



## **Cisco Application Control Engine Module System Message 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-11872-01

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

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

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

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

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

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

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0801R)

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



# CONTENTS

## **Preface ix**

- Audience **ix**
- How to Use This Guide **x**
- Related Documentation **x**
- Symbols and Conventions **xii**
- Obtaining Documentation, Obtaining Support, and Security Guidelines **xiii**
- Open Source License Acknowledgements **xiii**
  - OpenSSL/Open SSL Project **xiii**
  - License Issues **xiii**

---

## **CHAPTER 1**

## **Configuring System Message Logging 1-1**

- Understanding System Message Logging **1-2**
  - Logging Overview **1-2**
  - Log Message Format **1-3**
  - Logging Severity Levels **1-4**
  - Variables **1-4**
- System Message Logging Quick Start **1-6**
- Enabling System Message Logging **1-8**
- Specifying syslog Output Locations **1-8**
  - Sending syslog Messages to a Buffer **1-9**
  - Sending syslog Messages to a Telnet or SSH Session **1-9**
  - Sending syslog Messages to the Console **1-11**
  - Sending syslog Messages to a syslog Server **1-11**
  - Sending syslog Messages to an SNMP Network Management Station **1-13**
  - Sending syslog Messages to the Supervisor Engine **1-13**
  - Sending syslog Messages to Flash Memory on the ACE **1-14**
- Enabling Time Stamps on System Messages **1-15**
- Identifying Messages Sent to a syslog Server **1-15**
- Specifying a Device ID of the ACE to a syslog Server **1-16**
- Changing the syslog Logging Facility **1-17**
- Changing the Logging Message Queue **1-17**
- Disabling or Changing the Severity Level of syslog Messages **1-18**

Limiting the Syslog Rate 1-19

Enabling Logging on the Standby ACE 1-20

Rejecting New Connections Through these ACE 1-21

Enabling the Logging of Connection Setup and Teardown Syslog Messages Through the Fast Path 1-22

Clearing Log Messages 1-22

Viewing Log Message Information 1-23

**CHAPTER 2**

**System Messages 2-1**

Messages 100001 to 199006 2-1

100001 2-1

106021 2-2

106023 2-2

106028 2-3

111008 2-3

111009 2-4

199006 2-4

Messages 211001 to 254002 2-4

211001 2-4

212007 2-5

212008 2-5

251001 2-5

251002 2-6

251003 2-6

251004 2-6

251005 2-6

251006 2-7

251007 2-8

251008 2-8

251009 2-8

251010 2-9

251011 2-9

251012 2-10

251013 2-10

253001 2-10

253002 2-10

253003 2-11

253004 2-11

253005 2-11

253006 2-11

253007	2-12
253008	2-12
253009	2-12
253010	2-12
253011	2-13
254001	2-13
254002	2-13
Messages 302022 to 327001	2-14
302022	2-14
302023	2-14
302024	2-15
302025	2-15
302026	2-15
302027	2-16
302028	2-16
302029	2-16
302030	2-16
302031	2-17
303003	2-17
303004	2-17
304001	2-17
305009	2-18
313004	2-18
313006	2-18
313007	2-19
314001	2-19
322001	2-19
322002	2-20
322003	2-20
327001	2-20
Messages 400000 to 444007	2-21
400000	2-21
405001	2-21
405201	2-21
406001	2-22
406002	2-22
410001	2-22
411001	2-22
411002	2-23
411003	2-23

411004	2-23
412001	2-23
415004	2-24
415006	2-24
415007	2-24
415008	2-24
415009	2-25
415010	2-25
415011	2-25
415021	2-25
415022	2-26
415023	2-26
415024	2-26
415025	2-26
415026	2-27
415027	2-27
440002	2-27
440003	2-27
441001	2-28
441002	2-28
442001	2-28
442002	2-28
442003	2-29
442004	2-29
442005	2-29
442006	2-29
443001	2-30
444001	2-30
444002	2-30
444003	2-30
444004	2-31
444005	2-31
444006	2-31
444007	2-31
Messages 504001 to 504002	2-32
504001	2-32
504002	2-32
Messages 607001 to 615004	2-32
607001	2-32
607003	2-33

608001	2-33
608002	2-33
608003	2-33
608004	2-34
608005	2-34
615003	2-34
615004	2-34
Messages 727001 to 750002	2-35
727001	2-35
727002	2-35
727003	2-35
727004	2-36
727005	2-36
727006	2-36
727007	2-37
727008	2-37
727009	2-37
727010	2-38
727011	2-38
727012	2-38
727013	2-40
727014	2-40
727015	2-40
727016	2-40
727017	2-41
727018	2-41
727019	2-41
727020	2-42
727021	2-42
727022	2-42
727023	2-42
728001	2-43
728002	2-43
728003	2-43
728004	2-44
728005	2-44
728006	2-45
728007	2-45
728008	2-45
728009	2-46

728011	2-46
728012	2-46
728013	2-47
728014	2-47
728015	2-47
728016	2-48
728017	2-48
728018	2-48
728019	2-49
728020	2-49
728021	2-49
728022	2-50
728023	2-50
728024	2-50
728025	2-51
728026	2-51
728027	2-51
728028	2-52
728029	2-52
728030	2-53
728031	2-53
728032	2-53
729001	2-54
729002	2-54
729003	2-54
750001	2-55
750002	2-55

**CHAPTER 3**

**Messages Listed by Severity Level 3-1**

Alert Messages, Severity Level 1	3-1
Critical Messages, Severity Level 2	3-2
Error Messages, Severity Level 3	3-2
Warning Messages, Severity Level 4	3-4
Notification Messages, Severity Level 5	3-6
Informational Messages, Severity Level 6	3-7
Debugging Messages, Severity Level 7	3-9

**INDEX**



## Preface

---

This guide provides instructions on how to configure system message logging on the Cisco Application Control Engine (ACE) module for the Catalyst 6500 series switches or a Cisco 7600 series router, hereinafter referred to as the switch or router, respectively. It also provides a list of the system log messages generated by the ACE, numerically by message code and also by severity level.

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:

- Web master
- System administrator
- System operator

## How to Use This Guide

This guide is organized as follows:

Chapter	Description
<a href="#">Chapter 1, Configuring System Message Logging</a>	Describes how to configure system message logging on the ACE.
<a href="#">Chapter 2, System Messages</a>	Lists the ACE system log messages numerically by message code.
<a href="#">Chapter 3, Messages Listed by Severity Level</a>	Lists the ACE system log messages numerically by severity level.

## Related Documentation

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

Document Title	Description
<i>Release Note for the Cisco Application Control Engine Module</i>	Provides information about operating considerations, caveats, and command-line interface (CLI) commands for the ACE.
<i>Cisco Application Control Engine Module Hardware Installation Note</i>	Provides information for installing the ACE into the Catalyst 6500 series switch or a Cisco 7600 series router.
<i>Cisco Application Control Engine Module Getting Started Guide</i>	Describes how to perform the initial setup and configuration tasks for the ACE.
<i>Cisco Application Control Engine Module Administration Guide</i>	Describes how to perform the following administration tasks on the ACE: <ul style="list-style-type: none"> <li>• Setting up the ACE</li> <li>• Establishing remote access</li> <li>• Managing software licenses</li> <li>• Configuring class maps and policy maps</li> <li>• Managing the ACE software</li> <li>• Configuring SNMP</li> <li>• Configuring redundancy</li> <li>• Configuring the XML interface</li> <li>• Upgrading the ACE software</li> </ul>
<i>Cisco Application Control Engine Module Virtualization Configuration Guide</i>	Describes how to operate your ACE in a single context or in multiple contexts.

