# show running-config
Generating configuration....

logging enable

access-list acl1 line 10 extended permit ip any any

rserver type host real1
  address 16.1.1.102
  inservice
rserver type host real2
  address 16.1.1.103
  inservice
rserver type host real3
  address 16.1.1.105
  inservice

serverfarm type host serverfarm1
  predictor hash address
  real real1
    inservice
  real real2
    inservice
  real real3
    inservice

class-map match-any vipsmap1
  10 match virtual-address 17.1.2.1 tcp any

policy-map type loadbalance first-match policymap1
  class class-default
    serverfarm serverfarm1
```
Chapter 4  Managing the ACE Software

Saving Configuration Files

policy-map multi-match policy1
  class vipmap1
    loadbalance vip inservice
    loadbalance policymap1

interface vlan 16
  ip address 16.1.1.12 255.0.0.0
  access-group input acl1
  no shutdown
interface vlan 17
  ip address 17.1.1.12 255.0.0.0
  access-group input acl1
  service-policy input policy1
  no shutdown

context Admin
  member default

username admin password 5 $1$faXJEFBj$TUR1Lx7sLPTi5BZ97v08c/ role Admin domain default-domain
username www password 5 $1$UZIiw0k7$QMvYN1JASaycabrHkhGcs/ role Admin domain de fault-domain

snmp-server user www Network-Monitor
snmp-server user admin Network-Monitor

Viewing User Context Running-Config Files from the Admin Context

To display the ACE running-configuration file of a user context from the Admin context, use the invoke context command in Exec mode. The syntax of this command is as follows:

    invoke context context_name show running-config

The context_name argument is the name of the user context.

For example, to view the running-configuration file of the C1 context from the Admin context, enter:

    host1/AdmIn# invoke context C1 show running-config
    Generating configuration....
Clearing the Startup-Configuration File

To clear the contents of the ACE startup-configuration file of the current context in Flash memory, use either the `clear startup-config` or `write erase` command in Exec mode. Both commands reset the startup-configuration file to the default settings and take effect immediately. The running-configuration file is not affected. In addition, the `clear startup-config` or `write erase` commands do not clear the boot variables, such as config-register and boot system settings.

The `clear startup-config` and the `write erase` commands do not remove license files or crypto files from the ACE startup-configuration file. To remove license files, use the `license uninstall filename` command. To remove crypto files, use the `crypto delete filename` or the `crypto delete all` command.

Before you clear the contents of the ACE startup-configuration file, back up your startup-configuration file to a remote server (see the “Saving Configuration Files to a Remote Server” section). Once you clear the startup-configuration file, you can perform one of the following processes to recover a copy of an existing configuration:

- Copy the contents of the existing running-configuration file to the startup-configuration file by using the `copy running-config startup-config` command. See the “Saving the Configuration File in Flash Memory” section.
- Upload a backup of a previously saved startup-configuration file from a remote server. See the “Loading Configuration Files from a Remote Server” section.

For example, to reset the ACE startup-configuration file, enter:

```
host1/Admin# clear startup-config
```
Loading Configuration Files from a Remote Server

You can configure the ACE by loading configuration files previously backed up to a remote FTP, SFTP, or TFTP server. Before you begin loading a configuration file from a remote server, ensure the following:

- You know the location of the configuration file to be loaded from the remote server.
- The configuration file permissions are set to world-read.
- The ACE has a route to the remote server. The ACE and the remote server must be in the same subnetwork if you do not have a router or default gateway to route the traffic between subnets. To check connectivity to the remote server, use the `ping` or `traceroute` command in Exec mode. See the *Cisco Application Control Engine Module Routing and Bridging Configuration Guide* for details on how to use the `ping` and `traceroute` commands.

When you copy the backup configuration file to the ACE, you copy the configuration information to the context from where you initially executed the `copy` command. When you copy a configuration file to the ACE, ensure that the configuration file is appropriate for use in the current context. For example, you would copy the backup configuration file `startup-config-ctx1` to context 1.

To configure the ACE using a running-configuration file or startup-configuration file downloaded from a remote server, use the `copy` command in Exec mode.

The syntax for the command is as follows:

```
copy {ftp://server/path[/filename] | sftp://[username@]server/path[/filename] | tftp://server[:port]/path[/filename]} {running-config | startup-config}
```

The keywords, arguments, and options are as follows:

- `ftp://server/path[/filename]`—Specifies the FTP network server and, optionally, the configuration filename.
- `sftp://[username@]server/path[/filename]`—Specifies the SFTP network server and, optionally, the configuration filename.
- `tftp://server[:port]/path[/filename]`—Specifies the TFTP network server and, optionally, the configuration filename.
running-config—Specifies to replace the running-configuration file currently residing on the ACE in RAM (volatile memory).

startup-config—Specifies to replace the startup-configuration file currently residing on the ACE in Flash memory (nonvolatile memory).

For example, to copy a startup-configuration file from a remote FTP server to the ACE, enter:

```
Host/Admin# copy ftp://192.168.1.2/configs/startup-config-Adm_ctx startup-config
```

**Using the File System on the ACE**

Flash memory stores the operating system, startup-configuration files, software licenses, core dump files, system message log files, SSL certificates and keys, probe scripts, and other data on the ACE. Flash memory comprises a number of individual file systems, or partitions, that include this data.

The ACE contains the following file systems, or partitions:

- **disk0:**—Contains all startup-configuration files, software licenses, system message log files, SSL certificates and keys, and user-generated data for all existing contexts on the ACE.
- **image:**—Contains the system software images.
- **core:**—Contains the core files generated after each time that the ACE becomes unresponsive.
- **probe:**—Displays the contents of the probe: file system. This directory contains the Cisco-supplied scripts. For more information about these scripts, see the *Cisco Application Control Engine Module Server Load-Balancing Configuration Guide*. Both the Admin context and user contexts support the probe: directory.
- **volatile:**—Contains the files residing in the temporary (volatile:) directory. The volatile: directory provides temporary storage; files in temporary storage are erased when the ACE reboots.

The Admin context supports all five file systems in the ACE. The user context supports only the disk0:, probe:, and volatile: file systems.

When you create a new context, the ACE creates a new context directory in Flash memory to store context-specific data such as startup-configuration files.
The ACE provides a number of useful commands to help you manage software configuration and image and files. This section contains the following topics that will help you to manage files on the ACE:

- Listing the Files in a Directory
- Copying Files
- Uncompressing Files in the disk0: File System
- Untarring Files in the disk0: File System
- Creating a New Directory
- Deleting an Existing Directory
- Moving Files
- Deleting Files
- Displaying File Contents
- Saving show Command Output to a File

### Listing the Files in a Directory

To display the directory contents of a specified file system, use the `dir` command in Exec mode. This command displays a detailed list of directories and files contained within the specified file system on the ACE, including names, sizes, and time created. You may optionally specify the name of a directory to list.

The syntax of this command is as follows:

```
```

The keywords and arguments are as follows:

- **core:**—Displays the contents of the core: file system.
- **disk0:**—Displays the contents of the disk0: file system.
- **image:**—Displays the contents of the image: file system.
- **probe:**—Displays the contents of the probe: file system. This directory contains the Cisco-supplied scripts. For more information about these scripts, see the *Cisco Application Control Engine Module Server Load-Balancing Configuration Guide*. 
volatile:—Displays the contents of the volatile: file system.

directory/—(Optional) Contents of the specified directory.

filename—(Optional) Information that relates to the specified file, such as the file size and the date it was created. You can use wildcards in the filename. A wildcard character (*) matches all patterns. Strings after a wildcard are ignored.

For example, to list the files in the disk0: file system, enter:

```plaintext
host1/Admin# dir disk0:
host/Admin# dir disk0:
```

```
7465  Jan 03 00:13:22 2000  C2_dsb
2218  Mar 07 18:38:03 2006  ECHO_PROBE_SCRIPT4
1654692 Feb 27 21:42:07 2006  c6ace-tik9_dplug-mzg.3.0.0_A0_2.44.bin
1024  Feb 16 12:47:24 2006  core_copies_dsb/
1024  Jan 01 00:02:07 2000  cv/
1024  Mar 13 13:53:08 2006  dsb_dir/
12  Jan 30 17:54:26 2006  messages
7843  Mar 09 22:19:56 2006  running-config
4320  Jan 05 14:37:52 2000  startup-config
1024  Jan 01 00:02:28 2000  www/
```

Usage for disk0: filesystem

```
4254720 bytes total used
6909952 bytes free
11164672 total bytes
```

For example, to list the core dump files in Flash memory, enter:

```plaintext
host1/Admin# dir core:
```

```
253151  Mar 14 21:23:33 2006  0x401_vsh_log.8249.tar.gz
262711  Mar 15 21:22:18 2006  0x401_vsh_log.15592.tar.gz
250037  Mar 15 18:35:27 2006  0x401_vsh_log.16296.tar.gz
```

Usage for core: filesystem

```
1847296 bytes total used
64142336 bytes free
65989632 total bytes
```
Copying Files

This section contains the following topics:

- Copying Files to Another Directory on the ACE
- Copying Licenses
- Copying a Packet Capture Buffer
- Copying Files to a Remote Server
- Copying Files from a Remote Server
- Copying an ACE Software System Image to a Remote Server

Copying Files to Another Directory on the ACE

To copy a file from one directory in the disk0: file system of Flash memory to another directory in disk0:, use the `copy disk0:` command.

**Note**

To view the content of the running- and startup-configuration files, use the `dir disk0:` command.

The syntax of this command is as follows:

```
copy disk0: [path/]filename1 {disk0:[path/]filename2}
```

The keywords and arguments are as follows:

- `[path/]filename1` — Name of the file to copy. Use the `dir disk0:` command to view the files available in the disk0: file system. If you do not provide the optional path, the ACE copies the file from the root directory on the disk0: file system.

- `disk0:[path/]filename2` — Specifies the file destination in the disk0: directory of the current context. If you do not provide the optional path, the ACE copies the file to the root directory on the disk0: file system.

For example, to copy the file called SAMPLEFILE to the MYSTORAGE directory in the disk0: file system, enter:

```
host1/Admin# copy disk0:samplefile disk0:MYSTORAGE/SAMPLEFILE
```
Copying Licenses

To protect your license files, we recommend that you back up your license files to the ACE Flash memory as tar files. To create a backup license for the ACE licenses in .tar format and copy it to the disk0: file system, use the `copy licenses` command in Exec mode.

The syntax of this command is as follows:

```
copy licenses disk0: [path] filename.tar
```

The keyword and argument are as follows:

- `disk0:`—Specifies that the backup license file is copied to the disk0: file system.
- `[path/]filename.tar`—Destination filename for the backup licenses. The destination filename must have a .tar file extension. If you do not provide the optional path, the ACE copies the file to the root directory on the disk0: file system.

For example, enter:

```
host1/Admin# copy licenses disk0:mylicenses.tar
```

If you accidently remove or lose the license on the ACE, you can untar the backup file and reinstall it. To untar the backup license, use the `untar` command in Exec mode. The syntax of this command is as follows:

```
untar disk0: [path] filename.tar
```

The `filename.tar` is the filename of the .tar backup license file.

For example, to untar the mylicense.tar file on disk0, enter:

```
host1/Admin# untar disk0:mylicenses.tar
```

Copying a Packet Capture Buffer

To copy an existing packet capture buffer to the disk0: file system, use the `copy capture` command in Exec mode.

The syntax for the command is as follows:

```
copy capture capture_name disk0: [path] destination_name
```
Chapter 4      Managing the ACE Software

Using the File System on the ACE

The keywords, arguments, and options are as follows:

- **capture_name**—Name of the packet capture buffer on Flash memory. Specify a text string from 1 to 64 alphanumeric characters. If necessary, use the `show capture` command to view the files available in the disk0: file system. This list includes the name of existing packet capture buffers.

- **disk0:**—Specifies that the buffer is copied to the disk0: file system.

- **[path]destination_name**—Destination path (optional) and name for the packet capture buffer. Specify a text string from 1 to 80 alphanumeric characters. If you do not provide the optional path, the ACE copies the file to the root directory on the disk0: file system.

For example, to copy a packet capture buffer to the disk0: file system, enter:

```
host1/Admin# copy capture packet_capture_Jan_17_07
disk0:capture_Jan_17_07
```

**Copying Files to a Remote Server**

To copy a file from Flash memory on the ACE to a remote server using FTP, SFTP, or TFTP, use the `copy` command in Exec mode. The copy serves as a backup file for such files as the capture buffer file, core dump, ACE licenses in .tar format, running-configuration file, or startup-configuration file.

The syntax for the command is as follows:

```
```

The keywords, arguments, and options are as follows:

- **core:filename**—Specifies a core dump residing on the ACE in Flash memory (see the “Viewing and Copying Core Dumps” section). The `copy core:` command is available only in the Admin context. Use the `dir core:` command to view the core dump files available in the core: file system. Copy the complete filename (for example, 0x401_vsh_log.25256.tar.gz) by using the `copy core:` command.
- **disk0:[path]/filename**—Specifies a file in the disk0: file system of Flash memory (for example, a packet capture buffer file, ACE licenses in .tar format, or a system message log). Use the `dir disk0:` command to view the files available in the disk0: file system.

- **running-config**—Specifies the running-configuration file residing on the ACE in volatile memory.

- **startup-config**—Specifies the startup-configuration file currently residing on the ACE in Flash memory.

- **ftp://server/path/[filename]**—Specifies the FTP network server and, optionally, the renamed file.

- **sftp://username@server/path/[filename]**—Specifies the SFTP network server and, optionally, the renamed file.

- **tftp://server:[port]/path/[filename]**—Specifies the TFTP network server and, optionally, the renamed file.

When you select a destination file system using `ftp:`, `sftp:`, or `tftp:`, the ACE performs the following tasks:

- Prompts you for your username and password if the destination file system requires user authentication.

- Prompts you for the server information if you do not provide the information with the command.

- Copies the file to the root directory of the destination file system if you do not provide path information.

For example, to save a running-configuration file to a remote FTP server, enter:

```
host1/Admin# copy running-config ftp://192.168.215.124/running-config_Adminctx
Enter username[]? user1
Enter the file transfer mode[bin/ascii]: [bin]
Password: password1
Passive mode on.
Hash mark printing on (1024 bytes/hash mark).
```
For example, to save a core dump file to a remote FTP server, enter:

```
host1/Admin# copy core:0x401_vsh_log.8249.tar.gz ftp://192.168.1.2
```

### Copying Files from a Remote Server

To copy a file from a remote server to a location on the ACE using FTP, SFTP, or TFTP, use the `copy` command in Exec mode.

The syntax for the command is as follows:

```
copy {ftp://server/path/[filename] | sftp://[username@]server/path/[filename] | tftp://server:[port]/path/[filename]} {disk0:[path]/filename | image:image_name | running-config | startup-config}
```

The keywords, arguments, and options are as follows:

- **ftp://server/path/[filename]**—Specifies the FTP network server and, optionally, the filename.
- **sftp://[username@]server/path/[filename]**—Specifies the SFTP network server and, optionally, the filename.
- **tftp://server:[port]/path/[filename]**—Specifies the TFTP network server and, optionally, the filename.
- **disk0:[path]/filename**—Specifies a file destination in the disk0: file system of Flash memory. If you do not provide the optional path, the ACE copies the file to the root directory on the disk0: file system.
- **image:image_name**—Specifies to copy a system software image to Flash memory. Use the `boot system` command as described in Chapter 1, Setting Up the ACE to specify the BOOT environment variable. The BOOT environment variable specifies a list of image files on various devices from which the ACE can boot at startup.
- **running-config**—Specifies to replace the running-configuration file currently residing on the ACE in RAM (volatile memory).
- **startup-config**—Specifies to replace the startup-configuration file currently residing on the ACE in Flash memory (nonvolatile memory).
For example, to copy a startup-configuration file from a remote FTP server to the disk0: file system, enter:

```
host1/Admin# copy ftp://192.168.1.2/ startup-config
Enter source filename[]? startup_config_Adminctx
File already exists, do you want to overwrite?[y/n]: [y] y
Enter username[]? user1
Enter the file transfer mode[bin/ascii]: [bin]
Password:
Passive mode on.
Hash mark printing on (1024 bytes/hash mark).
```

Note

The **bin** (binary) file transfer mode is intended for transferring compiled files (executables). The **ascii** file transfer mode is intended for transferring text files, such as config files. The default selection of **bin** should be sufficient in all cases when copying files to a remote FTP server.

### Copying an ACE Software System Image to a Remote Server

To copy an ACE software system image from Flash memory to a remote server using FTP, SFTP, or TFTP, use the `copy image:` command in Exec mode. The `copy image:` command is available only in the Admin context.

**Note**

To view the software system images available in Flash memory, use the `dir image:` command and the `show version` command.

The syntax for the command is as follows:

```
```

The keywords, arguments, and options are as follows:

- **filename**—Name of the ACE system software image.
- **ftp://server/path[/filename]**—Specifies the FTP network server and, optionally, the renamed software system image.
- **sftp://[username@]server/path[/filename]**—Specifies the SFTP network server and, optionally, the renamed software system image.
- **tftp://server[:port]/path[/filename]**—Specifies the TFTP network server and, optionally, the renamed software system image.
When you select a destination file system using ftp, sftp, or tftp, the ACE performs the following tasks:

- Prompts you for your username and password if the destination file system requires user authentication.
- Prompts you for the server information if you do not provide the information with the command.
- Copies the file to the root directory of the destination file system if you do not provide path information.

For example, to save a software system image to a remote FTP server, enter:

```
host1/Admin# copy image:sb-ace.NOV_11 ftp://192.168.1.2
```

### Uncompressing Files in the disk0: File System

To uncompress (unzip) LZ77 coded files in the disk0: file system (for example, zipped probe script files), use the `gunzip` command in Exec mode. This command is useful in uncompressing large files. The filename must end with a .gz extension for the file to be uncompresssed using the `gunzip` command. The .gz extension indicates a file zipped by the gzip (GNU zip) compression utility.

The syntax for the command is as follows:

```
gunzip disk0:filename
```

The `filename` argument identifies the name of the compressed file on the disk0: file system. The filename must end with a .gz extension. To display a list of available zipped files on disk0:, use the `dir` command.

For example, to unzip a compressed series of probe script files residing in the disk0: file system, enter:

```
host1/Admin# gunzip disk0:PROBE_SCRIPTS.gz
```

### Untarring Files in the disk0: File System

A .tar file keeps related files together and facilitates the transfer of multiple files. A .tar file is a series of separate files, typically not compressed, added together into a single file by a UNIX TAR program. The resulting file is known as a tarball, which is similar to a ZIP file but without the compression. The files in a .tar file must be extracted before they can be used.
To untar a single file with a .tar extension in the disk0: file system, use the `untar` command in Exec mode. Use this command to untar the sample scripts file. You can also use this command to unzip a back-up licenses if a license becomes corrupted or lost. Before you can use the `untar` command, the filename must end with a .tar extension.

**Note**

The `copy licenses disk0:` command creates backup .tar license files on the ACE. If a license becomes corrupted or lost, or you accidently remove the license on the ACE, you can untar the license and reinstall it. See the “Copying Licenses” section.

The syntax for the command is as follows:

```
untar disk0:[path]/filename
```

The `filename` argument identifies the name of the .tar file in the disk0: file system. The filename must end with a .tar extension. You can optionally provide a path to the .tar file if it exists in another directory in the disk0: file system.

For example, to untar a series of license files in the mylicense.tar file in the disk0: file system, enter:

```
host1/Admin# untar disk0:mylicenses.tar
```

### Creating a New Directory

To create a directory in the disk0: file system of Flash memory, use the `mkdir disk0:` command in Exec mode. The syntax of this command is as follows:

```
mkdir disk0:[path]/directory
```

The `directory` argument provides the name of the directory to create in disk0:. If a directory with the same name already exists, the ACE does not create the new directory and the “Directory already exists” message appears.

For example, to create a directory called TEST_DIRECTORY in the disk0: file system, enter:

```
host1/Admin# mkdir disk0:TEST_DIRECTORY
```
Deleting an Existing Directory

To remove an existing directory from the disk0: file system of Flash memory, use the `rmdir disk0:` command in Exec mode. The directory must be empty before you can delete it.

**Note**

To remove a file from the ACE file system, use the `delete` command (see the “Deleting Files” section).

The syntax of this command is as follows:

```
   rmdir disk0:[path]/directory
```

The `directory` argument provides the name of the directory to delete from the disk0: file system. The directory must be empty before you can delete it. You can optionally provide a path to a directory in the disk0: file system.

For example, to delete a directory called TEST_DIRECTORY from the disk0: file system, enter:

```
host1/Admin# rmdir disk0:TEST_DIRECTORY
```

Moving Files

To move a file between directories in the disk0: file system, use the `move` command in Exec mode. If a file with the same name already exists in the destination directory, that file is overwritten by the moved file.

**Note**

To view the files available in the disk0: file system, use the `dir disk0:` command.

The syntax of this command is as follows:

```
   move disk0:[source_directory/][filename]
   disk0:[destination_directory/][filename]
```

The keywords and arguments are as follows:

- `source_directory`—(Optional) Name of the source directory in the disk0: file system.
Using the File System on the ACE

Managing the ACE Software

Chapter 4

4-24

Cisco Application Control Engine Module Administration Guide

OL-11865-01

- destination_directory—(Optional) Name of the destination directory in the disk0: file system.
- filename—Name of the file to move in the disk0: file system.

For example, to move the file called SAMPLEFILE to the MYSTORAGE directory in the disk0: file system, enter:

```
host1/Admin# move disk0:SAMPLEFILE disk0:MYSTORAGE/SAMPLEFILE
```

Deleting Files

To delete a file from a specific file system in the ACE, use the delete command in Exec mode. When you delete a file, the ACE erases the file from the specified file system.

```
To remove a directory from the ACE file system, use the rmdir command (see the “Deleting an Existing Directory” section).
```

The syntax of this command is as follows:

```
delete {core:filename | disk0:[directory/]filename | image:filename | volatile:filename}
```

The keywords and arguments are as follows:

- core:filename—Deletes the specified file from the core: file system (see the “Viewing and Copying Core Dumps” section). The delete cores: command is available only in the Admin context.
- disk0:[directory/]filename—Deletes the specified file from the disk0: file system (for example, a packet capture buffer file or system message log). You can optionally provide a path to a file in directory in the disk0: file system.
- image:filename—Deletes the specified file from the image: file system. The delete image: command is available only in the Admin context.
- volatile:filename—Deletes the specified file from the volatile: file system.

For example, to delete a copy of the running-configuration file called MY_RUNNING-CONFIG1 from the MYSTORAGE directory on the disk0: file system, enter:

```
host1/Admin# delete disk0:MYSTORAGE/MY_RUNNING-CONFIG1
```
Displaying File Contents

To display the contents of a specified file in a directory in Flash memory or in nonvolatile memory, use the `show file` command. The syntax of this command is:

```
show file { disk0: [path/]filename | volatile: filename } [cksum | md5sum]
```

The keywords, arguments, and options are as follows:

- `disk0: [path/]filename`—Specifies the name of a file residing in the disk0: file system of Flash memory (for example, a packet capture buffer file or system message log). You can optionally provide a path to a file in a directory in the disk0: file system.

- `volatile: filename`—Specifies the name of a file in the volatile memory file system of the ACE.

- `cksum`—(Optional) Displays the cyclic redundancy check (CRC) checksum for the file. The checksum values compute a CRC for each named file. Use this command to verify that the file is not corrupt. You compare the checksum output for the received file against the checksum output for the original file.

- `md5sum`—(Optional) Displays the MD5 checksum for the file. MD5 is an electronic fingerprint for the file. MD5 is the latest implementation of the internet standards described in RFC 1321 and is useful for data security and integrity.

For example, to display the contents of a file residing in the current directory, enter:

```
host1/Admin# show file disk0:myfile md5sum
3d8e05790155150734eb8639ce98a331
```

Saving show Command Output to a File

You can force all `show` screen output to be directed to a file by appending `>` `filename` to any command. For example, you can enter `show interface > filename` at the Exec mode CLI prompt to redirect the interface configuration command output to a file created at the same directory level.
The syntax for redirecting `show` command output is as follows:

```
show keyword [l | {begin pattern | count | end | exclude pattern | include pattern | last | more}] [> {filename | {disk0: | volatile}:{path/}[filename]}
 | {ftp://server/path/[filename]}
 | sftp://[username@[server]/path/[filename]}
 | tftp://server[:port]/path/[filename]}
```

The arguments, keywords, and options are as follows:

- `l`—(Optional) Enables an output modifier that filters the command output.
- `begin pattern`—Begins with the line that matches the pattern that you specify.
- `count`—Counts the number of lines in the output.
- `end pattern`—Ends with the line that matches the pattern that you specify.
- `exclude pattern`—Excludes the lines that match the pattern that you specify.
- `include pattern`—Includes the lines that match the pattern that you specify.
- `last`—Displays the last few lines of the output.
- `more`—Displays one window page at a time.
- `>`—(Optional) Enables an output modifier that redirects the command output to a file.
- `filename`—Name of the file that the ACE saves the output to on the volatile: file system.
- `disk0:`—Specifies that the destination is the disk0: file system on the ACE Flash memory.
- `volatile:`—Specifies that the destination is the volatile: file system on the ACE.
- `[path/][filename]`—(Optional) Path and filename to the disk0: or volatile: file system.
- `sftp://[username@[server]/path/[filename]`—Specifies the SFTP network server and, optionally, a filename.
- `tftp://server[:port]/path/[filename]`—Specifies the TFTP network server and, optionally, a filename.
Viewing and Copying Core Dumps

A core dump occurs when the ACE experiences a fatal error. The ACE writes information about the fatal error to the core: file system in Flash memory before a switchover or reboot occurs. The core: file system is the storage location for all core files generated during a fatal error. Three minutes after the ACE reboots, the saved last core file is restored from the core: file system back to its original RAM location. This restoration is a background process and is not visible to the user.

You can view the list of core files in the core: file system by using the `dir core:` command in Exec mode.

The `dir core:` command is available only in the Admin context.

**Note**

Core dump information is for Cisco Technical Assistance Center (TAC) use only. If the ACE becomes unresponsive, you can view the dump information in the core through the `show cores` command. We recommend that you contact TAC for assistance in interpreting the information in the core dump.

The time stamp on the restored last core file displays the time when the ACE booted up, not when the last core was actually dumped. To obtain the exact time of the last core dump, check the corresponding log file with the same process identifier (PID).

This section contains the following topics:

- Copying Core Dumps
- Clearing the Core Directory
- Deleting a Core Dump File

**Copying Core Dumps**

You can save a core dump from the ACE to the disk0: file system or to a remote server. To save a core to a remote server, use the `copy core:` command in Exec mode. The ACE copies a single file based on the provided process identifier. The `copy core:` command is available only in the Admin context.
To display the list of available core files, use the `dir core:` command. Copy the complete filename (for example, 0x401_vsh_log.25256.tar.gz) into the `copy core:` command.

The syntax for the `copy core:` Exec mode command is:

```
```

The keywords, arguments, and options are as follows:
- `filename`—Core dump that resides on the ACE in Flash memory. Use the `dir core:` command to view the core dump files available in the core: file system.
- `disk0:[path/][filename]`—Specifies a file location for the core dump in the disk0: file system and a filename for the core.
- `ftp://server/path/[filename]`—Specifies the FTP network server and, optionally, the renamed core dump.
- `sftp://[username@]server/path/[filename]`—Specifies the SFTP network server and, optionally, the renamed core dump.
- `tftp://server[:port]/path/[filename]`—Specifies the TFTP network server and, optionally, the renamed core dump.

When you select a destination file system using `ftp:`, `sftp:`, or `tftp:`, the ACE performs the following tasks:
- Prompts you for your username and password if the destination file system requires user authentication.
- Prompts you for the server information if you do not provide the information with the command.
- Copies the file to the root directory of the destination file system if you do not provide path information.

For example, to copy a core file from the ACE to a remote FTP server, enter:

```
host1/Admin# copy core:0x401_vsh_log.8249.tar.gz ftp://192.168.1.2
Enter the destination filename[]? [0x401_vsh_log.8249.tar.gz]
Enter username[]? user1
Enter the file transfer mode[bin/ascii]: [bin]
Password:
Passive mode on.
Hash mark printing on (1024 bytes/hash mark).
```
Chapter 4  Managing the ACE Software

Viewing and Copying Core Dumps

Note
The bin (binary) file transfer mode is intended for transferring compiled files (executables). The ascii file transfer mode is intended for transferring text files, such as config files. The default selection of bin should be sufficient in all cases when copying files to a remote FTP server.

Clearing the Core Directory

To clear out all of the core dumps stored in the core: file system, use the clear cores command in Exec mode of the Admin context. The syntax for the command is as follows:

```plaintext
clear cores
```

For example, to clear out all of the core dumps stored in the core: file system, enter:

```
host1/Admin# clear cores
```

Deleting a Core Dump File

To delete a core dump file from the core: file system in Flash memory, use the delete core: command in Exec mode of the Admin context. To view the core dump files available in Flash memory, use the dir core: command.

The syntax for the command is as follows:

```plaintext
delete core:filename
```

The filename argument specifies the name of a core dump file located in the core: file system.

For example, to delete the file 0x401_VSH_LOG.25256.TAR.GZ from the core: file system, enter:

```
host1/Admin# delete core:0x401_VSH_LOG.25256.TAR.GZ
```
Capturing and Copying Packet Information

Capturing packets is a useful aid in troubleshooting connectivity problems with the ACE or for monitoring suspicious activity. The ACE can track packet information for network traffic that passes through the ACE. The attributes of the packet are defined by an ACL. The ACE buffers the captured packets, and you can copy the buffered contents to a file in Flash memory on the ACE or to a remote server. You can also display the captured packet information on your console or terminal.

⚠️ Caution

The packet capture function uses ACL resources as can be seen with the `show np 1 access-list resource` command. If you have a large ACL configuration and you enable packet capturing, the ACE may oversubscribe the allocated ACL resources. If this happens, you may see one of the following error messages:

In exec mode,
```
Error: Device Name:[0x3FF] Instance:[63] Error Type:[]
```
code:[255]

In config mode,
```
Error: ACL merge add acl to list failed
```

For information about using the `show np 1 access-list resource` command to monitor ACL resources and how to resolve ACL oversubscription problems, see the “Troubleshooting ACLs” section of the ACE Module Troubleshooting Wiki.

This section contains the following topics:
- Capturing Packet Information
- Copying Capture Buffer Information
- Viewing Packet Capture Information
Capturing Packet Information

To enable the packet capture function on the ACE for packet sniffing and network fault isolation, use the `capture` command in Exec mode. As part of the packet capture process, you specify whether to capture packets from all input interfaces or an individual VLAN interface. The packet capture feature streams output on the console as packets are received by the ACE.

**Note**
The packet capture function enables access-control lists (ACLs) to control which packets are captured by the ACE on the input interface. If the ACLs are selecting an excessive amount of traffic for the packet capture operation, the ACE will see a heavy load, which can cause a degradation in performance. We recommend that you avoid using the packet capture function when high network performance is critical.

In addition, probe traffic will not hit a security ACL so ACLs cannot control the capture of those packets. In this case, probe traffic cannot be captured by the packet capture function.

The capture packet function works on an individual context basis. The ACE traces only the packets that belong to the current context where you execute the `capture` Exec mode command. The context ID, which is passed along with the packet, can be used to isolate packets that belong to a specific context. To trace the packets for a specific context, use the `changeto` Exec mode command to enter the specified context and then use the `capture` command.

**Note**
If you enable packet capture for jumbo packets, the ACE captures only the first 1,860 bytes of data.

The ACE does not automatically save the packet capture to a file. To copy the capture buffer information as a file in Flash memory or to a remote server, use the `copy capture` command (see the “Copying Capture Buffer Information” section). The syntax of this command is as follows:

```
capture buffer_name {all | {interface vlan number}} access-list name [bufsize buf_size [circular-buffer]] | remove | start | stop
```
The keywords, arguments, and options are as follows:

- **buffer_name**—Name of the packet capture buffer. The `buffer_name` argument associates the packet capture with a name. Specify a text string from 1 to 80 alphanumeric characters.

- **all**—Specifies capture packets for all input interfaces.

- **interface**—Specifies the interface from which to capture packets.

  **Note**  
  If you delete an interface that is in use by the packet capture function, the ACE stops the capture automatically. If you check the status of the packet capture using the `show capture status` command, you will notice that the capture stopped because of an interface deletion. At this point, you can perform any operation (for example, saving the old capture) on the capture except starting the capture. To restart the capture, you must delete the old capture and configure a new one.

- **vlan number**—Specifies the VLAN identifier associated with the specified input interface.

- **access-list name**—Selects packets based on a specific access list identification. A packet must pass the access list filters before the packet is stored in the capture buffer. Specify a previously created access list identifier. Enter an unquoted text string with a maximum of 64 alphanumeric characters.

  **Note**  
  Ensure that the access list is for an input interface. If you configure the packet capture on the output interface, the ACE will fail to match any packets.

- **bufsize buf_size**—(Optional) Specifies the buffer size, in kilobytes (KB), to store the packet capture. The range is from 1 to 5000 KB. The default is 64 KB.

- **circular-buffer**—(Optional) Enables the packet capture buffer to overwrite itself, starting from the beginning, when the buffer is full.

- **remove**—Removes the packet capture configuration.
Capturing and Copying Packet Information

- **start**—Starts the packet capture function and displays the messages on the session console as the ACE receives the packets. The CLI prompt returns and you can type other commands at the same time that the ACE is capturing packets. To stop the capture process, enter `stop`. The packet capture function automatically stops when the buffer is full unless you enable the circular buffer function.

- **stop**—Stops the packet capture process after a brief delay.

**Note** Under high traffic conditions, you may observe up to 64 packets printing on the console after you enter the `stop` keyword. These additional messages can occur because the packets were in transit or buffered before you entered the `stop` keyword.

If you delete an interface that is in use by the packet capture function, the ACE stops the capture automatically. If you check the status of the packet capture using the `show capture buffer_name status` command (see the “Viewing Packet Capture Information” section), you will notice that the capture stopped because of an interface deletion. At this point, you can perform any operation (for example, saving the old capture) on the capture except starting the capture. To restart the capture, you must delete the old capture and configure a new one. The ACE handles the deletion of an ACL or an ACL entry in a similar manner.

If you add an interface while you are already capturing all interfaces, the capture continues using all the original interfaces. If you add an ACL entry during an existing ACL capture, the capture continues normally using the original ACL criteria.

If the ACE stops a packet capture because of an interface or ACL deletion, the following additional information appears in the output of the `show capture buffer_name status` command:

Capture forced to stop due to change in [interface | access-list] config.
To restart the capture, remove and add the capture again.
To enable packet capture on an interface VLAN, enter:

```
host1/Admin# config
Enter configuration commands, one per line. End with CNTL/Z
host1/Admin(config)# access-list acl1 line 10 extended permit ip any any
host1/Admin(config)# exit
host1/Admin# capture capture1 interface vlan50 access-list acl1
host1/Admin# capture capture1 start
```

To stop packet capture, enter:

```
host1/Admin# capture capture1 stop
```

### Copying Capture Buffer Information

To copy an existing packet capture buffer to the disk0: file system, use the `copy capture` command in Exec mode.

The syntax for the command is as follows:

```
copy capture capture_name disk0:[path]/destination_name
```

The keywords, arguments, and options are as follows:

- `capture_name`—Name of the packet capture buffer in Flash memory. Specify a text string from 1 to 80 alphanumeric characters. If necessary, use the `show capture` command to view the files available in Flash memory. This list includes the name of existing packet capture buffers.

- `disk0:`—Specifies that the buffer is copied to the disk0: file system.

- `[path]/destination_name`—Destination path (optional) and name for the packet capture buffer. Specify a text string from 1 to 80 alphanumeric characters. If you do not provide the optional path, the ACE copies the file to the root directory on the disk0: file system.

For example, to copy a packet capture buffer to the disk0: file system as a file on disk0: called MYCAPTURE1, enter:

```
host1/Admin# copy capture packet_capture_Jan_17_06 disk0:MYCAPTURE1
```

To clear the capture packet buffer, use the `clear capture` command in Exec mode.
The syntax of this command is as follows:

```
clear capture buffer_name
```

The `buffer_name` argument specifies the name of the existing packet capture buffer to clear.

For example, to clear the capture buffer for the capture buffer `packet_capture_Jan_17_06`, enter:

```
host1/Admin# clear capture packet_capture_Jan_17_06
```

### Viewing Packet Capture Information

To display the captured packet information on your console or terminal, use the `show capture` command in Exec mode. The syntax of this command is as follows:

```
show capture buffer_name [detail [connid connection_id | range packet_start packet_end] | status]
```

The keywords, arguments, and options are as follows:

- `buffer_name`—Name of the packet capture buffer. Specify a text string from 1 to 80 alphanumeric characters.
- `detail`—(Optional) Displays additional protocol information for each packet.
- `connid connection_id`—(Optional) Displays protocol information for a specified connection identifier.
- `range packet_start packet_end`—(Optional) Displays protocol information for a range of captured packets.
- `status`—(Optional) Displays capture status information for each packet.

For all types of received packets, the console display is in tcpdump format.

For example, to display captured packet information for packet capture buffer `CAPTURE1`, enter:

```
host1/Admin# show capture CAPTURE1
0001: msg_type: ACE_HIT ace_id: 41 action_flag: 11
0002: msg_type: CON_SETUP con_id: 1090519041 out_con_id: 16777218
0003: msg_type: PKT_RCV con_id: 16777218 other_con_id: 0
0004: msg_type: PKT_RCV con_id: 16777218 other_con_id: 0
0005: msg_type: PKT_RCV con_id: 16777218 other_con_id: 0
0006: msg_type: PKT_RCV con_id: 16777218 other_con_id: 0
```
Capturing and Copying Packet Information

For example, to display packet capture status information, enter:

```
host1/Admin# show capture capture1 status
```

Capture session : cap1
Buffer size : 64 K
Circular : no
Buffer usage : 19.00%
Status : stopped

For example, to display protocol information for a range of captured packets, enter:

```
host1/Admin# show capture capture1 detail range 2-3
```

```
0002: msg_type: CON_SETUP
con_id: 1090519041 out_con_id: 16777218
src_addr: 10.7.107.11 src_port: 30212
dst_addr: 10.7.107.15 dst_port: 23
l3_protocol: 0 l4_protocol: 0
message_hex_dump:
   0x0000: 0000 0101 4100 0001 0100 0002 0000 0000 ........A........
   0x0010: 0a07 6b0b 0a07 6b0f 0619 0001 7604 0017 ..k...k......v...
   0x0020: 0000 0000 0002 0000 05b4 0004 4100 0001 00 ... ...........
   0x0030: 0000 0000 1020 0010 0000 19b2 fb3c ...............<
   0x0040: 0000 0000 0000 0000 0000 0000 0000 0000 ............
   0x0050: 0a07 6b0f 0a07 6b0b 0610 0001 0017 7604 ..k...k......v.
   0x0060: 0000 0000 0002 0000 05b4 0004 4100 0001 00 ... ...........
   0x0070: 0000 0000 0101 0000 0000 0000 0000 0000 ............
   0x0080: 0000 0000 0000 0000 0000 0000 0000 0000 ............
```