<b>Document Title</b>	<b>Description</b>
<i>Cisco Application Control Engine Module Routing and Bridging Configuration Guide</i>	<p>Describes how to configure the following routing and bridging tasks on the ACE:</p> <ul style="list-style-type: none"> <li>• VLAN interfaces</li> <li>• Routing</li> <li>• Bridging</li> <li>• Dynamic Host Configuration Protocol (DHCP)</li> </ul>
<i>Cisco Application Control Engine Module Server Load-Balancing Configuration Guide</i>	<p>Describes how to configure the following server load-balancing tasks on the ACE:</p> <ul style="list-style-type: none"> <li>• Real servers and server farms</li> <li>• Class maps and policy maps to load-balance traffic to real servers in server farms</li> <li>• Server health monitoring (probes)</li> <li>• Stickiness</li> <li>• Firewall load balancing</li> <li>• TCL scripts</li> </ul>
<i>Cisco Application Control Engine Module Security Configuration Guide</i>	<p>Describes how to perform the following ACE security configuration tasks:</p> <ul style="list-style-type: none"> <li>• Security access control lists (ACLs)</li> <li>• 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</li> <li>• Application protocol and HTTP deep packet inspection</li> <li>• TCP/IP normalization and termination parameters</li> <li>• Network address translation (NAT)</li> </ul>
<i>Cisco Application Control Engine Module SSL Configuration Guide</i>	<p>Describes how to configure the following Secure Sockets Layer (SSL) tasks on the ACE:</p> <ul style="list-style-type: none"> <li>• SSL certificates and keys</li> <li>• SSL initiation</li> <li>• SSL termination</li> <li>• End-to-end SSL</li> </ul>
<i>Cisco Application Control Engine Module Command Reference</i>	<p>Provides an alphabetical list and descriptions of all CLI commands by mode, including syntax, options, and related commands.</p>

# Symbols and Conventions

This publication uses the following conventions:

Convention	Description
<b>boldface font</b>	Commands, command options, and keywords are in <b>boldface</b> . Bold text also indicates a command in a paragraph.
<i>italic font</i>	Arguments for which you supply values are in <i>italics</i> . Italic text also indicates the first occurrence of a new term, book title, emphasized text.
{ }	Encloses required arguments and keywords.
[ ]	Encloses optional arguments and keywords.
{x   y   z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x   y   z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A unquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
screen font	Terminal sessions and information the system displays are in <i>screen font</i> .
<b>boldface screen font</b>	Information you must enter in a command line is in <b>boldface screen font</b> .
<i>italic screen font</i>	Arguments for which you supply values are in <i>italic screen font</i> .
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords are in angle brackets.

*Italic text* indicates the first occurrence of a new term, book title, emphasized text, and variables for which you supply values.

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 *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:

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

## 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](mailto: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](mailto: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 ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)). This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

#### **Original SSLeay License:**

© 1995-1998 Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)). All rights reserved.

This package is an SSL implementation written by Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)).

The implementation was written so as to conform with Netscapes 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](mailto: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 ([ey@cryptsoft.com](mailto:ey@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

## Configuring System Message Logging

---

This chapter describes how to configure system message logging on the Cisco Application Control Engine (ACE) module. Each ACE contains a number of log files that retain records of specified ACE-related activities and the performance of various ACE functions. You can access these log files using the ACE CLI to troubleshoot problems or to better understand the operation of the ACE.

This chapter includes the following major sections:

- [Understanding System Message Logging](#)
- [System Message Logging Quick Start](#)
- [Enabling System Message Logging](#)
- [Specifying syslog Output Locations](#)
- [Enabling Time Stamps on System Messages](#)
- [Identifying Messages Sent to a syslog Server](#)
- [Specifying a Device ID of the ACE to a syslog Server](#)
- [Changing the syslog Logging Facility](#)
- [Changing the Logging Message Queue](#)
- [Disabling or Changing the Severity Level of syslog Messages](#)
- [Limiting the Syslog Rate](#)
- [Enabling Logging on the Standby ACE](#)
- [Rejecting New Connections Through the ACE](#)
- [Enabling the Logging of Connection Setup and Teardown Syslog Messages Through the Fast Path](#)
- [Clearing Log Messages](#)
- [Viewing Log Message Information](#)

# Understanding System Message Logging

This section includes the following topics:

- [Logging Overview](#)
- [Log Message Format](#)
- [Logging Severity Levels](#)
- [Variables](#)

## Logging Overview

The system message logging function of the ACE saves these messages in a log file and allows you to send the logging messages to one or more output locations. System log messages provide you with logging information for monitoring and troubleshooting the operation of the ACE. By default, messages are not saved in a log file. You must enable the transmission of syslog messages to a specified output location.

The logging configuration is flexible and allows you to customize many aspects of how the ACE handles system messages. Using the system message logging feature, you can do the following:

- Specify one or more output locations where messages should be sent, including the console, an internal buffer, one or more syslog servers, an SNMP network management station, to Telnet or SSH sessions, the Catalyst supervisor engine, or to Flash memory on the ACE.
- Specify which messages should be logged.
- Specify the severity level of a message.
- Enable time stamps.
- Specify the unique device ID of the ACE that is sent to a syslog server.
- Change the size of the logging message queue.
- Limit the rate at which the ACE generates messages in the syslog.
- Reject new connections if a specified condition has been reached.
- Enable the logging of connection setup and teardown messages.

If the ACE is operating in multiple-context mode, you can configure the ACE to include an identifier for the virtual context and the virtual user responsible for executing the function in the log message.

To view logs generated by the ACE, you must configure an output location. You can choose to send all messages, or subsets of messages, to one or more output locations. You can limit which messages are sent to an output location by specifying the severity level of the message. Severity level values are 0 to 7; the lower the level number, the more severe the error. See [Table 1-1](#) for a listing of the log message severity levels.

**Note**

---

Not all system messages indicate an error condition. Some messages report normal events or log a configuration change.

---

The level you specify causes the ACE to apply the command to messages of that level or lower. For example, if you enter a command that specifies severity level 3, the ACE applies the command results to messages with a severity level of 0, 1, 2, and 3.

The ACE saves syslog messages in an internal buffer that can store up to 8192 messages. By default, the ACE can hold 80 syslog messages in the message queue while awaiting processing.

The ACE supports the EMBLEM syslog format for logging with each syslog server. The EMBLEM syslog format is consistent with the Cisco IOS software format and is compatible with CiscoWorks management applications. EMBLEM-format logging is available for UDP syslog messages only.

## Log Message Format

System log messages begin with a percent sign (%) and are structured as follows:

```
%<ACE>-Level-[Subfacility]-Message_number: Message_text
```

<i>ACE</i>	Identifies the message facility code for messages generated by the ACE. This value is always ACE.
<i>Level</i>	Level reflects the severity of the condition described by the message. The levels are 0 to 7. The lower the number, the more severe the condition. See <a href="#">Table 1-1</a> for a summary of logging severity levels. See <a href="#">Chapter 3, Messages Listed by Severity Level</a> for a listing of ACE system log messages by severity code.
<i>Subfacility</i>	(Optional) Name of the component or subcomponent that initiated the system log message (for example, IFMGR).
<i>Message_number</i>	Unique 6-digit number that identifies the message. See <a href="#">Chapter 2, System Messages</a> , for a detailed list of the ACE system log messages. The messages are listed numerically by message code.
<i>Message_text</i>	A text string describing the condition. This portion of the message sometimes includes virtual context, virtual user, IP addresses, port numbers, usernames, and so on.



### Note

Syslog messages received at the ACE serial console contain only the code portion of the message.

For example, this syslog message shows the information that is displayed when you assign a VLAN number to the ACE from the supervisor engine:

```
%ACE-6-615004 : VLAN <VLAN-number> available for configuring an interface
```

*VLAN-number* identifies the VLAN number assigned to the ACE. The ACE can use that VLAN to configure an interface and receive traffic.

## Logging Severity Levels

You instruct the ACE which system messages to log by specifying a logging level. The logging level designates that the ACE logs emergency, alert, critical, error, or warning messages for the various software functions. The ACE also logs notification, informational, and debugging messages. The ACE supports eight logging levels to identify a wide range of critical and noncritical logged events that may occur on an ACE.

Table 1-1 lists the log message severity levels.

**Table 1-1** Log Message Severity Levels

Level Number	Level Keyword	Description
0	<b>emergency</b>	System unusable (for example, the ACE has shut down and cannot be restarted, or it has experienced a hardware failure).
1	<b>alert</b>	Immediate action needed (for example, one of the ACE subsystems is not running).
2	<b>critical</b>	Critical condition (for example, the ACE has encountered a critical condition that requires immediate attention).
3	<b>error</b>	Error condition (for example, error messages about software or hardware malfunctions).
4	<b>warning</b>	Warning condition (for example, the ACE encountered an error condition that requires attention but is not interfering with the operation of the device).
5	<b>notification</b>	Normal but significant condition (for example, interface up/down transitions and system restart messages).
6	<b>informational</b>	Informational message only (for example, reload requests and low-process stack messages).
7	<b>debugging</b>	Appears during debugging only.

## Variables

Log messages often contain variables. Table 1-2 lists most variables that are used in this guide to describe ACE log messages. Some variables that appear in only one log message are not listed.

**Table 1-2** Variable Fields in Syslog Messages

Type	Variable	Type of Information
Misc.	<i>command</i>	Command name.
	<i>device</i>	Memory storage device. For example, Flash memory, TFTP, the failover standby unit, or the console terminal.
	<i>filename</i>	Filename of the type ACE image or configuration.