```
0003: msg_type: PKT_RCV
con_id: 16777218 other_con_id: 0
message_hex_dump:
   0x0000: 8900 004e 0050 8034 0038 000a 0010 0a06 ...N.P.4.8......
   0x0010: 0000 0005 9a3b 95d9 0011 5d6a f800 0800 ..........]j....
   0x0020: 45c0 002c b0de 0000 ff06 2005 0a07 6b0b E.............k.
```
Capturing and Copying Packet Information

For example, to display captured packet information in tcpdump format, enter:

```
host1/Admin# show capture capture1 detail
```

```
0001: msg_type: ACE_HIT
  ace_id: 41  action_flag: 0xb
  src_addr: 10.7.107.11  src_port: 30212
  dst_addr: 10.7.107.15  dst_port: 23
  l3_protocol: 0  l4_protocol: 6
  message_hex_dump:
  0x0000: 0000 0104 0000 0029 0000 0002 0a07 6b0b  .......)......k.
  0x0010: 0a07 6b0f 0609 0001 7604 0017 0000 0000  ..k.....v.......
  0x0020: 0000 0000 0000 0029 0b06 0000 0000 0000  ...........)....
  0x0030: 0000 0000 0000 0000 0000 0000 0000 0000  ................
  0x0040: 0000 0000 0000 0001                      ........
  0x0050: msg_type: CON_SETUP
  con_id: 1090519041  out_con_id: 16777218
  src_addr: 10.7.107.11  src_port: 30212
  dst_addr: 10.7.107.15  dst_port: 23
  l3_protocol: 0  l4_protocol: 0
  message_hex_dump:
  0x0000: 0000 0101 4100 0001 0100 0002 0000 0000  ....A...........
  0x0010: 0a07 6b0f 0a07 6b0f 0619 0001 7604 0017  ..k...k......v..
  0x0020: 0000 0000 0002 0000 05b4 0000 0100 0002  ................
  0x0030: 0000 0000 0010 0481 0208 0000 0000 0000  ................
  0x0040: 0000 0000 1020 0010 0000 0000 19b2 fb3c  ...............<
  0x0050: 000c 40ae 0000 0029 0000 0000 000c 40ae  ...@....)......@.
  0x0060: 0000 0000 0000 0000 0000 0000 0000 0000  ................
  0x0070: msg_type: PKT_RCV
  con_id: 1090519041  other_con_id: 0
  message_hex_dump:
  0x0000: 8900 004e 0050 8034 0038 000a 0010 0a06  ...N.P.4.8......
  0x0010: 0000 0005 9a3b 95d9 0011 5d6a f800 0800  ..........]j....
  0x0020: 45c0 002c b0de 0000 ff06 2005 0a07 6b0b E. ..........k.
  0x0030: 0a07 6b0f 7604 0017 19b2 fb3b 0000 0000  ..k.v.......;
  0x0040: 6002 1020 12d5 00                      `......
```

0004: msg_type: PKT_RCV
  con_id: 1090519041  other_con_id: 0
message_hex_dump:
0x0000: 0840 004e 0050 8034 0000 000a 0000 0000 .@.N.P.4........
0x0010: 0004 0115 6d6a f800 0005 9a3b 95d9 0800 .......j........
0x0020: 4500 002c 0000 4000 4006 50a4 0a07 6b0f E..,.@.P..k.
0x0030: 0a07 6b0f 0017 7604 f31b 6f71 19b2 fb3c ..k...v...og...<
0x0040: 6012 16d0 a986 00 `.....

0005: msg_type: PKT_RCV
con_id: 16777218 other_con_id: 0
message_hex_dump:
0x0000: 8900 005a 0050 8034 0038 000a 0010 0a06 ...Z.P.4.8......
0x0010: 0000 0005 9a3b 95d9 0011 5d6a f800 0800 ...........j....
0x0020: 45c0 003a b0e0 0000 ff06 1ff5 0a07 6b0f E..{...........k.
0x0030: 0a07 6b0f 7604 0017 19b2 fb3c f31b 6f72 ..k.v.........or
0x0040: 5010 1020 c7f3 00 P............

0006: msg_type: PKT_RCV
con_id: 16777218 other_con_id: 0
message_hex_dump:
0x0000: 0840 004e 0050 8034 0000 000a 0000 0000 .@.N.P.4........
0x0010: 0004 0115 6d6a f800 0005 9a3b 95d9 0800 .......j........
0x0020: 4500 002c 0000 4000 4006 50a4 0a07 6b0f E..,.@.P..k.
0x0030: 0a07 6b0f 7604 0017 19b2 fb3c f31b 6f72 ..k.v.........or
0x0040: 5010 1020 9a8a 0000 fffd 03ff fb18 fffb P............
0x0050: 17ff fb

0007: msg_type: PKT_RCV
con_id: 16777218 other_con_id: 0
message_hex_dump:
0x0000: 0840 004e 0050 8034 0000 000a 0000 0000 .@.N.P.4........
0x0010: 0004 0115 6d6a f800 0005 9a3b 95d9 0800 .......j........
0x0020: 4500 002c 0000 4000 4006 50a4 0a07 6b0f E..,.@.P..k.
0x0030: 0a07 6b0f 7604 0017 19b2 fb3c f31b 6f72 ..k.v.........or
0x0040: 5010 1020 c7e1 00 P............

0008: msg_type: PKT_RCV
con_id: 1090519041 other_con_id: 0
message_hex_dump:
0x0000: 0840 004e 0050 8034 0000 000a 0000 0000 .@.N.P.4........
0x0010: 0004 0115 6d6a f800 0005 9a3b 95d9 0800 .......j........
0x0020: 4500 002c 0000 4000 4006 50a4 0a07 6b0f E..,.@.P..k.
0x0030: 0a07 6b0f 0017 7604 f31b 6f72 19b2 fb4e ..k...v...or...N
0x0040: 5010 16d0 c131 00 P....1.
If the ACE stops a packet capture because of an interface or ACL deletion, the following additional information appears in the output of the `show capture buffer_name status` command:

Capture forced to stop due to change in [interface | access-list] config. To restart the capture, remove and add the capture again.

Using the Configuration Checkpoint and Rollback Service

This section describes how to make a checkpoint (or snapshot) of a running configuration on your ACE and how to use the rollback service to revert to the last known stable configuration. It contains the following topics:

- Overview
- Creating a Configuration Checkpoint
- Deleting a Configuration Checkpoint
- Rolling Back a Running Configuration
- Displaying Checkpoint Information

Overview

At some point, you may want to modify your running configuration. If you run into a problem with the modified configuration, you may need to reboot your ACE. To prevent having to reboot your ACE after unsuccessfully modifying a running configuration, you can create a checkpoint (a snapshot in time) of a known stable running configuration before you begin to modify it. If you encounter a problem with the modifications to the running configuration, you can roll back the configuration to the previous stable configuration checkpoint.
Before you upgrade your ACE software, we strongly recommend that you create a checkpoint in your running configuration. For details about upgrading your ACE software, see Appendix A, Upgrading Your ACE Software.

The ACE allows you to make a checkpoint configuration at the context level. The ACE stores the checkpoint for each context in a hidden directory in Flash memory. If, after you enter additional commands to modify the current running configuration, you enter the rollback command option, the ACE causes the running configuration to revert to the checkpointed configuration.

This section contains the following topics:

- Creating a Configuration Checkpoint
- Deleting a Configuration Checkpoint
- Rolling Back a Running Configuration

## Creating a Configuration Checkpoint

To create a configuration checkpoint, use the `checkpoint create` command in Exec mode in the context for which you want to create a checkpoint. The ACE supports a maximum of 10 checkpoints for each context.

Be sure that the current running configuration is stable and is the configuration that you want to make a checkpoint. If you change your mind after creating the checkpoint, you can delete it. See the “Deleting a Configuration Checkpoint” section.

The syntax of this command is as follows:

```
checkpoint create name
```

The `name` argument specifies the unique identifier of the checkpoint. Enter a text string with no spaces and a maximum of 25 alphanumeric characters.

For example, enter:

```
host1/Admin# checkpoint create MYCHECKPOINT
Generating configuration....
Created checkpoint 'MYCHECKPOINT'
```
Using the Configuration Checkpoint and Rollback Service

If the checkpoint already exists, you are prompted to overwrite it as follows:

Checkpoint already exists
Do you want to overwrite it? (y/n) [n] y Generating configuration....

Created checkpoint 'MYCHECKPOINT'

The default is n. If you do not want to overwrite the existing checkpoint, press Enter. To overwrite the existing checkpoint, enter y.

Deleting a Configuration Checkpoint

To delete a configuration checkpoint, use the checkpoint delete command in Exec mode. Before you use this command, make sure that you want to delete the checkpoint. When you enter this command, the ACE removes the checkpoint from Flash memory. The syntax of this command is as follows:

    checkpoint delete name

The name argument specifies the unique identifier of the checkpoint. Enter a text string with no spaces and a maximum of 25 alphanumeric characters.

For example, enter:

    host1/Admin# checkpoint delete MYCHECKPOINT
    Deleted checkpoint 'MYCHECKPOINT'

Rolling Back a Running Configuration

To roll back the current running configuration to the previously checkpointed running configuration for the current context, use the checkpoint rollback command in Exec mode. The syntax of this command is as follows:

    checkpoint rollback name

The name argument specifies the unique identifier of the checkpoint. Enter a text string with no spaces and a maximum of 25 alphanumeric characters.
For example, enter:

```plaintext
host1/Admin# checkpoint rollback MYCHECKPOINT
This operation will rollback the system's running configuration to the
checkpoint's configuration.
Do you wish to proceed? (y/n)  [n] y
Rollback in progress, please wait...
Generating configuration....
Rollback succeeded
switch/Admin#
```

**Displaying Checkpoint Information**

To display checkpoint information, use the `show checkpoint` command in Exec mode. The syntax of this command is as follows:

```
show checkpoint {all | detail name}
```

The keywords and arguments are as follows:

- `all`—Displays a list of all existing checkpoints
- `detail name`—Displays the running configuration of the specified checkpoint

For example, to display the running configuration for a specific checkpoint, enter:

```plaintext
host1/Admin# show checkpoint detail MYCHECKPOINT
```

Table 4-1 describes the fields that appear in the `show checkpoint all` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checkpoint</td>
<td>Name of the checkpoint</td>
</tr>
<tr>
<td>Size</td>
<td>Size (in bytes) of the checkpoint</td>
</tr>
<tr>
<td>Date</td>
<td>Date and time at which the checkpoint was created</td>
</tr>
</tbody>
</table>
Reformatting the Flash Memory

Caution

We recommend that you use the format command to reformat the ACE Flash memory only under the guidance and supervision of Cisco Technical Assistance Center (TAC).

The ACE uses the file allocation table (FAT16) as the base file system. The file system is used to allocate and organize storage space for various types of storage, such as startup-configuration files, SSL certificate storage, core files, image storage, and log files. To reformat Flash memory on the ACE, use the format command. The format command allows you to erase all data on the Flash memory and reformat it with the FAT16 version of the file allocation table. All user-defined configuration information is erased.

Before you reformat the Flash memory, we recommend that you copy the following ACE operation and configuration files or objects to a remote server:

- ACE software image
- ACE license
- Startup-configuration file of each context
- Running-configuration file of each context
- Core dump files of each context
- Packet capture buffers of each context
- SSL certificate and key pair files of each context

See the "Copying Files" section for details on how to use the copy command to save configuration files or objects, such as the existing startup-configuration files, running-configuration file, licenses, core dump files, or packet capture buffers, to a remote FTP, SFTP, or TFTP server.

See the Cisco Application Control Engine Module SSL Configuration Guide for details on how to use the crypto export command to export SSL certificate and key pair files to a remote FTP, SFTP, or TFTP server.

The syntax of this command is as follows:

format disk0:
For example, to erase all information in Flash memory, enter:

```
host1/Admin# format disk0:
Warning!! This will reboot the system after formatting disk0.
Do you wish to proceed anyway? [y/n] [n] y
```

After you reformat the Flash memory, perform the following actions:

- Reinstall the ACE software image by using the `copy image:` command (see Appendix A, Upgrading Your ACE Software).
- Reinstall the ACE license by using the `license install` command (see Chapter 3, Managing ACE Software Licenses).
- Import the startup and running-configuration files into the associated context by using the `copy` command (see the “Loading Configuration Files from a Remote Server” section).
- Import SSL certificate files and key pair files into the associated context using by the `crypto import` command (see the Cisco Application Control Engine Module SSL Configuration Guide).
Viewing ACE Hardware and Software Configuration Information

This chapter describes how to view ACE hardware and software configuration information. The ACE CLI provides a comprehensive set of `show` commands in Exec mode that you can use to gather ACE hardware and software configuration information. This chapter contains the following major sections:

- Displaying Software Version Information
- Displaying Software Copyright Information
- Displaying Hardware Information
- Displaying the Hardware Inventory
- Displaying System Processes
- Displaying Process Status Information and Memory Resource Limits
- Displaying System Information
- Displaying ICMP Statistics
- Displaying Technical Support Information

To view the contents of the current running-configuration file and startup-configuration file, see Chapter 4, Managing the ACE Software.

---

Note: The `show buffer`, `show cde`, `show fifo`, `show hyp`, `show lcp`, `show netio`, `show np`, `show scp`, and `show vnet` commands display internal system-level hardware `show` output for use by trained Cisco personnel as an aid in debugging and troubleshooting the ACE. See the Cisco Application Control Engine Module Command Reference for background information about those `show` commands.
Displaying Software Version Information

To display the version of system software that is currently running on the ACE in Flash memory, use the `show version` command. You use the `show version` command to verify the software version on the ACE before and after an upgrade.

The syntax of this command is as follows:

```
show version
```

For example, to display the entire output for the `show version` command, enter:

```
host1/Admin# show version
Cisco Application Control Software (ACSW)
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2006, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public License. A copy of the license is available at

Software
  loader: Version 12.2[117]
  system: Version 3.0(0)A1(1) [build 3.0(0)A1(1)
_01:26:21-2006/03/13_/auto/a
  dbu-rel/ws/REL_3_0_0_A1_1]
  system image file: [LCP] disk0:c6ace-t1k9-mzg.3.0.0_A1_1.bin
  licensed features: no feature license is installed
```
Hardware
Cisco ACE (slot: 3)
cpu info:
  number of cpu(s): 2
cpu type: SiByte
cpu: 0, model: SiByte SB1 V0.2, speed: 700 MHz
cpu: 1, model: SiByte SB1 V0.2, speed: 700 MHz
memory info:
  total: 957816 kB, free: 374588 kB
  shared: 0 kB, buffers: 2572 kB, cached 0 kB
cf info:
  filesystem: /dev/cf
  total: 500040 kB, used: 449976 kB, available: 50064 kB

last boot reason: reload command by admin
configuration register: 0x1
host kernel uptime is 1 days 10 hours 59 minute(s) 10 second(s)

Displaying Software Copyright Information

To display the software copyright information for the ACE, use the show copyright command. The syntax of this command is as follows:

  show copyright

For example, enter:

host1/Admin# show copyright
Cisco Application Control Software (ACSW)
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2006, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by other third parties and are used and distributed under license. Some parts of this software are covered under the GNU Public License. A copy of the license is available at http://www.gnu.org/licenses/gpl.html.
Displaying Hardware Information

To display ACE hardware inventory details, use the `show hardware` command. The syntax of this command is as follows:

```
show hardware
```

For example, to display the ACE hardware inventory details, enter:

```
host1/Admin # show hardware
```

Table 5-1 describes the fields in the `show hardware` command output.

**Table 5-1**  Field Descriptions for the `show hardware` Command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Number</td>
<td>Product number of the ACE</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Serial number of the ACE</td>
</tr>
<tr>
<td>Card Index</td>
<td>Location of the ACE, specified as an index value</td>
</tr>
<tr>
<td>Hardware Rev</td>
<td>Hardware revision of the ACE</td>
</tr>
<tr>
<td>Feature Bits</td>
<td>Enabled feature bits of the ACE hardware</td>
</tr>
<tr>
<td>Slot No.</td>
<td>Slot number in the switch or router chassis where the ACE is installed</td>
</tr>
<tr>
<td>Type</td>
<td>Type of module installed in the switch or router chassis</td>
</tr>
<tr>
<td>Module Mode</td>
<td>Supported internetworking speeds in Gigabits per second (Gbps)</td>
</tr>
</tbody>
</table>
Displaying the Hardware Inventory

To display the system hardware inventory of the ACE, use the show inventory command. This command displays information about the field replaceable units (FRUs) in the ACE, including product identifiers, serial numbers, and version identifiers.

The syntax of this command is as follows:

```
show inventory [raw]
```

The optional raw keyword displays information about each temperature sensor in the ACE.

For example, to display the ACE hardware inventory details, enter:

```
host1/Admin # show inventory
```

Table 5-2 describes the fields in the show inventory command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name assigned to the ACE in the switch or router chassis.</td>
</tr>
<tr>
<td>Descr</td>
<td>Description of the ACE installed in the switch or router chassis.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you specify the raw keyword, the Descr field also displays information about each temperature sensor in the ACE.</td>
</tr>
<tr>
<td>PID</td>
<td>Product identifier of the ACE.</td>
</tr>
<tr>
<td>VID</td>
<td>Version identifier of the ACE.</td>
</tr>
<tr>
<td>SN</td>
<td>Serial number of the ACE.</td>
</tr>
</tbody>
</table>
Table 5-3 describes the fields in the `show inventory raw` command output.

**Table 5-3  Field Descriptions for the show inventory raw Command**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name assigned to the temperature sensor in the ACE</td>
</tr>
<tr>
<td>Descr</td>
<td>Description of the temperature sensor</td>
</tr>
<tr>
<td>PID</td>
<td>Not applicable</td>
</tr>
<tr>
<td>VID</td>
<td>Not applicable</td>
</tr>
<tr>
<td>SN</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>

### Displaying System Processes

To display general information about all of the processes running on the ACE, use the `show processes` command. The `show processes` command displays summary CPU information for the SiByte 1250 Processor.

The `show processes` command is available only to users with an Admin role across all contexts. The displayed system processes information is at the CPU system level (the total CPU usage) and is not on a per-context level.

The syntax of this command is as follows:

```
show processes [cpu | log [details | pid process_id] | memory]
```

The keywords, arguments, and options are:

- **cpu**—Displays CPU information for the SiByte 1250 Processor, the BCM1250 dual core MIPS processor
- **log**—Displays information about process logs
- **details**—Displays process log information for all process identifiers
- **pid process_id**—Displays information about a specific process identifier
- **memory**—Displays memory information about the processes
For example, to display memory information for the SiByte 1250 Processor, enter:

```
host1/Admin# show processes mem
```

<table>
<thead>
<tr>
<th>PID</th>
<th>MemAlloc</th>
<th>StackBase/Ptr</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>14592</td>
<td>7fff7f40/7fff77d0</td>
<td>init</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0/0</td>
<td>keventd</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0/0</td>
<td>ksoftirqd_CPU0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0/0</td>
<td>ksoftirqd_CPU1</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0/0</td>
<td>kswapd</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0/0</td>
<td>bdflush</td>
</tr>
</tbody>
</table>

Table 5-4 describes the fields in the `show processes` command output. The `show processes` command displays summary CPU information for the SiByte 1250 Processor.

**Table 5-4 Field Descriptions for the show processes Command**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PID</td>
<td>Process identifier.</td>
</tr>
<tr>
<td>State</td>
<td>Process state. Included below is a summary of the different process state codes that can appear to describe the state of a process:</td>
</tr>
<tr>
<td></td>
<td>• D—Uninterruptible sleep (usually I/O related)</td>
</tr>
<tr>
<td></td>
<td>• ER—Error while running</td>
</tr>
<tr>
<td></td>
<td>• NR—Not running</td>
</tr>
<tr>
<td></td>
<td>• R—Running or runnable (on run queue)</td>
</tr>
<tr>
<td></td>
<td>• S—Interruptible sleep (waiting for an event to complete)</td>
</tr>
<tr>
<td></td>
<td>• T—Stopped, either by a job control signal or because it is being traced</td>
</tr>
<tr>
<td></td>
<td>• W—Paging</td>
</tr>
<tr>
<td></td>
<td>• X—Process is dead</td>
</tr>
<tr>
<td></td>
<td>• Z—Defunct (“zombie”) process, terminated but not reaped by its parent</td>
</tr>
<tr>
<td>PC</td>
<td>Current program counter in hex format.</td>
</tr>
</tbody>
</table>
Table 5-4  **Field Descriptions for the show processes Command**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start_cnt</td>
<td>Number of times a process has been started.</td>
</tr>
<tr>
<td>TTY</td>
<td>Terminal that controls the process. A “—” usually means a daemon is not running on any particular tty.</td>
</tr>
<tr>
<td>Process</td>
<td>Name of the process.</td>
</tr>
</tbody>
</table>

Table 5-5 describes the fields in the `show processes cpu` command output.

Table 5-5  **Field Descriptions for the show processes cpu Command**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Utilization</td>
<td>Lists the percentage of CPU utilization for the ACE for a 5-second interval, 1-minute interval, and a 5-minute interval</td>
</tr>
<tr>
<td>PID</td>
<td>Process identifier</td>
</tr>
<tr>
<td>Runtime (ms)</td>
<td>CPU time the process has used, expressed in milliseconds</td>
</tr>
<tr>
<td>Invoked</td>
<td>Number of times that the process has been invoked</td>
</tr>
<tr>
<td>uSecs</td>
<td>Microseconds of CPU time as an average for each process invocation</td>
</tr>
<tr>
<td>1 Sec</td>
<td>CPU utilization as a percentage for the last second</td>
</tr>
<tr>
<td>5 Sec</td>
<td>CPU utilization as a percentage for the last 5 seconds</td>
</tr>
<tr>
<td>1 Min</td>
<td>CPU utilization as a percentage for the last minute</td>
</tr>
<tr>
<td>5 Min</td>
<td>CPU utilization as a percentage for the last 5 minutes</td>
</tr>
<tr>
<td>Process</td>
<td>Name of the process</td>
</tr>
</tbody>
</table>
Table 5-6 describes the fields in the `show processes log` command output.

### Table 5-6   Field Descriptions for the `show processes log` Command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process</td>
<td>Name of the process</td>
</tr>
<tr>
<td>PID</td>
<td>Process identifier</td>
</tr>
<tr>
<td>Normal-exit</td>
<td>Status of whether the process exited normally</td>
</tr>
<tr>
<td>Stack</td>
<td>Status of whether a stack trace is in the log</td>
</tr>
<tr>
<td>Core</td>
<td>Status of whether a core file exists</td>
</tr>
<tr>
<td>Log-create-time</td>
<td>Time when the log file was generated</td>
</tr>
</tbody>
</table>

Table 5-7 describes the fields in the `show processes log details | pid` command output.

### Table 5-7   Field Descriptions for the `show processes log | pid details` Command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>Name of the service.</td>
</tr>
<tr>
<td>Description</td>
<td>Brief description of the service.</td>
</tr>
<tr>
<td>Started at</td>
<td>Time the process started.</td>
</tr>
<tr>
<td>Stopped at</td>
<td>Time the process stopped.</td>
</tr>
<tr>
<td>Uptime</td>
<td>Length of time that the process was active.</td>
</tr>
<tr>
<td>Start type</td>
<td>System manager option that indicates the process restartability characteristics (that is, whether it is a stateless restart or stateful restart).</td>
</tr>
<tr>
<td>Death reason</td>
<td>Reason that the system manager killed the process (for example, no sysmgr heartbeats).</td>
</tr>
<tr>
<td>Exit code</td>
<td>Exit code with which the process exited.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Normally, the Exit code provides the signal number which killed the process.</td>
</tr>
<tr>
<td>CWD</td>
<td>Current working directory.</td>
</tr>
</tbody>
</table>
Table 5-7 Field Descriptions for the show processes log | pid details Command (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual memory</td>
<td>Virtual memory addresses where the code, data heap, and stack of the process are located.</td>
</tr>
<tr>
<td>PID</td>
<td>Process identifier.</td>
</tr>
<tr>
<td>SAP</td>
<td>Service access point.</td>
</tr>
<tr>
<td>UUID</td>
<td>Universal unique identifier of the SiByte 1250 Processor.</td>
</tr>
</tbody>
</table>

Table 5-8 describes the fields in the show processes memory command output.

Table 5-8 Field Descriptions for the show processes memory Command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PID</td>
<td>Process identifier</td>
</tr>
<tr>
<td>MemAlloc</td>
<td>Total memory allocated by the process</td>
</tr>
<tr>
<td>StackBase/Ptr</td>
<td>Process stack base and current stack pointer in hex format</td>
</tr>
<tr>
<td>Process</td>
<td>Name of the process</td>
</tr>
</tbody>
</table>
Displaying Process Status Information and Memory Resource Limits

To display detailed process status information and memory resource limits, use the `show terminal internal info` Exec mode command.

The syntax of this command is as follows:

```
show terminal internal info
```

For example, enter:

```
host1/Admin# show terminal internal info
```

Table 5-9 describes the fields in the `show terminal internal info` command output.

**Table 5-9 Field Descriptions for the show terminal internal info Command**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Information</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Name of the executable that started the process.</td>
</tr>
</tbody>
</table>
State

Process state. Included below is a summary of the different process state codes that can appear to describe the state of a process:

- **D**—Uninterruptible sleep (usually I/O related)
- **ER**—Error while running
- **NR**—Not running
- **R**—Running or runnable (on run queue)
- **S**—Interruptible sleep (waiting for an event to complete)
- **T**—Stopped, either by a job control signal or because it is being traced
- **W**—Paging
- **X**—Process is dead
- **Z**—Defunct (“zombie”) process, terminated but not reaped by its parent

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TGID</td>
<td>Terminal group identifier.</td>
</tr>
<tr>
<td>PID</td>
<td>Process identifier.</td>
</tr>
<tr>
<td>PPID</td>
<td>Parent process identification number.</td>
</tr>
<tr>
<td>TracerPID</td>
<td>Tracer process identification number.</td>
</tr>
<tr>
<td>UID</td>
<td>Identifier of the user that started the process (four element list).</td>
</tr>
<tr>
<td>GID</td>
<td>Identifier of the group that the process belongs to (four element list).</td>
</tr>
<tr>
<td>FDSIZE</td>
<td>Process file descriptor size.</td>
</tr>
<tr>
<td>Groups</td>
<td>Total number of groups.</td>
</tr>
<tr>
<td>VmSize</td>
<td>Total amount of virtual memory used by the process (in KB).</td>
</tr>
<tr>
<td>VmLck</td>
<td>Total locked virtual memory (in KB).</td>
</tr>
</tbody>
</table>
### Table 5-9  Field Descriptions for the show terminal internal info Command (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VmRSS</td>
<td>Total amount of physical memory used by the process (in KB).</td>
</tr>
<tr>
<td>VmData</td>
<td>Virtual memory data size (in KB).</td>
</tr>
<tr>
<td>VmStk</td>
<td>Virtual memory stack size (in KB).</td>
</tr>
<tr>
<td>VmExe</td>
<td>Executable virtual memory (in KB).</td>
</tr>
<tr>
<td>VmLib</td>
<td>Virtual memory library size (in KB).</td>
</tr>
<tr>
<td>SigPnd</td>
<td>Signals pending.</td>
</tr>
<tr>
<td>SigBlk</td>
<td>Signals blocked.</td>
</tr>
<tr>
<td>SigIgn</td>
<td>Signals ignored.</td>
</tr>
<tr>
<td>SigCat</td>
<td>Signals caught.</td>
</tr>
<tr>
<td>CapInh</td>
<td>Capability inherited privilege.</td>
</tr>
<tr>
<td>CapPrm</td>
<td>Capability privilege (processor resource manager).</td>
</tr>
<tr>
<td>CapEff</td>
<td>Capability effective privilege.</td>
</tr>
</tbody>
</table>

#### Memory Limits

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core file size</td>
<td>Maximum size of core file (in blocks) that may be created.</td>
</tr>
<tr>
<td>Data seg size</td>
<td>Maximum size (in KB) of the data segment for a process.</td>
</tr>
<tr>
<td>File size</td>
<td>Maximum size (in blocks) of files created by the shell.</td>
</tr>
<tr>
<td>Max locked memory</td>
<td>Maximum size (in KB) which a process may lock into memory.</td>
</tr>
<tr>
<td>Max memory size</td>
<td>Maximum size (in KB) to which a process's resident set size may grow.</td>
</tr>
</tbody>
</table>

**Note**  This restriction imposes a limit on the amount of physical memory to be given to a process.

| Open files       | Maximum number of open files for this process.                               |
Displaying System Information

To display the system information, use the `show system` command. The syntax of this command is as follows:

```
show system {error-id \{hex_id | list\} | internal | kmem | resources | uptime}
```

The keywords are:
- `error-id`—Displays description about errors.
- `hex_id`—Error ID in hexadecimal format. The range is from 0x0 to 0xffffffff.
- `list`—Specifies all error IDs.
- `internal`—Specifies a series of internal system-level commands for use by trained Cisco personnel only.
- `kmem`—Displays the Linux kernel memory usage.
- `resources`—Displays system-related CPU and memory statistics.
- `uptime`—Displays how long the ACE has been up and running.

### Table 5-9 Field Descriptions for the `show terminal internal info` Command (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pipe size</td>
<td>Pipe buffer size (in bytes).</td>
</tr>
<tr>
<td>Stack size</td>
<td>Maximum size (in KB) of the stack segment for a process.</td>
</tr>
<tr>
<td>CPU time</td>
<td>Maximum amount of CPU time (in seconds) to be used by each process.</td>
</tr>
<tr>
<td>Max user processes</td>
<td>Maximum number of simultaneous processes for the user identifier.</td>
</tr>
<tr>
<td>Virtual memory</td>
<td>Maximum amount (in KB) of available virtual memory available to the process.</td>
</tr>
</tbody>
</table>
For example, to display CPU and memory statistics for the ACE, enter:

```
host1/Admin# show system resources
```

Table 5-11 describes the fields in the `show system kmem` command output.

### Table 5-10 Field Descriptions for the show system kmem Command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mem</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>Total usable Linux kernel RAM (physical RAM minus the reserved bits and the kernel binary code)</td>
</tr>
<tr>
<td>Used</td>
<td>Total Linux kernel RAM in use.</td>
</tr>
<tr>
<td>Free</td>
<td>Available Linux kernel RAM.</td>
</tr>
<tr>
<td>Shared</td>
<td>Always zero.</td>
</tr>
<tr>
<td>Buffers</td>
<td>Memory in buffer cache.</td>
</tr>
<tr>
<td>Cached</td>
<td>RAM used for the page cache (disk cache) minus the RAM used for the swap cache.</td>
</tr>
<tr>
<td>Swap</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>Total amount of physical swap memory.</td>
</tr>
<tr>
<td>Used</td>
<td>Total swap memory in use.</td>
</tr>
<tr>
<td>Free</td>
<td>Available swap memory.</td>
</tr>
<tr>
<td>MemTotal</td>
<td>Total usable Linux kernel RAM (physical RAM minus the reserved bits and the kernel binary code).</td>
</tr>
<tr>
<td>MemFree</td>
<td>Available Linux kernel RAM.</td>
</tr>
<tr>
<td>MemShared</td>
<td>Always zero.</td>
</tr>
<tr>
<td>Buffers</td>
<td>Memory in buffer cache.</td>
</tr>
<tr>
<td>Cached</td>
<td>RAM used for the page cache (disk cache) minus the RAM used for the swap cache.</td>
</tr>
<tr>
<td>SwapCached</td>
<td>Memory that once was swapped out, is swapped back in, but is still in the swap file. If this memory is needed, it does not need to be swapped out again because it is already in the swap file. This saves I/O.</td>
</tr>
</tbody>
</table>
### Table 5-10 Field Descriptions for the `show system kmem` Command (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Memory that has been used recently and usually not reclaimed unless it is absolutely necessary.</td>
</tr>
<tr>
<td>Inactive</td>
<td>Memory that is unused or easily freeable.</td>
</tr>
<tr>
<td>HighTotal</td>
<td>Total amount of memory in the high memory (highmem) region. Highmem is all memory above approximately 860 MB of physical RAM. The kernel uses indirect methods to access the high memory region. Data cache can go in this memory region.</td>
</tr>
<tr>
<td>HighFree</td>
<td>Total amount of available memory in the highmem area.</td>
</tr>
<tr>
<td>LowTotal</td>
<td>Amount of memory in the low memory region (non-highmem memory).</td>
</tr>
<tr>
<td>LowFree</td>
<td>Amount of free memory in the low memory region. The kernel can address low memory directly. All kernel data structures need to go into low memory.</td>
</tr>
<tr>
<td>SwapTotal</td>
<td>Total amount of physical swap memory.</td>
</tr>
<tr>
<td>SwapFree</td>
<td>Available swap memory.</td>
</tr>
<tr>
<td>Committed_AS</td>
<td>An estimate of how much RAM you would need to make a 99.99% guarantee that there never is an out-of-memory (OOM) condition for a particular workload. Normally, the kernel overcommits memory. For example, if you dynamically allocate 1 GB of memory, no demand is placed on that memory until you actually start using it. The Committed_AS is an estimate of how much RAM or swap memory you would need in a worst-case scenario.</td>
</tr>
</tbody>
</table>
Table 5-11 describes the fields in the `show system resources` command output.

Table 5-11  Field Descriptions for the show system resources Command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load average</td>
<td>Load that is defined as the number of running processes. The average reflects the system load over the past 1-minute, 5-minute, and 15-minute interval.</td>
</tr>
<tr>
<td>Processes</td>
<td>Number of processes in the system, and how many processes are actually running when you enter the command.</td>
</tr>
<tr>
<td>CPU states</td>
<td>CPU usage percentage in user mode, kernel mode, and idle time in the last second.</td>
</tr>
<tr>
<td>Memory usage</td>
<td>Total memory, used memory, free memory, memory used for buffers, and memory used for cache in KB. Buffers and cache are also included in the used memory statistics.</td>
</tr>
</tbody>
</table>

Table 5-12 describes the fields in the `show system uptime` command output.

Table 5-12  Field Descriptions for the show system uptime Command

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System start time</td>
<td>Date and time when the ACE was turned on</td>
</tr>
<tr>
<td>System uptime</td>
<td>Length of time that the ACE hardware and software have been running</td>
</tr>
<tr>
<td>Kernel uptime</td>
<td>Length of time that the operating system (OS) has been running</td>
</tr>
</tbody>
</table>
Displaying ICMP Statistics

To display Internet Control Message Protocol (ICMP) statistics, use the `show icmp statistics` command. The syntax of this command is as follows:

```
show icmp statistics
```

For example, enter:

```
host1/Admin # show icmp statistics
```

Use the `clear icmp statistics` command to clear the ICMP statistics.

Table 5-13 describes the fields in the `show icmp statistics` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Messages</td>
<td>Total number of ICMP messages transmitted or received by the ACE</td>
</tr>
<tr>
<td>Errors</td>
<td>Number of ICMP error messages transmitted or received by the ACE</td>
</tr>
<tr>
<td>Echo Request</td>
<td>Number of ICMP echo request messages transmitted or received by the ACE</td>
</tr>
<tr>
<td>Echo Reply</td>
<td>Number of ICMP echo reply messages transmitted or received by the ACE</td>
</tr>
<tr>
<td>Unreachable</td>
<td>Number of ICMP unreachable packets transmitted or received by the ACE</td>
</tr>
<tr>
<td>TTL Expired</td>
<td>Number of ICMP TTL-expired messages transmitted or received by the ACE</td>
</tr>
<tr>
<td>Redirect</td>
<td>Number of ICMP redirect messages transmitted or received by the ACE</td>
</tr>
<tr>
<td>Address Mask</td>
<td>Number of ICMP Address Mask Request messages transmitted or received by the ACE</td>
</tr>
<tr>
<td>Param problem</td>
<td>Number of ICMP Parameter Problem messages transmitted or received by the ACE</td>
</tr>
</tbody>
</table>
To display general information about the ACE when you report a problem, use the `show tech-support` command in Exec mode. You can also use this command to collect a large amount of information about your ACE and provide the output of this command to technical support representatives when you report a problem.

The `show tech-support` command displays the output of several `show` commands at once. The output from this command varies depending on your configuration.

You can choose to have detailed information for each command or even specify the output for a particular interface or module. Each command output is separated by the line and the command that precedes the output.

---

**Note**

Explicitly set the terminal length command to 0 (zero) to disable autoscrolling and enable manual scrolling. Use the `show terminal` command to view the configured terminal size. After obtaining the output of this command, reset your terminal length as required (see the “Configuring Terminal Display Attributes” section in Chapter 1, Setting Up the ACE).

---

**Note**

You can save the output of this command to a file by appending `> filename` to the `show tech-support` command (see Chapter 4, Managing the ACE Software). If you save this file, verify that you have sufficient space to do so; each file may take about 1.8 MB.

---

**Table 5-13  Field Descriptions for the show icmp-statistics Command**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Quench</td>
<td>Number of ICMP Source Quench messages transmitted or received by the ACE</td>
</tr>
<tr>
<td>Time Stamp</td>
<td>Number of ICMP Time Stamp (request) messages transmitted or received by the ACE</td>
</tr>
</tbody>
</table>
The default output of the `show tech-support` command includes, for example, the output of the following commands:

- **show hardware**—See the “Displaying Hardware Information” section
- **show interface**—See the *Cisco Application Control Engine Module Routing and Bridging Configuration Guide*
- **show process**—See the “Displaying System Processes” section
- **show running-config**—See Chapter 4, Managing the ACE Software
- **show version**—See the “Displaying Software Version Information” section

The syntax of this command is as follows:

```
show tech-support [details]
```

The optional `details` keyword provides detailed information for each `show` command.

For example, to display an excerpt of the current running state of the ACE, enter:

```
host1/Admin# show tech-support

`show version`
Cisco Application Control Software (ACSW)
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2006, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public License. A copy of the license is available at http://www.gnu.org/licenses/gpl.html.

Software
  loader:    Version 12.2[117]
  system:    Version 3.0(0)A1(1) [build 3.0(0)A1(1)
    _01:26:21-2006/03/13_/auto/a
dbu-rel/ws/REL_3_0_0_A1_1]
  system image file: [LCP] disk0:c6ace-t1k9-mzg.3.0.0_A1_1.bin
  licensed features: no feature license is installed
```
Chapter 5   Viewing ACE Hardware and Software Configuration Information

Displaying Technical Support Information

Hardware
Cisco ACE (slot: 3)
cpu info:
   number of cpu(s): 2
cpu type: SiByte
--More--Generating configuration....
cpu: 0, model: SiByte SB1 V0.2, speed: 700 MHz
cpu: 1, model: SiByte SB1 V0.2, speed: 700 MHz
memory info:
   total: 957816 kB, free: 367840 kB
   shared: 0 kB, buffers: 2928 kB, cached 0 kB
   cf info:
      filesystem: /dev/cf
      total: 500040 kB, used: 449976 kB, available: 50064 kB

last boot reason: reload command by admin
configuration register: 0x1
host kernel uptime is 2 days 16 hours 41 minute(s) 20 second(s)

`show inventory`
NAME: "module 3", DESCR: "Application Control Engine 8G"
PID: WS-SVC-NTS10-1-K9 , VID: V00, SN: SAD0837030D

`show hardware`

Hardware
   Product Number: WS-SVC-NTS10-1-K9
   Serial Number: SAD0837030D
   Card Index: 207
   Hardware Rev: 0.203
   Feature Bits: 0000 0001
   Slot No. : 3
   Type: ACE
   Module mode: 8G
To redirect the output of the `show tech-support` command to a file to the disk0: file system on the ACE or to a remote server using File Transfer Protocol (FTP), Secure Transfer Protocol (SFTP), or Trivial Transfer Protocol (TFTP), use the `tac-pac` command in Exec mode.

Note

The output of the `tac-pac` command is in gzip format. We recommend that you include the `.gz` extension in the filename so that it can be easily unzipped from the destination file system.

The syntax for the command is as follows:

```
```

The keywords, arguments, and options are as follows:

- `disk0:[path[/filename]`—Specifies that the file destination is the disk0: file system of the current context. If you do not provide the optional path, the ACE copies the file to the root directory on the disk0: file system.
- `ftp://server/path[/filename]`—Specifies the FTP network server and, optionally, the filename.
- `sftp://[username@]server/path[/filename]`—Specifies the SFTP network server and, optionally, the filename.
- `tftp://server[:port]/path[/filename]`—Specifies the TFTP network server and, optionally, the filename.

For example, to send the output of the `show tech-support` command to a remote FTP server, enter:

```
host1/Admin# tac-pac ftp://192.168.1.2/tac-output_10-7-07.gz
```
CHAPTER 6

Configuring Redundant ACE Modules

This chapter describes how to configure the Cisco Application Control Engine (ACE) module for redundancy, which provides fault tolerance for the stateful switchover of flows. It contains the following major sections:

- Overview of Redundancy
- Redundancy Configuration Quick Start
- Configuring Redundancy
- Configuring Tracking and Failure Detection
- Example of a Redundancy Configuration
- Displaying Redundancy Information
- Clearing Redundancy Statistics

Overview of Redundancy

Redundancy (or fault tolerance) uses a maximum of two ACEs in the same Catalyst 6500 series switch or in separate switches to ensure that your network remains operational even if one of the modules becomes unresponsive. Redundancy ensures that your network services and applications are always available.

Note

Redundancy is not supported between an ACE module and an ACE appliance operating as peers. Redundancy must be configured on the same ACE device type and software release.
Overview of Redundancy

Redundancy provides seamless switchover of flows in case an ACE becomes unresponsive or a critical host, interface, or HSRP group fails. Redundancy supports the following network applications that require fault tolerance:

- Mission-critical enterprise applications
- Banking and financial services
- E-commerce
- Long-lived flows such as FTP and HTTP file transfers

This section contains the following topics:

- Redundancy Protocol
- Stateful Failover
- FT VLAN
- Configuration Synchronization
- Configuration Requirements and Restrictions

Redundancy Protocol

You can configure a maximum of two ACEs (peers) in the same Catalyst 6500 series switch or in different chassis for redundancy. Each peer module can contain one or more fault-tolerant (FT) groups. Each FT group consists of two members: one active context and one standby context. For more information about contexts, see the Cisco Application Control Engine Module Virtualization Configuration Guide. 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. You can specify the pool of MAC addresses that the local ACE and the peer ACE use by configuring the shared-vlan-hostid command and the peer shared-vlan-hostid command, respectively. To avoid MAC address conflicts, be sure that the two pools are different on the two ACEs. For more information about VMACs and MAC address pools, see the Cisco Application Control Engine Module Routing and Bridging Configuration Guide.
Overview of Redundancy

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, interface, or HSRP group fails (see the “Configuring Tracking and Failure Detection” section).
- You enter the `ft switchover` command to force a switchover (see the “Forcing a Failover” section).

Figure 6-1 shows two possible redundancy configurations, where N is the number of ACEs configured for redundancy. The letters (A, B, C, and D) represent the active contexts in each redundancy group, while the primed letters (A’, B’, C’, and D’) are the standby contexts. The contexts are evenly distributed between the two ACEs. You always configure the active and the standby contexts on different ACEs.

**Figure 6-1 Even Distribution of Contexts**

![Even Distribution of Contexts](image)

**Figure 6-2** shows the uneven distribution of contexts between the two ACEs. As an example, it is possible that the FT groups A, B, C, and D use only half the resources that E and F require.
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. The ACE provides active-active redundancy with multiple-contexts only when there are multiple FT groups configured on each module and both modules 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. For details about configuring contexts, see the Cisco Application Control Engine Module Virtualization Configuration Guide.

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 the “Configuring an FT Peer” section.

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 using the no preempt command. To enable preemption after it has been disabled, use the preempt command. Entering this command causes the member with the higher priority always to assert itself and become active. See the “Configuring an FT Group” section.
If the two members have the same priority, the one with the higher IP address becomes the active member. We recommend that you always assign a higher priority to the member that you want to be the active.

**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.

*Note*  
The ACE does not replicate SSL and other terminated (proxied) connections from the active context to the standby context.

The state information passed to the standby module 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 module.
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.

**Note** During failover, the ACE sends failover traffic to destination addresses as Layer 3 unicast and Layer 2 broadcast. As a result, you may encounter high CPU utilization in the interrupt context on the switch that connects the two ACEs in the failover setup.

### FT VLAN

Redundancy uses a dedicated FT VLAN between redundant ACEs to transmit flow-state information and the redundancy heartbeat. You must configure this same VLAN on both peer modules. You also must configure a different IP address within the same subnet on each module for the FT VLAN.

**Note** Do not use this dedicated VLAN for any other network traffic, including HSRP and data.

The two redundant modules constantly communicate over the FT VLAN to determine the operating status of each module. 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 FT VLAN resides in the system configuration file. Each FT VLAN on the ACE has one unique MAC address associated with it. The ACE uses these device 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 FT VLAN do not change at switchover.

## Configuration Synchronization

For redundancy to function properly, both members of an FT group must have identical configurations. Ensure that both ACE modules include the same bandwidth software license (4 Gbps, 8 Gbps, or 16 Gbps) and the same virtual context software license. If there is a mismatch in a software license between the two ACE modules in an FT group, the following operational behavior can occur:

- If there is a mismatch in the virtual context software license, synchronization between the active ACE and standby ACE may not work properly.
- If both the active and the standby ACE modules have the same virtual context software license but have a different bandwidth software license, synchronization will work properly but the standby ACE may experience a potential loss of traffic on switchover from, for example, an 8-Gbps ACE module to a 4-Gbps ACE module.

For details about the available ACE software licenses, see Chapter 3, Managing ACE Software Licenses.

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.

For information about configuring config sync, see the “Synchronizing Redundant Configurations” section.
Configuration Requirements and Restrictions

Follow these requirements and restrictions when configuring the redundancy feature.

- Redundancy is not supported between an ACE module and an ACE appliance operating as peers. Redundancy must be of the same ACE device type and software release.
- In bridged mode (Layer 2), two contexts cannot share the same VLAN.
- To achieve active-active redundancy, a minimum of two contexts and two FT 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 the *Cisco Application Control Engine Module Routing and Bridging Configuration Guide*.

Redundancy Configuration Quick Start

Table 6-1 provides a quick overview of the steps required to configure redundancy for each ACE in the redundancy configuration. Each step includes the CLI command or a reference to the procedure required to complete the task. For a complete description of each feature and all the options associated with the CLI commands, see the sections following Table 6-1.
Table 6-1 Reconfiguration Configuration Quick Start

<table>
<thead>
<tr>
<th>Task and Command Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. If you are operating in multiple contexts, observe the CLI prompt to verify that you are operating in the desired context. If necessary, change to the correct context.</td>
</tr>
<tr>
<td>host1/Admin# changeto C1</td>
</tr>
<tr>
<td>host1/C1#</td>
</tr>
<tr>
<td>The rest of the examples in this table use the Admin context, unless otherwise specified. For details on creating contexts, see the Cisco Application Control Engine Module Virtualization Configuration Guide.</td>
</tr>
<tr>
<td>2. Enter configuration mode.</td>
</tr>
<tr>
<td>host1/Admin# config</td>
</tr>
<tr>
<td>host1/Admin(config)#</td>
</tr>
<tr>
<td>3. Configure a dedicated FT VLAN for communication between the members of the FT group. This FT VLAN is global and is shared by all contexts. Specify the IP address and netmask of the FT VLAN and the IP address and netmask of the remote peer.</td>
</tr>
<tr>
<td>host1/Admin(config)# ft interface vlan 60</td>
</tr>
<tr>
<td>host1/Admin(config-ft-intf)# ip address 192.168.12.1 255.255.255.0</td>
</tr>
<tr>
<td>host1/Admin(config-ft-intf)# peer ip address 192.168.12.15 255.255.255.0</td>
</tr>
<tr>
<td>host1/Admin(config-ft-intf)# no shutdown</td>
</tr>
<tr>
<td>host1/Admin(config-ft-intf)# exit</td>
</tr>
<tr>
<td>4. Configure the local redundancy peer module, associate the FT VLAN with the peer, and configure the heartbeat interval and count.</td>
</tr>
<tr>
<td>host1/Admin(config)# ft peer 1</td>
</tr>
<tr>
<td>host1/Admin(config-ft-peer)# ft-interface vlan 60</td>
</tr>
<tr>
<td>host1/Admin(config-ft-peer)# heartbeat count 20</td>
</tr>
<tr>
<td>host1/Admin(config-ft-peer)# heartbeat interval 300</td>
</tr>
<tr>
<td>host1/Admin(config-ft-intf)# exit</td>
</tr>
<tr>
<td>5. Create at least one FT group on each ACE.</td>
</tr>
<tr>
<td>host1/Admin(config)# ft group 1</td>
</tr>
<tr>
<td>host1/Admin(config-ft-group)#</td>
</tr>
</tbody>
</table>
Redundancy Configuration Quick Start

Table 6-1  Redundancy Configuration Quick Start (continued)

<table>
<thead>
<tr>
<th>Task and Command Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>6. Associate a context with each FT group. You must associate the local context and the corresponding peer context with the same FT group.</td>
</tr>
<tr>
<td>host1/Admin(config-ft-group)# associate-context C1</td>
</tr>
<tr>
<td>7. Associate the peer context with the FT group.</td>
</tr>
<tr>
<td>host1/Admin(config-ft-group)# peer 1</td>
</tr>
<tr>
<td>8. (Optional) Configure the priority of the FT group on the local module.</td>
</tr>
<tr>
<td>host1/Admin(config-ft-group)# priority 100</td>
</tr>
<tr>
<td>9. (Optional) Configure the priority of the FT group on the peer module.</td>
</tr>
<tr>
<td>host1/Admin(config-ft-group)# peer priority 200</td>
</tr>
<tr>
<td>10. Place the FT group in service.</td>
</tr>
<tr>
<td>host1/Admin(config-ft-group)# inservice</td>
</tr>
<tr>
<td>host1/Admin(config-ft-group)# exit</td>
</tr>
<tr>
<td>11. (Optional) Configure one or more critical objects (gateways or hosts, interfaces, or HSRP groups) to track for switchover. For example, to configure a critical interface for tracking, enter:</td>
</tr>
<tr>
<td>host1/Admin(config)# ft track interface VLAN100</td>
</tr>
<tr>
<td>host1/Admin(config-ft-track-intf)# track-interface vlan 100</td>
</tr>
<tr>
<td>host1/Admin(config-ft-track-intf)# peer track-interface vlan 100</td>
</tr>
<tr>
<td>host1/Admin(config-ft-track-intf)# priority 50</td>
</tr>
<tr>
<td>host1/Admin(config-ft-track-intf)# peer priority 150</td>
</tr>
<tr>
<td>host1/Admin(config-ft-track-intf)# ctrl-z</td>
</tr>
<tr>
<td>12. (Optional) Enable autosynchronization of the running- and/or startup-configuration file from the active to the standby context.</td>
</tr>
<tr>
<td>host1/Admin(config)# ft auto-sync running-config</td>
</tr>
<tr>
<td>host1/Admin(config)# ft auto-sync startup-config</td>
</tr>
<tr>
<td>13. (Optional) Save your configuration changes to Flash memory.</td>
</tr>
<tr>
<td>host1/Admin(config)# exit</td>
</tr>
<tr>
<td>host1/Admin# copy running-config startup-config</td>
</tr>
<tr>
<td>14. (Recommended) Verify your redundancy configuration by using the following commands in Exec mode:</td>
</tr>
<tr>
<td>host1/Admin# show running-config ft</td>
</tr>
<tr>
<td>host1/Admin# show running-config interface</td>
</tr>
</tbody>
</table>
Configuring Redundancy

To configure redundancy on the ACE, use the commands in the following sections. You must configure the **ft interface**, **ft peer**, and **ft group** commands on all ACEs that participate in the redundancy configuration. This section contains the following topics:

- Configuring an FT VLAN
- Configuring an Alias IP Address
- Configuring an FT Peer
- Configuring an FT Group
- Specifying the Peer Hostname
- Specifying the MAC Address Banks for a Shared VLAN
- Forcing a Failover
- Synchronizing Redundant Configurations

Configuring an FT VLAN

Peer ACEs communicate with each other over a dedicated FT VLAN. These redundant peers use the FT VLAN to transmit and receive heartbeat packets and state and configuration replication packets. You must configure the same VLAN on each peer module.

**Note**

Do not use this dedicated VLAN for any other network traffic, including HSRP and data.

This section contains the following topics:

- Creating an FT VLAN
- Configuring an FT VLAN IP Address
- Configuring the Peer IP Address
- Enabling the FT VLAN
Creating an FT VLAN

To create an FT VLAN, use the `ft interface` command in configuration mode. The syntax of this command is as follows:

```
ft interface vlan vlan_id
```

The `vlan_id` argument specifies a unique identifier for the FT VLAN. Enter an integer from 2 to 4094.

For example, enter:

```
host1/Admin(config)# ft interface vlan 200
host1/Admin(config-ft-intf)#
```

**Note**

To remove an FT VLAN, first remove it from the FT peer by using the `no ft-interface vlan` command in FT peer configuration mode. See the “Associating the FT VLAN with the Local Peer” section.

To remove the FT VLAN from the redundancy configuration, enter:

```
host1/Admin(config)# no ft interface vlan 200
```

Configuring an FT VLAN IP Address

After you create the FT VLAN, you must assign an IP address to the VLAN. To assign an IP address to the VLAN, use the `ip` command in FT interface configuration mode. The syntax of this command is as follows:

```
ip address ip_address netmask
```

The keyword and arguments of this command are:

- `address ip_address`—Specifies the IP address of the FT VLAN. Enter an IP address in dotted-decimal notation (for example, 192.168.12.1).
- `netmask`—Subnet mask of the FT VLAN. Enter a subnet mask in dotted-decimal notation (for example, 255.255.255.0).

For example, to configure an IP address for the FT VLAN, enter:

```
host1/Admin(config-ft-intf)# ip address 192.168.12.1 255.255.255.0
```

To remove the IP address from an FT VLAN, enter:

```
host1/Admin(config-ft-intf)# no ip address
```
## Configuring the Peer IP Address

The local member of the FT group communicates with the remote peer over the FT VLAN. To allow the local member to communicate with the remote peer, use the `peer ip address` command in FT interface configuration mode. The syntax of this command is as follows:

```
peer ip address ip_address netmask
```

The keyword and arguments of this command are:

- **address ip_address**—Specifies the IP address of the remote peer. Enter an IP address in dotted-decimal notation (for example, 192.168.12.15).
- **netmask**—Subnet mask of the remote peer. Enter a subnet mask in dotted-decimal notation (for example, 255.255.255.0).

For example, to configure an IP address on the remote peer, enter:

```
host1/Admin(config-ft-intf)# peer ip address 192.168.12.15 255.255.255.0
```

To remove an IP address from the remote peer, enter:

```
host1/Admin(config-ft-intf)# no peer ip address 192.168.12.15 255.255.255.0
```

## Enabling the FT VLAN

To enable the FT VLAN, use the `no shutdown` command in FT interface configuration mode. The syntax of this command is as follows:

```
no shutdown
```

For example, to enable the FT VLAN, enter:

```
host1/Admin(config-ft-intf)# no shutdown
```

To disable the FT VLAN after you have enabled it, enter:

```
host1/Admin(config-ft-intf)# shutdown
```
Configuring an Alias IP Address

When you configure redundancy, configure a VLAN interface that has an alias IP address that floats between the active and standby modules. The alias IP address serves as a shared gateway for the two ACE modules.

To configure an alias IP address, use the `alias` command in interface configuration mode. The syntax of this command is as follows:

```
alias ip_address netmask
```

The `ip_address netmask` arguments specify the IP address and netmask for the VLAN interface. Enter the IP address and subnet mask in dotted-decimal notation (for example, `192.168.1.1 255.255.255.0`).

For example, to configure an alias IP address, enter:

```
host1/Admin(config)# interface vlan 100
host1/Admin(config-if)# alias 192.168.1.1 255.255.255.0
```

To remove an alias IP address, enter:

```
host1/Admin(config-if)# no alias 192.168.1.1 255.255.255.0
```

Configuring an FT Peer

On both peer ACEs, configure an FT peer definition in the Admin context only. You can configure a maximum of two ACEs as redundancy peers.

To create an FT peer, use the `ft peer` command in configuration mode. The syntax of this command is as follows:

```
ft peer peer_id
```

The `peer_id` argument specifies a unique identifier for the peer. You can only enter 1.

For example, enter:

```
host1/Admin(config)# ft peer 1
```

**Note**

Before you can remove an FT peer from the configuration, remove the peer from the FT group. See the “Associating a Peer with an FT Group” section.
Configuring Redundancy

To remove the FT peer from the configuration, enter:

```
host1/Admin(config)# no ft peer 1
```

After you create an FT peer, configure the peer attributes as described in the following topics:

- Associating the FT VLAN with the Local Peer
- Configuring the Heartbeat Interval and Count
- Configuring a Query Interface

### Associating the FT VLAN with the Local Peer

After you create an FT peer, associate the existing FT VLAN with that local peer so that it can communicate with the remote peer. The redundancy peers use this dedicated FT VLAN to exchange heartbeat packets and flow-state information. For information about configuring an FT VLAN, see the “Configuring an FT VLAN” section.

To associate an FT VLAN with a peer, use the `ft-interface vlan` command in FT peer configuration mode. The syntax of this command is as follows:

```
ft-interface vlan vlan_id
```

The `vlan_id` argument specifies the identifier of an existing VLAN. Enter an integer from 2 to 4094.

For example, enter:

```
host1/Admin(config-ft-peer)# ft-interface vlan 200
```

To remove the FT VLAN from the peer configuration, enter:

```
host1/Admin(config-ft-peer)# no ft-interface vlan 200
```

### Configuring the Heartbeat Interval and Count

The heartbeat interval determines the frequency in milliseconds (ms) at which the active member of the FT group sends the heartbeat packets to the standby member. The heartbeat count is the number of missed heartbeats that the standby member must detect before determining that the active member is not available. To configure the heartbeat interval and count, use the `heartbeat` command in peer configuration mode. The syntax of this command is as follows:

```
heartbeat {count number | interval frequency}
```
The keywords and arguments are:

- **count number**—Specifies the number of heartbeat intervals that must transpire with no heartbeat packet received by the standby member before the standby member determines that the active member is not available. Enter an integer from 10 to 50. The default is 10 heartbeat intervals. If the standby member of the FT group does not receive a heartbeat packet from the active member, a time period equal to count number times interval frequency must elapse before a switchover can occur. For example, in the default case, where the heartbeat frequency is 300 ms and the heartbeat count is 10, if the standby member does not receive a heartbeat packet from the active member for 3000 ms (3 seconds), a switchover occurs.

- **interval frequency**—Specifies the interval in milliseconds (ms) between heartbeats. Enter an integer from 100 to 1000 ms. The default is 300 ms.

For example, to set the heartbeat count to 20, enter:

```plaintext
host1/Admin(config-ft-peer)# heartbeat count 20
```

To reset the heartbeat count to the default of 10, enter:

```plaintext
host1/Admin(config-ft-peer)# no heartbeat count
```

For example, to set the heartbeat interval to 500 ms, enter:

```plaintext
host1/Admin(config-ft-peer)# heartbeat interval 500
```

To reset the heartbeat interval to the default of 100 ms, enter:

```plaintext
host1/Admin(config-ft-peer)# no heartbeat interval
```

### Configuring a Query Interface

Configure a query interface to allow the standby member to determine whether the active member is down or if there is a connectivity problem with the FT VLAN. A query interface helps prevent two redundant contexts from becoming active at the same time for the same FT group. Before triggering a switchover, the ACE pings the active member to make sure that it is down. Configuring a query interface allows you to assess the health of the active member, but it increases switchover time.

To configure a query interface, use the `query-interface vlan` command in FT peer configuration mode. The syntax of this command is as follows:

```
query-interface vlan vlan_id
```
Chapter 6  Configuring Redundant ACE Modules

Configuring Redundancy

The `vlan_id` argument specifies the identifier of an existing VLAN. Enter an integer from 2 to 4094.

For example, to configure a query interface, enter:

```
host1/Admin(config-ft-peer)# query-interface vlan 400
```

To remove the query interface from the peer configuration, enter:

```
host1/Admin(config-ft-peer)# no query-interface vlan 400
```

**Note**

You cannot delete a query interface if it is associated with a peer. You must disassociate the interface from the peer first, and then you can delete the interface.

### Configuring an FT Group

On each ACE, you can create multiple FT groups, up to a maximum of 251 groups (250 user contexts and 1 Admin context). Each group consists of a maximum of two members (contexts): one active context on one module and one standby context on the peer module.

To create an FT group, use the `ft group` command in configuration mode. You must configure the same group ID on both peer modules. The syntax of this command is as follows:

```
ft group group_id
```

The `group_id` argument specifies a unique identifier of the group. Enter an integer from 1 to 255.

For example, enter:

```
host1/Admin(config)# ft group 1
host1/Admin(config-ft-group)#
```

To remove the group from the configuration, enter:

```
host1/Admin(config)# no ft group 1
```
After you create an FT group, configure the FT group attributes as described in the following topics:

- Associating a Context with an FT Group
- Associating a Peer with an FT Group
- Assigning a Priority to the Active FT Group Member
- Assigning a Priority to the Standby FT Group Member
- Configuring Preemption
- Placing an FT Group in Service
- Modifying an FT Group

**Associating a Context with an FT Group**

An FT group consists of two members (contexts) with the same name, each residing on a different ACE. To associate a context with an FT group, use the `associate-context` command in FT group configuration mode. You need to make this association for both redundant contexts in an FT group. The syntax of this command is as follows:

```
associate-context name
```

For the `name` argument, enter the unique identifier of the context that you want to associate with the FT group.

For example, enter:

```
host1/Admin(config-ft-group)# associate-context C1
```

**Note** Before you can remove a context from an FT group, you must first take the group out of service by using the `no inservice` command. See the “Placing an FT Group in Service” section.

To remove a context from an FT group, enter:

```
host1/Admin(config-ft-group)# no associate-context C1
```
Associating a Peer with an FT Group

To associate a peer ACE with an FT group, use the `peer` command in FT group configuration mode. The syntax of this command is as follows:

```
peer peer_id
```

For the `peer_id` argument, enter 1 as the identifier of an existing peer module. You can only enter 1.

For example, enter:
```
host1/Admin(config-ft-group)# peer 1
```

To remove the peer association with the FT group, enter:
```
host1/Admin(config-ft-group)# no peer
```

Assigning a Priority to the Active FT Group Member

A member (context) of an FT group becomes the active member through an election process based on the priority that you configure for the group on each peer. The group member with the higher priority becomes the active member. To ensure that the member with the higher priority always becomes the active member, use the `preempt` command, which is enabled by default. For details, see the “Configuring Preemption” section.

To configure the priority of an FT group on the active member, use the `priority` command in FT group configuration mode. You must configure the priority of an FT group on both modules. Configure a higher priority for the group on the ACE where you want the active member to initially reside. The syntax of this command is as follows:

```
priority number
```

The `number` argument specifies the priority of the FT group on the local peer. Enter an integer from 1 to 255. The default is 100.

Tip

Configure a higher priority on the FT group member that you want to be the active member.
For example, to configure the priority of the FT group on the active member, enter:

```
host1/Admin(config-ft-group)# priority 150
```

To restore the default priority of 100, enter:

```
host1/Admin(config-ft-group)# no priority
```

### Assigning a Priority to the Standby FT Group Member

To configure the priority of an FT group on the remote standby member, use the `peer priority` command in FT group configuration mode. You must configure the priority of an FT group on both redundant modules. Configure a lower priority for the FT group on the ACE where you want the standby member to initially reside. The syntax of this command is as follows:

```
peer priority number
```

The `number` argument specifies the priority of the FT group on the standby member. Enter an integer from 1 to 255. The default is 100.

**Tip**

Configure a lower priority on the FT group member that you want to be the standby member.

**Note**

The ACE does not perform bulk config synchronization (sync) on the `peer priority` command value in the FT group associated with the Admin context to the peer. Therefore, you may observe a peer priority value in the running-configuration file that is different from the actual operating value. For information on bulk config sync, see the “Synchronizing Redundant Configurations” section.

For example, to configure the priority of the FT group member on the remote standby member, enter:

```
host1/Admin(config-ft-group)# peer priority 50
```

To restore the default priority of 100, enter:

```
host1/Admin(config-ft-group)# no peer priority
```
Configuring Preemption

Preemption ensures that the group member with the higher priority always asserts itself and becomes the active member. By default, preemption is enabled. To configure preemption after it has been disabled, use the `preempt` command in FT group configuration mode. The syntax of this command is as follows:

```
preempt
```

For example, enter:

```
host1/Admin(config-ft-group)# preempt
```

To disable preemption, enter:

```
host1/Admin(config-ft-group)# no preempt
```

Note: If you disable preemption by using the `no preempt` command and a member with a higher priority is found after the other member has become active, the electing member becomes the standby member even though it has a higher priority.

Placing an FT Group in Service

Note: Before you place an FT group in service, be sure that you have associated one context with the FT group and that you have properly configured the two peers.

To place an FT group in service, use the `inservice` command in FT group configuration mode. The syntax of this command is as follows:

```
inservice
```

For example, to place an FT group in service, enter:

```
host1/Admin(config-ft-group)# inservice
```

To take the FT group out of service, enter:

```
host1/Admin(config-ft-group)# no inservice
```
Chapter 6      Configuring Redundant ACE Modules

Modifying an FT Group

If you need to modify an FT group, perform the following steps in FT group configuration mode:

**Step 1** Remove the FT group from service by using the **no inservice** command.

**Step 2** Make the necessary modifications to the FT group.

**Step 3** Place the FT group back in service by using the **inservice** command.

**Note** You can modify the **priority**, **peer priority**, and **preempt** command values without taking the FT group out of service.

Specifying the Peer Hostname

To specify the hostname of a peer ACE, use the **peer hostname** command in configuration mode in the Admin context. For details about this command, see Chapter 1, Setting Up the ACE.

Specifying the MAC Address Banks for a Shared VLAN

To specify the MAC address banks to be used by the local ACE and the peer ACE with a shared VLAN (FT VLAN), use the **shared-vlan-hostid** command and the **peer shared-vlan-hostid** command, respectively, in configuration mode in the Admin context. You configure these commands to prevent MAC address conflicts between the two peer ACEs. Be sure to select a bank of MAC addresses for the peer that is different from that used by the local ACE. For details about this command, see the Cisco Application Control Engine Module Routing and Bridging Configuration Guide.
Forcing a Failover

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 becoming the active member of the FT group, a switchover occurs.

Note
During failover, the ACE sends failover traffic to destination addresses as Layer 3 unicast and Layer 2 broadcast. As a result, you may encounter high CPU utilization in the interrupt context on the switch that connects the two ACEs in the failover setup.

To cause a switchover, use the `ft switchover` command in Exec mode. To use this command, you must disable preemption by using the `no preempt` command. For information on the `preempt` command, see the “Configuring Preemption” section.

The syntax of the `ft switchover` command is:

```
ft switchover [all [force] | force | [group_id [force]]]
```

The keywords, arguments, and options are:

- `all`—(Optional) Causes a switchover of all FT groups configured in the ACE simultaneously.
- `force`—(Optional) Causes a switchover while ignoring the state of the standby member. Use this option only when the FT VLAN is down.
- `group_id`—(Optional) FT group that you want to switch over. Enter the ID of an existing FT group as an integer from 1 to 255.

The `ft switchover` command exhibits the following behavior, depending on whether you enter the command from the Admin context or a user context:

- Admin context—If you specify an FT group ID, then the FT group specified by the group ID switches over. If you do not specify a group ID, then the Admin context switches over.
- User context—Because you cannot specify an FT group ID in a user context, the context in which you enter the command switches over.
For example, to cause a failover from the active module to the standby module of FT group1, enter:

```
host1/Admin# ft switchover 1
This command will cause card to switchover (yes/no)? [no] yes
host1/Admin#
```

### Synchronizing Redundant Configurations

The configurations on both the active context and the standby context must be identical. To ensure that the running configurations on both the active and the standby contexts of an FT group are identical, the ACE automatically synchronizes the running configurations between the two contexts. After the active context has accepted either a new configuration or modifications to an existing configuration, the ACE automatically applies the new configuration or configuration changes to the standby context and disables configuration mode in the standby context.

The ACE supports the following two types of configuration synchronizations:

- **Bulk config sync**—Synchronizes the entire active context configuration to the standby context when the peer comes up or when autosynchronization is enabled
- **Dynamic config sync**—Synchronizes the configuration applied to the active context to the standby context if the peer is already up

To enable automatic synchronization of the running-configuration and the startup-configuration files after they have been explicitly disabled, use the `ft auto-sync` command in configuration mode.

If the standby ACE has reached the maximum resource limit for a configuration object even if some of the configuration objects are not in the redundant context, if you configure one more object of the same type in the redundant context of the active ACE, configuration synchronization will fail. For example, suppose that you have configured two contexts on each ACE (Admin and C1) and the C1 context is the only one in the FT group. On the standby ACE, you have configured 8,192 `match source-address` statements in the Admin context and in the C1 context for a total of 16,384 `match source-address` statements (the ACE limit). When you configure one new `match source-address` statement on the active ACE in C1, configuration synchronization will fail, the new match statement will not be replicated to the standby, and syslog ACE-1-727005 is generated.
If you temporarily disable `ft auto-sync running-config` on the active ACE (for example, to test changes to your configuration), when you subsequently reenable config sync, any changes that you made to the active ACE are duplicated on the standby ACE. Note that the standby ACE remains in the STANDBY_HOT state even when config sync is disabled on the active ACE. (For more information about FT states, see Table 6-2.) If you operate the active ACE with config sync disabled for a prolonged period of time, you must manually duplicate any changes that you make to the active ACE on the standby ACE to ensure that connection replication works properly.

**Note**

If a license mismatch occurs between the two ACEs in a redundant configuration, the `auto-sync` command is automatically disabled and a syslog message is generated.

The syntax of this command is as follows:

```
ft auto-sync { running-config | startup-config }
```

The keywords are:

- `running-config`—Enables autosynchronization of the running-configuration file. The default is enabled.
- `startup-config`—Enables autosynchronization of the startup-configuration file. The default is enabled.

**Caution**

Toggling `ft auto-sync running-config` in the Admin context may have undesirable side effects if the same command is also disabled in an active user context. If `ft auto-sync running-config` is disabled in the active Admin context and in an active user context, and you subsequently enable `ft auto-sync running-config` in the active Admin context first, the entire configuration of the standby user context will be lost. Always enable `ft auto-sync running-config` in the active user context first, and then enable the command in the active Admin context.

**Note**

If the config sync fails, the running-configuration file reverts to the startup-configuration file.
The ACE does not copy or write changes in the running-configuration file to the startup-configuration file unless you enter the `copy running-config startup-config` command or the `write memory` command for the current context. To write the contents of the running-configuration file to the startup-configuration file for all contexts, use the `write memory all` command. At this time, if the `ft auto-sync startup-config` command is enabled, the ACE synchronizes the startup-configuration file on the active ACE to the standby ACE.

The ACE does not synchronize the SSL certificates and key pairs that are present in the active context with the standby context of an FT group. If the ACE performs a configuration synchronization and does not find the necessary certificates and keys in the standby context, config sync fails and the standby context enters the STANDBY_COLD state. For more information about FT states, see Table 6-2.

**Caution**

Do not enter the `no inservice` command followed by the `inservice` command on the active context of an FT group when the standby context is in the STANDBY_COLD state. Doing so may cause the standby context running-configuration file to overwrite the active context running-configuration file.

To copy the certificates and keys to the standby context, you must export the certificates and keys from the active context to an FTP or TFTP server using the `crypto export` command, and then import the certificates and keys to the standby context using the `crypto import` command. For more information about importing and exporting certificates and keys, see the *Cisco Application Control Engine Module SSL Configuration Guide*.

To return the standby context to the STANDBY_HOT state in this case, ensure that you have imported the necessary SSL certificates and keys to the standby context, and then perform a bulk sync of the active context configuration by entering the following commands in configuration mode in the active context of the FT group:

1. `no ft auto-sync running-config`
2. `ft auto-sync running-config`

For example, to enable autosynchronization of the running-configuration file in the C1 context after it has been disabled, enter:

```
host1/C1(config)# ft auto-sync running-config
```
Configuring Tracking and Failure Detection

This section describes the tracking and failure detection feature of the ACE. This feature allows you to designate certain network items as critical so that, if one or more items fail, the ACE reduces the priority of the associated active FT group accordingly. If the priority of the active FT group falls below the priority of the corresponding FT group on the standby, a switchover occurs.

This section contains the following topics:

- Overview of Tracking and Failure Detection
- Configuring Tracking and Failure Detection for a Host or Gateway
- Configuring Tracking and Failure Detection for an Interface
- Creating a Tracking and Failure Detection Process for an HSRP Group

Overview of Tracking and Failure Detection

The ACE supports the tracking and failure detection of several network items. You can configure an ACE to track and detect failures in the following items in the Admin context and any user context:

- Gateways or hosts
- Interfaces
- Hot Standby Router Protocol (HSRP) groups

If one of the items that you configure for tracking and failure detection becomes unresponsive and is associated with the active member of an FT group, by default, the ACE subtracts a value of 0 from the configured priority of the active member. If you configure a nonzero value for the tracking priority and the resulting priority value of the active member 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 that exist at the time of the switchover continue uninterrupted on the new active member of the FT group.

When the failed item comes back up, the ACE increments the priority of the associated group member by a value of 0 by default. If you configure a non-zero value for the tracking priority and the resulting priority of the standby member is greater than the priority of the active member, a switchover occurs back to the original active group member.
You can configure the unit priority associated with tracked items to be greater than 0. This option allows you to fine tune the switchover scenario so that a switchover occurs when either all or any of the tracked objects fails.

**Note**
To prevent an unexpected switchover from occurring, we strongly recommend that you disable preemption before you configure tracking. After you configure tracking and before you reenable preemption, ensure that the tracked network objects are up and operating properly. A switchover may occur immediately when you reenable preemption. Preemption must be enabled for a tracking switchover to work. For details about preemption, see the “Configuring an FT Group” section.

For example, suppose that on ACE 1 you configure the active FT group member with a priority of 100 and on ACE 2 you configure the standby FT group member with a priority of 70. Assume that you configure the FT group to track three critical interfaces, each with a unit priority of 15. To trigger a switchover, all three interfaces must fail so that the priority of the active member is less than the priority of the standby member (100 – 45 = 55).

To illustrate the “any” scenario, assume the FT group members have the same individual priorities as in the previous example (100 and 70, respectively). However, this time you configure the three tracked interfaces, each with a unit priority of 40. If any one of the interfaces associated with the active member goes down, then the priority of the active member falls below the priority of the standby member and a switchover occurs. If that failed interface later returns to service, the ACE increments the associated group member priority by 40, and a switchover would occur back to the original active member. To guarantee a switchover if any tracked item goes down, configure the unit priority on each tracked item equal to the group member’s priority. In this case, you could configure the unit priority to be 100.
Chapter 6  Configuring Redundant ACE Modules

Configuring Tracking and Failure Detection

Configuring Tracking and Failure Detection for a Host or Gateway

This section describes how to configure tracking and failure detection for a gateway or a host. It contains the following topics:

- Creating a Tracking and Failure Detection Process for a Host or Gateway
- Configuring the Gateway or Host IP Address Tracked by the Active Member
- Configuring a Probe on the Active Member for Host Tracking
- Configuring a Priority on the Active Member for Multiple Probes
- Configuring the Gateway or Host IP Address Tracked by the Standby Member
- Configuring a Probe on the Standby Member for Host Tracking
- Configuring a Priority on the Standby Member for Multiple Probes
- Example of a Tracking Configuration for a Gateway

Creating a Tracking and Failure Detection Process for a Host or Gateway

To create a tracking and failure detection process for a gateway or host, use the `ft track host` command in configuration mode. The syntax of this command is as follows:

```
ft track host name
```

For the `name` argument, enter a unique identifier of the tracking process as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

For example, to create a tracking process for a gateway, enter:

```
host1/Admin(config)# ft track host TRACK_GATEWAY1
host1/Admin(config-ft-track-host)#
```

To remove the gateway-tracking process, enter:

```
host1/Admin(config)# no ft track host TRACK_GATEWAY1
```
Configuring the Gateway or Host IP Address Tracked by the Active Member

To allow the active member to track a gateway or host, you need to configure the IP address of the gateway or host. To configure the IP address, use the `track-host` command in FT track host configuration mode. The syntax of this command is as follows:

```
track-host ip_address
```

The `ip_address` argument specifies the IP address of the gateway or host that you want the active FT group member to track. Enter the IP address in dotted-decimal notation (for example, 192.168.12.101).

For example, to track the gateway located at 192.168.12.101, enter:

```
host1/Admin(config-ft-track-host)# track-host 192.168.12.101
```

Configuring a Probe on the Active Member for Host Tracking

Configure one or more probes on the active FT group member to track the health of the gateway or host. For details about creating probes, see the Cisco Application Control Engine Module Server Load-Balancing Configuration Guide.

To associate an existing probe with a gateway or host for tracking by the active member, use the `probe` command in FT track host configuration mode. The syntax of this command is as follows:

```
probe name priority number
```

The keyword and arguments are:

- `name`—Identifier of an existing probe that you want to associate with a gateway or host for tracking.
- `priority number`—Specifies the priority of the probe sent by the active member. Enter 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 gateway or host that the probe is tracking. If the probe goes down, the ACE decrements the priority of the FT group on the active member by the value of the `number` argument. If the resulting priority of the FT group on the active member is less than the priority of the FT group on the standby member, a switchover occurs.
If you remove a probe from the active FT group member configuration and you have not configured a tracking priority for the FT group (see the “Configuring a Priority on the Active Member for Multiple Probes” section), the ACE increments the net FT group priority by the priority value of the deleted probe. You cannot delete a probe from the running-configuration file if the ACE is using the probe for tracking.

For example, enter:

```
host1/Admin(config-ft-track-host)# probe TCP_PROBE1 priority 50
```

To remove the tracking probe from the active member, enter:

```
host1/Admin(config-ft-track-host)# no probe TCP_PROBE1
```

### Configuring a Priority on the Active Member for Multiple Probes

You can assign a tracking priority that the active member uses when multiple tracking probes are defined. To assign a priority for multiple probes on the active member, use the `priority` command in FT track host configuration mode. The syntax of this command is as follows:

```
priority number
```

The `number` argument specifies the priority of the probes on the active member. Enter a priority value 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 gateway or host that the probes are tracking. If all the probes go down, the ACE decrements the priority of the FT group on the active member by the value of the `number` argument. If the resulting priority of the FT group on the active member is less than the priority of the FT group on the standby member, a switchover occurs.

For example, enter:

```
host1/Admin(config-ft-track-host)# priority 50
```

To reset the priority to the default value of 0, enter:

```
host1/Admin(config-ft-track-host)# no priority 50
```
Configuring the Gateway or Host IP Address Tracked by the Standby Member

To allow the standby member to track a gateway or host, you need to configure the IP address of the gateway or host. To configure the IP address, use the `peer track-host` command in FT track host configuration mode. The syntax of this command is as follows:

```
peer track-host ip_address
```

The `ip_address` argument specifies the IP address of the gateway or host that you want the standby FT group member to track. Enter the IP address in dotted-decimal notation (for example, 172.16.27.1).

For example, to track the gateway located at 172.16.27.1, enter:

```
host1/Admin(config-ft-track-host)# peer track-host 172.16.27.1
```

To remove the host tracked by the standby member, enter:

```
host1/Admin(config-ft-track-host)# no peer track-host 172.16.27.1
```

Configuring a Probe on the Standby Member for Host Tracking

Configure one or more probes on the standby member to track the health of the gateway or host. For details about creating probes, see the *Cisco Application Control Engine Module Server Load-Balancing Configuration Guide*. To associate an existing probe with a gateway or host for tracking by the standby member, use the `peer probe` command in FT track host configuration mode. The syntax of this command is as follows:

```
peer probe name priority number
```

The keyword and arguments are:

- `name`—Identifier of an existing probe that you want to associate with a gateway or host for tracking
- `priority number`—Specifies the priority of the probe sent by the standby member. Enter 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 gateway or host that the probe is tracking. If the probe goes down, the ACE decrements the priority of the FT group on the standby member by the value of the `number` argument.
For example, enter:

```bash
host1/Admin(config-ft-track-host)# peer probe TCP_PROBE1 priority 25
```

To remove the tracking probe from the standby member, enter:

```bash
host1/Admin(config-ft-track-host)# no peer probe TCP_PROBE1
```

### Configuring a Priority on the Standby Member for Multiple Probes

You can configure a tracking priority that the standby member of an FT group uses when multiple tracking probes are defined. To assign a priority for multiple probes on the standby member, use the `peer priority` command in FT track host configuration mode. The syntax of this command is as follows:

```
peer priority number
```

The `number` argument specifies the priority of the probes configured for the gateway or host on the standby member. Enter a priority value 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 gateway or host that the probes are tracking. If all the probes go down, the ACE decrements the priority of the FT group on the standby member by the value of the `number` argument.

For example, enter:

```bash
host1/Admin(config-ft-track-host)# peer priority 25
```

To reset the multiple-probe priority to the default value of 0 on the standby member, enter:

```bash
host1/Admin(config-ft-track-host)# no peer priority 25
```

### Example of a Tracking Configuration for a Gateway

The following example demonstrates a tracking configuration for a gateway on the active member of an FT group:

```
ft track host TRACK_GATEWAY
  track-host 192.161.100.1
  probe GATEWAY_TRACK1 priority 10
  probe GATEWAY_TRACK2 priority 20
  priority 50
```
In this configuration example, if the GATEWAY_TRACK1 probe goes down, the ACE reduces the priority of the FT group on the active member by 10. If the GATEWAY_TRACK2 probe goes down, the ACE reduces the priority of the FT group on the active member by 20. If both probes go down, the ACE reduces the priority of the FT group on the active member by 50. If at any time 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.

To configure tracking on the standby member, use the `peer` commands described in the “Configuring a Probe on the Standby Member for Host Tracking” and the “Configuring a Priority on the Standby Member for Multiple Probes” sections.

### Configuring Tracking and Failure Detection for an Interface

This section describes the commands that you enter to configure tracking and failure detection for an interface. It contains the following topics:

- Creating a Tracking and Failure Detection Process for an Interface
- Configuring the Interface Tracked by the Active Member
- Configuring a Priority for a Tracked Interface on the Active Member
- Configuring the Interface Tracked by the Standby Member
- Configuring a Priority for a Tracked Interface on the Standby Member
- Example of a Tracking Configuration for an Interface

### Creating a Tracking and Failure Detection Process for an Interface

To create a tracking and failure detection process for an interface, use the `ft track interface` command in configuration mode. The syntax of this command is as follows:

```
ft track interface name
```

For the `name` argument, enter a unique identifier for the tracking process as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
Chapter 6      Configuring Redundant ACE Modules

Configuring Tracking and Failure Detection

Note

You cannot delete an interface if the ACE is using the interface for tracking. Also, you cannot configure the FT VLAN for tracking.

For example, enter:

host1/Admin(config)# ft track interface TRACK_VLAN100

To remove the interface-tracking process, enter:

host1/Admin(config)# no ft track interface TRACK_VLAN100

Configuring the Interface Tracked by the Active Member

To configure the interface that you want the active member to track, use the track-interface vlan command in FT track interface configuration mode. The syntax of this command is as follows:

```
track-interface vlan vlan_id
```

For the `vlan_id` argument, enter the VLAN ID of an existing VLAN configured on the active member as an integer from 2 to 4094.

For example, to track the critical interface VLAN 100, enter:

host1/Admin(config-ft-track-intf)# track-interface vlan 100

To remove VLAN 100 from the tracking process, enter:

host1/Admin(config-ft-track-intf)# no track-interface vlan 100

Configuring a Priority for a Tracked Interface on the Active Member

To assign a priority to the interface that the active member is tracking, use the priority command in FT track interface configuration mode. The syntax of this command is as follows:

```
priority number
```

The `number` argument specifies the priority of the interface on the active member. Enter a priority value 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 interface that you are tracking.
If the tracked interface goes down, the ACE decrements the priority of the FT group on the active member by the value of the `number` argument. 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.

For example, enter:

```
host1/Admin(config-ft-track-intf)# priority 50
```

To reset the interface priority on the active member to the default value of 0, enter:

```
host1/Admin(config-ft-track-intf)# no priority 50
```

### Configuring the Interface Tracked by the Standby Member

To configure the interface that you want the standby member to track, use the `peer track-interface vlan` command in FT track interface configuration mode. The syntax of this command is as follows:

```
peer track-interface vlan vlan_id
```

For the `vlan_id` argument, enter the VLAN ID of an existing VLAN configured on the standby member as an integer from 2 to 4094.

For example, to track the critical interface VLAN 200, enter:

```
host1/Admin(config-ft-track-intf)# peer track-interface vlan 200
```

To remove VLAN 200 from the tracking process, enter:

```
host1/Admin(config-ft-track-intf)# no peer track-interface vlan 200
```

### Configuring a Priority for a Tracked Interface on the Standby Member

To assign a priority to the tracked interface that the standby member is tracking, use the `peer priority` command in FT track interface configuration mode. The syntax of this command is as follows:

```
peer priority number
```

The `number` argument specifies the priority of the interface on the standby member. Enter a priority value 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 interface that you are tracking.
If the tracked interface goes down, the ACE decrements the priority of the FT group on the standby member by the value of the `number` argument. 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.

For example, enter:

```
host1/Admin(config-ft-track-intf)# peer priority 25
```

To reset the interface priority on the standby member to the default value of 0, enter:

```
host1/Admin(config-ft-track-intf)# no peer priority 25
```

### Example of a Tracking Configuration for an Interface

The following example demonstrates a tracking configuration for an interface on the active member of an FT group:

```
ft track interface TRACK_VLAN100
  track-interface vlan 100
  priority 50
```

In the above configuration example, if VLAN 100 goes down, the ACE reduces the priority of the FT group on the active member by 50. If at any time 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.

To configure tracking on the standby member, use the `peer` commands described in the “Configuring the Interface Tracked by the Standby Member” and the “Configuring a Priority for a Tracked Interface on the Standby Member” sections.
Configuring Tracking and Failure Detection for an HSRP Group

This section describes the commands required to configure a tracking and failure detection process for a Hot Standby Router Protocol (HSRP) group that you have previously configured on the Catalyst 6500 supervisor engine. It contains the following topics:

- Before You Begin
- Creating a Tracking and Failure Detection Process for an HSRP Group
- Configuring the HSRP Group to Track on the Active Member
- Configuring a Priority for the HSRP Group Tracked by the Active Member
- Configuring the HSRP Group to Track on the Standby Member
- Configuring a Priority for a Tracked HSRP Group on the Standby Member
- Example of a Tracking Configuration for an HSRP Group

Before You Begin

Note

For best results, observe the following configurational requirements before you attempt to configure HSRP tracking and failure detection on the ACE.

Before you configure an HSRP tracking and failure detection process on the ACE, you must configure the HSRP group on the supervisor engine. For example, if the HSRP group (including the name) is configured on the supervisor engine and it is not in the Active or the Standby state, you will see the following output when you enter the `show ft track detail` command on the ACE:

```
Track type                   : TRACK_HSRP
HSRP Group Name              : test
State                        : TRACK_DOWN (HSRP Group does not exist on the Supervisor or it is in the INIT State)
Priority                     : 20
Transitions                  : 1
```
For example, if the HSRP group is in the Standby state, you will see the following output when you enter the `show ft track detail` command on the ACE:

- **Track type**: TRACK_HSRP
- **HSRP Group Name**: test
- **State**: TRACK_DOWN (HSRP Group is Standby on the Supervisor)
- **Priority**: 20
- **Transitions**: 1

For example, if the HSRP group is in the Active state, you will see the following output when you enter the `show ft track detail` command on the ACE:

- **Track type**: TRACK_HSRP
- **HSRP Group Name**: test
- **State**: TRACK_UP
- **Priority**: 20
- **Transitions**: 2

If the HSRP group (including the name) is configured on the supervisor engine after the HSRP tracking process is initially configured on the ACE, you may or may not obtain the expected results when you enter the `show ft track detail` command on the ACE.

If the HSRP group name is changed on the supervisor engine after the HSRP tracking process is configured on the ACE, further state notifications will not be sent to the ACE. You must delete the HSRP tracking process on the ACE after the HSRP group name is changed on the supervisor engine.

### Creating a Tracking and Failure Detection Process for an HSRP Group

To create a tracking and failure detection process for an HSRP group, use the `ft track hsrp` command in configuration mode. The syntax of this command is as follows:

```
ft track hsrp tracking_process_name
```

For the `tracking_process_name` argument, enter a unique identifier of the tracking process as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters. The ACE allows you to track up to 250 HSRP groups.

For example, enter:

```
host1/Admin(config)# ft track hsrp HSRPTRACK_PROCESS1
host1/Admin(config-ft-track-hsrp)#
```
To remove the HSRP group-tracking process, enter:

```
host1/Admin(config)# no ft track hsrp HSRP_TRACK_PROCESS1
```

### Configuring the HSRP Group to Track on the Active Member

To track an HSRP group on the active member of an FT group, use the `track-hsrp` command in FT track-HSRP configuration mode. The syntax of this command is as follows:

```
track-hsrp name
```

For the `name` argument, enter the identifier of an HSRP group previously configured on the Catalyst supervisor that you want to track on the active member. Enter the name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters. The ACE allows you to track up to 250 HSRP groups.

To obtain the correct HSRP group identifier to use for tracking on the ACE, enter the `show standby vlan` command on the Catalyst 6500 series switch or 7600 series router.

For example, enter the following command:

```
sh-ace-6k-1# show standby vlan 120
Vlan120 - Group 120
  Local state is Active, priority 200, may preempt
  Hellotime 3 sec, holdtime 10 sec
  Next hello sent in 2.022
  Virtual IP address is 192.168.120.254 configured
  Active router is local
  Standby router is 192.168.120.252 expires in 8.360
  Virtual mac address is 0000.0c07.ac78
  7 state changes, last state change 21:54:53
  Priority tracking 1 interface or object, 1 up:
  Interface or object Decrement State
  GigabitEthernet4/35          110      Up
```

Use the IP redundancy name (shown in bold in the above output example) as the HSRP group name. The switch or router automatically assigns this name to the HSRP group.

For example, enter:

```
host1/Admin(config-ft-track-hsrp)# track-hsrp hsrp-vl120-120
```
To remove the HSRP group from the tracking process, enter:

```
host1/Admin(config-ft-track-hsrp)# no track-hsrp
```

**Configuring a Priority for the HSRP Group Tracked by the Active Member**

To assign a priority to the HSRP group that you are tracking on the active member of an FT group, use the `priority` command in FT track HSRP configuration mode. The syntax of this command is as follows:

```
priority number
```

For the number argument, 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 by the value of the `number` argument. 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.

---

**Note**

When you configure HSRP tracking on the FT group member and the HSRP group does not exist on the supervisor engine, the ACE marks the tracking process as `TRACK_DOWN` and automatically decrements the net priority of the FT group by the tracking priority value.

For example, enter:

```
host1/Admin(config-ft-track-hsrp)# priority 50
```

To reset the priority to the default value of 0, enter:

```
host1/Admin(config-ft-track-hsrp)# no priority 50
```

**Configuring the HSRP Group to Track on the Standby Member**

To track an HSRP group on the standby member of an FT group, use the `peer track-hsrp` command in FT track HSRP configuration mode. The syntax of this command is as follows:

```
peer track-hsrp name
```
For the *name* argument, enter the identifier of an HSRP group previously configured on the supervisor engine that you want to track on the standby member of an FT group. Enter the name as an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

For example, enter:

```bash
host1/Admin(config-ft-track-hsrp)# peer track-hsrp HSRP_GRP1
```

To remove the HSRP group from the tracking process, enter:

```bash
host1/Admin(config-ft-track-hsrp)# no peer track-hsrp HSRP_GRP1
```

### Configuring a Priority for a Tracked HSRP Group on the Standby Member

To assign a priority to the HSRP group that you are tracking on the standby member of an FT group, use the `peer priority` command in FT track HSRP configuration mode. The syntax of this command is as follows:

```bash
peer priority number
```

For the *number* argument, 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 standby member by the value of the *number* argument.

For example, enter:

```bash
host1/Admin(config-ft-track-hsrp)# peer priority 25
```

To reset the priority to the default value of 0, enter:

```bash
host1/Admin(config-ft-track-hsrp)# no peer priority 25
```

### Example of a Tracking Configuration for an HSRP Group

The following example demonstrates a tracking configuration for an HSRP group on the active member of an FT group:

```bash
ft track hsrp TRACK_HSRP_GRP1
track-hsrp HSRP_GRP1
priority 50
```
In the configuration example, if the HSRP_GRP1 group goes down, the ACE reduces the priority of the FT group on the active member by 50. If at any time 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.

To configure tracking on the standby member, use the `peer` commands described in the “Configuring the HSRP Group to Track on the Standby Member” and the “Configuring a Priority for a Tracked HSRP Group on the Standby Member” sections.

### Example of a Redundancy Configuration

The following example illustrates a running-configuration that defines fault tolerance (FT) for a single ACE module operating in a redundancy configuration. You must configure a maximum of two ACE modules (peers) for redundancy to fail over from the active module to the standby module.

```
hostname ACE_Module_1

access-list ACL1 line 10 extended permit ip any any
```

```
class-map type management match-any L4_REMOTE-MGT_CLASS
  2 match protocol telnet any
  3 match protocol ssh any
  4 match protocol icmp any
  5 match protocol http any
  7 match protocol ssmtp any
  8 match protocol https any
```

This configuration addresses the following redundancy components:

- A dedicated FT VLAN for communication between the members of an FT group. You must configure this same VLAN on both peer modules.
- An FT peer definition.
- An FT group that is associated with the Admin context.
- A critical tracking and failure detection process for an interface.

The redundancy configuration appears in bold in the example.
policy-map type management first-match L4_REMOTE-MGT_POLICY
  class L4_REMOTE-MGT_CLASS
    permit

interface vlan 100
  ip address 192.168.83.219 255.255.255.0
  peer ip address 192.168.83.230 255.255.255.0
  alias 192.168.83.200 255.255.255.0
  access-group input ACL1
  service-policy input L4_REMOTE-MGT_POLICY
  no shutdown

ft interface vlan 200
  ip address 192.168.1.1 255.255.255.0
  peer ip address 192.168.1.2 255.255.255.0
  no shutdown

ft peer 1
  ft-interface vlan 200
  heartbeat interval 300
  heartbeat count 10

ft group 1
  peer 1
  priority 200
  associate-context Admin
  inservice

ft track interface TRACK_VLAN100
  track-interface vlan 100
  peer track-interface vlan 200
  priority 50
  peer priority 5

ip route 0.0.0.0 0.0.0.0 192.168.83.1
Displaying Redundancy Information

This section describes how you can use the `show` commands to display configuration information and statistics for your redundancy configuration and contains the following topics:

- Displaying Redundancy Configurations
- Displaying FT Group Information
- Displaying the Redundancy Internal Software History
- Displaying the IDMAP Table
- Displaying Memory Statistics
- Displaying Peer Information
- Displaying FT Statistics
- Displaying FT Tracking Information

Displaying Redundancy Configurations

To display redundancy configurations, use the `show running-config ft` command in Exec mode. The syntax of this command is as follows:

```
show running-config ft
```

For example, enter:

```
host1/Admin# show running-config ft
```

Displaying FT Group Information

To display redundancy statistics per context, use the `show ft group` command in Exec mode. The syntax of this command is as follows:

```
show ft group {brief | [[group_id] [detail | status | summary]]}
```
The keywords, arguments, and options are:

- **brief**—Displays the group ID, local state, peer state, context name, and context ID of all the FT groups that are configured in the ACE.

- **group group_id**—Displays FT group statistics for the specified FT group. In the Admin context, this keyword displays statistics for all FT groups in the ACE. Also, in the Admin context, you can specify an FT group number to display statistics for an individual group. In a user context, this keyword displays statistics only for the FT group to which the user context belongs.

- **detail**—Displays detailed information for all FT groups or the specified FT group. The **detail** keyword includes the status of autosync and whether it is disabled or enabled for both the running-config and the startup-config.

- **status**—Displays the current operating status for all FT groups or the specified FT group.

- **summary**—Displays summary information for all FT groups or the specified FT group.

For example, enter:

```
host1/Admin# show ft group 1 detail
```

Table 6-2 describes the fields in the **show ft group** command output.

**Table 6-2 Field Descriptions for the show ft group Command Output**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FT Group</td>
<td>FT group identifier.</td>
</tr>
<tr>
<td>No. of Contexts</td>
<td>Number of contexts associated with the FT group.</td>
</tr>
<tr>
<td>Context Name</td>
<td>Name of the context associated with the FT group.</td>
</tr>
<tr>
<td>Context ID</td>
<td>Identifier of the context associated with the FT group.</td>
</tr>
<tr>
<td>Configured Status</td>
<td>Configured state of the FT group. Possible states are the in-service or out-of-service states.</td>
</tr>
</tbody>
</table>
### Table 6-2  Field Descriptions for the show ft group Command Output
(continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintenance Mode</td>
<td>Current maintenance mode of the local context in an FT group. Applications can turn on maintenance mode when there is an inability to communicate with the peer, license mismatches, too many application errors, and so on. Possible states are:</td>
</tr>
<tr>
<td></td>
<td>• MAINT_MODE_OFF—Maintenance mode is turned off.</td>
</tr>
<tr>
<td></td>
<td>• MAINT_MODE_PARTIAL—All standby contexts transition to the FSM_FT_STATE_STANDBY_COLD state (see the “My State” field description). The ACE enters this mode if configuration synchronization fails.</td>
</tr>
<tr>
<td></td>
<td>• MAINT_MODE_FULL—All contexts on the ACE become nonredundant causing their peer contexts to become active. The ACE enters this mode just before you reboot the module and is used primarily when you upgrade the ACE software.</td>
</tr>
</tbody>
</table>
Displaying Redundancy Information

Table 6-2  Field Descriptions for the show ft group Command Output
(continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| My State       | State of the FT group member in the local ACE. Possible states are:  
|                |   • FSM_FT_STATE_INIT—Configuration for the FT group exists but the group is not in service. This is the initial state for each member (local and peer) of an FT group.  
|                |   • FSM_FT_STATE_ELECT—When you configure the inservice command for an FT group, the local group member enters this state. Through the election process, the local context negotiates with its peer context in the FT group to determine their states. One member enters the ACTIVE state and the other member enters the STANDBY_CONFIG state.  
|                |   • FSM_FT_STATE_ACTIVE—Local member of the FT group is active and processing flows.  
|                |   • FSM_FT_STATE_STANDBY_COLD—Either the FT VLAN is down, but the peer device 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.  
|                |   • FSM_FT_STATE_STANDBY_CONFIG—Local standby context is waiting to receive configuration information from its active peer context in the FT group. The active peer context receives a notification to send a snapshot of its running-configuration file to the local standby context.  
|                |   • FSM_FT_STATE_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. |
Table 6-2   Field Descriptions for the show ft group Command Output  
(continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>My State (Cont.)</td>
<td>• FSM_FT_STATE_STANDBY_HOT—Local standby context has all the state information it needs to statefully assume the active state if a switchover occurs.</td>
</tr>
<tr>
<td>My Config Priority</td>
<td>Priority configured on the FT group in the local ACE.</td>
</tr>
<tr>
<td>My Net Priority</td>
<td>Priority of the FT group equal to the configured priority minus the priority of the FT tracking failures if any.</td>
</tr>
<tr>
<td>My Preempt</td>
<td>Preemption value of the FT group in the local ACE. Possible values are Enabled or Disabled.</td>
</tr>
<tr>
<td>Peer State</td>
<td>State of the FT group in the remote ACE. For possible state values, see the “My State” field description.</td>
</tr>
<tr>
<td>Peer Config Priority</td>
<td>Priority configured for the FT group in the remote ACE.</td>
</tr>
<tr>
<td>Peer Net Priority</td>
<td>Priority of the FT group in the remote ACE computed from the configured priority and the priority of the FT tracking failures.</td>
</tr>
<tr>
<td>Peer Preempt</td>
<td>Preemption value of the FT group in the remote ACE. Possible values are Enabled or Disabled.</td>
</tr>
<tr>
<td>Peer ID</td>
<td>FT peer identifier.</td>
</tr>
<tr>
<td>Last State Change Time</td>
<td>Time and date that the peer last changed from the active to standby state, or standby to active state.</td>
</tr>
<tr>
<td>Running Cfg Sync Enabled</td>
<td>Configured state of config sync for the running-config. Possible values are Enabled or Disabled.</td>
</tr>
<tr>
<td>Running Cfg Sync Status</td>
<td>Current status of config sync for the running-config. For example, Running configuration sync has completed.</td>
</tr>
<tr>
<td>Startup Cfg Sync Enabled</td>
<td>Configured state of config sync for the startup-config. Possible states are Enabled or Disabled.</td>
</tr>
<tr>
<td>Startup Cfg Sync Status</td>
<td>Current status of config sync for the startup-config. For example, Startup configuration sync is disabled.</td>
</tr>
</tbody>
</table>
Displaying the Redundancy Internal Software History

To display the redundancy internal software history, use the `show ft history` command in Exec mode. The syntax of this command is as follows:

```
show ft history {cfg_cntlr | ha_dp_mgr | ha_mgr}
```

The keywords are:

- `cfg_cntlr`—Displays the configuration controller debug log
- `ha_dp_mgr`—Displays the high availability (HA) dataplane manager debug log
- `ha_mgr`—Displays the HA manager debug log

For example, enter:

```
host1/Admin# show ft history cfg_cntlr
```
Displaying the IDMAP Table

The IDMAP table contains a list of the local ACE to peer (standby) ACE ID mappings for each of the seven object types in the ACE. The local ID and the peer ID for each object type may or may not be the same, but the mappings (local ID to peer ID) should be the same on both the active ACE and the standby ACE. The ACE uses these mappings for configuration synchronization and state replication. To display the IDMAP table, use the `show ft idmap` command in Exec mode. The syntax of this command is as follows:

```
show ft idmap
```

Table 6-3 lists the IDMAP table object types available in the ACE.

<table>
<thead>
<tr>
<th>Object Type</th>
<th>Object Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>REAL ID</td>
</tr>
<tr>
<td>1</td>
<td>RSERVER ID</td>
</tr>
<tr>
<td>2</td>
<td>SERVERFARM ID</td>
</tr>
<tr>
<td>3</td>
<td>POLICY ID</td>
</tr>
<tr>
<td>4</td>
<td>STICKY GROUP ID</td>
</tr>
<tr>
<td>5</td>
<td>IF ID</td>
</tr>
<tr>
<td>6</td>
<td>CONTEXT ID</td>
</tr>
</tbody>
</table>

For example, enter:

```
host1/Admin# show ft idmap
```
Displaying Memory Statistics

To display redundancy statistics per context, use the `show ft memory` command in Exec mode. The syntax of this command is as follows:

```plaintext
show ft memory [detail]
```

The optional `detail` keyword displays detailed HA manager memory statistics in the Admin context only.

For example, enter:

```
host1/Admin# show ft memory detail
```

Displaying Peer Information

To display peer information, use the `show ft peer` command in Exec mode. The syntax of this command is as follows:

```plaintext
show ft peer peer_id {detail | status | summary}
```

The keywords and arguments are:

- `peer_id`—Unique identifier of the remote peer
- `detail`—Displays detailed peer information
- `status`—Displays the current operating status of the peer
- `summary`—Displays summary peer information

For example, enter:

```
host1/Admin# show ft peer 1
```

Table 6-4 describes the fields in the `show ft peer` command output.
### Table 6-4 Field Descriptions for the show ft peer Command Output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer ID</td>
<td>Identifier of the remote context in the FT group.</td>
</tr>
<tr>
<td>State</td>
<td>Current state of the peer. Possible states are:</td>
</tr>
<tr>
<td></td>
<td>FSM_PEER_STATE_INIT—Initial state of the peer after you configure it.</td>
</tr>
<tr>
<td></td>
<td>FSM_PEER_STATE_MY_IPADDR—Local ACE IP address is missing. Waiting for the local IP address to be configured.</td>
</tr>
<tr>
<td></td>
<td>FSM_PEER_STATE_PEER_IPADDR— Peer IP address is missing. Waiting for the peer IP address to be configured.</td>
</tr>
<tr>
<td></td>
<td>FSM_PEER_STATE_START_HB—Peer configuration is complete. Starting the heartbeat to see if there is a peer device.</td>
</tr>
</tbody>
</table>
### Table 6-4  
Field Descriptions for the show ft peer Command Output (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State (continued)</td>
<td>FSM_PEER_STATE_TL_SETUP—Heartbeat has detected the presence of the peer device. Redundancy is in the process of establishing a TCP connection to the peer. This connection carries configuration data, application state information, and redundancy protocol packets.</td>
</tr>
<tr>
<td></td>
<td>FSM_PEER_STATE_SRG_CHECK—Checking for software version compatibility with the peer device.</td>
</tr>
<tr>
<td></td>
<td>FSM_PEER_STATE_LIC_CHECK—Checking for license compatibility with the peer device.</td>
</tr>
<tr>
<td></td>
<td>FSM_PEER_STATE_COMPATIBLE—Version and license checks indicate that the peer is compatible for redundancy.</td>
</tr>
<tr>
<td></td>
<td>FSM_PEER_STATE_FT_VLAN_DOWN—FT VLAN is down, but, through the query interface, the local ACE has determined that the peer is still alive.</td>
</tr>
<tr>
<td></td>
<td>FSM_PEER_STATE_DOWN—Peer device is down.</td>
</tr>
<tr>
<td></td>
<td>FSM_PEER_STATE_ERROR—Status of whether an error has occurred with the peer. Possible errors are version mismatch, license mismatch, or failure to establish a TCP connection to the peer. A syslog message appears with more detailed information.</td>
</tr>
</tbody>
</table>
### Table 6-4  Field Descriptions for the show ft peer Command Output (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Maintenance Mode       | Current maintenance mode of the peer context in an FT group. Applications can turn on maintenance mode when there is an inability to communicate with the peer, license mismatches, too many application errors, and so on. Possible states are:  
  - MAINT_MODE_OFF—Maintenance mode is turned off.  
  - MAINT_MODE_PARTIAL—All standby contexts transition to the STANDBY_COLD state. The ACE enters this mode if configuration synchronization fails.  
  - MAINT_MODE_FULL—All contexts on the ACE become nonredundant causing their peer contexts to become active. The ACE enters this mode just before you reboot the module and is used primarily when you upgrade the ACE software. |
| FT VLAN                | Identifier of the interface that is configured as the FT VLAN or Not Configured.                                                              |
| FT VLAN IF State       | Current status of the FT VLAN interface. Possible states are UP or DOWN.                                                                     |
| My IP Addr             | IP address of the local ACE.                                                                                                                  |
| Peer IP Addr           | IP address of the peer ACE.                                                                                                                   |
| Query VLAN             | Identifier of the interface that is configured as the query VLAN or Not Configured.                                                           |
| Query VLAN IF State    | Current status of the Query VLAN interface (if configured). Possible states are UP or DOWN.                                                   |
| Peer Query IP Addr     | IP address of the query interface used to obtain the state of the peer’s health when the FT VLAN is down.                                      |
| Heartbeat interval     | Time in seconds that the ACE waits between sending heartbeat packets.                                                                          |
| Heartbeat Count        | Number of missed heartbeats that an ACE must detect before declaring the peer down.                                                           |
### Table 6-4  Field Descriptions for the show ft peer Command Output (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tx Packets</td>
<td>Total number of packets that the local ACE sent to the peer.</td>
</tr>
<tr>
<td>Tx Bytes</td>
<td>Total number of bytes that the local ACE sent to the peer.</td>
</tr>
<tr>
<td>Rx Packets</td>
<td>Total number of packets that the local ACE received from the peer.</td>
</tr>
<tr>
<td>Rx Bytes</td>
<td>Total number of bytes that the local ACE received from the peer.</td>
</tr>
<tr>
<td>Rx Error Bytes</td>
<td>Total number of error bytes that the local ACE received from the peer.</td>
</tr>
<tr>
<td>Tx Keepalive Packets</td>
<td>Total number of keepalive packets that the local ACE sent to the peer.</td>
</tr>
<tr>
<td>Rx Keepalive Packets</td>
<td>Total number of keepalive packets that the local ACE received from the peer.</td>
</tr>
<tr>
<td>TL_CLOSE Count</td>
<td>Number of Transport Layer close events (TL_CLOSE) received on the redundant TCP connection from the TL driver.</td>
</tr>
<tr>
<td>FT_VLAN_DOWN Count</td>
<td>Number of times that the FT VLAN was unavailable.</td>
</tr>
<tr>
<td>PEER_DOWN Count</td>
<td>Number of times that the remote ACE was unavailable.</td>
</tr>
<tr>
<td>SRG Compatibility</td>
<td>Status of whether the software version of the local ACE and the software version of the peer ACE are compatible. Possible states are the INIT, COMPATIBLE, or INCOMPATIBLE state.</td>
</tr>
<tr>
<td>License Compatibility</td>
<td>Status of whether the license of the local ACE and the license of the peer ACE are compatible. Possible states are the INIT, COMPATIBLE, or INCOMPATIBLE state.</td>
</tr>
<tr>
<td>FT Groups</td>
<td>Number of FT groups.</td>
</tr>
</tbody>
</table>
Displaying FT Statistics

To display peer information, use the `show ft stats` command in Exec mode. The syntax of this command is as follows:

```
show ft stats group_id
```

The `group_id` argument displays additional load-balancing statistics (LB statistics) for the specified group.

For example, enter:

```
host1/Admin# show ft stats 1
```

Table 6-5 describes the fields in the `show ft stats` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HA Heartbeat Statistics</td>
<td></td>
</tr>
<tr>
<td>Number of Heartbeats Sent</td>
<td>Total number of heartbeat packets sent by the local ACE.</td>
</tr>
<tr>
<td>Number of Heartbeats Received</td>
<td>Total number of heartbeat packets received by the local ACE.</td>
</tr>
<tr>
<td>Number of Heartbeats Missed</td>
<td>Total number of heartbeat intervals that transpired with no heartbeats received.</td>
</tr>
<tr>
<td>Number of Unidirectional HBs Received</td>
<td>Number of heartbeats (HBs) received by the local peer that indicate the remote peer is not receiving HBs. The remote peer is sending heartbeats, but not receiving any.</td>
</tr>
</tbody>
</table>

*Note* Both peer modules send heartbeat packets and each packet indicates whether the other peer has been receiving heartbeats.
### Table 6-5  Field Descriptions for the show ft stats Command Output (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of HB Timeout Mismatches</td>
<td>Number of times that the local peer received a heartbeat (HB) from the remote peer with a mismatched heartbeat interval. If the heartbeat intervals do not match, a peer adjusts its interval to the lower of the two intervals. Note The heartbeat interval should be the same on both peer modules. Each heartbeat packet contains the configured interval in the packet. When a peer receives a heartbeat packet, it checks to see if the interval in the heartbeat packet matches the interval configured locally.</td>
</tr>
<tr>
<td>Num of Peer Up Events Sent</td>
<td>Number of times that the local ACE sent a Peer Up message to the remote ACE.</td>
</tr>
<tr>
<td>Num of Peer Down Events Sent</td>
<td>Number of times that the local ACE sent a Peer Down message to the remote ACE.</td>
</tr>
<tr>
<td>Successive HBs Miss Intervals Counter</td>
<td>Number of successive heartbeat misses detected by the heartbeat module.</td>
</tr>
<tr>
<td>Successive Uni HBsRecv Counter</td>
<td>Number of successive unidirectional heartbeats received by the heartbeat module.</td>
</tr>
</tbody>
</table>

### LB Stats for FT Group N

<table>
<thead>
<tr>
<th>Send-side Stats</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Sticky Entries Shared</td>
<td>Number of sticky database entries that the local ACE sent to the remote ACE.</td>
</tr>
<tr>
<td>Number of Replication Packets Sent</td>
<td>Number of packets that contain replication information that the local ACE sent to the remote ACE.</td>
</tr>
</tbody>
</table>
Chapter 6 Configuring Redundant ACE Modules

Displaying Redundancy Information

To display tracking information, use the `show ft track` command in Exec mode. The syntax of this command is as follows:

```
show ft track {detail | status | summary}
```

The keywords are:
- `detail`—Displays detailed tracking information
- `status`—Displays the current operating status of the peer plus additional information
- `summary`—Displays summary peer information

For example, enter:

```
host1/Admin# show ft track detail
```
For more information about the `show ft track` command output for HSRP tracking, see the “Before You Begin” section.

Table 6-6 describes the fields in the `show ft track` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FT Group</td>
<td>FT group identifier.</td>
</tr>
<tr>
<td>Status</td>
<td>Configured state of the FT group. Possible states are the in-service or out-of-service state.</td>
</tr>
<tr>
<td>Maintenance Mode</td>
<td>Current maintenance mode of the local context in an FT group. Applications can turn on maintenance mode when there is an inability to communicate with the peer, license mismatches, too many application errors, and so on. Possible states are:</td>
</tr>
<tr>
<td></td>
<td>• MAINT_MODE_OFF—Maintenance mode is turned off.</td>
</tr>
<tr>
<td></td>
<td>• MAINT_MODE_PARTIAL—All standby contexts transition to the FSM_FT_STATE_STANDBY_COLD state (see the “My State” field description). The ACE enters this mode if configuration synchronization fails.</td>
</tr>
<tr>
<td></td>
<td>• MAINT_MODE_FULL—All contexts on the ACE become nonredundant causing their peer contexts to become active. The ACE enters this mode just before you reboot the module and is used primarily when you upgrade the ACE software.</td>
</tr>
</tbody>
</table>
### Table 6-6  Field Descriptions for the show ft track Command

*Output (continued)*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>My State</td>
<td>State of the FT group member in the local ACE. Possible states are:</td>
</tr>
<tr>
<td></td>
<td>- FSM_FT_STATE_INIT—Initial state for each member (local and peer) of an FT group. The configuration for the FT group exists but the group is not yet in service.</td>
</tr>
<tr>
<td></td>
<td>- FSM_FT_STATE_ELECT—State that the local group member enters when you configure the <code>inservice</code> command for an FT group. Through the election process, the local context negotiates with its peer context in the FT group to determine their states. One member enters the ACTIVE state and the other member enters the STANDBY_CONFIG state.</td>
</tr>
<tr>
<td></td>
<td>- FSM_FT_STATE_ACTIVE—State that indicates that the local member of the FT group is active and processing flows.</td>
</tr>
<tr>
<td></td>
<td>- FSM_FT_STATE_STANDBY_COLD—State that indicates if either the FT VLAN is down but the peer device 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.</td>
</tr>
<tr>
<td></td>
<td>- FSM_FT_STATE_STANDBY_CONFIG—State that indicates that the local standby context is waiting to receive configuration information from its active peer context in the FT group. The active peer context receives a notification to send a snapshot of its running-configuration file to the local standby context.</td>
</tr>
<tr>
<td></td>
<td>- FSM_FT_STATE_STANDBY_BULK—State that indicates that the 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.</td>
</tr>
</tbody>
</table>
### Table 6-6  Field Descriptions for the show ft track Command Output (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>My State (Cont.)</td>
<td>• FSM_FT_STATE_STANDBY_HOT—State that indicates that the local standby context has all the state information it needs to statefully assume the active state if a switchover occurs.</td>
</tr>
<tr>
<td>My Config Priority</td>
<td>Priority configured on the FT group in the local ACE.</td>
</tr>
<tr>
<td>My Net Priority</td>
<td>Priority of the FT group equal to the configured priority minus the priority of the FT tracking process failures, if any.</td>
</tr>
<tr>
<td>My Preempt</td>
<td>Preemption value of the FT group in the local ACE. Possible values are Enabled or Disabled.</td>
</tr>
<tr>
<td>Context Name</td>
<td>Name of the context that is associated with the FT group.</td>
</tr>
<tr>
<td>Context ID</td>
<td>Identifier of the context that is associated with the FT group.</td>
</tr>
<tr>
<td>Track Type</td>
<td>Type of object being tracked. Possible values are TRACK_HOST, TRACK_HSRP, or TRACK_INTERFACE.</td>
</tr>
<tr>
<td>HSRP Group name</td>
<td>Identifier of the HSRP group that is configured on the Catalyst 6500 series switch that you are tracking.</td>
</tr>
<tr>
<td>State</td>
<td>State of the tracking process. Possible values are TRACK_UP or TRACK_DOWN.</td>
</tr>
<tr>
<td>Priority</td>
<td>Priority of the tracking process.</td>
</tr>
<tr>
<td>Transitions</td>
<td>Number of times that the active member of the FT group switched over to the standby member.</td>
</tr>
<tr>
<td>Probe Count</td>
<td>Number of probes associated with a TRACK_HOST process.</td>
</tr>
<tr>
<td>Probes Down</td>
<td>Number of failed probes.</td>
</tr>
</tbody>
</table>
Clearing Redundancy Statistics

To clear redundancy statistics, use the commands described in the following sections. You must enter all commands in this section in the Admin context unless otherwise indicated.

Note

If you configure redundancy on the ACE, then you must explicitly clear statistics on both the active and the standby ACEs. Clearing statistics on the active module only does not clear the statistics on the standby module.

This section contains the following topics:
- Clearing Transport-Layer Statistics
- Clearing Heartbeat Statistics
- Clearing Tracking-Related Statistics
- Clearing All Redundancy Statistics
- Clearing the Redundancy History

Clearing Transport-Layer Statistics

To clear all transport layer-related counters that the ACE displays as part of the show ft peer detail command output, use the clear ft ha-stats command in Exec mode. The syntax of this command is as follows:

```
clear ft ha-stats
```

This command clears the following transport-layer counters:
- Tx Packets
- Tx Bytes
- Rx Packets
- Rx Bytes
- Rx Error Bytes

For an explanation of these fields, see the “Displaying Peer Information” section.
Clearing Redundancy Statistics

For example, enter:

    host1/Admin# clear ft ha-stats

Clearing Heartbeat Statistics

To clear all heartbeat-related statistics, use the `clear ft hb-stats` command in Exec mode. When you enter this command for the first time, the ACE sets the heartbeat statistics counters to zero and stores a copy of the latest statistics locally. From that point on, when you enter the `show ft hb-stats` command, the ACE displays the difference between the statistics that are stored locally and the current statistics. The syntax of this command is as follows:

    clear ft hb-stats

For example, enter:

    host1/Admin# clear ft hb-stats

Clearing Tracking-Related Statistics

To clear tracking-related statistics for the Admin FT group only, a user context FT group only, or for all FT groups that are configured in the ACE, use the `clear ft-track stats` command in Exec mode. The syntax of this command is as follows:

    clear ft track-stats [all]

Use the optional `all` keyword in the Admin context only to clear tracking statistics for all FT groups that are configured in the ACE. If you enter this command in the Admin context without the `all` keyword, it clears the tracking statistics only for the FT group associated with the Admin context. In a user context, you cannot enter the `all` keyword, so you can clear the tracking statistics only for the FT group associated with the user context.

For example, to clear tracking statistics for all FT groups that are configured in the ACE, enter:

    host1/Admin# clear ft track-stats all
Clearing All Redundancy Statistics

To clear all redundancy statistics, including all TL, heartbeat, and tracking counters, use the `clear ft all` command in Exec mode in the Admin context only. The syntax of this command is as follows:

```
clear ft all
```

*Note*  
This command does not affect the redundancy history. To clear the redundancy history, use the `clear ft history` command. For details, see the “Clearing the Redundancy History” section.

For example, enter:

```
host1/Admin# clear ft all
```

Clearing the Redundancy History

To clear the redundancy history, use the `clear ft history` command in Exec mode in the Admin context only. The syntax of this command is as follows:

```
clear ft history {cfg_cntlr | ha_dp_mgr | ha_mgr}
```

The keywords are:

- `cfg_cntlr`—Clears the Configuration Controller debug log
- `ha_dp_mgr`—Clears the HA (redundancy) dataplane manager debug log
- `ha_mgr`—Clears the HA (redundancy) manager debug log

For example, enter:

```
host1/Admin# clear ft history cfg_cntlr
```
This chapter describes how to configure Simple Network Management Protocol (SNMP) to query the Cisco Application Control Engine (ACE) module for Cisco Management Information Bases (MIBs) and to send event notifications to a network management system (NMS).

This chapter contains the following major sections:

- SNMP Overview
- SNMP Configuration Quick Start
- Configuring SNMP Users
- Defining SNMP Communities
- Configuring an SNMP Contact
- Configuring an SNMP Location
- Configuring SNMP Notifications
- Assigning a VLAN Interface as the Trap-Source Address in SNMPv1 Traps
- Accessing ACE User Context Data Through the Admin Context IP Address
- Configuring an SNMPv3 Engine ID for an ACE Context
- Configuring SNMP Management Traffic Services
- Example of an SNMP Configuration
- Displaying SNMP Statistics
SNMP Overview

SNMP is an application-layer protocol that facilitates the exchange of management information between an NMS, SNMP agents, and managed devices such as the ACE. You can configure the ACE to send traps (event notifications) to an NMS, or you can use the NMS to browse the MIBs that reside on the ACE.

The ACE contains an SNMP agent that provides support for network monitoring. The ACE supports SNMP Version 1 (SNMPv1), SNMP Version 2c (SNMPv2c), and SNMP Version 3 (SNMPv3).

SNMPv1 and SNMPv2c use a community string match for authentication. Community strings provide a weaker form of access control. SNMPv3 utilizes an SNMP user for authentication and provides improved access control by using strong authentication. SNMPv3 should be utilized instead of SNMPv1 and SNMPv2c wherever possible.

SNMPv3 is an interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by using a combination of authenticating and encrypting frames over the network. The SNMPv3 provides the following security features:

- Message integrity—Ensures that a packet has not been tampered with in-transit.
- Authentication—Determines that the message is from a valid source.
- Encryption—Scrambles the packet contents to prevent it from being seen by unauthorized sources.

This section contains the following topics:

- Managers and Agents
- SNMP Manager and Agent Communication
- SNMP Traps and Informs
- SNMPv3 CLI User Management and AAA Integration
- Supported MIBs and Notifications
- SNMP Limitations
Managers and Agents

SNMP uses software entities called managers and agents to manage network devices:

- The manager monitors and controls all other SNMP-managed devices (network nodes) in the network. At least one SNMP manager must be in a managed network. The manager is installed on a workstation somewhere in the network.

- An agent resides in a managed device (a network node). An agent is a specialized software module that receives instructions from the SNMP manager and also sends management information back to the SNMP manager as events occur. For example, an agent might report such data as the number of bytes and packets in and out of the device or the number of broadcast messages sent and received.

There are many different SNMP management applications, but they all perform the same basic task. These applications allow SNMP managers to communicate with agents to monitor, configure, and receive alerts from the network devices. The ACE supports traps and SNMP get requests but does not support SNMP set requests to configure values on the device. You can use any SNMP-compatible NMS to monitor the ACE.

In SNMP, each variable is referred to as a managed object. A managed object is anything that an agent can access and report back to the NMS. All managed objects are contained in the MIB, which is a database of the managed objects called MIB objects. Each MIB object controls one specific function, such as counting how many bytes are transmitted through an agent’s port. The MIB object consists of MIB variables, which define the MIB object name, description, and default value. The ACE maintains a database of values for each definition.

Browsing a MIB entails issuing an SNMP get request from the NMS. You can use any SNMPv3, MIB-II compliant browser to receive SNMP traps and browse MIBs.
SNMP Manager and Agent Communication

The SNMP manager and the agent can communicate in several ways. The Protocol Data Unit (PDU) is the message format that SNMP managers and agents use to send and receive information.

- The SNMP manager can perform the following operations:
  - Retrieve a value (a **get** operation) from an agent. The SNMP manager requests information from the agent, such as the number of users logged on to the agent device, or the status of a critical process on that device. The agent gets the value of the requested MIB object and sends the value back to the manager (a **get-response** operation). The variable binding (varbind) is a list of MIB objects that allows a request recipient to see what the originator wants to know. Variable bindings are object identifiers (OID)=value pairs that make it easy for the NMS to identify the information that it needs when the recipient fills the request and sends back a response.
  
  - Retrieve the value immediately after the variable that you name (a **get-next** operation). A **get-next** operation retrieves a group of values from a MIB by issuing a sequence of commands. By performing a **get-next** operation, you do not need to know the exact MIB object instance that you are looking for; the SNMP manager takes the variable that you name and then uses a sequential search to find the desired variables.
  
  - Retrieve a number of values (a **get-bulk** operation). The get-bulk operation retrieves large blocks of data, such as multiple rows in a table, which would otherwise require the transmission of many small blocks of data. The SNMP manager performs a number of **get-next** operations that you specify.

- An agent can send an unsolicited message to the SNMP manager at any time if a significant, predetermined event takes place on the agent. This message is called an event notification. SNMP event notifications (traps or inform requests) are included in many MIBs and help to alleviate the need for the NMS to frequently poll (gather information through a **get** operation) the managed devices. For details on MIB objects and SNMP notifications supported by the ACE, see the “Supported MIBs and Notifications” section.
SNMP Traps and Informs

You can configure the ACE to send notifications (such as traps or inform requests) to SNMP managers when particular events occur. In some instances, traps can be unreliable because the receiver does not send any acknowledgment when it receives a trap and the sender cannot determine if the trap was received. However, an SNMP manager that receives inform requests acknowledges the message with an SNMP Response PDU. If the sender never receives a Response, the inform request is usually retransmitted. Inform requests are more likely to reach their intended destination.

Notifications may contain a list of MIB variable bindings that clarify the status being relayed by the notification. The list of variable bindings associated with a notification is included in the notification definition in the MIB. For standard MIBs, Cisco has enhanced some notifications with additional variable bindings that further clarify the cause of the notification.

Note

The clogOriginID and clogOriginIDType variable bindings appended with each notification can be used by the NMS application to uniquely identify the device originating the trap. You can configure the values for clogOriginID and clogOriginIDType varbind to uniquely identify the device by using the `logging device-id` configuration mode command. For details on the `logging device-id` command, see the Cisco Application Control Engine Module System Message Guide.

Use the SNMP-TARGET-MIB to obtain more information on trap destinations and inform requests.

For details on SNMP notifications supported by the ACE, see the “Supported MIBs and Notifications” section.
SNMP Overview

SNMPv3 CLI User Management and AAA Integration

The ACE implements RFC 3414 and RFC 3415, including the SNMPv3 User-based Security Model (USM) for message security and role-based access control. SNMP v3 user management can be centralized at the authentication and accounting (AAA) server level (as described in the Cisco Application Control Engine Module Security Configuration Guide). This centralized user management allows the ACE SNMP agent to use the user authentication service of a AAA server. After user authentication is verified, the SNMP protocol data units (PDUs) further processed. The AAA server is also used to store user group names. SNMP uses the group names to apply the user access and role policy that is locally available in the ACE.

CLI and SNMP User Synchronization

Any configuration changes to the user group, role, or password, results in the database synchronization for both SNMP and AAA. To create a CLI user by using the username command, see the Cisco Application Control Engine Module Virtualization Configuration Guide. To create an SNMP user by using the snmp-server user command, see the “Configuring SNMP Users” section.

Users are synchronized as follows:

- If you delete a user by using the no username command, the user is also deleted from both SNMP and the CLI. However, if you delete a user by using the no snmp-server user command, the user is deleted only from SNMP and not from the CLI.
- User-role mapping changes are synchronized in SNMP and the CLI.

Note: When you specify a password in a localized key or encrypted format for security encryption, the password is not synchronized.

- The password specified in the username command is synchronized as the auth and priv passwords for the SNMP user.
- Existing SNMP users can continue to retain the auth and priv information without any changes.
If you create a new user that is not present in the SNMP database by using the `username` command without a password, the SNMP user is created with the `noAuthNoPriv` security level.

**Supported MIBs and Notifications**

Table 7-1 identifies the supported MIBs for the ACE.

<table>
<thead>
<tr>
<th>MIB Support</th>
<th>Capability MIB</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Supervisor Module MIBs</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CISCO-ENTITY-FRU-CONTROL-MIB</td>
<td>CISCO-ENTITY-FRU-CONTROL-CAPABILITY</td>
<td>Acts as an extension to the ENTITY-MIB. It monitors the operational state of the ACE. The CISCO-ENTITY-FRU-CONTROL-MIB is supported only in the Admin context.</td>
</tr>
<tr>
<td>CISCO-ENTITY-VENDORTYPE-OID-MIB</td>
<td>N/A</td>
<td>Defines the object identifiers (OIDs) assigned to various ACE components. The OIDs in this MIB are used by the <code>entPhysicalTable</code> of the ENTITY-MIB as values for the <code>entPhysicalVendorType</code> field in the <code>entPhysicalTable</code>. Each OID uniquely identifies a type of physical entity, such as a chassis, line cards, or port adapters. The following list contains the <code>entPhysicalVendorType</code> OID values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Product Name (PID)</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>entPhysicalVendorType</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ACE10-6500-K9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cevCat6kAce10K9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ACE20-MOD-K9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cevCat6kAce10K9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(cevModuleCat6000Type120)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Inlet Temperature</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cevSensorModuleInletTemp</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(cevSensor 36)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Outlet Temperature</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cevSensorModuleOutletTemp</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(cevSensor 35)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Other device temperature sensors</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cevSensorModuleDeviceTemp</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(cevSensor 31)</td>
</tr>
</tbody>
</table>
### SNMP Overview

#### Table 7-1  SNMP MIB Support (continued)

<table>
<thead>
<tr>
<th>MIB Support</th>
<th>Capability MIB</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENTITY-MIB</td>
<td>CISCO-ENTITY-CAPABILITY</td>
<td>Provides basic management and identification of physical and logical entities within a network device. Software support for the ENTITY-MIB focuses on the physical entities within the ACE. This MIB provides details on each module, power supply, and fan tray within a switch chassis. It gives enough information to correctly map the containment of these entities within the ACE, creating a chassis view. The ENTITY-MIB is supported only in the Admin context. The ENTITY-MIB is described in RFC 4133.</td>
</tr>
<tr>
<td>ENTITY-SENSOR-MIB</td>
<td>CISCO-ENTITY-SENSOR-RFC-CAPABILITY</td>
<td>Contains a single group called the entitySensorValueGroup, which allows objects to convey the current value and status of a physical sensor. The entitySensorValueGroup contains a single table, called the ent PhySensorTable, which provides a few read-only objects that identify the type of data units, scaling factor, precision, current value, and operational status of the sensor. The ENTITY-SENSOR-MIB is supported only in the Admin context. The ENTITY-SENSOR-MIB is described in RFC 3433.</td>
</tr>
</tbody>
</table>
Table 7-1  SNMP MIB Support (continued)

<table>
<thead>
<tr>
<th>MIB Support</th>
<th>Capability MIB</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMPv3 Agent MIBs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNMP-COMMUNITY-MIB</td>
<td>CISCO-SNMP-COMMUNITY-CAPABILITY</td>
<td>Contains objects for mapping between community strings and version-independent SNMP message parameters. In addition, this MIB provides a mechanism for performing source address validation on incoming requests and for selecting community strings based on target addresses for outgoing notifications. Note SNMP communities are applicable only for SNMPv1 and SNMPv2c. SNMPv3 requires user configuration information such as specifying the role group that the user belongs to, authentication parameters for the user, the authentication password, and message encryption parameters. The SNMP-COMMUNITY-MIB is described in RFC 3584.</td>
</tr>
<tr>
<td>SNMP-FRAMEWORK-MIB</td>
<td>CISCO-SNMP-FRAMEWORK-CAPABILITY</td>
<td>Defines the elements of SNMP Management Frameworks, including an SNMP engine and Access Control Subsystem. The SNMP-FRAMEWORK-MIB is described in RFC 3411.</td>
</tr>
<tr>
<td>SNMP-MPD-MIB</td>
<td>CISCO-SNMP-MPD-CAPABILITY</td>
<td>Describes the Message Processing Subsystem and Dispatcher for SNMP. The Dispatcher in the SNMP engine sends and receives SNMP messages. It also dispatches SNMP PDUs to SNMP applications. A Message Processing Model processes an SNMP version-specific message and coordinates the interaction with the Security Subsystem to ensure that proper security is applied to the SNMP message being handled. The SNMP-MPD-MIB is described in RFC 3412.</td>
</tr>
</tbody>
</table>
### SNMP Overview

SNMP-NOTIFICATION-MIB

Contains a table for the destination information and SNMP parameters in the management target message. Multiple transport end points may be associated with a particular set of SNMP parameters, or a particular transport end point may be associated with several sets of SNMP parameters.

The SNMP-TARGET-MIB is described in RFC 3413.

<table>
<thead>
<tr>
<th>MIB Support</th>
<th>Capability MIB</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP-NOTIFICATION-MIB</td>
<td>CISCO-SNMP-NOTIFICATION-CAPABILITY</td>
<td>Defines MIB objects that provide a mechanism to remotely configure the parameters used by an SNMP entity for the generation of notifications. The SNMP-NOTIFICATION-MIB is described in RFC 3413.</td>
</tr>
<tr>
<td>SNMP-TARGET-MIB</td>
<td>CISCO-SNMP-TARGET-CAPABILITY</td>
<td>Contains a table for the destination information and SNMP parameters in the management target message. Multiple transport end points may be associated with a particular set of SNMP parameters, or a particular transport end point may be associated with several sets of SNMP parameters. The SNMP-TARGET-MIB is described in RFC 3413.</td>
</tr>
</tbody>
</table>
SNMP-USER-BASED-SM-MIB

Provides management information definitions for the User-based Security Model (USM) for SNMPv3. The SNMPv3 architecture introduces the User-based Security Model (USM) for message security.

The USM module decrypts incoming messages. The module then verifies the authentication data and creates the PDUs. For outgoing messages, the USM module encrypts PDUs and generates the authentication data. The module then passes the PDUs to the message processor, which then invokes the dispatcher.

The USM module's implementation of the SNMP-USER-BASED-SM-MIB enables the SNMP manager to issue commands to manage users and security keys. The MIB also enables the agent to ensure that a requesting user exists and has the proper authentication information. When authentication is done, the request is carried out by the agent.

The SNMP-USER-BASED-SM-MIB is described in RFC 3414.

Note

User configuration is applicable only for SNMPv3; SNMPv1 and SNMPv2c use a community string match for user authentication.

Table 7-1   SNMP MIB Support (continued)

<table>
<thead>
<tr>
<th>MIB Support</th>
<th>Capability MIB</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP-USER-BASED-SM-MIB</td>
<td>CISCO-SNMP-USM-CAPABILITY</td>
<td>Provides management information definitions for the User-based Security Model (USM) for SNMPv3. The SNMPv3 architecture introduces the User-based Security Model (USM) for message security. The USM module decrypts incoming messages. The module then verifies the authentication data and creates the PDUs. For outgoing messages, the USM module encrypts PDUs and generates the authentication data. The module then passes the PDUs to the message processor, which then invokes the dispatcher. The USM module's implementation of the SNMP-USER-BASED-SM-MIB enables the SNMP manager to issue commands to manage users and security keys. The MIB also enables the agent to ensure that a requesting user exists and has the proper authentication information. When authentication is done, the request is carried out by the agent. The SNMP-USER-BASED-SM-MIB is described in RFC 3414.</td>
</tr>
</tbody>
</table>

Note

User configuration is applicable only for SNMPv3; SNMPv1 and SNMPv2c use a community string match for user authentication.
### SNMP Overview

The SNMP-VIEW-BASED-ACM-MIB specifies objects that are needed to control access to all MIB data that is accessible through the SNMP agent. Upon initialization, the VACM module registers as the access control module with the agent infrastructure. The VACM module implements access control checks according to several parameters that are derived from the SNMP message.

The SNMP-VIEW-BASED-ACM-MIB is described in RFC 3415.

### Other MIBs

<table>
<thead>
<tr>
<th>MIB Support</th>
<th>Capability MIB</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP-VIEW-BASED-ACM-MIB</td>
<td>CISCO-SNMP-VACM-CAPABILITY</td>
<td>Provides the View-based Access Control Model (VACM) for SNMPv3. The SNMPv3 architecture introduces VACM for access control. The SNMP-VIEW-BASED-ACM-MIB specifies objects that are needed to control access to all MIB data that is accessible through the SNMP agent. Upon initialization, the VACM module registers as the access control module with the agent infrastructure. The VACM module implements access control checks according to several parameters that are derived from the SNMP message. The SNMP-VIEW-BASED-ACM-MIB is described in RFC 3415.</td>
</tr>
</tbody>
</table>
| CISCO-AAA-SERVER-EXT-MIB | CISCO-AAA-SERVER-EXT-CAPABILITY    | Acts as an extension to CISCO-AAA-SERVER-MIB. It enhances the casConfigTable of the CISCO-AAA-SERVER-MIB to include other types of server addresses. The CISCO-AAA-SERVER-EXT-MIB manages the following configuration functions:  
  - Generic configurations as applied on the authentication and accounting module.  
  - Configuration settings (settings for all the AAA servers instrumented in one instance of this MIB).  
  - AAA server group configuration.  
  - Application-to-AAA function-to-server group mapping configuration. |
### SNMP Overview

The CISCO-AAA-SERVER-MIB provides the following information:

- A table for configuring AAA servers.
- Identities of external AAA servers.
- Statistics for each AAA function.
- Status of servers that provide AAA functions.

A server is defined as a logical entity that provides any of the AAA functions. The ACE can use a Remote Access Dial-In User Service (RADIUS), Terminal Access Controller Access Control System Plus (TACACS+), or Lightweight Directory Access Protocol (v3) (LDAP) protocols for remote authentication and designation of access rights.

### Table 7-1  SNMP MIB Support (continued)

<table>
<thead>
<tr>
<th>MIB Support</th>
<th>Capability MIB</th>
<th>Description</th>
</tr>
</thead>
</table>
| CISCO-AAA-SERVER-MIB      | CISCO-AAA-SERVER-CAPABILITY             | Provides configuration and statistics that reflect the state of an AAA server operation within the device and AAA communications with external servers. The CISCO-AAA-SERVER-MIB provides the following information:  
  - A table for configuring AAA servers.  
  - Identities of external AAA servers.  
  - Statistics for each AAA function.  
  - Status of servers that provide AAA functions. A server is defined as a logical entity that provides any of the AAA functions. The ACE can use a Remote Access Dial-In User Service (RADIUS), Terminal Access Controller Access Control System Plus (TACACS+), or Lightweight Directory Access Protocol (v3) (LDAP) protocols for remote authentication and designation of access rights. |
| CISCO-ENHANCED-SLB-MIB    | CISCO-ENHANCED-SLB-CAPABILITY           | Extends the tables that are defined in CISCO-SLB-MIB and CISCO-SLB-EXT-MIB and supports the following server load-balancing functions:  
  - A real server configuration with a real server that is identified by a name. The cesRserverTable provides information for real servers.  
  - A real server configuration in a server farm.  
  - A health probe configuration in a real server.  
  - A sticky configuration for an HTTP header, an HTTP cookie and client IP address, and Secure Sockets Layer (SSL). The slbEntity Index used in the table is the slot number of the ACE. |
### Table 7-1 SNMP MIB Support (continued)

<table>
<thead>
<tr>
<th>MIB Support</th>
<th>Capability MIB</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO-IF-EXTENSION-MIB</td>
<td>CISCO-IF-EXTENSION-CAPABILITY</td>
<td>Provides a table that returns ifName to ifIndex mapping to assign the ifIndex to interfaces. The CISCO-IF-EXTENSION-MIB is described in RFC 2863.</td>
</tr>
<tr>
<td>CISCO-IP-PROTOCOL-FILTER-MIB</td>
<td>CISCO-IP-PROTOCOL-FILTER-CAPABILITY</td>
<td>Manages information to support packet filtering on IP protocols (RFC 791). The cippIpProfileTable allows users to create, delete, and get information about filter profiles. Filter profiles are uniquely identified by the profile names. Filter profiles can be either simple or extended usage types. The usage type cannot be changed once it has been created. The cippIpProfileTable applies the filtering profiles to device interfaces that run IP. A filter profile can be applied to multiple interfaces. The cippIpFilterTable contains ordered lists of IP filters for all filtering profiles. Filters and profiles are related if they have the same filter profile name. Filters can be created only if their associated filter profiles already exist in the cippIpProfileTable. Filters of the same profile name belong to a common profile. The interface-based cippIpProfileTable can be configured with information that is independent of the other tables. However, if the profile name in this table matches any profile name in the cippIpProfileTable and the profile name of any filter entry in the cippIpFilterTable, the profile is active and the filter entry is applied to IP traffic that passes through the attached device interfaces. Any change to the filters in the cippIpFilterTable or the profile in the cippIpProfileTable affects all the attached interfaces. The IP protocol is described in RFC 791.</td>
</tr>
</tbody>
</table>
### SNMP Overview

**CISCO-L4L7RESOURCE LIMIT-MIB**
- **Capability MIB**: CISCO-L4L7MODULE-RESOURCE LIMIT-CAPABILITY
- **Description**: Manages resource classes and configuring minimum/maximum limits to different resources. The resources referenced in this MIB are in addition to resource information that is available in other MIBs. This MIB applies to Layer 4 through 7 modules that support managing resource limits using a centralized approach. Some resources configured include categories such as TCP/IP connections, MAC addresses, syslog buffer, ACL memory, and NAT translations. Support for this MIB is limited to the data from your configuration. The value of entPhysicalIndex will always be 1.

**CISCO-MODULE VIRTUALIZATION MIB**
- **Capability MIB**: CISCO-MODULE VIRTUALIZATION-CAPABILITY
- **Description**: Provides a way to create and manage ACE user contexts (also referred as virtual contexts). A user context is a logical partition of a physical device (the ACE). A user context provides different service types that can be managed independently. Each user context is an independent entity with its own configuration. A user-created context supports most of the options that you can configure in the Admin context (the default ACE context). Each context can have a separate management IP address that allows you to establish a remote connection to the ACE with the Secure Shell (SSH) or Telnet protocols and send other requests (such as SNMP or FTP).

This MIB contains tables that allow you to create or delete ACE user contexts and assign interfaces and interface ranges to user contexts.

**CISCO-PROCESS MIB**
- **Capability MIB**: CISCO-PROCESS-CAPABILITY
- **Description**: Displays memory and process CPU utilization on Cisco devices. This information should be used only as an estimate. The value of cpmCPU.TotalPhysicalIndex will always be 1.

The displayed system processes information is at the CPU system level (the total CPU usage) and is not on a per-context level.

---

### Table 7-1 SNMP MIB Support (continued)

<table>
<thead>
<tr>
<th>MIB Support</th>
<th>Capability MIB</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO-L4L7RESOURCE LIMIT-MIB</td>
<td>CISCO-L4L7MODULE-RESOURCE LIMIT-CAPABILITY</td>
<td>Manages resource classes and configuring minimum/maximum limits to different resources. The resources referenced in this MIB are in addition to resource information that is available in other MIBs. This MIB applies to Layer 4 through 7 modules that support managing resource limits using a centralized approach. Some resources configured include categories such as TCP/IP connections, MAC addresses, syslog buffer, ACL memory, and NAT translations. Support for this MIB is limited to the data from your configuration. The value of entPhysicalIndex will always be 1.</td>
</tr>
<tr>
<td>CISCO-MODULE VIRTUALIZATION MIB</td>
<td>CISCO-MODULE VIRTUALIZATION-CAPABILITY</td>
<td>Provides a way to create and manage ACE user contexts (also referred as virtual contexts). A user context is a logical partition of a physical device (the ACE). A user context provides different service types that can be managed independently. Each user context is an independent entity with its own configuration. A user-created context supports most of the options that you can configure in the Admin context (the default ACE context). Each context can have a separate management IP address that allows you to establish a remote connection to the ACE with the Secure Shell (SSH) or Telnet protocols and send other requests (such as SNMP or FTP). This MIB contains tables that allow you to create or delete ACE user contexts and assign interfaces and interface ranges to user contexts.</td>
</tr>
<tr>
<td>CISCO-PROCESS MIB</td>
<td>CISCO-PROCESS-CAPABILITY</td>
<td>Displays memory and process CPU utilization on Cisco devices. This information should be used only as an estimate. The value of cpmCPU.TotalPhysicalIndex will always be 1. The displayed system processes information is at the CPU system level (the total CPU usage) and is not on a per-context level.</td>
</tr>
</tbody>
</table>
### Table 7-1  SNMP MIB Support (continued)

<table>
<thead>
<tr>
<th>MIB Support</th>
<th>Capability MIB</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO-PRODUCTS-MIB</td>
<td>N/A</td>
<td>Contains the OIDs that can be reported in the sysObjectID object in the SNMPv2-MIB. The sysObjectID OID value is listed below:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Product Name (PID) sysObjectID</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ACE10-6500-K9/ACE20-MOD-K9 ciscoACE10K9 (ciscoProducts 730)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following MIB objects for the ACE include non-SLB related connections as well:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• cslbxStatsCurrConnections</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• cslbxStatsTimedOutConnections</td>
</tr>
</tbody>
</table>
Table 7-1  SNMP MIB Support (continued)

<table>
<thead>
<tr>
<th>MIB Support</th>
<th>Capability MIB</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO-SLB-MIB</td>
<td>CISCO-SLB-CAPABILITY</td>
<td>Manages the Server Load-Balancing (SLB) Manager(s). This MIB monitors the SLB connections statistics, server farms, real servers, VIP status and statistics, and so on.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The slbEntity Index used in the table is the slot number of the ACE. Because the slot numbers value is not applicable for the ACE module, the slbEntity Index will always have a value of one.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following MIB objects for the ACE include non-SLB related connections as well:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>•  slbStatsCreatedConnections</td>
</tr>
<tr>
<td></td>
<td></td>
<td>•  slbStatsCreatedHCConnections</td>
</tr>
<tr>
<td></td>
<td></td>
<td>•  slbStatsEstablishedConnections</td>
</tr>
<tr>
<td></td>
<td></td>
<td>•  slbStatsEstablishedHCConnections</td>
</tr>
<tr>
<td></td>
<td></td>
<td>•  slbStatsDestroyedConnections</td>
</tr>
<tr>
<td></td>
<td></td>
<td>•  slbStatsDestroyedHCConnections</td>
</tr>
<tr>
<td></td>
<td></td>
<td>•  slbStatsReassignedConnections</td>
</tr>
<tr>
<td>CISCO-SYSLOG-EXT-MIB</td>
<td>CISCO-SYSLOG-EXT-CAPABILITY</td>
<td>Extends the CISCO-SLB-MIB, provides additional server farm configuration parameters (cslbxServerFarmTable), and configures and monitors system log (syslog) management parameters for the ACE. Use this MIB to set up syslog servers and set logging severity levels.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The syslog is described by RFC 3164.</td>
</tr>
</tbody>
</table>
### Table 7-1 SNMP MIB Support (continued)

<table>
<thead>
<tr>
<th>MIB Support</th>
<th>Capability MIB</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO-SYSLOG-MIB</td>
<td>CISCO-SYSLOG-CAPABILITY</td>
<td>Describes and stores the system messages (syslog messages) generated by the ACE. The CISCO-SYSLOG-MIB provides access to the syslog messages through SNMP. The MIB also contains a history of syslog messages and objects to enable or disable the transmission of syslog notifications.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> This MIB does not track messages that are generated from debug commands entered through the CLI.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The syslog is described by RFC 3164.</td>
</tr>
<tr>
<td>IF-MIB</td>
<td>CISCO-IF-CAPABILITY</td>
<td>Reports generic information on interfaces (for example, VLANs). The IF-MIB is described in RFC 2863.</td>
</tr>
<tr>
<td>IP-MIB</td>
<td>CISCO-IP-CAPABILITY</td>
<td>Defines managed objects for managing implementations of the IP and its associated Internet Control Message Protocol (ICMP), but excludes their management of IP routes. The IP-MIB is described in RFC 4293.</td>
</tr>
<tr>
<td>SNMPv2-MIB</td>
<td>CISCO-SNMPv2-CAPABILITY</td>
<td>Provides the Management Information Base for SNMPv2. The management protocol, SNMPv2, provides for the exchange of messages that convey management information between the agents and the management stations. The SNMPv2-MIB is described in RFC 3418.</td>
</tr>
</tbody>
</table>
Chapter 7  Configuring SNMP

SNMP Overview

Table 7-1  SNMP MIB Support (continued)

<table>
<thead>
<tr>
<th>MIB Support</th>
<th>Capability MIB</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP-MIB</td>
<td>CISCO-TCP-STD-CAPABILITY</td>
<td>Defines managed objects for managing the implementation of the Transmission Control Protocol (TCP). The TCP MIB is described in RFC 4022.</td>
</tr>
<tr>
<td>UDP-MIB</td>
<td>CISCO-UDP-STD-CAPABILITY</td>
<td>Defines managed objects for managing implementation of the User Datagram Protocol (UDP). The UDP MIB is described in RFC 4113.</td>
</tr>
</tbody>
</table>

Table 7-2 identifies the supported SNMP notifications (traps) for the ACE.

The clogOrigin ID and clogOriginIDType variable bindings are appended to each notification listed in Table 7-2 to identify from which chassis, slot, and context combination that the event trap has originated.

Table 7-2  SNMP Trap Support

<table>
<thead>
<tr>
<th>Notification Name</th>
<th>Location of the Notification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authenticationFailure</td>
<td>SNMPv2-MIB</td>
<td>SNMP request fails because the NMS did not authenticate with the correct community string.</td>
</tr>
<tr>
<td>cesRealServerStateUp</td>
<td>CISCO-ENHANCED-SLB-MIB</td>
<td>State of a real server configured in a server farm is up due to user intervention.</td>
</tr>
<tr>
<td>cesRealServerStateDown</td>
<td>CISCO-ENHANCED-SLB-MIB</td>
<td>State of a real server configured in a server farm is down due to user intervention.</td>
</tr>
<tr>
<td>cesRealServerStateChange</td>
<td>CISCO-ENHANCED-SLB-MIB</td>
<td>State of a real server configured in a server farm changed to a new state as a result of something other than a user intervention. This notification is sent for situations such as ARP failures, probe failures, and so on.</td>
</tr>
</tbody>
</table>
**SNMP Trap Support (continued)**

<table>
<thead>
<tr>
<th>Notification Name</th>
<th>Location of the Notification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cesRserverStateUp</td>
<td>CISCO-ENHANCED-SLB-MIB</td>
<td>State of a global real server is up due to user intervention.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> No separate cesRealServerStateUp notifications are sent for each</td>
</tr>
<tr>
<td></td>
<td></td>
<td>real server that listens on this rserver.</td>
</tr>
<tr>
<td>cesRserverStateDown</td>
<td>CISCO-ENHANCED-SLB-MIB</td>
<td>State of a global real server is down due to user intervention.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> No separate cesRealServerStateDown notifications are sent for</td>
</tr>
<tr>
<td></td>
<td></td>
<td>each real server that listens on this rserver.</td>
</tr>
<tr>
<td>cesRserverStateChange</td>
<td>CISCO-ENHANCED-SLB-MIB</td>
<td>State of a global real server changed to a new state as a result of</td>
</tr>
<tr>
<td></td>
<td></td>
<td>something other than a user intervention. This notification is sent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>for situations such as ARP failures, probe failures, and so on.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> No separate cesRealServerStateChange notifications are sent for</td>
</tr>
<tr>
<td></td>
<td></td>
<td>each real server that listens on this rserver.</td>
</tr>
</tbody>
</table>
### SNMP Overview

- **ciscoSlbVServerVIPStateChange**
  - Notification Name: `ciscoSlbVServerVIPStateChange`
  - Location of the Notification: `CISCO-SLB-MIB.my`
  - Description: State of Vserver changes. This notification is sent with the following var-binds:
    - `slbVServerState`
    - `slbVServerStateChangeDescr`
    - `slbVServerClassMap`
    - `slbVServerPolicyMap`
    - `slbVServerIpAddressType`
    - `slbVServerIpAddress`
    - `slbVServerProtocol`

  The change in the Vserver state could be due to different reasons, such as binding to the interface, removing an active server farm from the policy, and associating the virtual IP address (VIP) with a class map. The `ciscoSlbVServerVIPStateChange` is specified in the CISCO-SLB-MIB.

- **ciscoSlbVServerStateChange**
  - Notification Name: `ciscoSlbVServerStateChange`
  - Location of the Notification: `CISCO-SLB-MIB.my`
  - Description: Notification that a virtual IP address (VIP) is removed from a class map. This notification is sent with the following var-binds:
    - `slbVServerState`
    - `slbVServerStateChangeDescr`
    - `slbVServerClassMap`
    - `slbVServerPolicyMap`

  The `ciscoSlbVServerStateChange` is specified in the CISCO-SLB-MIB.

- **clogMessageGenerated**
  - Notification Name: `clogMessageGenerated`
  - Location of the Notification: `CISCO-SYSLOG-MIB`
  - Description: ACE generated one or more syslog messages.

### Table 7-2  SNMP Trap Support (continued)

<table>
<thead>
<tr>
<th>Notification Name</th>
<th>Location of the Notification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ciscoSlbVServerVIPStateChange</code></td>
<td><code>CISCO-SLB-MIB.my</code></td>
<td>State of Vserver changes. This notification is sent with the following var-binds:</td>
</tr>
</tbody>
</table>
|                                   |                             | - `slbVServerState`
|                                   |                             | - `slbVServerStateChangeDescr`
|                                   |                             | - `slbVServerClassMap`
|                                   |                             | - `slbVServerPolicyMap`
|                                   |                             | - `slbVServerIpAddressType`
|                                   |                             | - `slbVServerIpAddress`
|                                   |                             | - `slbVServerProtocol`
|                                   |                             | The change in the Vserver state could be due to different reasons, such as binding to the interface, removing an active server farm from the policy, and associating the virtual IP address (VIP) with a class map. The `ciscoSlbVServerVIPStateChange` is specified in the CISCO-SLB-MIB. |
| `ciscoSlbVServerStateChange`      | `CISCO-SLB-MIB.my`          | Notification that a virtual IP address (VIP) is removed from a class map. This notification is sent with the following var-binds: |
|                                   |                             | - `slbVServerState`
|                                   |                             | - `slbVServerStateChangeDescr`
|                                   |                             | - `slbVServerClassMap`
|                                   |                             | - `slbVServerPolicyMap`
|                                   |                             | The `ciscoSlbVServerStateChange` is specified in the CISCO-SLB-MIB. |
| `clogMessageGenerated`            | `CISCO-SYSLOG-MIB`          | ACE generated one or more syslog messages. |
### SNMP Overview

#### SNMP Limitations

If any SNMP MIB table has more than one string index that contains more than 48 characters, the index may not show up in the MIB table when you perform an SNMP walk. According to SNMP standards, SNMP requests, responses, or traps cannot have more than 128 subidentifiers. The following list contains object names:

- Context name
- Real server name
- Server farm name
- Probe name

### Table 7-2  SNMP Trap Support (continued)

<table>
<thead>
<tr>
<th>Notification Name</th>
<th>Location of the Notification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clmLicenseExpiryNotify</td>
<td>CISCO-LICENSE-MGR-MIB</td>
<td>Notification that an installed feature license expires.</td>
</tr>
<tr>
<td>clmLicenseFileMissingNotify</td>
<td>CISCO-LICENSE-MGR-MIB</td>
<td>Notification that the system detects that one or more installed license files are missing.</td>
</tr>
<tr>
<td>clmLicenseExpiryWarningNotify</td>
<td>CISCO-LICENSE-MGR-MIB</td>
<td>Notification that the system detects an installed feature license is about to expire.</td>
</tr>
<tr>
<td>clmNoLicenseForFeatureNotify</td>
<td>CISCO-LICENSE-MGR-MIB</td>
<td>Notification that the system detects that no license is installed for a specific feature.</td>
</tr>
<tr>
<td>cmVirtContextAdded, cmVirtContextRemoved</td>
<td>CISCO-MODULE-VIRTUALIZATION-MIB</td>
<td>Notification that you created or deleted an ACE user context, also referred as a virtual context.</td>
</tr>
<tr>
<td>coldStart</td>
<td>SNMPv2-MIB</td>
<td>SNMP agent started after a cold restart (full power cycle) of the ACE.</td>
</tr>
<tr>
<td>linkUp, linkDown</td>
<td>SNMPv2-MIB</td>
<td>VLAN interface is up or down. A VLAN interface can be down, for example, if you specified the shut command followed by the no shut command, or the VLAN was removed from the switch configuration.</td>
</tr>
</tbody>
</table>
SNMP Overview

- HTTP header name
- ACL name
- Class map name
- Policy map name
- Resource class name

Table 7-3 identifies a list of tables that have more than one string index.

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>Table</th>
<th>String Indices</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO-ENHANCED-SLB-MIB.my</td>
<td>cesRserverProbeTable</td>
<td>cesRserverName, cesRserverProbeName</td>
</tr>
<tr>
<td>CISCO-ENHANCED-SLB-MIB.my</td>
<td>cesServerFarmRserverTable</td>
<td>slbServerFarmName, cesRserverName</td>
</tr>
<tr>
<td>CISCO-SLB-EXT-MIB.my</td>
<td>cslbxServerFarmProbeFarmName</td>
<td>cslbxServerFarmProbeFarmName, cslbxServerFarmProbeProbeName</td>
</tr>
<tr>
<td>CISCO-SLB-HEALTH-MON-MIB.my</td>
<td>cslbxProbeHeaderCfgTable</td>
<td>cslbxProbeHeaderProbeName, cslbxProbeHeaderFieldName</td>
</tr>
</tbody>
</table>

Table 7-3: SNMP MIB Tables with More Than One String Index
SNMP Configuration Quick Start

Table 7-4 provides a quick overview of the steps required to configure SNMP on the ACE. Each step includes the CLI command required to complete the task.

Table 7-4 SNMP Management Configuration Quick Start

<table>
<thead>
<tr>
<th>Task and Command Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. If you are operating in multiple contexts, observe the CLI prompt to verify that you are operating in the desired context. If necessary, log directly in to, or change to, the correct context.</td>
</tr>
<tr>
<td>host1/Admin# changeto C1</td>
</tr>
<tr>
<td>host1/C1#</td>
</tr>
<tr>
<td>The rest of the examples in this table use the Admin context, unless otherwise specified. For details on creating contexts, see the Cisco Application Control Engine Module Virtualization Configuration Guide.</td>
</tr>
<tr>
<td>2. Enter configuration mode.</td>
</tr>
<tr>
<td>host1/Admin# config</td>
</tr>
<tr>
<td>Enter configuration commands, one per line. End with CNTL/Z</td>
</tr>
<tr>
<td>host1/Admin(config)#</td>
</tr>
<tr>
<td>3. Configure one or more SNMP users from the ACE CLI.</td>
</tr>
<tr>
<td>host1/Admin(config)# snmp-server user joe Network-Monitor auth sha abcd1234</td>
</tr>
<tr>
<td>host1/Admin(config)# snmp-server user sam Network-Monitor auth md5 abcdefgh</td>
</tr>
<tr>
<td>host1/Admin(config)# snmp-server user Bill Network-Monitor auth sha abcd1234 priv abcdefgh</td>
</tr>
<tr>
<td>4. Create an SNMP community and identify access privileges.</td>
</tr>
<tr>
<td>host1/Admin(config)# snmp-server community SNMP_Community1 group Network-Monitor</td>
</tr>
<tr>
<td>5. Specify the contact name for the SNMP system.</td>
</tr>
<tr>
<td>host1/Admin(config)# snmp-server contact “User1 <a href="mailto:user1@cisco.com">user1@cisco.com</a>”</td>
</tr>
<tr>
<td>6. Specify the SNMP system location.</td>
</tr>
<tr>
<td>host1/Admin(config)# snmp-server location “Boxborough MA”</td>
</tr>
</tbody>
</table>
Chapter 7  Configuring SNMP

SNMP Configuration Quick Start

Table 7-4   SNMP Management Configuration Quick Start (continued)

Task and Command Example

7. Specify which host is to receive SNMP notifications.

   host1/Admin(config)# snmp-server host 192.168.1.1 traps version 2c SNMP_Community1 udp-port 500

8. Enable the ACE to send SNMP traps and inform requests to the NMS.

   host1/Admin(config)# snmp-server enable traps slb

9. Create a class map that permits network management traffic to be received by the ACE based on the SNMP management protocol and client source IP address.

   host1/Admin(config)# class-map type management match-all SNMP-ALLOW_CLASS
   host1/Admin(config-cmap-mgmt)# match protocol snmp source-address 172.16.10.0 255.255.255.254
   host1/Admin(config-cmap-mgmt)# exit
   host1/Admin(config)#

10. Configure a policy map that activates the SNMP management protocol classifications.

    host1/Admin(config)# policy-map type management first-match SNMP-ALLOW_POLICY
    host1/Admin(config-pmap-mgmt)# class SNMP-ALLOW_CLASS
    host1/Admin(config-pmap-mgmt-c)# permit
    host1/Admin(config-pmap-mgmt-c)# exit
    host1/Admin(config-pmap-mgmt)# exit
    host1/Admin(config)#

11. Attach the traffic policy to a single VLAN interface or globally to all VLAN interfaces in the same context. For example, to specify an interface VLAN and apply the SNMP management policy map to the VLAN, enter:

    host1/Admin(config)# interface vlan 50
    host1/Admin(config-if)# ip address 172.16.10.0 255.255.255.254
    host1/Admin(config-if)# service-policy input SNMP-ALLOW_POLICY
    host1/Admin(config-if)# exit

12. (Optional) Save your configuration changes to Flash memory.

    host1/Admin(config)# exit
    host1/Admin# copy running-config startup-config
Configuring SNMP Users

You configure SNMP users from the ACE CLI. User configuration includes information such as specifying the role group that the user belongs to, authentication parameters for the user, the authentication password, and message encryption parameters. Use the `snmp-server user` command in configuration mode to configure SNMP user information.

**Note**
User configuration through the `snmp-server user` command is applicable only for SNMPv3; SNMPv1 and SNMPv2c use a community string match for user authentication (see the “Defining SNMP Communities” section).

The ACE synchronizes the interactions between the user created by the `username` command and by the `snmp-server user` command; updates to a user through the ACE CLI are automatically reflected in the SNMP server. For example, deleting a user automatically results in the user being deleted for both SNMP and CLI. In addition, user-role mapping changes are reflected in SNMP.

**Caution**
If you change the SNMP engine ID for an Admin or user context, all configured SNMP users become invalid. You must recreate all SNMP users by using the `snmp-server user` command in configuration mode. For more information on the SNMPv3 engine ID, see the “Configuring an SNMPv3 Engine ID for an ACE Context” section.

The syntax of the `snmp-server user` command is as follows:

```
    snmp-server user user_name [group_name] [auth {md5 | sha} password1 [localizedkey | priv {password2 | aes-128 password2}]]
```

The keywords, arguments, and options are as follows:

- `user_name`—Username. Enter an unquoted text string with no space and a maximum of 24 alphanumeric characters.
- `group_name`—(Optional) User role group to which the user belongs. Enter `Network-Monitor`, the default group name and the only role that is supported.
Note

Only network monitoring operations are supported through the ACE implementation of SNMP. In this case, all SNMP users are automatically assigned the system-defined default group of Network-Monitor. For details on creating users, see the Cisco Application Control Engine Module Virtualization Configuration Guide.

- **auth**—(Optional) Sets authentication parameters for the user. Authentication determines that the message is from a valid source.
- **md5**—Specifies the HMAC Message Digest 5 (MD5) encryption algorithm for user authentication.
- **sha**—Specifies the HMAC Secure Hash Algorithm (SHA) encryption algorithm for user authentication.
Chapter 7  Configuring SNMP

Configuring SNMP Users

- **password1**—User authentication password. Enter an unquoted text string with no space and a maximum of 130 alphanumeric characters. The ACE automatically synchronizes the SNMP authentication password as the password for the CLI user. The ACE supports the following special characters in a password:

  , . / = + ^ @ ! % ~ # $ * ( )

  Note that the ACE encrypts clear text passwords in the running-config.

- **localizedkey**—(Optional) Specifies that the password is in a localized key format for security encryption.

- **priv**—(Optional) Specifies encryption parameters for the user. The **priv** option and the **aes-128** option indicate that this privacy password is for generating 128-bit AES key.

- **aes-128**—Specifies the 128-byte Advanced Encryption Standard (AES) algorithm for privacy. AES is a symmetric cipher algorithm and is one of the privacy protocols for SNMP message encryption. It conforms with RFC 3826.

  **Note** For an SNMPv3 operation using the external AAA server, user configurations on this server require AES for SNMP PDU encryption.

- **password2**—Encryption password for the user. The AES **priv** password can have a minimum of eight characters. If the passphrases are specified in clear text, you can specify a maximum of 64 alphanumeric characters. If you use the localized key, you can specify a maximum of 130 alphanumeric characters. Spaces are not allowed. The ACE supports the following special characters in a password:

  , . / = + ^ @ ! % ~ # $ * ( )

  Note that the ACE encrypts clear text passwords in the running-config.

For example, to set the user information, enter:

```
host1/Admin# config
Enter configuration commands, one per line. End with CNTL/Z
host1/Admin(config)# snmp-server user joe Network-Monitor auth sha abcd1234
host1/Admin(config)# snmp-server user sam Network-Monitor auth md5 abcd1234
host1/Admin(config)# snmp-server user Bill Network-Monitor auth sha abcd1234 priv abcd1234
```
Defining SNMP Communities

To disable the SNMP user configuration or to remove an SNMP user, use the `no` form of the command. For example, enter:

```
host1/Admin(config)# no snmp-server user Bill Network-Monitor auth sha abcd1234 priv abcdefgh
```

Each SNMP device or member is part of a community. An SNMP community determines the access rights for each SNMP device. SNMP uses communities to establish trust between managers and agents.

You supply a name to the community. After that, all SNMP devices assigned to that community as members have the same access rights (as described in RFC 2576). The ACE allows read-only access to the MIB tree for devices included in this community. The read-only community string allows a user to read data values, but prevents that user from modifying modify the data.

To create or modify SNMP community names and access privileges, use the `snmp-server community` command in configuration mode.

**Note**

SNMP communities are applicable only for SNMPv1 and SNMPv2c. SNMPv3 requires user configuration information such as specifying the role group that the user belongs to, authentication parameters for the user, authentication password, and message encryption parameters (see the “Configuring SNMP Users” section).

**Caution**

If you change the SNMP engine ID for an Admin or user context, all configured SNMP communities are deleted. You must recreate all SNMP communities by using the `snmp-server community` command in configuration mode. For more information on the SNMPv3 engine ID, see the “Configuring an SNMPv3 Engine ID for an ACE Context” section.

The syntax of this command is as follows:

```
    snmp-server community community_name [group group_name | ro]
```

The keywords, arguments, and options are as follows:
Configuring an SNMP Contact

To specify the contact information for the SNMP system, use the `snmp-server contact` command in configuration mode. You can specify information for only one contact name. The syntax of this command is as follows:

```
snmp-server contact contact_information
```
Configuring an SNMP Location

Enter the contact_information argument as a text string with a maximum of 240 alphanumeric characters, including spaces. If the string contains more than one word, enclose the string in quotation marks (" "). You can include information on how to contact the person; for example, you can provide a phone number or an e-mail address.

For example, to specify SNMP system contact information, enter:

```
host1/Admin(config-context)# snmp-server contact "User1 user1@cisco.com"
```

To remove the specified SNMP contact name, enter:

```
host1/Admin(config)# no snmp-server contact
```

Configuring an SNMP Location

To specify the SNMP system location, use the snmp-server location command in configuration mode. You can specify only one location. The syntax of this command is as follows:

```
snmp-server location location
```

Enter the location as the physical location of the system. Enter a text string with a maximum of 240 alphanumeric characters, including spaces. If the string contains more than one word, enclose the string in quotation marks (" ").

For example, to specify SNMP system location information, enter:

```
host1/Admin(config)# snmp-server location "Boxborough MA"
```

To remove the specified SNMP system location information, enter:

```
host1/Admin(config)# no snmp-server location
```

Configuring SNMP Notifications

You can configure the ACE to send traps or inform requests as notifications to an SNMP manager when a particular event occurs. In some instances, traps are unreliable because the receiver does not send any acknowledgment when it receives a trap. The sender cannot determine if the trap was received. However, an SNMP manager that receives inform requests acknowledges the message with
Configuring SNMP Notifications

an SNMP Response PDU. If the sender never receives a Response, the inform request is normally retransmitted. Inform requests are more likely to reach their intended destination.

**Note**  
Use the SNMP-TARGET-MIB to obtain more information on the destinations to which notifications are to be sent either as traps or as SNMP inform requests. See the “Supported MIBs and Notifications” section for details.

This section contains the following topics:

- Configuring SNMP Notification Hosts
- Enabling SNMP Notifications
- Enabling the IETF Standard for SNMP linkUp and linkDown Traps

### Configuring SNMP Notification Hosts

Use the `snmp-server host` command in configuration mode to specify which host receives SNMP notifications. In order to send notifications, you must configure at least one `snmp-server host` command. The ACE supports a maximum of 10 SNMP hosts per context.

The syntax of this command is as follows:

```
   snmp-server host host_address {community-string_username | informs | traps | version {1 {udp-port} | 2c {udp-port} | 3 [auth | noauth | priv]}}
```

The keywords, arguments, and options are as follows:

- `host_address`—IP address of the host (the targeted recipient). Enter the address in dotted-decimal IP notation (for example, 192.168.11.1).
- `community-string_username`—SNMP community string or username with the notification operation. Enter an unquoted text string with no space and a maximum of 32 alphanumeric characters.
- `informs`—Sends SNMP inform requests to the identified host, which allows for manager-to-manager communication. Inform requests can be useful when the need arises for more than one NMS in the network.
• **traps**—Sends SNMP traps to the identified host. A trap is the method for an agent to tell the NMS that a problem has occurred. The trap originates from the agent and is sent to the trap destination, as configured within the agent itself. Typically the trap destination is the IP address of the NMS.

• **version**—Specifies the version of SNMP used to send the traps. SNMPv3 is the most secure model because it allows packet encryption with the `priv` keyword.

• **1**—Specifies SNMPv1. This option is not available for use with SNMP inform requests. SNMPv1 has one optional keyword (`udp-port`) that specifies the UDP port of the host to use. The default is 162.

• **2c**—Specifies SNMPv2C. SNMPv2C has one optional keyword (`udp-port`) that specifies the UDP port of the host to use. The default is 162.

• **3**—Specifies SNMPv3. SNMPv3 has three optional keywords (`auth`, `no auth`, or `priv`).

• **auth**—(Optional) Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication.

• **noauth**—(Optional) Specifies the noAuthNoPriv security level.

• **priv**—(Optional) Enables Data Encryption Standard (DES) packet encryption (privacy).

For example, to specify the recipient of an SNMP notification, enter:

```
host1/Adm(config)# snmp-server host 192.168.1.1 traps version 2c SNMP_Community1 udp-port 500
```

To remove the specified host, use the `no` form of the command. For example, enter:

```
host1/Adm(config)# no snmp-server host 192.168.1.1 traps version 2c SNMP_Community1 udp-port 500
```
Enabling SNMP Notifications

Notification traps and inform requests are system alerts that the ACE generates when certain events occur. SNMP notifications can be sent to the NMS as traps or inform requests. By default, no notification is defined or issued. To enable the ACE to send SNMP traps and informs to the NMS, use the `snmp-server enable traps` command in configuration mode. This command enables both traps and inform requests for the specified notification types.

To configure the ACE to send the SNMP notifications, specify at least one `snmp-server enable traps` command. To enable multiple types of notifications, you must enter a separate `snmp-server enable traps` command for each notification type and notification option. If you enter the command without any keywords, the ACE enables all notification types and traps.

The `snmp-server enable traps` command is used with the `snmp-server host` command (see the “Configuring SNMP Notification Hosts” section). The `snmp-server host` command specifies which host receives the SNMP notifications. To send notifications, you must configure at least one SNMP server host.

---

**Note**

The notification types used in the `snmp-server enable traps` command all have an associated MIB object that globally enables or disables them. However, not all of the notification types available in the `snmp-server host` command have notificationEnable MIB objects, so some of the notification types cannot be controlled by using the `snmp-server enable` command.

---

The syntax of this command is as follows:

```
snmp-server enable traps [notification_type] [notification_option]
```

The keywords, arguments, and options are as follows:

- `notification_type`—(Optional) Type of notification to enable. If no type is specified, the ACE sends all notifications. Specify one of the following keywords as the `notification_type`:
  - `license`—Sends SNMP license manager notifications. This keyword appears only in the Admin context.
  - `slb`—Sends server load-balancing notifications. When you specify the `slb` keyword, you can specify a `notification_option` value.
Chapter 7      Configuring SNMP

Configuring SNMP Notifications

- **snmp**—Sends SNMP notifications. When you specify the `snmp` keyword, you can specify a *notification_option* value.

- **syslog**—Sends error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the *logging history level* command.

---

**Note**

To enable system messages to be sent as traps to the NMS, you can specify the *logging history* command. You must also enable syslog traps by using the `snmp-server enable traps` command. See the *Cisco Application Control Engine Module System Message Guide* for details.

---

- **virtual-context**—Sends virtual context (ACE user context) change notifications. This keyword appears only in the Admin context.

- **notification_option**—(Optional) One of the following SNMP notifications:
  - When you specify the `snmp` keyword, specify the authentication, coldstart, linkdown, or linkup keyword to enable SNMP notifications. This selection generates a notification if the community string provided in the SNMP request is incorrect, or when a VLAN interface is either up or down. The coldstart keyword appears only in the Admin context.
  - When you specify the `slb` keyword, specify the real or vserver keyword to enable server load-balancing notifications. This selection generates a notification if the following state change occurs:

    The real server changes state (up or down) due to user intervention, ARP failures, or probe failures.

    The virtual server changes state (up or down). The virtual server represents the servers behind the content switch in the ACE to the outside world and consists of the following attributes: the destination address (can be a range of IP addresses), the protocol, the destination port, or the incoming VLAN.

For example, to enable the ACE to send server load-balancing traps to the host at IP address 192.168.1.1 using the community string public, enter:

```
host1/Admin(config)# snmp-server host 192.168.1.1
host1/Admin(config)# snmp-server community SNMP_Community1 group Network-Monitor
host1/Admin(config)# snmp-server enable traps slb real
```
To disable SNMP server notifications, use the `no` form of the command. For example, enter:

```
host1/Admin(config)# no snmp-server enable traps slb real
```

### Enabling the IETF Standard for SNMP linkUp and linkDown Traps

By default, the ACE sends the Cisco implementation of linkUp and linkDown traps to the NMS. The ACE sends the Cisco Systems IF-MIB variable bindings, which consists of ifIndex, ifAdminStatus, ifOperStatus, ifName, ifType, clogOriginID, and clogOriginIDType. You can configure the ACE to send the Internet Engineering Task Force (IETF) standards-based implementation for linkUp and linkDown traps (as outlined in RFC 2863). The `snmp-server trap link ietf` configuration mode command instructs the ACE to send the linkUp and linkDown traps with the IETF standard IF-MIB (RFC 2863) variable bindings, consisting of ifIndex, ifAdminStatus, and ifOperStatus.

The syntax of this command is as follows:

````snmp-server trap link ietf`
```

For example, to configure the linkUp and linkDown traps comply with RFC 2863, enter:

```
host1/Admin(config)# snmp-server trap link ietf
```

To revert to the Cisco implementation of linkUp and linkDown traps, enter:

```
host1/Admin(config)# no snmp-server trap link ietf
```
Assigning a VLAN Interface as the Trap-Source Address in SNMPv1 Traps

By default, the ACE uses the trap source IP address from the internal routing table, depending on the destination host address, where the ACE will send the notification. To specify the use of the IP address configured on a VLAN as the trap-source address in the SNMPv1 trap PDU, use the `snmp-server trap-source vlan` command in configuration mode. The syntax of this command is as follows:

```
snmp-server trap-source vlan number
```

The `number` argument specifies the VLAN number of the configured interface. Enter a value from 2 to 4094 for an existing VLAN.

For example, to specify VLAN 50 as the VLAN interface as the source address in the SNMPv1 trap PDUs, enter:

```
host1/Admin(config)# snmp-server trap-source vlan 50
```

To remove the specified VLAN as the source address in the SNMPv1 trap PDU and reset the default behavior, enter:

```
host1/Admin(config)# no snmp-server trap-source
```

**Note**

If the VLAN interface does not have a valid IP address, the SNMPv1 trap notification fails.

Accessing ACE User Context Data Through the Admin Context IP Address

The ACE Admin context and each ACE user context has its own IP address. The SNMP agent supports a community string for SNMPv1 and SNMPv2 and a username for SNMPv3 on a per-context basis. SNMP managers can send requests to a context by using the IP address to get the data that corresponds to the context.

You can also retrieve data for user contexts by using the IP address for the Admin context. The Admin context credentials also allow access to user context data, such as performance and configuration information.
The notifications for user contexts cannot be sent through the Admin context.

This section contains the following topics:
- Accessing User Context Data When Using SNMPv1/v2
- Accessing User Context Data When Using SNMPv3

### Accessing User Context Data When Using SNMPv1/v2

For SNMPv1/v2, SNMP managers can access MIBs available for a user context through an Admin context IP address by specifying the appropriate SNMP version, the Admin context IP address, and the Admin context community string embedded with the name of the user context. The format for the community string is as follows:

```
admin_community_string@ACE_context_name
```

The `ACE_context_name` can be Admin or any ACE user context. If you do not specify a context name, the request is for the Admin context.

For example, to return data for user context C1 when the Admin context has a configured community string of adminCommunity and an IP address of 10.6.252.63, enter:

```
snmpget -v2c -c adminCommunity@C1 10.6.252.63 udpDatagrams.0
```

### Accessing User Context Data When Using SNMPv3

For SNMPv3, SNMP managers can access MIBs for a user context through an Admin context IP address by using the Admin context IP address, the appropriate SNMP version, the Admin context username, and the user context name supported by the Admin context in the SNMPv3 packet. The ACE uses the user context name in the SNMPv3 context field of the request.
The SNMPv3 engine represents a logically separate SNMP agent. The ACE automatically creates an SNMP engine ID for each context or you can configure it. For more information on configuring an SNMPv3 engine ID, see the “Configuring an SNMPv3 Engine ID for an ACE Context” section.

For example, to return data from user context C2 when the Admin context has a configured SNMP user snmpuser and an IP address of 10.6.252.63, enter:

```
snmpgetnext -v 3 -a MD5 -A cisco123 -u snmpuser -1 authNoPriv
10.6.252.63 system -n C2
```

The ACE uses the user context C2 in place of the SNMPv3 context field in the request.

The SNMPv3 request is dropped if the request is sent to the IP address of the user context with a SNMPv3 context name field set to an empty string (“”).

---

**Configuring an SNMPv3 Engine ID for an ACE Context**

By default, the ACE automatically creates an SNMP engine ID for the Admin context and each user context. The SNMP engine represents a logically separate SNMP agent. The IP address for an ACE context provides access to only one SNMP engine ID.

---

**Caution**

If you change the SNMP engine ID for an Admin or user context, all configured SNMP users become invalid and all SNMP communities are deleted. You must recreate all SNMP users by using the `snmp-server user` command in configuration mode, and recreate all SNMP communities by using the `snmp-server community` command in configuration mode.
The ACE allows you to configure an SNMP engine ID for the Admin or user context. To configure the SNMP engine ID for an ACE context, use the `snmp-server engineid` command in configuration mode for the context. The syntax of this command is as follows:

```
snmp-server engineid number
```

The `number` argument is the SNMPv3 engine ID that you want to configure. Enter a range of 10 to 64 hexadecimal digits.

For example, to configure an engine ID 88439573498573888843957349857388 for the Admin context, enter:

```
host1/Admin(config)# snmp-server engineID 88439573498573888843957349857388
```

To reset the default engine ID for the Admin context, enter:

```
host1/Admin(config)# no snmp-server engineID
```

To display the engine ID for a context, use the `show snmp engineID` command in Exec mode for the context. For example, to display the engine ID for the Admin context, enter:

```
host1/Admin# show snmp engineID
```

### Configuring SNMP Management Traffic Services

You configure SNMP management traffic to and from the ACE through the use of class maps, policy maps, and service policies. The following items summarize the role of each function in configuring remote network management access to the ACE:

- **Class map**—Provides the remote network traffic match criteria to permit SNMP management traffic based on the SNMP management protocol and the client source IP address.
- **Policy map**—Enables remote network management access for a traffic classification that matches the criteria listed the class map.
- **Service policy**—Activates the policy map, and attaches the traffic policy to a VLAN interface or globally on all VLAN interfaces.
SNMP remote access sessions are established to the ACE per context. For details on creating contexts and users, see the Cisco Application Control Engine Module Virtualization Configuration Guide.

This section contains the following topics:
- Creating and Configuring a Layer 3 and Layer 4 Class Map
- Creating a Layer 3 and Layer 4 Policy Map
- Applying a Service Policy

Creating and Configuring a Layer 3 and Layer 4 Class Map

To create a Layer 3 and Layer 4 class map to classify the SNMP management traffic that can be received by the ACE, use the `class-map type management` command in configuration mode. This command allows the ACE to receive the network management traffic by identifying the incoming IP protocols that the ACE can receive and the client source host IP address and subnet mask as the matching criteria. A class map of type `management` defines the allowed network traffic as a form of management security for protocols such as SNMP.

A class map can have multiple `match` commands. You can configure class maps to define multiple SNMP management protocol and source IP address commands in a group that you then associate with a traffic policy. The `match-all` and `match-any` keywords determine how the ACE evaluates multiple match statements operations when multiple match criteria exist in a class map.

The syntax of this command is as follows:

```
class-map type management [match-all | match-any] map_name
```

The keywords, arguments, and options are as follows:
- `match-all` | `match-any`—(Optional) Determines how the ACE evaluates Layer 3 and Layer 4 network traffic when multiple match criteria exist in a class map. The class map is considered a match if the `match` commands meet one of the following conditions:
  - `match-all` —(Default) All of the match criteria listed in the class map match the network traffic class in the class map (typically, `match` commands of the same type).
– **match-any**—Only one of the match criteria listed in the class map matches the network traffic class in the class map (typically, `match` commands of different types).

- **map_name**—Name assigned to the class map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

When you use the `class-map type management` command, you will access class map management configuration mode. This mode allows you to configure a description or the matching criteria for the class map.

For example, to allow SNMP access between the ACE and the host located at IP address 192.168.1.1 255.255.255.0, enter:

```
host1/Admin(config)# class-map type management match-all SNMP-ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# match protocol snmp source-address 192.168.1.1 255.255.255.0
done
```

To remove a Layer 3 and Layer 4 SNMP protocol management class map from the ACE, enter:

```
host1/Admin(config)# no class-map type management match-all SNMP-ALLOW_CLASS
```

To provide a class map description, see the “Defining a Class Map Description” section.

To classify the remote SNMP protocol management traffic received by the ACE, include one or more of the associated commands to configure the match criteria for the class map by using the `match protocol` command. For more information on this command, see the “Defining SNMP Protocol Match Criteria” section.

### Defining a Class Map Description

To provide a brief summary about the Layer 3 and Layer 4 remote management class map, use the `description` command in class map management configuration mode.

The syntax of this command is as follows:

```
description text
```

The `text` argument is the description that you want to provide. Enter an unquoted text string with a maximum of 240 alphanumeric characters.
For example, to specify a description that the class map is to allow SNMP access, enter:

```
host1/Admin(config)# class-map type management SNMP-ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# description Allow SNMP access
```

To remove the description from the class map, enter:

```
host1/Admin(config-cmap-mgmt)# no description
```

### Defining SNMP Protocol Match Criteria

To configure the class map to specify that SNMP can be received by the ACE and an NMS, use the `match protocol snmp` command in class map management configuration mode. You configure the associated policy map to permit SNMP access to the ACE. As part of the network management access traffic classification, you also specify either a client source host IP address and subnet mask as the matching criteria or instruct the ACE to allow any client source address for the management traffic classification.

The syntax of this command is as follows:

```
[line_number] match protocol snmp {any | source-address ip_address [mask]}
```

The keywords, arguments, and options are as follows:

- **line_number**—(Optional) Line number to identify individual `match` commands to help you edit or delete them. Enter an integer from 2 to 255. You can enter `no line_number` to delete long `match` commands instead of entering the entire line. The line numbers do not dictate a priority or sequence for the match statements.
- **any**—Specifies any client source address for the management traffic classification.
- **source-address**—Specifies a client source host IP address and subnet mask as the network traffic matching criteria. As part of the classification, the ACE implicitly obtains the destination IP address from the interface on which you apply the policy map.
- **ip_address**—Source IP address of the client. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
- **mask**—Subnet mask of the client in dotted-decimal notation (for example, 255.255.255.0).
For example, to specify that the class map allows SNMP access to the ACE from source address 192.168.10.1 255.255.255.0, enter:

```
host1/Admin(config)# class-map type management SNMP-ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# match protocol snmp source-address 192.168.10.1 255.255.255.0
```

To deselect the specified SNMP protocol match criteria from the class map, enter:

```
host1/Admin(config-cmap-mgmt)# no match protocol snmp
```

**Creating a Layer 3 and Layer 4 Policy Map**

A Layer 3 and Layer 4 policy map defines the actions executed on SNMP network management traffic that matches the specified classifications. This section contains the following topics:

- Creating a Layer 3 and Layer 4 Policy Map for SNMP Network Management Traffic Received by the ACE
- Specifying a Layer 3 and Layer 4 Traffic Class with the Traffic Policy
- Specifying Layer 3 and Layer 4 Policy Actions

**Creating a Layer 3 and Layer 4 Policy Map for SNMP Network Management Traffic Received by the ACE**

To configure a Layer 3 and Layer 4 policy map that permits the ACE to receive the SNMP management protocol, use the `policy-map type management` command in configuration mode. The ACE executes the action for the first matching classification. The ACE does not execute any additional actions.

The syntax of this command is as follows:

```
policy-map type management first-match map_name
```

The `map_name` argument specifies the name assigned to the Layer 3 and Layer 4 network management policy map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

When you use this command, you will access policy map management configuration mode.
For example, to create a Layer 3 and Layer 4 network traffic management policy map, enter:

```
host1/Admin(config) # policy-map type management first-match
SNMP-ALLOW_POLICY
```

To remove a network traffic management policy map from the ACE, enter:

```
host1/Admin(config)# no policy-map type management first-match
SNMP-ALLOW_POLICY
```

### Specifying a Layer 3 and Layer 4 Traffic Class with the Traffic Policy

To specify a Layer 3 and Layer 4 traffic class created with the `class-map` command to associate network traffic with the traffic policy, use the `class` command. This command enters the policy map management class configuration mode.

The syntax of this command is as follows:

```
class {name1 [insert-before name2] | class-default}
```

The arguments keywords, and options are as follows:

- `name1`—Name of a previously defined Layer 3 and Layer 4 traffic class, configured with the `class-map` command, to associate traffic to the traffic policy. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

- `insert-before name2`—(Optional) Places the current class map ahead of an existing class map or inline match condition specified by the `name2` argument in the policy map configuration. The ACE does not save the sequence reordering as part of the configuration. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.
• **class-default**—Specifies the class-default class map for the Layer 3 and Layer 4 traffic policy. This class map is a reserved class map created by the ACE. You cannot delete or modify this class. All network 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 match, the ACE then matches the action specified under the **class class-default** command. The class-default class map has an implicit **match any** statement in it and is used to match any traffic classification.

For example, to specify an existing class map within the Layer 3 and Layer 4 remote access policy map, enter:

```
host1/Admin(config-pmap-mgmt)# class SNMP-ALLOW_CLASS
host1/Admin(config-pmap-mgmt-c)#
```

To use the **insert-before** command to define the sequential order of two class maps in the policy map, enter:

```
host1/Admin(config-pmap-mgmt)# class L4_SSH_CLASS insert-before L4_REMOTE_ACCESS_CLASS
```

To specify the class-default class map for the Layer 3 and Layer 4 traffic policy, enter:

```
host1/Admin(config-pmap-mgmt)# class class-default
host1/Admin(config-pmap-mgmt-c)#
```

To remove a class map from a Layer 3 and Layer 4 policy map, enter:

```
host1/Admin(config-pmap-mgmt)# no class SNMP-ALLOW_CLASS
```

### Specifying Layer 3 and Layer 4 Policy Actions

To allow the network management traffic listed in the Layer 3 and Layer 4 class map to be received or rejected by the ACE, specify either the **permit** or **deny** command in policy map class configuration mode as follows:

- Use the **permit** command in policy map class configuration mode to allow the SNMP management protocols listed in the class map to be received by the ACE.
- Use the **deny** command in policy map class configuration mode to refuse the SNMP management protocols listed in the class map to be received by the ACE.
For example, to specify the permit action for the Layer 3 and Layer 4 policy map, enter:

```plaintext
host1/Admin(config-pmap-mgmt-c)# permit
host1/Admin(config-pmap-mgmt-c)# exit
```

## Applying a Service Policy

The `service-policy` command allows you to perform the following tasks:

- Apply a previously created policy map.
- Attach the traffic policy to a specific VLAN interface or globally to all VLAN interfaces in the same context.
- Specify that the traffic policy is to be attached to the input direction of an interface.

The `service-policy` command is available at both configuration mode and interface configuration mode. Specifying a policy map in the interface configuration mode applies the policy map to a specific VLAN interface. Specifying a policy map in the configuration mode applies the policy to all of the VLAN interfaces associated with a context.

The syntax of this command is as follows:

```plaintext
service-policy input policy_name
```

The keywords and arguments are as follows:

- `input`—Specifies that the traffic policy is to be attached to the input direction of an interface. The traffic policy evaluates all traffic received by that interface.
- `policy_name`—Name of a previously defined policy map, configured with a previously created `policy-map` command. The name can be a maximum of 40 alphanumeric characters.

For example, to specify an interface VLAN and apply the SNMP management policy map to a VLAN, enter:

```plaintext
host1/Admin(config)# interface vlan 50
host1/Admin(config-if)# ip address 172.20.1.100 255.255.0.0
host1/Admin(config-if)# service-policy input SNMP_MGMT_ALLOW_POLICY
```
For example, to globally apply the SNMP management policy map to all of the VLANs associated with a context, enter:

```
host1/Admin(config)# service-policy input SNMP_MGMT_ALLOW_POLICY
```

To detach the SNMP management policy from an interface VLAN, enter:

```
host1/Admin(config-if)# no service-policy input SNMP_MGMT_ALLOW_POLICY
```

To globally detach the SNMP management policy from all VLANs associated with a context, enter:

```
host1/Admin(config)# no service-policy input SNMP_MGMT_ALLOW_POLICY
```

You can detach a traffic policy by one of these methods:

- Individually from the last VLAN interface on which you applied the service policy
- Globally from all VLAN interfaces in the same context

When you detach a policy, the ACE automatically resets the associated service policy statistics to provide a new starting point for the service policy statistics the next time that you attach a traffic policy to a specific VLAN interface or globally to all VLAN interfaces in the same context.

The following guidelines and restrictions apply when you create a service policy:

- Policy maps, applied globally in a context, are internally applied on all interfaces existing in the context.
- A policy activated on an interface overwrites any specified global policies for overlapping classification and actions.
- The ACE allows only one policy of a specific feature type to be activated on an interface.

To display service policy statistics for a Layer 3 and Layer 4 SNMP management policy map, use the `show service-policy` command in Exec mode.

The syntax of this command is as follows:

```
show service-policy policy_name [detail]
```

**Note**

The ACE updates the counters that the `show service-policy` command displays after the applicable connections are closed.
The keywords, options, and arguments are as follows:

- **policy_name**—Identifier of an existing policy map that is currently in service (applied to an interface) as an unquoted text string with a maximum of 64 alphanumeric characters.

- **detail**—(Optional) Displays a more detailed listing of policy map statistics and status information.

For example, to display service policy statistics for the SNMP_MGMT_ALLOW_POLICY policy map, enter:

```
host1/Admin# show service-policy SNMP_MGMT_ALLOW_POLICY
Status     : ACTIVE
Description: Allow mgmt protocols
-----------------------------------------
Context Global Policy:
   service-policy: SNMP_MGMT_ALLOW_POLICY
```

To clear the service policy statistics, use the `clear service-policy` command. The syntax of this command is as follows:

```
clear service-policy policy_name
```

For the `policy_name` argument, enter the identifier of an existing policy map that is currently in service (applied to an interface).

For example, to clear the statistics for the policy map SNMP_MGMT_ALLOW_POLICY that is currently in service, enter:

```
host1/Admin# clear service-policy SNMP_MGMT_ALLOW_POLICY
```
Example of an SNMP Configuration

The following example illustrates a running-configuration that verifies the current status of a real server through SNMP and the CLI. It also verifies that SNMP traps are sent when a real server or virtual server is not operational. This example illustrates that you can restrict the client source host IP address allowed to connect to the ACE. The policy map is applied to all of the VLAN interfaces associated with the context. The SNMP configuration appears in bold in the example.