**Table 1-2 Variable Fields in Syslog Messages (continued)**

Type	Variable	Type of Information
Misc. continued	<i>privilege_level</i>	User privilege level.
	<i>reason</i>	Text string describing the reason for the message.
	<i>string</i>	Text string (for example, a username).
	<i>url</i>	URL.
	<i>user</i>	Username.
Numbers	<i>number</i>	Number. The exact form depends on the log message.
	<i>bytes</i>	Number of bytes.
	<i>code</i>	Decimal number returned by the message to indicate the cause or source of the error, depending on the message.
	<i>connections</i>	Number of connections.
	<i>time</i>	Duration, in the format <i>hh:mm:ss</i> .
	<i>dec</i>	Decimal number.
	<i>hex</i>	Hexadecimal number.
	<i>octal</i>	Octal number.
Addresses	<i>IP_address</i>	IP address in the form <i>n.n.n.n</i> , where <i>n</i> is an integer from 1 to 255.
	<i>MAC_address</i>	MAC address.
	<i>global_address</i>	Global IP address, an address on a lower security level interface.
	<i>source_address</i>	Source address of a packet.
	<i>dest_address</i>	Destination address of a packet.
	<i>real_address</i>	Real IP address, before Network Address Translation (NAT).
	<i>mapped_address</i>	Translated IP address.
	<i>gateway_address</i>	Network gateway IP address.
	<i>netmask</i>	Subnet mask.
Interfaces	<i>interface_number</i>	Interface number, <b>1</b> to <i>n</i> , where the number is determined by the order the interfaces load in the ACE. Use the <b>show interface internal</b> command to view detailed information about the interfaces.
	<i>interface_name</i>	Name assigned to the interface. Use the <b>show interface</b> command to view the interfaces and their names.
Ports, Services, and Protocols	<i>port</i>	TCP or UDP port number.
	<i>source_port</i>	Source port number.
	<i>dest_port</i>	Destination port number.
	<i>real_port</i>	Real port number, before NAT.
	<i>mapped_port</i>	Translated port number.
	<i>global_port</i>	Global port number.
	<i>protocol</i>	Protocol of the packet, for example, ICMP, TCP, or UDP.
	<i>service</i>	Service specified by the packet, for example, SNMP or Telnet.

# System Message Logging Quick Start

Table 1-3 provides a quick overview of the steps required to configure system message logging on the ACE. Each step includes the CLI command required to complete the task.

**Table 1-3 System Message Logging Configuration Quick Start**

---

## Task and Command Example

---

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 by entering **config**.

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

3. Enable logging to send system log messages to one or more output locations.

```
host1/Admin(config)# logging enable
```

4. Configure the ACE system software to send system logging messages to the output locations of your choice.

For example, to set the logging buffer level to 3 for logging error messages, enter:

```
host1/Admin(config)# logging buffered 3
```

For example, to send log messages to a syslog server, enter:

```
host1/Admin(config)# logging host 192.168.10.1
```

5. (Optional) Enable the display of a time stamp on system logging messages.

```
host1/Admin(config)# logging timestamp
```

6. (Optional) Limit the number of messages sent to a syslog server based on severity.

```
host1/Admin(config)# logging trap 6
```

7. (Optional) Display a unique device ID in non-EMBLEM format syslog messages sent to the syslog server.

```
host1/Admin(config)# logging device-id hostname
```

8. (Optional) Set the syslog logging facility to a value other than the default of 20 (LOCAL4).

```
host1/Admin(config)# logging facility 16
```

9. (Optional) Change the number of syslog messages that can appear in the message queue while awaiting processing.

```
host1/Admin(config)# logging queue 100
```

---

**Table 1-3 System Message Logging Configuration Quick Start (continued)**

---

**Task and Command Example**

---

10. (Optional) Disable the display of a specific syslog message or change the severity level of a specific system log message.
- For example, to disable the %<ACE>-6-615004 syslog message, enter:
- ```
host1/Admin(config)# no logging message 615004
```
- For example, to change the level of the 615004 syslog message, enter:
- ```
(config)# logging message 615004 level 5
```
- 
11. (Optional) Limit the rate at which the ACE generates messages in the syslog.
- ```
host1/Admin(config)# logging rate-limit 42 60 level 6
```
- 
12. (Optional) Enable logging on the failover standby ACE.
- ```
host1/Admin(config)# logging standby
```
- 
13. (Optional) Set the severity level at which syslog messages are sent to the supervisor engine in the Catalyst 6500 series chassis.
- ```
host1/Admin(config)# logging supervisor 3
```
- 
14. (Optional) Define if the ACE prohibits new connections from passing through the device if a specified condition has been met.
- ```
host1/Admin(config)# logging reject-newconn rate-limit-reached
```
- 
15. (Optional) Enable the logging of connection setup and teardown messages at a faster rate (that is, at the connection rate).
- ```
host1/Admin(config)# logging fastpath
```
- 
16. (Optional) Save your configuration changes to Flash memory.
- ```
host1/Admin(config)# exit  
host1/Admin# copy running-config startup-config
```
-

# Enabling System Message Logging

Message logging is disabled by default. You must enable logging if you want to send messages to one or more output locations. When enabled, log messages are sent to a logging process, which logs messages to designated locations asynchronously to the processes that generated the messages. You must set a logging output location to view any logs (see the “[Specifying syslog Output Locations](#)” section).

To enable message logging, use the **logging enable** configuration mode command. The syntax of this command is as follows:

## **logging enable**

For example, to enable message logging to all output locations, enter:

```
host1/Admin(config)# logging enable
```

To stop message logging to all output locations, enter:

```
host1/Admin(config)# no logging enable
```

# Specifying syslog Output Locations

You configure the ACE to send syslog messages to the output location of your choice. The ACE provides several output locations for sending syslog messages:

- An internal buffer on the ACE
- One or more syslog servers running on hosts
- A Telnet or SSH connection
- The console



---

**Note** We recommend sending syslog messages directly to the console only during testing.

---

- An SNMP network management station
- Catalyst supervisor engine
- Flash memory

You must enable logging on the ACE using the **logging enable** command before messages are sent to the specified output device. See the “[Enabling System Message Logging](#)” section.

This section includes the following topics:

- [Sending syslog Messages to a Buffer](#)
- [Sending syslog Messages to a Telnet or SSH Session](#)
- [Sending syslog Messages to the Console](#)
- [Sending syslog Messages to a syslog Server](#)
- [Sending syslog Messages to an SNMP Network Management Station](#)
- [Sending syslog Messages to the Supervisor Engine](#)
- [Sending syslog Messages to Flash Memory on the ACE](#)

## Sending syslog Messages to a Buffer

By default, logging to the local buffer on the ACE is disabled. To enable system logging to a local buffer and to limit the messages sent to the buffer based on severity, use the **logging buffered** configuration mode command. New messages append to the end of the buffer. The first message displayed is the oldest message in the buffer. When the log buffer fills, the ACE deletes the oldest message to make space for new messages.

The syntax of this command is as follows:

```
logging buffered severity_level
```

The *severity\_level* argument specifies the maximum level for system log messages sent to the buffer. The severity level that you specify indicates that you want syslog messages at that level and messages less than the level. For example, if the specified level is 3, the syslog displays level 3, 2, 1, and 0 messages.

Allowable entries are as follows:

- **0—emergencies** (System unusable messages)
- **1—alerts** (Take immediate action)
- **2—critical** (Critical condition)
- **3—errors** (Error message)
- **4—warnings** (Warning message)
- **5—notifications** (Normal but significant condition)
- **6—informational** (Information message)
- **7—debugging** (Debug messages)

To view the messages logged in the local buffer, use the **show logging** command. To clear the buffer so that viewing new messages is easier, use the **clear logging** command.

For example, to set the logging buffer level to severity level 3 for logging error messages, enter:

```
host1/Admin(config)# logging buffered 3
```

To disable message logging, enter:

```
host1/Admin(config)# no logging buffered
```

## Sending syslog Messages to a Telnet or SSH Session

By default, logging to a remote connection using the Secure Shell (SSH) or Telnet is disabled on the ACE. You can display log messages on a remote SSH or Telnet connection by setting the logging preferences for Telnet and SSH sessions. To display syslog messages as they occur when accessing the ACE through an SSH or Telnet sessions, use the **logging monitor** configuration mode command. You can limit the display of messages based on severity.

To display system message logs during the SSH or Telnet session, use the **terminal monitor** Exec mode command (see the *Cisco Application Control Engine Module Administration Guide*). This command enables syslog messages for all sessions in the current context. The **logging monitor** command sets the logging preferences for all SSH and Telnet sessions, while the **terminal monitor** command controls logging for each individual Telnet session. However, in each session, the **terminal monitor** command controls whether syslog messages appear on the terminal during the session.

**Note**

If you have not done so already, enable remote access on the ACE and establish a remote connection using the Secure Shell (SSH) or Telnet protocols from a PC. See the *Cisco Application Control Engine Module Administration Guide* for details.

The syntax of this command is as follows:

**logging monitor** *severity\_level*

The *severity\_level* argument specifies the maximum level for system log messages displayed during the current SSH or Telnet session. The severity level that you specify indicates that you want syslog messages at that level and messages less than the level. For example, if the specified level is 3, the syslog displays level 3, 2, 1, and 0 messages.

Allowable entries are as follows:

- **0—emergencies** (System unusable messages)
- **1—alerts** (Take immediate action)
- **2—critical** (Critical condition)
- **3—errors** (Error message)
- **4—warnings** (Warning message)
- **5—notifications** (Normal but significant condition)
- **6—informational** (Information message)
- **7—debugging** (Debug messages)

For example, to send informational system message logs to the current Telnet or SSH session, enter:

```
host1/Admin# terminal monitor
host1/Admin# config
Enter configuration commands, one per line. End with CNTL/Z
host1/Admin(config)# logging monitor 6
```

To disable system message logging to the current Telnet or SSH session, enter:

```
host1/Admin(config)# no logging monitor
```

To disable the terminal monitor function, enter:

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

## Sending syslog Messages to the Console

By default, the ACE does not display syslog messages during console sessions. To enable the logging of syslog messages during console sessions and to limit the display of messages based on severity, use the **logging console** configuration command.

Logging to the console can degrade system performance. Use the **logging console** command only when you are testing and debugging problems, or when there is minimal load on the network. Do not use this command when the network is busy, as it can reduce ACE performance. When the ACE is active, use the following commands:

- The **logging buffered** command to store messages
- The **show logging** command to view messages
- The **clear logging** command to clear the messages displayed by the **logging buffered** command

The syntax of this command is as follows:

```
logging console severity_level
```

The *severity\_level* argument specifies the maximum level for system log messages sent to the console. The severity level that you specify indicates that you want syslog messages at that level and messages less than the level. For example, if the specified level is 3, the syslog displays level 3, 2, 1, and 0 messages. We recommend that you use a lower severity level, such as 3, since logging at a high rate may impact the performance of the ACE.

Allowable entries are as follows:

- **0—emergencies** (System unusable messages)
- **1—alerts** (Take immediate action)
- **2—critical** (Critical condition)
- **3—errors** (Error message)
- **4—warnings** (Warning message)
- **5—notifications** (Normal but significant condition)
- **6—informational** (Information message)
- **7—debugging** (Debug messages)

For example, to enable the logging of syslog messages during console sessions and set the severity level to 3, enter:

```
host1/Admin(config)# logging console 3
```

To disable message logging to the console, enter:

```
host1/Admin(config)# no logging console
```

## Sending syslog Messages to a syslog Server

By default, logging to a syslog server on a host is disabled on the ACE. If you choose to send log messages to a host, the ACE sends those messages using either UDP or TCP. The host must run a program (known as a server) called `syslogd`. `syslogd` is a daemon that accepts messages from other applications and the network, and writes them out to system wide log files. UNIX provides the syslog server as part of its operating system. For Microsoft Windows, you must obtain a syslog server for the Windows operating system.

To specify a host (the syslog server) that receives the syslog messages sent by the ACE, use the **logging host** configuration command. You can configure a maximum of two servers to receive the syslog messages.

You can use either UDP or TCP to send messages to the syslog server. UDP-based logging does not prevent the ACE from passing traffic if the syslog server fails. If you use TCP as the logging transport protocol, the ACE denies new network access sessions as a security measure if the ACE is unable to reach the syslog server, if the syslog server is misconfigured, if the TCP queue is full, or if the disk is full.

In addition, you can configure the ACE to prohibits new connections from passing through the device by using the **logging-reject-newconn tcp-queue-full** configuration mode command (see the [“Rejecting New Connections Through the ACE”](#) section). Through this command, the ACE rejects new connections when syslogs can no longer reach the TCP syslog server. By default, this function is disabled.

The **format emblem** keyword allows you to enable EMBLEM-format logging for each syslog server. EMBLEM-format logging is available for either TCP or UDP syslog messages. If you enable EMBLEM-format logging for a particular syslog host, then the messages are sent to that host.

The syntax of this command is as follows:

```
logging host ip_address [tcp | udp [/port#]] | [default-udp] | [format emblem]]
```

The keywords, arguments, and options are as follows:

- *ip\_address*—IP address of the host to be used as the syslog server.
- **tcp**—(Optional) Specifies to use TCP to send messages to the syslog server. A server can only be specified to receive either UDP or TCP, not both.
- **udp**—(Optional) Specifies to use UDP to send messages to the syslog server. A server can only be specified to receive either UDP or TCP, not both.
- *port#*—(Optional) Port that the syslog server listens to for syslog messages. Valid values are as from 1025 to 65535. The default protocol and port are UDP/514. The default TCP port, if specified, is 1470.
- **default-udp**—(Optional) Instructs the ACE to default to UDP if the TCP transport fails to communicate with the syslog server.
- **format emblem**—(Optional) Enables EMBLEM-format logging for each syslog server. The Cisco Resource Management Environment (RME) is a network management application that collects syslogs. RME can process syslog messages only if they are in EMBLEM format.



**Note** If you enter the **logging timestamp** command, the messages are sent to the syslog server with a time stamp (see the [“Enabling Time Stamps on System Messages”](#) section).

For example, the EMBLEM format for a message with a time stamp appears as follows:

```
ipaddress or dns name [Dummy Value/Counter]: [mmm dd hh:mm:ss TimeZone]:  
%FACILITY-[SUBFACILITY-]SEVERITY-MNEMONIC: [vtl-ctx: context id] Message-text
```

For example, to send log messages to a syslog server, enter:

```
host1/Admin(config)# logging host 192.168.10.1 tcp1025 format emblem default-udp
```

To disable logging to a syslog server, enter:

```
host1/Admin(config)# no logging host 192.168.10.1
```

## Sending syslog Messages to an SNMP Network Management Station

By default, the ACE does not send traps and inform requests to an SNMP network management station (NMS). Notification traps and inform requests are system alerts that the ACE generates when certain events occur. To enable the ACE to send SNMP traps and inform requests to an NMS, use the **snmp-server enable traps** configuration command. For details on configuring SNMP, see the *Cisco Application Control Engine Module Administration Guide*.

To set the SNMP trap message severity level when sending log messages to an NMS, use the **logging history** configuration command.

The syntax of this command is as follows:

```
logging history severity_level
```

The *severity\_level* argument specifies the maximum level for system log messages sent as traps to the NMS. The severity level that you specify indicates that you want syslog messages at that level and messages less than the level. For example, if the specified level is 3, the syslog displays level 3, 2, 1, and 0 messages.

Allowable entries are as follows:

- **0—emergencies** (System unusable messages)
- **1—alerts** (Take immediate action)
- **2—critical** (Critical condition)
- **3—errors** (Error message)
- **4—warnings** (Warning message)
- **5—notifications** (Normal but significant condition)
- **6—informational** (Information message)
- **7—debugging** (Debug messages)

**Note**

We recommend that you use the debugging (7) level during initial setup and during testing. After setup, set the level from debugging (7) to a lower value for use in your network.

For example, to send informational system message logs to an SNMP NMS, enter:

```
host1/Admin(config)# logging history 6
```

To disable sending system message logs to an SNMP NMS, enter:

```
host1/Admin(config)# no logging history
```

## Sending syslog Messages to the Supervisor Engine

The ACE can forward syslog messages to the supervisor engine in the Catalyst 6500 series switch or Cisco 7600 series router. To set the severity level at which syslog messages are sent to the supervisor engine, use the **logging supervisor** configuration mode command.

The syntax of this command is as follows:

```
logging supervisor severity_level
```

**Note**

Use care when you send syslog messages to the supervisor engine, especially when you expect a high volume of syslog messages (for example, using logging level 6 or 7). Sending a high volume of syslog messages to the supervisor engine may slow down the operation of the ACE and the supervisor engine.

The *severity\_level* argument specifies the maximum level for system log messages sent to the supervisor engine. The severity level that you specify indicates that you want syslog messages at that level and messages less than the level. For example, if the specified level is 3, the syslog displays level 3, 2, 1, and 0 messages. We recommend that you use a lower severity level, such as 3, since logging at a high rate to the supervisor engine may impact the performance of the Catalyst system.

Allowable entries are as follows:

- **0—emergencies** (System unusable messages)
- **1—alerts** (Take immediate action)
- **2—critical** (Critical condition)
- **3—errors** (Error message)
- **4—warnings** (Warning message)
- **5—notifications** (Normal but significant condition)
- **6—informational** (Information message)
- **7—debugging** (Debug messages)

For example, to send informational system message logs to the supervisor engine in the switch, enter:

```
host1/Admin(config)# logging supervisor 6
```

To disable system message logging to the supervisor engine, enter:

```
host1/Admin(config)# no logging supervisor
```

## Sending syslog Messages to Flash Memory on the ACE

By default, logging to Flash memory is disabled on the ACE. The ACE allows you to specify that system message logs that you want to keep after a system reboot by saving them to Flash memory. To send specific log messages to Flash memory on the ACE, use the **logging persistent** configuration mode command.

The syntax of this command is as follows:

```
logging persistent severity_level
```

The *severity\_level* argument sets the maximum level for system log messages sent to Flash memory. The severity level that you specify indicates that you want syslog messages at that level and messages less than the level. For example, if the specified level is 3, the syslog displays level 3, 2, 1, and 0 messages. We recommend that you use a lower severity level, such as 3, since logging at a high rate to Flash memory on the ACE may impact performance.