```
access-list ACL1 line 10 extended permit ip any any
rserver host SERVER1
   ip address 192.168.252.245
   inservice
rserver host SERVER2
   ip address 192.168.252.246
   inservice
rserver host SERVER3
   ip address 192.168.252.247
   inservice

serverfarm host SFARM1
   probe HTTP_PROBE
   rserver SERVER1
      conn-limit max 3 min 2
      inservice
serverfarm host SFARM2
   probe HTTP
   rserver SERVER2
      conn-limit max 500 min 2
      inservice
   rserver SERVER3
      conn-limit max 500 min 2
      inservice

class-map type http loadbalance match-all L7_INDEX-HTML_CLASS
   2 match http url /index.html
class-map match-all L4_MAX-CONN-VIP_105_CLASS
   2 match virtual-address 192.168.120.105 any
class-map type management match-any L4_REMOTE-ACCESS-LOCAL_CLASS
description Enables SNMP remote management for local users
   1 match protocol snmp source-address 192.168.0.0 255.255.255.0
   2 match protocol snmp source-address 172.16.64.0 255.255.255.0
class-map type http loadbalance match-all L7_URL_*_CLASS
   2 match http url .*
```
policy-map type management first-match L4_SNMP-REMOTE-MGT_POLICY
   class L4_REMOTE-ACCESS-LOCAL_CLASS
      permit
policy-map type loadbalance first-match L7_LB-SF_MAX-CONN_POLICY
   class L7_INDEX-HTML_CLASS
      serverfarm SFARM1
   class L7_URL_CLASS
      serverfarm SFARM2
policy-map multi-match L4_VIP_POLICY
   class L4_MAX-CONN-VIP_105_CLASS
      loadbalance vip inservice
      loadbalance policy L7_LB-SF_MAX-CONN_POLICY
      loadbalance vip icmp-reply
      appl-parameter http advanced-options PERSIST-REBALANCE

service-policy input L4_REMOTE-MGT_POLICY

snmp-server user user1 Network-Monitor auth sha “adcd1234”
snmp-server community ACE-public group ro
snmp-server contact “User1 user1@cisco.com”
snmp-server location “San Jose CA”
snmp-server host 192.168.0.236 traps version 2c ACE-public
snmp-server enable traps slb vserver
snmp-server enable traps slb real
snmp-server enable traps syslog
snmp-server enable traps snmp authentication
snmp-server enable traps snmp linkup
snmp-server enable traps snmp linkdown

Displaying SNMP Statistics

To display SNMP statistics and configured SNMP information, use the show
snmp commands in Exec mode. By default, this command displays the ACE
contact, ACE location, packet traffic information, community strings, and user
information. You can instruct the ACE to display specific SNMP information by
including the appropriate keyword.

The syntax of this command is as follows:

    show snmp [community | engineID | group | host | sessions | user]
The keywords are as follows:

- **community**—(Optional) Displays SNMP community strings.
- **engineID**—(Optional) Displays the identification of the local SNMP engine and all remote engines that have been configured on the ACE.
- **group**—(Optional) Displays the names of groups on the ACE, the security model, the status of the different views, and the storage type of each group.
- **host**—(Optional) Displays the configured SNMP notification recipient host, User Datagram Protocol (UDP) port number, user, and security model.
- **sessions**—(Optional) Displays the IP address of the targets for which traps or informs have been sent.
- **user**—(Optional) Displays SNMPv3 user information.

Table 7-5 describes the fields in the `show snmp community` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sys contact</td>
<td>Contact name for the SNMP system</td>
</tr>
<tr>
<td>Sys location</td>
<td>SNMP system location</td>
</tr>
<tr>
<td>SNMP packets input</td>
<td>Total number of SNMP packets received by the ACE</td>
</tr>
<tr>
<td>Bad SNMP versions</td>
<td>Number of packets with an invalid SNMP version</td>
</tr>
<tr>
<td>Unknown community name</td>
<td>Number of SNMP packets with an unknown community name</td>
</tr>
<tr>
<td>Illegal operation for community name supplied</td>
<td>Number of packets that request an operation not allowed for that community</td>
</tr>
<tr>
<td>Encoding errors</td>
<td>Number of SNMP packets that were improperly encoded</td>
</tr>
<tr>
<td>Number of requested variables</td>
<td>Number of variables requested by SNMP managers</td>
</tr>
<tr>
<td>Number of altered variables</td>
<td>Number of variables altered by SNMP managers</td>
</tr>
</tbody>
</table>
Chapter 7 Configuring SNMP

Displaying SNMP Statistics

Table 7-5 Field Descriptions for the show snmp Command Output (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get-request PDUs</td>
<td>Number of get requests received</td>
</tr>
<tr>
<td>Get-next PDUs</td>
<td>Number of get-next requests received</td>
</tr>
<tr>
<td>Set-request PDUs</td>
<td>Number of set requests received</td>
</tr>
<tr>
<td>SNMP packets output</td>
<td>Total number of SNMP packets sent by the ACE</td>
</tr>
<tr>
<td>Too big errors</td>
<td>Number of SNMP packets that were larger than the maximum packet size</td>
</tr>
<tr>
<td>No such name errors</td>
<td>Number of SNMP requests that specified a MIB object that does not exist</td>
</tr>
<tr>
<td>Bad values errors</td>
<td>Number of SNMP set requests that specified an invalid value for a MIB object</td>
</tr>
<tr>
<td>General errors</td>
<td>Number of SNMP set requests that failed due to some other error, such as a noSuchName error, badValue error, or any of the other specific errors</td>
</tr>
<tr>
<td>Community</td>
<td>SNMP community name for the ACE</td>
</tr>
<tr>
<td>Group/Access</td>
<td>Access rights for the community, read-only</td>
</tr>
<tr>
<td>User</td>
<td>String that identifies the name of the SNMP user</td>
</tr>
<tr>
<td>Auth</td>
<td>Authentication of a packet without encryption</td>
</tr>
<tr>
<td>Priv</td>
<td>Authentication of a packet with encryption</td>
</tr>
<tr>
<td>Group</td>
<td>User role group to which the user belongs</td>
</tr>
</tbody>
</table>

Table 7-6 describes the fields in the show snmp community command output.

Table 7-6 Field Descriptions for the show snmp community Command Output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community</td>
<td>SNMP community name for the ACE</td>
</tr>
<tr>
<td>Group/Access</td>
<td>Access rights for the community, read-only</td>
</tr>
</tbody>
</table>
Table 7-7 describes the fields in the `show snmp engineID` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local SNMP engineID</td>
<td>Identification number of the local SNMP engine on the ACE</td>
</tr>
</tbody>
</table>

Table 7-8 describes the fields in the `show snmp group` command output.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group name</td>
<td>Name of the SNMP group or collection of users that have a common access policy</td>
</tr>
<tr>
<td>Security model</td>
<td>Security model used by the group, either v1, v2c, or v3</td>
</tr>
<tr>
<td>Security level</td>
<td>Security level used by the group</td>
</tr>
<tr>
<td>Read view</td>
<td>String that identifies the read view of the group</td>
</tr>
<tr>
<td>Write view</td>
<td>String that identifies the write view of the group</td>
</tr>
<tr>
<td>Notify view</td>
<td>String that identifies the notify view of the group</td>
</tr>
<tr>
<td>Storage-type</td>
<td>Status of whether the settings have been set in volatile or temporary memory on the device or in nonvolatile or persistent memory where settings will remain after the device has been turned off and on again</td>
</tr>
<tr>
<td>Row status</td>
<td>Indicates whether the Row status for the SNMP group is active or inactive</td>
</tr>
</tbody>
</table>

Table 7-9 describes the fields in the `show snmp host` command output.
Chapter 7      Configuring SNMP

Displaying SNMP Statistics

Table 7-9  Field Descriptions for the show snmp host Command Output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>IP address of the target host</td>
</tr>
<tr>
<td>Port</td>
<td>UDP port number to which notifications will be sent</td>
</tr>
<tr>
<td>Version</td>
<td>Version of SNMP used to send the trap, either v1, v2c, or v3</td>
</tr>
<tr>
<td>Level</td>
<td>Method for authentication and privacy</td>
</tr>
<tr>
<td>Type</td>
<td>Type of notification configured</td>
</tr>
<tr>
<td>SecName</td>
<td>Security name for scanning the target host</td>
</tr>
</tbody>
</table>

Table 7-10 describes the fields in the show snmp sessions command output.

Table 7-10  Field Descriptions for the show snmp sessions Command Output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>IP address of a target for which traps or informs have been sent</td>
</tr>
</tbody>
</table>

Table 7-11 describes the fields in the show snmp user command output.

Table 7-11  Field Descriptions for the show snmp user Command Output

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>String identifying the name of the SNMP user</td>
</tr>
<tr>
<td>Auth</td>
<td>Authentication of a packet without encryption</td>
</tr>
<tr>
<td>Priv</td>
<td>Authentication of a packet with encryption</td>
</tr>
<tr>
<td>Group</td>
<td>User role group to which the user belongs</td>
</tr>
</tbody>
</table>
Displaying SNMP Statistics
This chapter describes how to use Extensible Markup Language (XML) to remotely configure a Cisco Application Control Engine (ACE) module from a network management station (NMS). Any command that you can configure from the ACE CLI can be configured remotely from a NMS by exchanging XML documents over HTTP or secure HTTP (HTTPS). You can transmit, exchange, and interpret data among the applications. In addition, you can configure the ACE to transfer show command output to an NMS in XML format for result monitoring and analysis. To use the ACE XML interface, you must have the Admin user role.

This chapter contains the following major sections:

- XML Overview
- XML Configuration Quick Start
- Configuring HTTP and HTTPS Management Traffic Services
- Enabling the Display of Raw XML Request show Command Output in XML Format
- Accessing the ACE DTD File

**Note**

The ACE creates two default user accounts at startup: admin and www. The admin user is the global administrator and cannot be deleted. The ACE uses the www user account for the XML interface and www cannot be deleted.
Caution

If you upgrade your ACE software to version A2(1.1) or higher, you must change the default www user password if you have not already done so. Otherwise, after you upgrade the ACE software, the www user will be disabled and you will not be able to use XML to remotely configure an ACE until you change the default www user password. See Chapter 2, Configuring Virtualization, in the Cisco Application Control Engine Module Virtualization Configuration Guide for details on changing a user account password. In this case, the user would be www.

XML Overview

This section contains the following topics:

- XML Usage with the ACE
- HTTP and HTTPS Support with the ACE
- HTTP Return Codes
- Document Type Definition
- Sample XML Configuration

XML Usage with the ACE

Web services provide network-based software applications that use XML to transmit, exchange, and interpret data among applications that would otherwise have difficulty interoperating together.

XML provides an application-independent way of sharing data between computer systems. Similar to HTML, XML consists of text delimited by tags so it is easily conveyed over the Internet. In XML, the tags define the meaning and structure of the information, enabling computer applications to use the information directly. Unlike HTML, XML tags identify the data, rather than specifying how to display it. An XML tag acts like a field name in your program; it puts a label on a piece of data that identifies it (for example: <message>...</message>).

An XML document that contains configuration commands and output results is easily transformed between the devices by using standard Internet protocols such as HTTP or secure HTTP (HTTPS) as the transfer protocol.
The XML application programming interface (API) allows you to automate the programmatic configuration of the ACE by using a Document Type Definition (DTD). The XML format is a translation of the CLI commands into an equivalent XML syntax. Each ACE CLI command has an equivalent XML tag, and all of the parameters of the CLI command are attributes of that element. The ACE uses an Apache HTTP server to provide the XML management interface and to provide HTTP services between the ACE and the management client. To use the ACE XML API, you must have the Admin user role.

You can use XML to do the following:

- Provide a mechanism using XML to transfer, configure, and monitor objects in the ACE. This XML capability allows you to easily shape or extend the CLI query and reply data in XML format to meet different specific business needs.
- Transfer `show` command output from the ACE CLI interface in an XML format for statistics and status monitoring. This capability allows you to query and extract data from the ACE.
- Use the ACE XML DTD schema for formatting CLI queries or parsing the XML results from the ACE to enable third-party software development through XML communications.
- Provide remote user authentication through AAA.
- Provide session and context management by the global administrator and other privileged users that have the Admin user role.

A network management station (NMS), such as the CiscoWorks Hosting Solution Engine (HSE), can connect to the ACE and push new configurations to it over HTTP or HTTPS.

**HTTP and HTTPS Support with the ACE**

The ACE and an NMS can easily send and receive an XML document containing configuration commands or output results by using standard Internet protocols, such as HTTP or secure HTTP (HTTPS), as the transfer protocol. HTTPS uses Secure Sockets Layer (SSL) to provide encrypted communication between the management client and the ACE.

The administrator of the system designates a website as the entry point to the API, and all requests and queries are made through those URLs. This website also provides the DTDs that define the XML for requests, queries, and responses.
The XML input is submitted through the data portion of an HTTP POST request. A field named “xml” contains the XML string that defines the request or query. The response to this HTTP POST represents a pure XML response with either a success or failure indicator for a request or the response to a query.

When you use XML to transfer configuration data and results, the NMS connects to the ACE and sends a new configuration in an XML document to the ACE over HTTP or HTTPS. The ACE then applies the new configuration.

The following example shows the HTTP conversation between the client and the server, as related to the XML implementation on the ACE:

******** Client **************
POST /bin/xml_agent HTTP/1.1
Authorization: Basic VTpQ
Content-Length: 95
xml_cmds=<request_xml>
<interface type="vlan" number="80">
<access-group access-type="input" name="acl1"/>
<ip_address address="60.0.0.145" netmask="255.255.255.0"/>
<shutdown sense="no"/>
</interface>
<show_running-config/>
</request_xml>

******** Server **************
HTTP/1.1 200 OK
Content-Length: 21
<response_xml>
<config_command>
<command>
interface vlan 80
ip address 60.0.0.145 255.255.255.0
access-group input acl1
no shutdown
</command>
<status code="100" text="XML_CMD_SUCCESS"/>
</config_command>
</response_xml>

******** Client **************
POST /bin/xml_agent HTTP/1.1
Content-Length: 95
xml_cmds=<request_xml>
<show_running-config/>
</request_xml>
HTTP Return Codes

HTTP return codes indicate the status of the request and reports errors between the server and the client. The Apache HTTP server return status codes follow the standards outlined in RFC 2616. Table 8-1 lists the supported HTTP return codes.

<table>
<thead>
<tr>
<th>Return Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>OK</td>
</tr>
<tr>
<td>201</td>
<td>Created</td>
</tr>
<tr>
<td>202</td>
<td>Accepted</td>
</tr>
<tr>
<td>203</td>
<td>Non-Authoritative Information</td>
</tr>
<tr>
<td>206</td>
<td>Partial Content</td>
</tr>
<tr>
<td>301</td>
<td>Moved Permanently</td>
</tr>
<tr>
<td>302</td>
<td>Found</td>
</tr>
<tr>
<td>400</td>
<td>Bad Request</td>
</tr>
<tr>
<td>401</td>
<td>Unauthorized (credentials required, but not provided)</td>
</tr>
<tr>
<td>403</td>
<td>Forbidden (illegal credentials submitted; syslog also generated)</td>
</tr>
<tr>
<td>404</td>
<td>Not Found (“/xml-config” not specified)</td>
</tr>
<tr>
<td>405</td>
<td>Method Not Allowed</td>
</tr>
<tr>
<td>406</td>
<td>Not Acceptable</td>
</tr>
<tr>
<td>408</td>
<td>Request Time-out (more than 30 seconds has passed waiting on receive)</td>
</tr>
<tr>
<td>411</td>
<td>Missing Content-Length (missing or zero Content-Length field)</td>
</tr>
<tr>
<td>500</td>
<td>Internal Server Error</td>
</tr>
</tbody>
</table>
The following HTTP headers are supported:

- **Content-Length** (nonzero value required for all POSTs)
- **Connection** (*close* value indicates that a request should not be persistent)
- **WWW-Authenticate** (sent to the client when credentials are required and missing)
- **Authorization** (sent from the client to specify basic credentials in base 64 encoding)

For example, when an XML error occurs, the HTTP response contains a 200 return code. The portion of the original XML document with the error is returned with an error element that contains the error type and description.

The following is a typical example of an XML error response:

```xml
<response_xml>
  <config_command>
    <command>
      interface vlan 20
      no shut
      description xyz
      exit
    </command>
  </config_command>
  <status code = '200' text='XML_CMD_FAILURE'>
    <error_command> description xyz </error_command>
    <error_message> unrecognized element - description </error_message>
  </status>
</response_xml>
```
The returned error codes correspond to the attributes of the configuration element. The possible returned XML error can include any of the following:

- XML_ERR_WELLFORMEDNESS /* not a well formed xml document */
- XML_ERR_ATTR_INVALID     /* found invalid value attribute */
- XML_ERR_ELEM_INVALID     /* found invalid value unrecognized */
- XML_ERR_CDL_NOT_FOUN     /* parser cdl file not found */
- XML_ERR_INTERNAL         /* internal memory or coding error */
- XML_ERR_COMM_FAILURE     /* communication failure */
- XML_ERR_VSH_PARSER       /* vsh parse error on the given command */
- XML_ERR_VSH_CONF_APPLY   /* vsh unable to apply the configuration */

Document Type Definition

A DTD is the basis for XML configuration documents that you create using the ACE. The purpose of a DTD is to define the legal building blocks of an XML document by defining the document structure with a list of legal elements.

DTD designates an XML list that specifies precisely which elements can appear in a request, query, or response document. It also specifies the contents and attributes of the elements. A DTD can be declared inline in your XML document or as an external reference.

The ACE DTD file, cisco_ace.dtd, is included as part of the software image and is accessible from a web browser using either HTTP or HTTPS. See the “Accessing the ACE DTD File” section for details. You can use a web browser to either directly access the cisco_ace.dtd file or open the cisco_ace.dtd file from the Cisco ACE Module Management page.

The following example shows the sequence of ACE CLI commands for creating a real server followed by the associated DTD XML rserver elements for the commands:

```
[no] rserver [host | redirect] name
[no] conn-limit max maxconns [min minconns]
[no] description string
[no] inservice
[no] ip address {ip_address}
[no] probe name
[no] weight number
```
Elements, Attributes and Entities required for rserver

-->

<!--
probe-name is a string of length 1 to 32.
-->  
<!ELEMENT probe_rserver EMPTY>
<!ATTLIST probe_rserver
  sense  CDATA  #FIXED  "no"
  probe-name  CDATA  #REQUIRED
>

<!--
relocation-str length is 1 to 127
-->  
<!ELEMENT webhost-redirection EMPTY>
<!ATTLIST webhost-redirection
  sense  (yes | no)  #IMPLIED
  relocation-string  CDATA  #REQUIRED
  redirection-code  (301 | 302)  #IMPLIED
>

<!--
type is optional for host.
ip, probe and weight are valid only when type = host.
address-type is valid only when type=host.
name length is 1 to 32.
webhost-redirection is valid only if type=redirect.
-->  
<!ELEMENT rserver (description, ip_address, conn-limit, probe_rserver, weight, inservice, webhost-redirection)*>
<!ATTLIST rserver
  sense  CDATA  #FIXED  "no"
  type  (redirect | host)  #IMPLIED
  name  CDATA  #REQUIRED
>
Sample XML Configuration

The following example shows a typical VShell (VSH) CLI command configuration and its equivalent XML configuration commands:

```
# TO/FROM CP CONFIGURATION#
conf t
access-list acl1 extended permit ip any any
int vlan 80
access-group input acl1
ip address 60.0.0.145 255.255.255.0
no shut
exit
ip route 0.0.0.0 0.0.0.0 60.0.0.1
end

<access-list id="acl1" config-type="extended" perm-value="permit"
protocol-name="ip" src-type="any" dest-type="any"/>
<int INTERFACE type="vlan" number="80">
<access-group type="input" name="acl1"/>
<ip_address address="60.0.0.145" netmask="255.255.255.0"/>
<shutdown sense="no"/>
</interface>

<ip_route dest-address="0.0.0.0" dest-mask="0.0.0.0"
gateway="60.0.0.1"/>

# BRIDGING CONFIGURATION#
conf t

access-list acl1 extended permit ip any any
int vlan 80
access-group input acl1
bridge-group 1
no shut
exit
int vlan 90
access-group input acl1
bridge-group 1
no shut
exit
end
```
<access-list id="acl1" config-type="extended" perm-value="permit" protocol-name="ip" src-type="any" dest-type="any"/>
<interface type="vlan" number="80">
  <access-group type="input" name="acl1"/>
  <bridge-group value="1"/>
  <shutdown sense="no"/>
</interface>
<interface type="vlan" number="90">
  <access-group type="input" name="acl1"/>
  <bridge-group value="1"/>
  <shutdown sense="no"/>
</interface>
XML Configuration Quick Start

Table 8-2 provides a quick overview of the steps required to configure XML usage with the ACE. Each step includes the CLI command required to complete the task.

Table 8-2  ACE XML Configuration Quick Start

<table>
<thead>
<tr>
<th>Task and Command Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. If you are operating in multiple contexts, observe the CLI prompt to verify that you are operating in the desired context. If necessary, log directly in to, or change to, the correct context.</td>
</tr>
<tr>
<td>host1/Admin# changeto C1</td>
</tr>
<tr>
<td>host1/C1#</td>
</tr>
<tr>
<td>The rest of the examples in this table use the Admin context, unless otherwise specified. For details on creating contexts, see the Cisco Application Control Engine Module Virtualization Configuration Guide.</td>
</tr>
<tr>
<td>2. Enter configuration mode.</td>
</tr>
<tr>
<td>host1/Admin# config</td>
</tr>
<tr>
<td>Enter configuration commands, one per line. End with CNTL/Z.</td>
</tr>
<tr>
<td>host1/Admin(config)#</td>
</tr>
<tr>
<td>3. Create a Layer 3 and Layer 4 class map to classify the HTTP or HTTPS management traffic that can be received by the ACE.</td>
</tr>
<tr>
<td>host1/Admin(config)# class-map type management match-all HTTPS-ALLOW_CLASS</td>
</tr>
<tr>
<td>host1/Admin(config-cmap-mgmt)# match protocol https source-address 192.168.1.1 255.255.255.255</td>
</tr>
<tr>
<td>host1/Admin(config-cmap-mgmt)# exit</td>
</tr>
<tr>
<td>4. Configure a Layer 3 and Layer 4 HTTP or HTTPS traffic management policy.</td>
</tr>
<tr>
<td>host1/Admin(config)# policy-map type management first-match MGMT_HTTPS_POLICY</td>
</tr>
<tr>
<td>host1/Admin(config-pmap-mgmt)# class HTTPS-ALLOW_CLASS</td>
</tr>
<tr>
<td>host1/Admin(config-pmap-mgmt-c)# permit</td>
</tr>
<tr>
<td>host1/Admin(config-pmap-mgmt-c)# exit</td>
</tr>
</tbody>
</table>
Configuring HTTP and HTTPS Management Traffic Services

The ACE provides support for remote management using XML over either HTTP or HTTPS to configure, monitor, and manage software objects. You configure HTTP and HTTPS remote management traffic to the ACE through class maps, policy maps, and service policies.

The following items summarize the role of each function in configuring HTTP or HTTPS network management access to the ACE:

- **Class map**—Provides the remote network traffic match criteria to permit HTTP and HTTPS management traffic based on HTTP or HTTPS network management protocols or host source IP addresses.

- **Policy map**—Enables remote network management access for a traffic classification that matches the criteria listed the class map.

**Task and Command Example**

5. Attach the traffic policy to a single interface or globally on all VLAN interfaces associated with a context, and specify the direction in which the policy should be applied. For example, to specify an interface VLAN and apply multiple service policies to the VLAN, enter:

```bash
host1/Admin(config)# interface vlan50
host1/Admin(config-if)# ip address 192.168.10.1 255.255.0.0
host1/Admin(config-if)# service-policy input MGMT_HTTPS_POLICY
host1/Admin(config-if)# exit
host1/Admin(config)# exit
```

6. (Optional) Enable the display of raw XML request show command output in XML format.

   **Note**  
   True XML responses always automatically appear in XML format.

   ```bash
   host1/Admin# xml-show on
   ```

7. (Optional) Save your configuration changes to Flash memory.

   ```bash
   host1/Admin# copy running-config startup-config
   ```
Chapter 8 Configuring the XML Interface

Configuring HTTP and HTTPS Management Traffic Services

• Service policy—Activates the policy map and attaches the traffic policy to an interface or globally on all interfaces.

HTTP or HTTPS sessions are established to the ACE per context. For details on creating contexts and users, see the Cisco Application Control Engine Module Virtualization Configuration Guide.

This section contains the following topics:
• Creating and Configuring a Class Map
• Creating a Layer 3 and Layer 4 Policy Map
• Applying a Service Policy

Creating and Configuring a Class Map

To create a Layer 3 and Layer 4 class map to classify the HTTP or HTTPS management traffic that can be received by the ACE, use the class-map type management configuration command. This command allows network management traffic by identifying the incoming IP protocols that the ACE can receive and the client source host IP address and subnet mask as the matching criteria. A class map of type management defines the allowed network traffic as a form of management security for protocols such as HTTP and HTTPS.

A class map can have multiple match commands in a class map. You can configure class maps to define multiple HTTP or HTTPS management protocol or source IP address match commands in a group that you then associate with a traffic policy. The match-all and match-any keywords determine how the ACE evaluates multiple match statements operations when multiple match criteria exist in a class map.

The syntax of this command is as follows:

class-map type management [match-all | match-any] map_name

The keywords, arguments, and options are as follows:
• match-all | match-any—(Optional) Determines how the ACE evaluates Layer 3 and Layer 4 network traffic when multiple match criteria exist in a class map. The class map is considered a match if the match commands meet one of the following conditions:
- **match-all**—(Default) All of the match criteria listed in the class map match the network traffic class in the class map.
- **match-any**—Only one of the match criteria listed in the class map matches the network traffic class in the class map.

*map_name*—Name assigned to the class map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters. The class name is used for both the class map and to configure a policy for the class in the policy map.

When you use the **class-map type management** command, you will access class map management configuration mode. This mode allows you to configure a description or the matching criteria for the class map.

You may include multiple **match protocol** commands in a class map.

For example, to allow HTTPS access between the ACE HTTP server and the management client located at IP address 192.168.1.1 255.255.255.255, enter:

```
host1/Admin(config)# class-map type management match-all HTTPS-ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# match protocol https source-address 192.168.1.1 255.255.255.255
```

To remove a Layer 3 and Layer 4 network management class map from the ACE, enter:

```
host1/Admin(config)# no class-map type management match-all HTTPS-ALLOW_CLASS
```

To classify the remote HTTP or HTTPS management traffic received by the ACE, include one or more of the following commands to configure the match criteria for the class map:

- **description**—See the “Defining a Class Map Description” section
- **match protocol**—See the “Defining HTTP and HTTPS Protocol Match Criteria” section
Defining a Class Map Description

To provide a brief summary about the Layer 3 and Layer 4 remote management class map, use the `description` command in class map management configuration mode.

The syntax of this command is as follows:

```
description text
```

The `text` argument is the description that you want to provide. Enter an unquoted text string with a maximum of 240 alphanumeric characters.

For example, to specify a description that the class map is to allow HTTPS access, enter:

```
host1/Admin(config)# class-map type management match-all HTTPS-ALLOW_CLASS
host1/Admin(config-cmap-mgmt)# description Allow HTTPS access to the ACE
```

To remove the description from the class map, enter:

```
host1/Admin(config-cmap-mgmt)# no description
```

Defining HTTP and HTTPS Protocol Match Criteria

To configure the class map to specify that the HTTP or HTTPS remote network management protocol can be received by the ACE, use the `match protocol` command in class map management configuration mode. You configure the associated policy map to permit access to ACE for the specified management protocol. For XML support, a class map of type management allows IP protocols such as HTTP and HTTPS. As part of the network management access traffic classification, you also specify either a client source host IP address and subnet mask as the matching criteria or instruct the ACE to allow any client source address for the management traffic classification.

The syntax of this command is as follows:

```
[line_number] match protocol {http | https} {any | source-address ip_address mask}
```
The keywords, arguments, and options are as follows:

- **line_number**—(Optional) Line number that allows you to edit or delete individual match commands. Enter an integer from 2 to 255 as the line number. For example, you can enter `no line_number` to delete long match commands instead of entering the entire line.

- **http**—Configures management access between the ACE HTTP server and the management client over HTTP.

- **https**—Configures management access between the ACE HTTP server and the management client over secure HTTP.

- **any**—Specifies any client source address for the management traffic classification.

- **source-address**—Specifies a client source host IP address and subnet mask as the network traffic matching criteria. As part of the classification, the ACE implicitly obtains the destination IP address from the interface on which you apply the policy map.

- **ip_address**—Source IP address of the client. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).

- **mask**—Subnet mask of the client in dotted-decimal notation (for example, 255.255.255.0).

For example, to specify that the class map allows HTTPS access to the ACE, enter:

```
(config)# class-map type management HTTPS-ALLOW_CLASS
(config-cmap-mgmt)# match protocol https source-address 192.168.10.1 255.255.0.0
```

To deselect the specified network management protocol match criteria from the class map, enter:

```
host1/Admin(config-cmap-mgmt)# no match protocol https source-address 192.168.10.1 255.255.0.0
```
Creating a Layer 3 and Layer 4 Policy Map

A Layer 3 and Layer 4 policy map defines the actions executed on HTTP or HTTPS management traffic that matches the specified classifications. This section contains the following topics:

- Creating a Layer 3 and Layer 4 Policy Map for Network Management Traffic Received by the ACE
- Specifying a Layer 3 and Layer 4 Traffic Class with the Traffic Policy
- Specifying Layer 3 and Layer 4 Policy Actions

Creating a Layer 3 and Layer 4 Policy Map for Network Management Traffic Received by the ACE

To configure a Layer 3 and Layer 4 policy map that permits the management traffic received by the ACE use the `policy-map type management` command in configuration mode. The ACE executes the action for the first matching classification. The ACE does not execute any additional actions.

The syntax of this command is as follows:

```
policy-map type management first-match map_name
```

The `map_name` argument specifies the name assigned to the Layer 3 and Layer 4 network management policy map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

When you use this command, you will access policy map management configuration mode.

For example, to create a Layer 3 and Layer 4 network traffic management policy map, enter:

```
host1/Admin(config)# policy-map type management first-match MGMT_HTTPS_POLICY
```

To remove a policy map from the ACE, enter:

```
host1/Admin(config)# no policy-map type management first-match MGMT_HTTPS_POLICY
```
Specifying a Layer 3 and Layer 4 Traffic Class with the Traffic Policy

To specify the HTTP or HTTPS traffic management traffic class created with the `class-map` command to associate traffic with the traffic policy, use the `class` command. This command enters the policy map management class configuration mode.

The syntax of this command is as follows:

```
class {name1 [insert-before name2] | class-default}
```

The arguments, keywords, and options are as follows:

- `name1`—Name of a previously defined Layer 3 and Layer 4 traffic class, configured with the `class-map` command, to associate traffic to the traffic policy. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

- `insert-before name2`—(Optional) Places the current class map ahead of an existing class map or inline match condition specified by the `name2` argument in the policy map configuration. The ACE does not save the sequence reordering as part of the configuration. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

- `class-default`—Specifies the class-default class map for the Layer 3 and Layer 4 traffic policy. This class map is a reserved class map created by the ACE. You cannot delete or modify this class. All network 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 match, the ACE then matches the action specified under the `class class-default` command. The class-default class map has an implicit `match any` statement in it and is used to match any traffic classification.

For example, to specify an existing class map within the Layer 3 and Layer 4 remote access policy map, enter:

```
host1/Admin(config-pmap-mgmt)# class HTTPS-ALLOW_CLASS
```

To use the `insert-before` command to define the sequential order of two class maps in the policy map, enter:

```
host1/Admin(config-pmap-mgmt)# class HTTPS-ALLOW_CLASS insert-before L4_REMOTE_ACCESS_CLASS
```
To specify the class-default class map for the Layer 3 and Layer 4 traffic policy, enter:

```
host1/Admin(config-pmap-mgmt)# class class-default
host1/Admin(config-pmap-mgmt-c)#
```

To remove a class map from a Layer 3 and Layer 4 policy map, enter:

```
host1/Admin(config-pmap-mgmt)# no class HTTPS-ALLOW_CLASS
```

### Specifying Layer 3 and Layer 4 Policy Actions

To allow the network management traffic listed in the Layer 3 and Layer 4 class map to be received or rejected by the ACE, specify either the `permit` or `deny` command in policy map class configuration mode as follows:

- Use the `permit` command in policy map class configuration mode to allow the HTTP or HTTPS management traffic listed in the class map to be received by the ACE.
- Use the `deny` command in policy map class configuration mode to refuse the HTTP or HTTPS management traffic listed in the class map to be received by the ACE.

For example, to specify the permit action for the Layer 3 and Layer 4 policy map, enter:

```
host1/Admin(config-pmap-mgmt-c)# permit
host1/Admin(config-pmap-mgmt-c)# exit
```

### Applying a Service Policy

Use the `service-policy` command to do the following:

- Apply a previously created policy map.
- Attach the traffic policy to a specific VLAN interface or globally to all VLAN interfaces in the same context.
- Specify that the traffic policy is to be attached to the input direction of an interface.
The `service-policy` command is available at both the VLAN interface configuration mode and at the configuration mode. Specifying a policy map in the interface configuration mode applies the policy map to a specific VLAN interface. Specifying a policy map in the configuration mode applies the policy to all of the VLAN interfaces associated with a context.

The syntax of this command is as follows:

```
service-policy input policy_name
```

The keywords and options are as follows:

- **input**—Specifies that the traffic policy is to be attached to the input direction of an interface. The traffic policy evaluates all traffic received by that interface.

- **policy_name**—Name of a previously defined policy map, configured with a previously created `policy-map` command. The name can be a maximum of 40 alphanumeric characters.

For example, to specify an interface VLAN and apply an HTTPS traffic management policy to the VLAN, enter:

```
host1/Admin(config)# interface vlan 50
host1/Admin(config-if)# ip address 192.168.10.1 255.255.0.0
host1/Admin(config-if)# service-policy input MGMT_HTTPS_POLICY
```

For example, to globally apply an HTTPS traffic management policy to all of the VLANs associated with a context, enter:

```
host1/Admin(config)# service-policy input MGMT_HTTPS_POLICY
```

To detach the HTTPS traffic management policy from an interface, enter:

```
host1/Admin(config-if)# service-policy input MGMT_HTTPS_POLICY
```

To globally detach the HTTPS traffic management policy from all VLANs associated with a context, enter:

```
host1/Admin(config)# no service-policy input MGMT_HTTPS_POLICY
```
When you detach a traffic policy either individually from the last VLAN interface on which you applied the service policy or globally from all VLAN interfaces in the same context, the ACE automatically resets the associated service policy statistics. The ACE performs this action to provide a new starting point for the service policy statistics the next time that you attach a traffic policy to a specific VLAN interface or globally to all VLAN interfaces in the same context.

Follow these guidelines when you create a service policy:

- Policy maps, applied globally in a context, are internally applied on all interfaces existing in the context.
- A policy activated on an interface overwrites any specified global policies for overlapping classification and actions.
- The ACE allows only one policy of a specific feature type to be activated on a given interface.

To display service policy statistics for a Layer 3 and Layer 4 HTTP or HTTPS traffic management policy map, use the `show service-policy` command in Exec mode.

The syntax of this command is as follows:

```
show service-policy policy_name [detail]
```

The keywords, options, and arguments are as follows:

- `policy_name`—Identifier of an existing policy map that is currently in service (applied to an interface) as an unquoted text string with a maximum of 64 alphanumeric characters.
- `detail`—(Optional) Displays a more detailed listing of policy map statistics and status information.

**Note**

The ACE updates the counters that the `show service-policy` command displays after the applicable connections are closed.
For example, to display service policy statistics for the MGMT_HTTPS_POLICY policy map, enter:

```
host1/Admin# show service-policy MGMT_HTTPS_POLICY
Status     : ACTIVE
Description: Allow mgmt protocols
-----------------------------------------
Context Global Policy:
    service-policy: MGMT_HTTPS_POLICY
```

To clear the service policy statistics, use the `clear service-policy` command. The syntax of this command is as follows:

```
clear service-policy policy_name
```

For the `policy_name` argument, enter the identifier of an existing policy map that is currently in service (applied to an interface) as an unquoted text string with a maximum of 64 alphanumeric characters.

For example, to clear the statistics for the policy map MGMT_HTTPS_POLICY that is currently in service, enter:

```
host1/Admin# clear service-policy MGMT_HTTPS_POLICY
```
Enabling the Display of Raw XML Request show Command Output in XML Format

By default, XML responses will automatically appear in XML format if the corresponding CLI `show` command output supports the XML format. However, if you are running commands on the CLI console or you are running raw XML responses from NMS, the XML responses appear in regular CLI display format.

You can enable the display of raw XML request `show` command output in XML format by performing one of the following actions:

- Specifying the `xml-show on` command in Exec mode from the CLI.
- Including the `xml-show on` command in the raw XML request itself (CLI commands included in an XML wrapper).

Selection of the `xml-show on` command is not required if you are running true XML (as shown in the example below).

For details on the `show` command output supported in XML format, consult the ACE DTD file, `cisco_ace.dtd`, that is included as part of the software image (see the “Accessing the ACE DTD File” section). The ACE DTD file contains the information on the XML attributes for those `show` commands that have output that supports the XML format.

For example, if you specify the `show interface vlan 10` command, the DTD for the `show interface` command appears as follows:

```xml
<!--
interface-number is req for show-type vlan | bvi.
interface-number is between 1 and 4095 for vlan and 8191 for bvi.
-->
<!ENTITY % show-interface
  "interface-type      (vlan | bvi | eobc)      #IMPLIED
  interface-number      CDATA      #IMPLIED" />
```

The XML representation of the `show interface` command appears as follows:

```xml
<show_interface interface-type='vlan' interface-number='10'/>
```
The following example illustrates the XML representation of the `show interface` command output:

```xml
<response_xml>
  <exec_command>
    <command>
      show interface vlan 10
    </command>
    <status code="100" text="XML_CMD_SUCCESS"/>
    <xml_show_result>
      <xml_show_interface>
        <xml_interface_entry>
          <xml_interface>
            <interface_name>vlan10</interface_name>
            <interface_status>up</interface_status>
            <interface_hardware>VLAN</interface_hardware>
            <interface_mac>
              <macaddress>00:05:9a:3b:92:b1</macaddress>
            </interface_mac>
            <interface_mode>routed</interface_mode>
            <interface_ip>
              <ipaddress>10.20.105.101</ipaddress>
              <ipmask>255.255.255.0</ipmask>
            </interface_ip>
            <interface_ft_status>non-redundant</interface_ft_status>
            <interface_description>
              <interface_description>not set</interface_description>
            </interface_description>
            <interface_mtu>1500</interface_mtu>
            <interface_last_cleared>never</interface_last_cleared>
            <interface_alias>
              <ipaddress>not set</ipaddress>
            </interface_alias>
            <interface_standby>
              <ipaddress>not set</ipaddress>
            </interface_standby>
            <interface_sup_enabled>Assigned</interface_sup_enabled>
            <interface_auto_status>up</interface_auto_status>
          </xml_interface>
        </xml_interface_entry>
      </xml_show_interface>
    </xml_show_result>
  </exec_command>
</response_xml>
```
Chapter 8      Configuring the XML Interface

Enabling the Display of Raw XML Request show Command Output in XML Format

The syntax of this command is as follows:

```
xml-show { off | on | status }
```

The keywords are as follows:

- **off**—Displays CLI `show` command output in regular CLI display output, not in XML format.
- **on**—Displays CLI `show` command output in XML format unless a specific `show` command is not implemented to display its output in XML format. For details on the `show` command output supported in XML format, consult the the ACE DTD file, `cisco_ace.dtd`, that is included as part of the software image (see the “Accessing the ACE DTD File” section).
- **status**—Displays the results of the `xml show` command status; on or off. The `status` keyword allows you to determine the status of the `xml show` command setting.

For example, to enable the display of raw XML request `show` command output in XML format from the CLI, enter:

```
host1/Admin# xml-show on
```

To return to displaying CLI `show` command output in regular CLI output, enter:

```
host1/Admin# xml-show off
```
Accessing the ACE DTD File

The ACE DTD file, cisco_ace.dtd, is included as part of the software image and is accessible from a web browser using either HTTP or HTTPS. To access the cisco_ace.dtd file, use a web browser to perform one of the following tasks:

- Directly access the cisco_ace.dtd file.
- Open the cisco_ace.dtd file from the Cisco ACE Module Management page.

To access and view the Cisco ACE DTD 3.0 file, perform the following steps:

**Step 1**
If you have not done so, create a Layer 3 and Layer 4 class map and policy map to classify the HTTP or HTTPS management traffic that can be received by the ACE. See the “Configuring HTTP and HTTPS Management Traffic Services” section.

**Step 2**
Open your preferred Internet web browser application, such as Microsoft Internet Explorer or Netscape Navigator.

**Step 3**
To directly access the cisco_ace.dtd file, specify the HTTP or secure HTTP (HTTPS) address of your ACE in the address field, followed by cisco_ace.dtd. For example, enter:

https://ace_ip_address/cisco_ace.dtd

http://ace_ip_address/cisco_ace.dtd

You can choose to either open the cisco_ace.dtd file or save it to your computer.

**Step 4**
Access the cisco_ace.dtd file from the Cisco ACE Module Management page as follows:

a. Specify the HTTP or secure HTTP (HTTPS) address of your ACE in the address field:

   https://ace_ip_address
   http://ace_ip_address
b. Click Yes at the prompt to accept (trust) and install the signed certificate from Cisco. To install the signed certificate, do one of the following:

   – If you are using Microsoft Internet Explorer, in the Security Alert dialog box, click View Certificate, choose the Install Certificate option, and follow the prompts of the Certificate Manager Import Wizard.

   – If you are using Netscape Navigator, in the New Site Certificate dialog box, click Next and follow the prompts of the New Site Certificate Wizard.

c. Enter your username and password in the fields provided, and then click OK. The Cisco ACE Module Management page appears.

d. Click the CISCO ACE DTD 3.0 link under the Resources column of the Cisco ACE Module Management page to access the cisco_ace.dtd file. You can choose to either open the cisco_ace.dtd file or save it to your computer.
Upgrading Your ACE Software

This appendix provides information to upgrade your Cisco Application Control Engine (ACE) module. It contains the following major sections:

- Overview of Upgrading ACE Software
- Before You Begin
- ACE Software Upgrade Quick Start
- Copying the Software Upgrade Image to the ACE
- Configuring the ACE to Autoboot the Software Image
- Reloading the ACE Module
- Recovering the ACE from the ROMMON Utility
- Displaying Software Image Information

Overview of Upgrading ACE Software

Your ACE comes preloaded with the operating system software. To take advantage of new features and bug fixes, you can upgrade your ACE with a new version of software when it becomes available.

In the Admin context, you will use the `copy` command in Exec mode to manually install the software on each ACE. After the software installation is finished, set the boot variable and configuration register to autoboot the software image. Then, reload the modules to load the new image.
To minimize any disruption to existing network traffic during a software upgrade or downgrade, deploy your ACE modules in a redundant configuration. For details about redundancy, see Chapter 6, Configuring Redundant ACE Modules.

Note
Software version A2(1.0) introduces hardware-assisted SSL (HTTPS) probes. For that reason, the ACE uses the all option for the default SSL version and uses the routing table (which may bypass the real server IP address) to direct HTTPS probes to their destination regardless of whether you specify the routed option or not in the ip address command. If you are using HTTPS probes in your A1(6.x) configuration with the default SSL version (SSLv3) or without the routed option, you may observe that your HTTPS probes behave differently with version A2(1.0). For more information about HTTPS probes, see the Cisco Application Control Engine Module Server Load-Balancing Configuration Guide.

Before You Begin
Before you upgrade your ACE software, please read this appendix in its entirety so that you fully understand the entire upgrade process. Please be sure that your ACE configurations meet the upgrade prerequisites in the following sections:

- Changing the Admin Password
- Changing the www User Password
- Creating a Checkpoint
- Updating Your Application Protocol Inspection Configurations

Changing the Admin Password

Before you upgrade to software version A2(1.1) or higher, you must change the default Admin password if you have not already done so. Otherwise, after you upgrade the ACE software, you will be able to log in to the ACE only through the console port or through the supervisor engine of the Catalyst 6500 series switch or the Cisco 7600 series router until you change the default Admin password. For details about changing the Admin password, see Chapter 1, Setting Up the ACE.
Appendix A Upgrading Your ACE Software

Before You Begin

Changing the www User Password

Before you upgrade to software version A2(1.1) or higher, you must change the default www user password if you have not already done so. Otherwise, after you upgrade the ACE software, the www user will be disabled and you will not be able to use Extensible Markup Language (XML) to remotely configure an ACE until you change the default www user password. For details about changing the www user password, see Chapter 2, Configuring Virtualization in the Cisco Application Control Engine Module Virtualization Configuration Guide. In this case, the username would be www.

Checking Your Configuration for FT Priority and Preempt

If you want the currently active ACE to remain active after the software upgrade, be sure that the active ACE has a higher priority than the standby (peer) ACE and that the `preempt` command is configured. To check the redundant configuration of your ACEs, use the `show running-config ft` command. Note that the `preempt` command is enabled by default and does not appear in the running-config.

Creating a Checkpoint

We strongly recommend that you create a checkpoint in the running-configuration file of each context in your ACE. A checkpoint creates a snapshot of your configuration that you can later roll back to in case a problem occurs with an upgrade and you want to downgrade the software to a previous release. Use the `checkpoint create` command in Exec mode in each context for which you want to create a configuration checkpoint and name the checkpoint. For details about creating a checkpoint and rolling back a configuration, see Chapter 4, Managing the ACE Software. For information about downgrading your ACE, see the Downgrading Your ACE Software section in the Release Note for the Cisco Application Control Engine Module.
Updating Your Application Protocol Inspection Configurations

Because the ACE version A2(1.x) software has stricter error checks for application protocol inspection configurations than A1(x) software versions, be sure that your inspection configurations meet the guidelines that follow. The error checking process in A2(1.x) software denies misconfigurations in inspection classifications (class maps) and displays error messages. If such misconfigurations exist in your startup- or running-configuration file before you load the A2(1.x) software, the standby ACE in a redundant configuration may boot up to the STANDBY_COLD state. For information about redundancy states, see Chapter 6, Configuring Redundant ACE Modules.

If the class map for the inspection traffic is generic (match . . . any or class-default is configured) so that noninspection traffic is also matched, the ACE displays an error message and does not accept the inspection configuration. For example:

```
switch/Admin(config)# class-map match-all TCP_ANY
switch/Admin(config-cmap)# match port tcp any
```

```
switch/Admin(config)# policy-map multi-match FTP_POLICY
switch/Admin(config-pmap)# class TCP_ANY
switch/Admin(config-pmap-c)# inspect ftp
Error: This class doesn’t have tcp protocol and a specific port
```

The following examples show some of the generic class-map match statements and an ACL that are not allowed in A2(1.x) inspection configurations:

- match port tcp any
- match port udp any
- match port tcp range 0 65535
- match port udp range 0 65535
- match virtual-address 192.168.12.15 255.255.255.0 any
- match virtual-address 192.168.12.15 255.255.255.0 tcp any
- access-list acl1 line 10 extended permit ip any any

For application protocol inspection, the class map must have a specific protocol (related to the inspection type) configured and a specific port or range of port numbers.
For HTTP, FTP, RTSP, Skinny, and ILS protocol inspection, the class map must have TCP as the configured protocol and a specific port or range of ports. For example, enter the following commands:

```bash
host1/Admin(config)# class-map match-all L4_CLASS
host1/Admin(config-cmap)# match port tcp eq www
```

For SIP protocol inspection, the class map must have TCP or UDP as the configured protocol and a specific port or range of ports. For example, enter the following commands:

```bash
host1/Admin(config)# class-map match-all L4_CLASS
host1/Admin(config-cmap)# match port tcp eq 124
```

or

```bash
host1/Admin(config-cmap)# match port udp eq 135
```

For DNS inspection, the class map must have UDP as the configured protocol and a specific port or range of ports. For example, enter the following commands:

```bash
host1/Admin(config)# class-map match-all L4_CLASS
host1/Admin(config-cmap)# match port udp eq domain
```

For ICMP protocol inspection, the class map must have ICMP as the configured protocol. For example, enter the following commands:

```bash
host1/Admin(config)# access-list ACL1 extended permit icmp 192.168.12.15 255.255.255.0 192.168.16.25 255.255.255.0 echo
host1/Admin(config)# class-map match-all L4_CLASS
host1/Admin(config-cmap)# match access-list ACL1
```

ACE Software Upgrade Quick Start

Table A-1 provides a quick overview of the steps required to upgrade the software on each ACE. Each step includes the CLI command or a reference to the procedure required to complete the task. For a complete description of each feature and all the options associated with the CLI commands, see the sections that follow Table A-1. For clarity, the original active ACE is referred to as ACE-1 and the original standby ACE is referred to as ACE-2 in the following quick start.
Table A-1  ACE Software Upgrade Quick Start

Task and Command Example

1. Log in to each ACE. The Exec mode prompt appears at the CLI. If you are operating in multiple contexts, observe the CLI prompt to verify that you are operating in the Admin context. If necessary, log directly in to, or change to the Admin context by entering the `changeto` command.

   ACE-1/Admin#

2. Save the running configurations of every context by entering the `write memory all` command in Exec mode in the Admin context of each ACE.

   ACE-1/Admin# write memory all

3. Create a checkpoint in each context of both ACEs by entering the `checkpoint create` command in Exec mode.

   ACE-1/Admin# checkpoint create ADMIN_CHECKPOINT
   ACE-1/Admin# changeto C1
   ACE-1/C1# checkpoint create C1_CHECKPOINT

4. Enter either the `copy ftp`, `copy sftp`, or the `copy tftp` command in Exec mode to copy the new software image to the image: directory of each ACE. For example, to copy the image with the name c6ace-t1k9-A2_1.bin using FTP, enter:

   ACE-1/Admin# copy ftp://server1/images/c6ace-t1k9-mz.A2_1.bin

5. If you are running software version A2(1.2) or later, check the MD5 checksum of the new software image on both ACEs to ensure that the new image is the same as the image posted on Cisco.com. For example, enter:

   ACE-1/Admin# show file image:c6ace-t1k9-mz.A2_3_0.bin md5sum
Appendix A  Upgrading Your ACE Software

Table A-1  ACE Software Upgrade Quick Start (continued)

Task and Command Example

6. Configure ACE-1 to automatically boot from the new image. To set the boot variable and configuration register to 1, use the `boot system image:` and `config-register` commands in configuration mode. For example, enter:

```
ACE-1/Admin# config
ACE-1/Admin(config)# boot system image:c6ace-t1k9-mz.A2_1.bin
ACE-1/Admin(config)# config-register 1
ACE-1/Admin(config)# exit
ACE-1/Admin#
```

You can set up to two images through the `boot system` command. If the first image fails, the ACE tries to boot from the second image.

**Note** Use the `no boot system image:` command to remove the previously configured boot variable.

7. Verify that the boot variable was synchronized to ACE-2 by entering the following command on ACE-2:

```
ACE-2/Admin# show bootvar
BOOT variable = "disk0:c6ace-t1k9-mz.A2_1.bin"
Configuration register is 0x1
ACE-2/Admin#
```

8. Enter the `show ft group detail` command in Exec mode to verify the state of each module. Upgrade the ACE that has its Admin context in the STANDBY_HOT state (ACE-2) first by entering the `reload` command in Exec mode. After ACE-2 boots up, it may take a few minutes to reach the STANDBY_HOT state again. Configuration synchronization is still enabled and the connections through ACE-1 are still being replicated to ACE-2.

**Note** Do not add any more commands to the ACE-1 configuration. At this point in the upgrade procedure, any incremental commands that you add to the ACE-1 configuration may not be properly synchronized to the ACE-2 configuration.

```
ACE-2/Admin# reload
This command will reboot the system
Save configurations for all the contexts. Save? [yes/no]: [yes]
```
Table A-1  ACE Software Upgrade Quick Start (continued)

**Task and Command Example**

<table>
<thead>
<tr>
<th>Task</th>
<th>Command/Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>9. Disable preemption on ACE-1.</td>
<td>ACE-1/Admin# config&lt;br&gt;ACE-1/Admin(config)# ft group 1&lt;br&gt;ACE-1/Admin(config-ft-group)# no preempt&lt;br&gt;Press Ctrl-z to return to Exec mode.</td>
</tr>
<tr>
<td>10. Perform a graceful failover of all contexts from ACE-1 to ACE-2 by entering the ft switchover all command in Exec mode on ACE-1. ACE-2 becomes the new active ACE and assumes mastership of all active connections with no interruption to existing connections.</td>
<td>ACE-1/Admin# ft switchover all&lt;br&gt;</td>
</tr>
<tr>
<td>11. Upgrade ACE-1 by reloading it and verify that ACE-1 enters the STANDBY_HOT state (may take several minutes) by entering the show ft group detail command in Exec mode. Because both ACE-1 and ACE-2 are running the same version of software now, configuration mode is enabled. The configuration is synchronized from ACE 2 (currently active) to ACE-1.</td>
<td>ACE-1/Admin# reload&lt;br&gt;</td>
</tr>
<tr>
<td>12. Reenable preempt on ACE-2. If ACE-1 is configured with a higher priority and preempt is configured on the FT group, ACE-1 reasserts mastership after it has received all configuration and state information from ACE-2, making ACE-2 the new standby. ACE-1 becomes the active ACE once again.</td>
<td>ACE-2/Admin# config&lt;br&gt;ACE-2/Admin(config)# ft group 1&lt;br&gt;ACE-2/Admin(config-ft-group)# preempt&lt;br&gt;Press Ctrl-z to return to Exec mode.</td>
</tr>
<tr>
<td>13. Enter the show ft group detail command to verify that ACE-1 is in the ACTIVE state and ACE-2 is in the STANDBY_HOT state.</td>
<td></td>
</tr>
</tbody>
</table>
Copying the Software Upgrade Image to the ACE

To copy a software image to the ACE, use the `copy` command in the Admin context from the Exec mode. You can copy a software image to the ACE from a variety of sources, including:

- FTP server
- SFTP server
- TFTP server

The `copy` command allows you to rename the image copied to the ACE.

The syntax of this command is as follows:

```
copy {ftp://server/path/[filename] | sftp://[username@]server/path/[filename] | tftp://server[:port]/path/[filename]} image:[name]
```

The keywords, arguments, and options are as follows:

- `ftp://server/path/[filename]`—Specifies the URL of the software image located on an FTP server. This path is optional because the ACE prompts you for this information if you omit it.
- `sftp://[username@]server/path/[filename]`—Specifies the URL of a software image on a secure FTP server. This path is optional because the ACE prompts you for this information if you omit it.
- `tftp://server[:port]/path/[filename]`—Specifies the URL of a software image on a trivial FTP server. This path is optional because the ACE prompts you for this information if you omit it.
- `image:[name]`—Specifies the name for the software image copied to the ACE. If you do not enter the `name` argument, the ACE uses the default name of the image.

For example, to copy the image `c6ace-t1k9-mz.A2_1.bin` located on an FTP server to the ACE, enter:

```
host1/Admin# copy ftp://server1/images/c6ace-t1k9-mz.A2_1.bin image:
```

To set the boot variable and configure the ACE to autoboot this image, see the “Configuring the ACE to Autoboot the Software Image” section.
Configuring the ACE to Autoboot the Software Image

After you copy the image on to the ACE, configure it to autoboot the image by setting the boot variable and the configuration register. The boot variable specifies the image from which the ACE boots at startup. The configuration variable can be set to autoboot the image defined by the boot variable.

This section contains the following topics:

- Setting the Boot Variable
- Configuring the Configuration Register to Autoboot the Boot Variable
- Verifying the Boot Variable and Configuration Register

For detailed information on the boot variable and configuration register, see Chapter 1, Setting Up the ACE.

Setting the Boot Variable

To set the boot variable, use the `boot system image:` command in the Admin context in configuration mode. The syntax of this command is as follows:

```
boot system image:image_name
```

The `image_name` argument is the name of the installed image.

⚠️ **Caution**

If you set a single image through the `boot system image:` command, be sure to enter the image name correctly. Otherwise, when you attempt to reload the ACE, it uses the incorrect image name, fails the reload, and accesses the ROMMON utility. For information on recovering from this problem, see the “Recovering the ACE from the ROMMON Utility” section.

You can set up to two images through the `boot system` command. If the first image fails, the ACE tries the second image.

For example, to set the boot variable with the c6ace-t1k9-mz.A2_1.bin image, enter:

```
host1/Admin(config)# boot system image:c6ace-t1k9-mz.A2_1.bin
```
Use the `no boot system image:` command to unset the previously configured boot variable.

### Configuring the Configuration Register to Autoboot the Boot Variable

To configure the ACE to autoboot the system image identified in the boot environment variable, use the `config-register` command in the Admin context from the configuration mode and set the configuration register to 1.

**Note**

A `config-register` setting of 0 instructs the ACE to boot to the rommon prompt upon a reboot. The ACE remains in ROMMON mode at startup.

For example, to set the register to 1, enter:

```
host1/Admin(config)# config-register 1
```

### Verifying the Boot Variable and Configuration Register

To verify the boot variable and configuration register, use the `show bootvar` command in the Admin context from the Exec mode. For example, enter:

```
host1/Admin# show bootvar
BOOT variable = "disk0:c6ace-t1k9-mz.A2_1.bin"
Configuration register is 0x1
host1/Admin#
```

The 0x1 indicates that the configuration register is set to 1.

### Reloading the ACE Module

To allow the ACE to use the installed software upgrade, reload the ACE module. To reload the ACE, use the `reload` command in the Admin context in Exec mode. The syntax of this command is as follows:

```
reload
```
For example, enter:

```
host1/Admin# reload
This command will reboot the system
Save configurations for all the contexts. Save? [yes/no]: [yes]
```

If you reload the ACE and the rommon mode prompt appears, a problem with the upgrade or the ACE has occurred. See the “Recovering the ACE from the ROMMON Utility” section for more information.

### Recovering the ACE from the ROMMON Utility

If you reload the ACE and the rommon mode prompt appears, one of the following problems may have occurred:

- You entered the installed image name incorrectly. This problem assumes that you correctly installed the image on the ACE.
- The downloaded ACE image is corrupted.
- The ACE compact Flash had a hardware failure.

If you incorrectly entered the image name, boot the ACE from the rommon prompt and then after the ACE reboots, correct the image name in the boot variable. For more information, see the “Booting the ACE from ROMMON with the Correct Image Name” section.

If the downloaded image is corrupted or the compact Flash failed, copy the ACE image on the supervisor engine and boot the ACE from the supervisor engine. For more information, see the “Copying the ACE Image to the Supervisor Engine” section.

### Booting the ACE from ROMMON with the Correct Image Name

If you set a single image through the `boot system` command, you must enter the image name correctly for the ACE to reload successfully. Otherwise, when you attempt to reload the ACE, it uses the incorrect image name, fails the reload, and accesses the ROMMON utility as indicated by the rommon mode prompt.

After the attempted reload, a boot message (similar to the following) appears in the CLI indicating that the image could not load:

```
boot: cannot load "disk0:c6ace-t1k9mz.A2_1.bin"
```
Appendix A      Upgrading Your ACE Software

Recovering the ACE from the ROMMON Utility

Verify whether the image name is correct. If it is, then the problem could be a corrupted image or a compact Flash failure. For more information on how to reload the ACE from these conditions, see the “Copying the ACE Image to the Supervisor Engine” section.

In this example, the image name is incorrect. The c6ace-t1k9mz.A2_1.bin image in the message should be c6ace-t1k9-mz.A2_1.bin.

To boot the ACE with the correct image name from rommon mode and correct the image name in the boot variable, perform the following steps:

**Step 1** Access the disk0: directory to view the correct image name.

```
rommon 1> dir disk0:
Directory of disk0:
20903  28583947 -rw- c6ace-t1k9-mz.A2_1.bin <correct image
2    74448896 -rw- TN-CONFIG
....
rommon 2>
```

**Step 2** Set the boot image that is on ACE.

```
rommon 2> BOOT=disk0:c6ace-t1k9-mz.A2_1.bin
```

**Step 3** Verify the boot image in the configuration variables.

```
rommon 3> set
PS1=rommon !>
RELOAD_REASON=reload command by admin
?=0
BOOT=c6ace-t1k9-mz.A2_1.bin
rommon 4>
```

**Step 4** Boot the image on the ACE.

```
rommon 4> boot
Loading disk0:c6ace-t1k9-mz.A2_1.bin. Please wait...
```

The boot process may take several minutes to finish.

**Step 5** When the login prompt appears, log in to the ACE.

```
host1 login: admin
Password:
Cisco Application Control Software (ACSW)
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2006, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license. Some parts of this software are covered under the GNU Public License. A copy of the license is available at http://www.gnu.org/licenses/gpl.html.

Step 6 Access configuration mode in the Admin context and unset the previously configured boot variable by using the `no boot system image:` command.

```bash
host1/Admin# config
host1/Admin(config)# no boot system image:c6ace-t1k9mz.A2_1.bin
```

Step 7 Reset the boot variable with the correct image name by using the `boot system image:` command.

```bash
host1/Admin(config)# boot system image:c6ace-t1k9-mz.A2_1.bin
```

Step 8 To verify that the boot variable has the correct image name, use the `show bootvar` command in the Admin context from the Exec mode.

```bash
host1/Admin# show bootvar
BOOT variable = "c6ace-t1k9-mz.A2_1.bin"
Configuration register is 0x1
host1/Admin#
```

### Copying the ACE Image to the Supervisor Engine

If you download a corrupted ACE image or the ACE compact Flash has failed, you can boot the ACE from an image copied to the supervisor engine.

From the supervisor engine CLI, perform the following steps:

Step 1 Copy the ACE image to disk0: on the supervisor engine by using the `copy` command. For example, to copy `c6ace-t1k9-mz.3.0.0_A1_4.bin` image from an TFTP server to disk0:, enter:

```bash
Router# copy tftp://192.168.144.14/tftpboot/c6ace-t1k9-mz.A2_1.bin disk0:
Destination filename [c6ace-t1k9-mz.A2_1.bin]?
Accessing tftp://192.168.144.14/tftpboot/c6ace-t1k9-mz.A2_1.bin ... Loading /tftpboot/c6ace-t1k9-mz.A2_1.bin from 192.168.144.14 (via VLAN 12):!!!!!!!!!!!!!!!!!!!!!!!!!!!... [OK - 29251568 bytes]
```
Appendix A  Upgrading Your ACE Software

Recovering the ACE from the ROMMON Utility

29251568 bytes copied in 81.600 secs (358475 bytes/sec)
Router#

Step 2  After the image is copied to the supervisor engine, access configuration mode and set the boot variable for the ACE and the image. For example, to access configuration mode and set the boot variable if the ACE is in slot 3, enter:

Router# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#boot device module 3 disk0:c6ace-t1k9-mz.A2_1.bin
Device BOOT variable = disk0:c6ace-t1k9-mz.A2_1.bin
Warning: Device list is not verified
Router#

From the ACE, perform the following steps:

Step 1  Boot the ACE from the image on the supervisor engine by using the boot eobc command.

rommon 1> boot eobc:

Step 2  When the login prompt appears, log in to the ACE.

host1 login: admin
Password:
Cisco Application Control Software (ACSW)
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2006, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public License. A copy of the license is available at http://www.gnu.org/licenses/gpl.html.
host1/Admin#

Step 3  If the image on the ACE is corrupted, copy another image onto the ACE as described in the “Copying the Software Upgrade Image to the ACE” section. Then configure the ACE to autoboot the image as described in the “Configuring the ACE to Autoboot the Software Image” section.

If the compact Flash on the ACE had a hardware failure, contact TAC support for assistance.
Displaying Software Image Information

To display the software image on the ACE, use the `show version` command in Exec mode. The syntax of this command is as follows:

```
show version
```

For example, enter:

```
host1/Admin# show version
```
INDEX

**A**

ACE
- boot configuration 1-22
- capturing packet information 5-30
- configuration checkpoint and rollback service 5-39
- configuration files, loading from remote server 5-11
- configuration files, saving 5-1
- console connection 1-2
- date and time, configuring 1-12
- Flash memory, reformating 5-43
- inactivity timeout 1-9
- information, displaying 6-1
- licenses, managing 3-1
- logging in 1-3
- message-of-the-day banner 1-10
- MIBs 8-7
- naming 1-8
- password, changing administrative 1-5
- password, changing CLI account 1-7
- recovery from the ROMMON utility A-12
- redundant configuration 7-1

remote access 2-1
restarting 1-27
setting up 1-1
shutting down 1-28
SNMP 8-1
terminal settings 1-17
upgrading A-1
username, changing 1-5
using file system 5-12
XML, configuring 9-1
admin user 1-3, 9-1
alias IP address 7-14

**B**

boot configuration
- BOOT environment variable 1-25, 5-19
- booting from rommon prompt 1-24, A-12
- boot method 1-23, A-10
- configuration register, setting boot method 1-23, A-10
- displaying 1-26
- modifying 1-22
- upgrading A-10
BOOT environment variable, setting 1-25, 5-19
boot method, setting 1-23, A-10

capturing packets 5-31
copying buffer 5-34
displaying buffer 5-35
checkpoint, configuration
creating 5-40
deleting 5-41
displaying 5-42
rolling back to 5-41
class map
Layer 3 and 4, creating for management traffic 9-13
Layer 3 and 4, for SNMP 8-41
remote management 2-5
remote management description 2-6
remote management protocol match criteria 2-7
SNMP management traffic 8-41
XML 9-13
CLI
account password, changing 1-7
restarting ACE from 1-27
saving session 1-3
user management of SNMP 8-6
clock
daylight saving time, setting 1-15
timezone, setting 1-12
viewing system clock settings 1-17
communities, SNMP 8-29
configurational examples
redundancy 7-43
remote access 2-23
SNMP 8-50
configuration checkpoint and rollback service
creating configuration checkpoint 5-40
deleting configuration checkpoint 5-41
displaying checkpoint information 5-42
overview 5-39
rolling back configuration 5-41
using 5-39
configuration files
clearing startup file 5-10
copying to disk0 file system 5-5
displaying 5-6
displaying user context from the Admin context 5-9
loading from remote server 5-11
merging startup with running 5-6
saving 5-1
saving in Flash memory 5-2
saving to remote server 5-3
configuration register
rommon prompt 1-24
setting boot method 1-23, A-10
values 1-23
configuration synchronization
  overview 7-7
  SSL certs and keys 7-24, 7-26
console
  connection to ACE 1-2
  console line settings 1-20
contact, SNMP 8-30
context
  associating with FT group 7-18
  directly accessing with SSH 2-21
copying
  configuration files 5-3, 5-5
  core dumps 5-27
  files 5-15
  files from remote server 5-19
  files to remote server 5-17
  licenses 5-16
  packet capture buffer 5-16
  software image 5-20
  upgrade image A-9
copyright, displaying 6-3
core dumps 5-27
  clearing core directory 5-29
  copying 5-27
  deleting 5-29

D

date and time

configuring 1-12
daylight saving time setting 1-15
time zone setting 1-12
viewing system clock 1-17
daylight saving time setting 1-15
default user
  admin 1-3, 9-1
  www 1-3, 9-1
demo license, replacing with permanent license 3-7
directory
  copying files 5-15
  creating in disk0 5-22
  deleting from disk0 5-23
  listing files 5-13
disk0
  creating new directory in 5-22
  deleting directory in 5-23
  moving files in 5-23
  overview 5-12
  uncompressing files in 5-21
  untarring files in 5-21
display attributes, terminal 1-18
displaying
  copyright 6-3
  file contents 5-25
  FT group information 7-45
  FT peer information 7-52
  FT statistics 7-57
  FT tracking information 7-59
<table>
<thead>
<tr>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>hardware information 6-4</td>
</tr>
<tr>
<td>hardware inventory 6-5</td>
</tr>
<tr>
<td>ICMP statistics 6-18</td>
</tr>
<tr>
<td>information on ACE 6-1</td>
</tr>
<tr>
<td>memory statistics 7-52</td>
</tr>
<tr>
<td>process status 6-11</td>
</tr>
<tr>
<td>redundancy configuration 7-45</td>
</tr>
<tr>
<td>redundancy history 7-50</td>
</tr>
<tr>
<td>software version 6-2</td>
</tr>
<tr>
<td>system information 6-14</td>
</tr>
<tr>
<td>system processes 6-6</td>
</tr>
<tr>
<td>technical support information 6-19</td>
</tr>
<tr>
<td>DTD</td>
</tr>
<tr>
<td>accessing 9-26</td>
</tr>
<tr>
<td>overview 9-7</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

F

failover

forcing 7-23

stateful 7-5

failure detection 7-27

host or gateway 7-29

host or gateway, example configuration 7-33

host or gateway, IP address 7-30, 7-32

host or gateway, probe 7-30, 7-32

host or gateway, probe priority 7-31, 7-33

host or gateway, process 7-29

HSRP group 7-38
untarring files in disk0  5-21
using ACE  5-12
Flash memory
  file system overview  5-12
  reformatting  5-43
  saving configuration files in  5-2
FT group
  assigning priority to group member  7-19
  assigning priority to standby group member  7-20
  associating context  7-18
  associating peer  7-19
  configuring  7-17
  displaying information  7-45
  modifying  7-22
  placing in service  7-21
  preemption, configuring  7-21
FT peer
  associating with FT group  7-19
  associating with FT VLAN  7-15
  configuring  7-14
  displaying information  7-52
  heartbeat configuration  7-15
  query interface, configuring  7-16
FT tracking, displaying information  7-59
FT VLAN  7-6, 7-11
  associating with FT peer  7-15
  creating  7-12
  enabling  7-13
  IP address  7-12
peer IP address  7-13

G

  gateway failure detection
    See failure detection

H

  hardware information, displaying  6-4, 6-5
  heartbeat
    configuration  7-15
  host failure detection
    See failure detection
  HSRP group
    failure detection  7-38
    tracking requirements  7-38
  HTTP
    return codes between server and client  9-5
  HyperTerminal
    launching  1-2
    saving session  1-3

I

  ICMP
    displaying statistics  6-18
    enabling messages to the ACE  2-19
image
  autobooting image A-10
  BOOT environment variable 1-25
  copying and booting from the supervisor engine A-14
  copying to remote server 5-20
  copying upgrade image to ACE A-9
  software image information, displaying A-16
  version A-16
inactivity timeout 1-9
interface failure detection
  See failure detection
inventory, displaying hardware 6-5
IP address
  alias 7-14

K
key
  generating for license 3-3
  pair for SSH host 2-17

L
Layer 3 and Layer 4 policy map
  description 2-10
  for management traffic 2-9, 9-17
  SNMP, creating 8-44
  specifying traffic class 2-11
Layer 3 and Layer 4 class map
  management traffic, creating for 9-13
  SNMP, creating for 8-41
licenses
  backing up 3-13
  copying 5-16
  copying to ACE 3-4
  displaying configuration and statistics 3-14
  generating key 3-3
  installing 3-5
  list of available 3-2
  managing 3-1
  ordering upgrade license 3-3
  removing 3-8
  replacing demo with permanent 3-7
location, SNMP 8-31
logging
  into ACE 1-3

M
management access
  Layer 3 and 4 traffic 9-17
  Layer 3 and 4 traffic policy 2-9
  SSH, configuring 2-16
  Telnet 2-15
message-of-the-day banner 1-10
MIBs 8-7
monitoring
   See SNMP
moving files in disk0  5-23

N
naming the ACE  1-8
notifications
   error messages  8-35
   IETF standard, enabling  8-36
options  8-35
   SLB  8-34
SNMP  8-19, 8-31, 8-35
SNMP, enabling  8-34
SNMP host, configuring  8-32
SNMP license manager  8-34
types  8-34
virtual context change  8-35

P
packet buffer  5-30
   capturing packets  5-31
   copying capture buffer  5-16, 5-34
displaying capture buffer  5-35
password
   changing administrative  1-5
   changing CLI account  1-7
peer
   See FT peer
ping, enabling  2-19
policy map
   actions for remote access  2-12
   actions for SNMP  8-46, 9-19
   Layer 3 and 4, for management traffic  2-9, 9-17
   Layer 3 and 4, for SNMP  8-44
   Layer 3 and 4, specifying traffic class  2-11
   Layer 3 and 4 policy map description  2-10
   remote access  2-9
   SNMP management traffic  8-44
   XML  9-17
probe
   for failure detection  7-30, 7-32
processes
   displaying  6-6
   displaying status of  6-11
protocol match criteria, for remote class map  2-7

Q
query interface for FT peer  7-16
quick start
   redundancy  7-8
   remote access  2-2
   SNMP  8-24
   upgrading  A-5
   XML  9-11
recovering the ACE from the ROMMON utility  A-12
redundancy  7-1
  configuration, displaying  7-45
  configuration examples  7-43
  configuration requirements  7-8
configuration synchronization overview  7-7
configuring  7-11
failure detection and tracking  7-27
forcing failover  7-23
FT group, configuring  7-17
FT group information, displaying  7-45
FT peer, configuring  7-14
FT peer information, displaying  7-52
FT statistics, displaying  7-57
FT tracking information, displaying  7-59
FT VLAN  7-6
FT VLAN, configuring  7-11
history, displaying  7-50
memory statistics, displaying  7-52
overview  7-1
protocol  7-2
quick start  7-8
stateful failover  7-5
statistics, clearing  7-63
synchronizing  7-24
synchronizing SSL certs and keys  7-26
reformatting Flash memory  5-43
remote access
class map, creating  2-5
class map description  2-6
class map protocol match criteria  2-7
configuration examples  2-23
enabling  2-1
network management traffic services, configuring  2-4
policy actions  2-12
policy map  2-9
quick start  2-2
service policy  2-13
SSH, configuring  2-16
Telnet  2-15
terminating user session  2-19
remote server
copying files from  5-19
copying files to  5-17
copying image to  5-20
loading configuration files from  5-11
saving configuration files to  5-3
restarting ACE  1-27
  from ACE CLI  1-27
  from Catalyst CLI  1-28
retrieving user context through the Admin context IP address when using SNMP  8-37
rollback service
  See configuration checkpoint and rollback service
rommon
  configuration register, setting 1-24
  mode 1-23
  prompt 1-24
  prompt, booting the ACE from 1-24
  recovering the ACE from A-12
running configuration
  copying to disk0 file system 5-5
  merging with startup 5-6
  saving to startup configuration file 5-2
  viewing 5-6
  viewing user context from the Admin context 5-9

S

service policy
  HTTP management policy map, applying 9-19
  HTTPS management policy map, applying 9-19
  remote access policy map, applying 2-13
  SNMP management policy map, applying 8-47
session
  maximum number for SSH 2-16
  SSH information, showing 2-25
  SSH key details, showing 2-26
  Telnet information, showing 2-24
  terminating SSH or Telnet 2-19
  to ACE 1-3
  setting up ACE 1-1
  show command
    enabling the exchange of output in XML 9-23
    saving output to file 5-25
    viewing hardware and software configuration information 6-1
  shutting down ACE 1-28
Simple Network Management Protocol
  See SNMP
SNMP
  AAA integration 8-6
  agents, communication 8-4
  agents, overview 8-3
  class map, creating 8-41
  CLI user management 8-6
  communities 8-29
  configuration examples 8-50
  configuring the engine ID 8-39
  contact 8-30
  IETF standard 8-36
  limitations 8-22
  linkDown trap 8-36
  linkUp trap 8-36
  location 8-31
  management traffic, configuring 8-40
  managers, communication 8-4
  managers, overview 8-3
  MIBs 8-7
  notifications 8-31
overview 8-2
policy actions 8-46, 9-19
policy map, creating 8-44
quick start 8-24
retrieving user context through the Admin context IP address 8-37
service policy 8-47
statistics 8-51
traps 8-19
traps and informs 8-5
users, configuring 8-26
VLAN interface, assigning 8-37
software licenses
See licenses
software version, displaying 6-2
SSH 2-16
directly accessing a user context 2-21
host key pairs 2-17
management access 2-16
maximum sessions 2-16
RSA key 2-18
showing key details 2-26
showing session information 2-25
terminating session 2-19
version 2-8
SSL
certificates and keys, synchronizing 7-26
startup configuration
copying to disk0 file system 5-5
merging with running 5-6
saving to remote server 5-3
updating with running configuration 5-2
viewing 5-6
stateful failover 7-5
statistics
FT 7-57
FT, clearing 7-64
license 3-14
memory 7-52
redundancy history, clearing 7-65
SNMP 8-51
stopping ACE 1-28
synchronizing
configuration 7-7
SSL certs and keys 7-24
synchronizing redundant configurations 7-24
system information, displaying 6-14
system processes
displaying 6-6
displaying status of 6-11

T
technical support information, displaying 6-19
Telnet
management access, configuring 2-15
showing information 2-24
terminating session 2-19
terminal settings
configuring 1-17  
console line settings 1-20  
display attributes 1-18  
virtual terminal line settings 1-21  
time zone setting 1-12  
tracking  
  See failure detection  
traps, SNMP 8-5, 8-19  

V  
version, software 6-2, A-16  
virtual terminal line settings 1-21  
VLANs  
  for SNMP traps 8-37  
  FT VLAN for redundancy 7-6, 7-11  
volatile file system 5-12  

W  
www user 1-3, 9-1  

X  
XML  
  class map, creating 9-13  
  DTD, accessing 9-26  
  DTD, overview 9-7  
  HTTP and HTTPS support 9-3  
  HTTP return codes 9-5  
  management traffic, configuring 9-12  
  overview 9-2  
  policy map, creating 9-17  
  quick start 9-11  
  sample configuration 9-9  
  service policy 9-19  
  show command output 9-23  

uncompressing files in disk0 5-21  
untarring files in disk0 5-21  
upgrade license 3-3  
upgrading  
  booting image A-10  
  copying image to ACE A-9  
  image information A-16  
  overview A-1  
  quick start A-5  
  recovery from the ROMMON utility A-12  
reloding ACE A-11  
user  
  configuring for SNMP 8-26  
user context  
  accessing by SNMP through the Admin context IP address 8-37  
  directly accessing with SSH 2-21  
username  
  changing 1-5