Allowable entries are as follows:

- **0—emergencies** (System unusable messages)
- **1—alerts** (Take immediate action)
- **2—critical** (Critical condition)

- **3—errors** (Error message)
- **4—warnings** (Warning message)
- **5—notifications** (Normal but significant condition)
- **6—informational** (Information message)
- **7—debugging** (Debug messages)

For example, to send informational system message logs to Flash memory on the ACE, enter:

```
host1/Admin(config)# logging persistent 6
```

To disable logging to Flash memory on the ACE, enter:

```
host1/Admin(config)# no logging persistent
```

## Enabling Time Stamps on System Messages

By default, the ACE does not include the date and time in syslog messages. To specify that syslog messages should include the date and time that the message was generated, use the **logging timestamp** configuration mode command.

The syntax of this command is as follows:

**logging timestamp**

For example, to enable the time stamp display on system logging messages, enter:

```
host1/Admin(config)# logging timestamp
```

To disable the time stamp display from syslog messages, enter:

```
host1/Admin(config)# no logging timestamp
```

## Identifying Messages Sent to a syslog Server

To identify which messages are sent to a syslog server, use the **logging trap** configuration command. The **logging trap** command limits the logging messages sent to a syslog server based on severity.

The syntax of this command is as follows:

**logging trap severity\_level**

The *severity\_level* argument specifies the maximum level for system log messages sent to a syslog server. The severity level that you specify indicates that you want syslog messages at that level and messages less than the level. For example, if the specified level is 3, the syslog displays level 3, 2, 1, and 0 messages.

Allowable entries are as follows:

- **0—emergencies** (System unusable messages)
- **1—alerts** (Take immediate action)
- **2—critical** (Critical condition)
- **3—errors** (Error message)
- **4—warnings** (Warning message)

- **5—notifications** (Normal but significant condition)
- **6—informational** (Information message)
- **7—debugging** (Debug messages)

To send logging messages to a syslog server, use the **logging host** command to specify the name or IP address of the host to be used as the syslog server (see the “[Sending syslog Messages to a syslog Server](#)” section).

For example, to send informational system message logs to the syslog server, enter:

```
host1/Admin(config)# logging trap 6
```

To disable sending message logs to the syslog server, enter:

```
host1/Admin(config)# no logging trap
```

## Specifying a Device ID of the ACE to a syslog Server

The ACE allows you to include a unique device ID in non-EMBLEM format syslog messages sent to the syslog server. The message includes the specified device ID (either the hostname and IP address of the specified interface [even if the message comes from another interface] or a string) in messages sent to a syslog server. The device ID does not appear in EMBLEM-formatted messages.

Use the **logging device-id** configuration mode command to specify that the device ID of the ACE is included in the syslog message. Once enabled, the ACE displays the device ID in all non-EMBLEM-formatted syslog messages. The device ID specification does not affect the syslog message text that is in EMBLEM format.



### Note

The device ID part of the syslog message is viewed through the syslog server only and not directly on the ACE.

The syntax of this command is as follows:

```
logging device-id { context-name | hostname | ipaddress interface_name | string text }
```

The keywords, arguments, and options are as follows:

- **context-name**—Specifies the name of the current context as the device ID to uniquely identify the syslog messages sent from the ACE.
- **hostname**—Specifies the hostname of the ACE as the device ID to uniquely identify the syslog messages sent from the ACE.
- **ipaddress** *interface\_name*—Specifies the IP address of the interface as the device ID to uniquely identify the syslog messages sent from the ACE. If you use the **ipaddress** keyword, syslog messages sent to an external server contain the IP address of the interface specified, regardless of which interface the ACE uses to send the log data to the external server. The maximum *interface\_name* length is 64 characters.
- **string** *text*—Specifies a text string to uniquely identify the syslog messages sent from the ACE. The maximum **string** length is 64 characters without spaces. You cannot use the following characters: & (ampersand), ' (single quote), " (double quote), < (less than), > (greater than), or ? (question mark).

For example, to instruct the ACE to use the hostname of the ACE to uniquely identify the syslog messages, enter:

```
host1/Admin(config)# logging device-id hostname
```

To disable the use of the hostname of the ACE, enter:

```
host1/Admin(config)# no logging device-id hostname
```

## Changing the syslog Logging Facility

If necessary, you can change the logging facility to a value other than the default of 20 (LOCAL4) by using the **logging facility** configuration mode command. Most UNIX systems expect the messages to use facility 20. The ACE allows you to change the syslog facility type to identify the behavior of the syslog daemon (syslogd) on the host. The syslog daemon uses the specified syslog facility to determine how to process messages. Each logging facility configures how the syslog daemon on the host handles a message. Syslog servers file messages based on the facility number in the message. There are eight possible facilities, 16 (LOCAL0) through 23 (LOCAL7).

**Note**

For more information on the syslog daemon and facility levels, see your syslog daemon documentation.

The syntax of this command is as follows:

```
logging facility number
```

The *number* argument specifies the syslog facility. Valid values are 16 (LOCAL0) through 23 (LOCAL7). The default is 20 (LOCAL4).

For example, to set the syslog facility as 16 (LOCAL0) in syslog messages, enter:

```
host1/Admin(config)# logging facility 16
```

To change the syslog facility back to the default of 20 (LOCAL4), enter:

```
host1/Admin(config)# no logging facility 16
```

## Changing the Logging Message Queue

By default, the ACE can hold 80 syslog messages in the message queue while awaiting processing. To change the number of syslog messages that can appear in the message queue, use the **logging queue** configuration mode command.

**Note**

Set the queue size before the ACE processes syslog messages. When traffic is heavy, messages may be discarded.

The syntax of this command is as follows:

```
logging queue queue_size
```

The *queue\_size* argument specifies the size of the queue for storing syslog messages. Valid values are from 1 to 8192 messages. The default is 80 messages.

For example, to change the size of the syslog message queue to 1000, enter:

```
host1/Admin(config)# logging queue 1000
```

To reset the logging queue size to the default of 80 messages, enter:

```
host1/Admin(config)# no logging queue 0
```

## Disabling or Changing the Severity Level of syslog Messages

When you enable system message logging (see the “[Enabling System Message Logging](#)” section), all syslog messages are enabled. Use the **logging message** configuration mode command to control the following:

- The display of a specific system logging message (enabled or disabled).
- The severity level associated with a specific system logging message.

You can use the **show logging** command to determine the severity level currently assigned to a message and whether the system logging message is enabled.

The syntax of this command is as follows:

```
logging message syslog_id [level severity_level]
```

The keywords, arguments, and options are as follows:

- *syslog\_id*—Specific message that you want to disable or to enable. For example, if a message is listed in the syslog as %<ACE>-4-411001, enter **411001** as the *syslog\_id*. See [Chapter 2, System Messages](#), for a detailed list of the ACE system log messages. The messages are listed numerically by message code.
- **level severity\_level**—(Optional) Changes the default severity level associated with a specific system log message. For example, the %<ACE>-4-411001 message listed in the syslog has the default severity level of 4 (warning message). You can change the assigned default severity level to a different level. See [Chapter 2, System Messages](#), for a detailed list of the ACE system log messages and associated default severity codes.

Allowable entries are as follows:

- **0—emergencies** (System unusable messages)
- **1—alerts** (Take immediate action)
- **2—critical** (Critical condition)
- **3—errors** (Error message)
- **4—warnings** (Warning message)
- **5—notifications** (Normal but significant condition)
- **6—informational** (Information message)
- **7—debugging** (Debug messages)

For example, to disable the %<ACE>-6-615004 syslog message (VLAN available for configuring an interface), enter:

```
host1/Admin(config)# no logging message 615004
```

To resume logging of the disabled syslog message, enter:

```
host1/Admin(config)# logging message 615004 level 6
```

For example, to change the severity level of the 615004 syslog message from the default of 6 (informational) to a severity level of 5 (notification), enter:

```
(config)# logging message 615004 level 5
```

To return the severity level of the 615004 syslog message to the default of 6, enter:

```
host1/Admin(config)# no logging message 615004
```

## Limiting the Syslog Rate

By default, the ACE disables rate limiting for messages in the syslog. To limit the rate at which the ACE generates messages in the syslog, use the **logging rate-limit** configuration mode command. You can limit the number of syslog messages generated by the ACE for specific messages.

The syntax of this command is as follows:

```
logging rate-limit {num {interval | level severity_level | message syslog_id} | unlimited {level severity_level | message syslog_id}}
```

The keywords, arguments, and options are:

- *num*—Number at which the syslog is to be rate limited.
- *interval*—Time interval (in seconds) over which the system message logs should be limited. The default time interval is one second.
- **level severity\_level**—Specifies the syslog level that you want to rate limit. The severity level you enter indicates that you want all syslog messages at the specified level to be rate-limited. For example, if you specify a severity level of 7, the ACE applies a rate limit only to level 7 (debugging messages). If you want to apply a logging rate limit on a different severity level, you must configure the **logging rate-limit** command for that level as well.

Allowable entries are as follows:

- **0—emergencies** (System unusable messages)
- **1—alerts** (Take immediate action)
- **2—critical** (Critical condition)
- **3—errors** (Error message)
- **4—warnings** (Warning message)
- **5—notifications** (Normal but significant condition)
- **6—informational** (Information message)
- **7—debugging** (Debug messages)
- **message syslog\_id**—Identifies the ID of the specific message you want to suppress reporting. For example, if a message is listed in the syslog as %ACE-4-411001, enter **411001** as the *syslog\_id*. See [Chapter 2, System Messages](#), for a detailed list of the ACE system log messages. The messages are listed numerically by message code.
- **unlimited**—Disables rate limiting for messages in the syslog.



**Note** Disabled rate limiting is the default setting. In this case, the **logging rate-limit unlimited** command will not be displayed in the ACE running-configuration file.

**Note**

If you configure rate limiting for syslogs 302028 through 302031 (connection setup and teardown syslogs that are formatted in the data plane), the ACE always rate-limits these syslogs at level 6. Even if you change the logging level to a different value using the **logging message** command and the new logging level appears on the syslog server or other destination, the ACE will continue to rate-limit these syslogs at level 6.

For example, to limit the syslog rate to a 60-second time interval for informational messages (level 6), enter:

```
host1/Admin(config)# logging rate-limit 42 60 level 6
```

For example, to suppress reporting of system message 302022, enter:

```
host1/Admin(config)# logging rate-limit 42 60 302022
```

To disable rate limiting, enter:

```
host1/Admin(config)# no logging rate-limit 42 60 level 6
```

## Enabling Logging on the Standby ACE

To enable logging on the failover standby ACE, use the **logging standby** configuration mode command. When enabled, the standby ACE syslog messages remain synchronized should failover occur. When enabled, this command causes twice the message traffic on the syslog server. This command is disabled by default.

The syntax of this command is as follows:

### **logging standby**

To enable logging on the failover standby ACE, enter:

```
host1/Admin(config)# logging standby
```

To disable logging on the standby ACE, enter:

```
host1/Admin(config)# no logging standby
```

# Rejecting New Connections Through the ACE

To define if the ACE prohibits new connections from passing through the device if a specified condition has been met, use the **logging-reject-newconn** configuration mode command.

The syntax of this command is as follows:

```
logging reject-newconn {cp-buffer-full | rate-limit-reached | tcp-queue-full}
```

The keywords, arguments, and options are as follows:

- **cp-buffer-full**—Specifies that the ACE rejects new connections when the syslog daemon internal buffer is full.
- **rate-limit-reached**—Specifies that the ACE rejects new connections if the syslog message rate specified through the **logging rate-limit** command has been reached (see the “[Limiting the Syslog Rate](#)” section).
- **tcp-queue-full**—Specifies that the ACE rejects new connections when syslogs can no longer reach the TCP syslog server.

By default, the **tcp-queue-full** condition is enabled and the **cp-buffer-full** and **rate-limit-reached** conditions are disabled.

For example, to configure the ACE to reject new connections if the specified syslog message rate has been reached, enter:

```
host1/Admin(config)# logging reject-newconn rate-limit-reached
```

To disable the ACE from rejecting new connections (the default condition), enter:

```
host1/Admin(config)# no logging reject-newconn rate-limit-reached
```

# Enabling the Logging of Connection Setup and Teardown Syslog Messages Through the Fast Path

By default, the ACE logs the following connection setup and teardown syslog messages through the control plane:

- 106023
- 302022
- 302023
- 302024
- 302025

Because of the large number of these syslog messages that are generated by connection setup and teardown, you can instruct the ACE to send these syslogs through the fast path instead of the control plane. The fast path supports a much higher rate of syslogs than the control plane does. When you instruct the ACE to send these syslogs through the fast path, the message formatting changes (different message spacing) and the syslog IDs change to 106028, 302028, 302029, 302030, and 302031, respectively.

To enable the logging of connection setup and teardown messages through the fast path, use the **logging fastpath** configuration mode command. When you enable this command, the syslog messages do not arrive at the output destination in the correct order. In addition, the syslog messages are sent only to the external syslog servers and are not seen on the other enabled syslog output destinations, such as the local buffer, the console, or the supervisor module.

The syntax of the **logging fastpath** command is as follows:

## **logging fastpath**

For example, to configure the ACE to log connection setup and teardown syslog messages through the fast path, enter:

```
host1/Admin(config)# logging fastpath
```

To reset the ACE behavior to the default of logging connection setup and teardown syslog messages through the control plane, enter:

```
host1/Admin(config)# no logging fastpath
```

## Clearing Log Messages

To clear the syslog messages contained in the message buffer created with the **logging buffered** configuration mode command, use the **clear logging** command.

The syntax of this command is as follows:

## **clear logging [disabled | rate-limit]**

The keywords, arguments, and options are as follows:

- **disabled**—(Optional) Clears all disabled syslog messages.
- **rate-limit**—(Optional) Clears the rate-limit configuration at which the ACE generates the syslog, as specified by the **logging rate-limit** command.

For example, to clear all syslog messages, enter:

```
host1/Admin# clear logging
```

## Viewing Log Message Information

Use the **show logging** configuration mode command in privileged Exec mode to view the current severity level and state of all syslog messages stored in the buffer or to display information related to specific syslog messages. This command lists the current syslog messages and identifies which **logging** command options are enabled. To view the contents of the syslog buffer, configure the buffer output location (see the “[Sending syslog Messages to a Buffer](#)” section).

The syntax of this command is as follows:

```
show logging [disabled | history | internal {event-history dbg | facility} | message [syslog_id | all
| disabled] | persistent | queue | rate-limit | statistics]
```

The keywords, arguments, and options are as follows:

- **disabled**—Displays the status of disabling syslog messages.
- **history**—Displays the syslog message history file.
- **internal**—Displays syslog internal messages.
- **event-history db**—Displays the debug history for the syslog server.




---

**Note** The ACE debug commands are intended for use by trained Cisco personnel only.

---

- **facility**—Lists the various internal facilities contained within the ACE.
- **message**—Displays a list of syslog messages that have been modified from the default settings. These are syslog messages that have been assigned a different severity level or messages that have been disabled.
- *syslog\_id*—Specific system log message (by message ID), the assigned default severity level, and whether the message is enabled or disabled. See [Chapter 2, System Messages](#), for a detailed list of the ACE system log messages. The messages are listed numerically by message code.
- **all**—Displays all system log message IDs, the assigned default severity level, and identifies whether each message is enabled or disabled.
- **disabled**—Displays a complete list of disabled syslog messages.
- **persistent**—Displays statistics for the log messages sent to Flash memory on the ACE.
- **queue**—Displays statistics for the internal syslog queue.
- **rate-limit**—Displays the current syslog rate-limit configuration.
- **statistics**—Displays syslog statistics.

For example, to display the message configuration detail for syslog message 615004 (VLAN available for configuring an interface), enter:

```
host/Admin# show logging message 615004
Message logging:
    message 615004: default-level 6 (enabled)
```

[Table 1-4](#) describes the fields in the **show logging** command output.

**Table 1-4** *Field Descriptions for the show logging Command*

<b>Field</b>	<b>Description</b>
Syslog Logging	Status of system message logging for the ACE: Enabled or Disabled.
Facility	System message logging facility setting.
History Logging	Status of the system message logging history setting: Enabled or Disabled.
Supervisor Logging	Status of the supervisor engine logging trap level setting: Enabled or Disabled.
Trap Logging	Status of the syslog server trap level setting: Enabled or Disabled.
Timestamp Logging	Status of including the date and time on syslog messages: Enabled or Disabled.
Fastpath Logging	Status of syslog fastpath logging: Enabled or Disabled.
Persist Logging	Status of logging to Flash memory on the ACE: Enabled or Disabled.
Standby Logging	Status of logging to the failover standby ACE: Enabled or Disabled.
Rate-limit logging	Status of limiting the rate at which the ACE generates syslog messages: Enabled or Disabled.
Console Logging	Status of logging to the console: Enabled or Disabled.
Monitor Logging	Status of logging to a remote connection using the Secure Shell (SSH) or Telnet: Enabled or Disabled.
Device ID	Status of including a unique device ID in non-EMBLEM format syslog messages sent to the syslog server: Enabled or Disabled.
Reject-newconn	Defines if the ACE prohibits new connections from passing through the device if a specified condition has been met.
rate-limit-reached	Status on whether the ACE rejects new connections if the syslog message rate specified through the <b>logging rate-limit</b> command has been reached. The state is either Enabled or Disabled.
tcp-queue-full	Status on whether the ACE rejects new connections when syslogs can no longer reach the TCP syslog server. The state is either Enabled or Disabled.
cp-buffer-state	Status on whether the ACE rejects new connections when the syslog daemon internal buffer is full. The state is either Enabled or Disabled.
Message Logging	Status of disabled syslog messages or syslog messages with a modified severity level. The state is either Enabled or Disabled.
Buffered Logging	Status of logging to the local buffer on the ACE is disabled: Enabled or Disabled.
Buffer Info	Presents information about the syslog message buffer.
Current Size	The current size of the syslog buffer memory on the ACE.
Global Pool	Total size of available syslog buffer memory.
Used Pool	Total size of used syslog buffer memory.
Min.	The minimum available syslog buffer memory.
Max.	The maximum available syslog buffer memory.

**Table 1-4** *Field Descriptions for the show logging Command (continued)*

Field	Description
Cur Ptr	Current pointer location in syslog buffer memory. Cur Ptr is automatically advanced after each buffer memory read or write.
Wrapped	Indicates if wraparound has occurred to the data in the syslog buffer memory.

Table 1-5 describes the fields in the **show logging disabled** command output.

**Table 1-5** *Field Descriptions for the show logging disabled Command*

Field	Description
Message Logging	Status of disabled syslog messages in the ACE: Enabled or Disabled.

Table 1-6 describes the fields in the **show logging history** command output.

**Table 1-6** *Field Descriptions for the show logging history Command*

Field	Description
syslog_trinity_show_history for context x	Status of the syslog message history setting for the active user context: Enabled or Disabled.

Table 1-7 describes the fields in the **show logging internal facility** command output.

**Table 1-7** *Field Descriptions for the show logging internal facility Command*

Field	Description
Syslog registered x facilities	Displays a list of all syslog registered facilities.

Table 1-8 describes the fields in the **show logging persistent** command output.

**Table 1-8** *Field Descriptions for the show logging persistent Command*

Field	Description
Current Size	Current size of the syslog buffer memory on the ACE.
Global Pool	Total size of available syslog buffer memory.
Used Pool	Total size of used syslog buffer memory.
Min.	Minimum available syslog buffer memory.
Max.	Maximum available syslog buffer memory.
Cur Ptr	Current pointer location in syslog buffer memory. Cur Ptr is automatically advanced after each buffer memory read or write.
Wrapped	Indicates if wraparound has occurred to the data in the syslog buffer memory.

Table 1-9 describes the fields in the **show logging queue** command output.

**Table 1-9 Field Descriptions for the show logging queue Command**

Field	Description
Logging Queue length limit	Number of syslog messages that can appear in the message queue along with the number of discarded messages.
Current x msg on queue, xxx msgs most on queue	Number of messages currently in the logging queue along with the default number of syslog messages that can appear in the message queue.
CP messages received	Number of messages received from the control plane along with the number of discarded messages.
IXP messages received	Number of messages received from the IXP2800 Network Processor along with the number of discarded messages.
Xscale messages received	Number of messages received from the Xscale CPU.
System Max Queue size	Maximum size of the logging queue.
System Free Queue size for allocation	Available space in the logging queue.

Table 1-10 describes the fields in the **show logging rate-limit** command output.

**Table 1-10 Field Descriptions for the show logging rate-limit Command**

Field	Description
Rate-limit Logging	Current syslog rate-limit configuration.

Table 1-11 describes the fields in the **show logging statistics** command output.

**Table 1-11 Field Descriptions for the show logging statistics Command**

Field	Description
Syslog Statistics	System message log-specific statistics.
Messages sent	
Console	Total number of messages sent to the console.
Buffer	Total number of messages sent to the local buffer on the ACE.
Persistent	Total number of messages sent to Flash memory on the ACE.
Supervisor	Total number of messages sent to the supervisor engine.
History	Total number of SNMP messages sent to an NMS.
Host	Total number of messages sent to a syslog server on a host.
Misc	Total number of miscellaneous system logging messages.
Messages Discarded	
Cfg rate-limit	Total number of messages discarded due to the syslog message rate specified through the <b>logging rate-limit</b> command.

**Table 1-11** *Field Descriptions for the show logging statistics Command (continued)*

<b>Field</b>	<b>Description</b>
Hard rate-limit	Total number of messages discarded due to the internally set syslog message rate.
Server down	Total number of messages discarded due to a syslog server failure on a host.
Queue full	Total number of messages discarded because the message queue is full.
Errors	Total number of messages discarded due to an error condition.
<b>SNMP-related Counters</b>	
Notifications sent	Total number of times the ACE sent SNMP traps (event notifications) to an NMS.
History table flushed	Total number of times the syslog message trap history table has been flushed.
Messages ignored	Total number of SNMP messages ignored by the ACE.
<b>NP-related Counters</b>	
To-CP dropped	Total number of messages sent by the network processor that were dropped by the control plane.
Fastpath sent	Total number of connection setup and teardown messages sent by the ACE.
Fastpath dropped	Total number of connection setup and teardown messages dropped by the ACE.





## CHAPTER 2

# System Messages

---

This chapter lists the ACE system log messages. The messages are listed numerically by message code. To view a list of the majority of variables used in ACE system log messages, see [Table 1-2 in Chapter 1, Configuring System Message Logging](#). To view ACE system log messages listed by severity level, see [Chapter 3, Messages Listed by Severity Level](#).

This chapter includes the following sections:

- [Messages 100001 to 199006](#)
- [Messages 211001 to 254002](#)
- [Messages 302022 to 327001](#)
- [Messages 400000 to 444007](#)
- [Messages 504001 to 504002](#)
- [Messages 607001 to 615004](#)
- [Messages 727001 to 750002](#)

## Messages 100001 to 199006

This section contains messages from [100001](#) to [199006](#).

### 100001

**Error Message** %ACE-2-100001: EOL function *chars* from library *chars* exited due to Signal *dec*

**Explanation** An error occurred in the CLI end of line (EOL) function.

**Recommended Action** No action is required.

## 106021

**Error Message** %ACE-1-106021: Deny protocol reverse path check from *source\_address* to *dest\_address* on interface *interface\_name*

**Explanation** An attack is in progress. Someone is attempting to spoof an IP address on an inbound connection. Unicast reverse path forwarding (RPF), also known as reverse route lookup, detected a packet that does not have a source address represented by a route and assumes that it is part of an attack on the ACE.

This message appears when you have enabled Unicast RPF with the **ip verify reverse-path** command (see the *Cisco Application Control Engine Module Security Configuration Guide*). Reverse path forwarding works on packets that are sent to an interface. If you configure this command on the outside, then the ACE checks packets arriving from the outside.

The ACE looks up a route based on the source address. If an entry is not found and a route is not defined, then this system log message appears and the connection is discarded.

If a route is defined, the ACE checks which interface to which it corresponds. If the packet arrived on another interface, it is either a spoof or there is an asymmetric routing environment that has more than one path to a destination. The ACE does not support asymmetric routing.

If the ACE is configured on an internal interface, it checks static route command statements or RIP, and if the source address is not found, then an internal user is spoofing their address.

**Recommended Action** Even though an attack is in progress, if this feature is enabled, no user action is required. The ACE repels the attack.

## 106023

**Error Message** %ACE-4-106023: Deny protocol *number* | *name* *src*  
*incoming-interface:src-ip* *dst* *outgoing-interface:dst-ip* by *access-group*  
*"acl-name"* (*hash 1*, *hash 2*)

**Explanation** An IP packet was denied by the ACL. This message appears even if you do not have the log option enabled for an ACL. If a packet hits an input ACL, the outgoing interface will not be known. In this case, the ACE prints the outgoing interface as undetermined. The source IP and destination IP addresses are the unmapped and mapped addresses for the input and output ACLs, respectively, when used with NAT.

The *hash 1* field is a 32-bit hexadecimal (0xnnnnnnnn) MD5-hash value that the ACE computes from the **access-list** command immediately when you configure an ACL. The ACE includes this hash value in deny syslog messages to help you identify the ACL entry that caused the syslog in the output of the **show access-list name detail** command. This hash value is line-number independent.

The *hash 2* field is a 16-bit hexadecimal (0xnnnn) MD5-hash value that the ACE computes from the expanded access-list entries resulting from the object groups that you configure in an ACL. The ACE computes the *hash 2* value when you activate the ACL on an interface. For ACLs that do not have object groups, the *hash 2* value is always 0x0. The ACE also includes the *hash 2* value in deny syslog messages to help you identify the expanded ACL entry that caused the syslog. This hash value is also line-number independent. To uniquely identify the expanded ACL entry that caused the syslog, you need to search for an entry in the **show access-list name detail** command output that matches both the *hash 1* and the *hash 2* hexadecimal values.

To prevent possible discrepancies between the hash numbers in the deny syslog message and the output of the **show access-list detail** command after a reboot, be sure to use Tab completion or type entire keywords in the CLI when you configure individual entries in an ACL.

**Recommended Action** If messages persist from the same source address, contact the remote host administrators. Such messages may indicate a foot-printing or port-scanning attempt.

## 106028

**Error Message** %ACE-1-106028: *String* Incomplete rule is currently applied on interface *interface-name*. Manual rollback to a previous access rule configuration on this interface is needed.

**Explanation** Possible String values are:

- WARNING: Access rules memory exhausted while processing *component*
- WARNING: Unknown error while processing *component*

Possible values for *component* are

- Access-list
- Service-policy
- Merged list

For example:

WARNING: Unknown error while processing service-policy. Incomplete rule is currently applied on interface VLAN100. Manual roll back to a previous access rule configuration on this interface is needed.

The access control list (ACL) compilation process has run out of memory, which does not allow new ACL entries to be applied to the specified interface. The ACL configuration downloaded in hardware for that interface may not be in a known state because of this failure.

**Recommended Action** The ACL configuration downloaded to the network processors is incomplete. Remove and recreate the affected interface to recover to a known state. If the message is “Access rules memory exhausted,” either allocate more memory to that context or remove some of the access group or service policy configuration to reduce the memory usage. If the message is “Unknown error,” then there may be an issue with the configuration manager or the ACL merge process.

## 111008

**Error Message** %ACE-5-111008: User *user* executed the command *string*

**Explanation** This message is informational. The user entered a command that modified the configuration.

**Recommended Action** None required.

## 111009

**Error Message** %ACE-7-111009: User *user* executed cmd:*string*

**Explanation** This message is informational. The user entered a command that does not modify the configuration.

**Recommended Action** None required.

## 199006

**Error Message** %ACE-2-199006 : Orderly reload started at *when* by *whom*. Reload reason: *reason*

**Explanation** This message logs a reload record of the ACE and the reason for the reload.

The *reason* variable describes why the reload occurred. Possible reasons are as follows:

- reload command
- sup request
- CF format
- hardware failure

The *when* variable specifies the time at which the orderly reload operation begins.

The *whom* variable specifies the name of the user who entered the **reload** command. If the reload is caused by other reasons, “System” is specified.

**Recommended Action** None required.

## Messages 211001 to 254002

This section contains messages from 211001 to 254002.

## 211001

**Error Message** %ACE-3-211001: Memory allocation Error

**Explanation** Failed to allocate RAM system memory.

**Recommended Action** If this message occurs periodically, it can be ignored. If it repeats frequently, contact Cisco TAC.

## 212007

**Error Message** %ACE-2-212007: SNMPD initialization failed while *Variable1*

**Explanation** This is an SNMP message that is logged when the SNMP daemon fails to initialize. The SNMP daemon is created during device initialization.

The possible values of the *Variable1* variable are the following:

- loading mib module
- performing mts\_bind
- performing mts\_options\_set
- initializing kernel memory map
- registering read/write file descriptor
- creating socket endpoint
- creating daemon process

**Recommended Action** Reboot the ACE (see the *Cisco Application Control Engine Module Administration Guide* for details). If the SNMP daemon still fails to initialize, contact Cisco TAC and provide them with the output of **show processes** and **show np** commands.

## 212008

**Error Message** %ACE-3-212008: Failed while allocating memory in snmpd

**Explanation** This is an SNMP message that is logged after a memory allocation failure in the SNMPD process. When this error occurs, SNMPD processes (for example, SNMP Get/GetNext responses, trap generation, or SNMP CLI) may be affected.

**Recommended Action** Check for the system memory using the **show system** command. If the ACE is low on memory, reboot it (see the *Cisco Application Control Engine Module Administration Guide* for details). If the memory is not low, contact the Cisco TAC and provide them with the output of the **show system resources** and **show processes cpu memory** commands.

## 251001

**Error Message** %ACE-3-251001: Probe configuration error, memory allocation failure.

**Explanation** The ACE does not have enough memory to support the specified probe configuration. When the Config Manager sends a probe configuration to the Health Monitor module, the Health Monitor module needs to reserve memory to set up the probe. If memory is not available when the Health Monitor is setting up the probe, the syslog message is sent.

**Recommended Action** Reduce the size of the probe configuration.

## 251002

**Error Message** %ACE-4-251002: The configured health probe script *script-name* for server *A.B.C.D* on port *P* is empty

**Explanation** An empty script is configured for the scripted health probe for server *A.B.C.D* on port *P*.

**Recommended Action** Update the script file with appropriate probe information, unload, and then reload the script (see the *Cisco Application Control Engine Module Server Load-Balancing Configuration Guide* for details). You can also reconfigure the health probe to use a nonempty script.

## 251003

**Error Message** %ACE-3-251003: Could not load script *script-name* - File not found

**Explanation** The ACE is unable to find the script file that it needs to load.

**Recommended Action** Create a new script file, unload the old file, and then load the new file (see the *Cisco Application Control Engine Module Server Load-Balancing Configuration Guide* for details).

## 251004

**Error Message** %ACE-3-251004: Could not load script *script-name* - memory allocation failure

**Explanation** The ACE does not have sufficient memory to load the specified script file.

**Recommended Action** Reduce the size of the configuration or unload any unused script files.

## 251005

**Error Message** %ACE-4-251005: Could not unload script *script-name*

**Explanation** The ACE is unable to load the specified script file due to an internal error.

**Recommended Action** Contact Cisco TAC if this error frequently occurs.

## 251006

**Error Message** %ACE-3-251006: Health probe failed for server *A.B.C.D* on port *P*, internal error: *error message*

**Explanation** The configured service on port *P* of server *A.B.C.D*. failed its health checks because the ACE encountered an internal error while performing the probe. Because the error is internal to the system, the real health of the server is unknown.

The possible values of the *error message* variable are the following:

- failed to setup a socket
- forced disconnect
- failed to allocate memory
- failed to create SSL context
- failed to create SSL session
- failed to assign socket to SSL session
- failed to build a server query
- failed to initialize LDAP
- failed to bind to LDAP
- invalid probe request
- failed to set LDAP option
- failed to get LDAP option

**Recommended Action** Contact Cisco TAC if this error frequently occurs.

## 251007

**Error Message** %ACE-3-251007: ICMP health probe failed for server A.B.C.D, internal error: *error message*

**Explanation** The configured service on port *P* of server A.B.C.D. failed its health checks because the ACE encountered an internal error while performing the ICMP probe. Because the error is internal to the system, the real health of the server is unknown.

The possible values of the *error message* variable are the following:

- general encap-decap failure
- write failure
- received bad file descriptor
- data entry being modified
- transmit queue is full

**Recommended Action** Contact Cisco TAC if this error frequently occurs.

## 251008

**Error Message** %ACE-3-251008: Health probe failed for server A.B.C.D on port *P*, connectivity error: server open timeout (no SYN ACK)

**Explanation** The configured service on port *P* of server A.B.C.D. failed its health checks because a probe was unable to reach the server due to network problem.

**Recommended Action** Verify network connectivity to the server, and then reprobe the server.

## 251009

**Error Message** %ACE-3-251009: ICMP health probe failed for server A.B.C.D, connectivity error: *error message*

**Explanation** The configured real server A.B.C.D. failed its health checks because an ICMP health probe was unable to reach the server due to a network connectivity problem.

The possible values of the *error message* variable are as follows:

- host unreachable, no route found to destination
- ARP not resolved for destination ip address
- network down
- interface has no ip address
- ICMP host unreachable
- ICMP destination unreachable

**Recommended Action** Verify network connectivity to the server, and then reprobe the server.

## 251010

**Error Message** %ACE-3-251010: Health probe failed for server *A.B.C.D* on port *P*, *error message*

**Explanation** The configured service on port *P* of server *A.B.C.D*. failed its health checks because the server response is not as expected.

The possible values of the *error message* variable are the following:

- connection reset by server
- connection refused by server
- authentication failed
- unrecognized or invalid response
- server reply timeout
- graceful disconnect timeout (no FIN ACK)
- user defined Reg-Exp was not found in host response
- expect status code mismatch
- received invalid status code
- MD5 checksum mismatch
- invalid server greeting
- received Out-Of-Band data

**Recommended Action** Check the service running on the affected server.

## 251011

**Error Message** %ACE-3-251011: ICMP health probe failed for server *A.B.C.D*, *error message*.

**Explanation** The configured real server *A.B.C.D*. failed its health checks because the ICMP server response is not as expected.

The possible values of the *error message* variable are the following:

- ICMP time exceeded
- ICMP redirect
- received ICMP Echo request
- received ICMP Stale packet
- received unexpected ICMP packet type
- received packet is too short
- received packet is too long
- server reply timeout

**Recommended Action** Check the service running on the affected server.

## 251012

**Error Message** %ACE-3-251012: Could not load script *script-name* - Error reading *script-file*

**Explanation** The ACE is unable to read the script file that it is attempting to load. The file may be corrupted.

**Recommended Action** Verify if the file contents are correct. If correct, unload, and then reload the script file (see the *Cisco Application Control Engine Module Server Load-Balancing Configuration Guide* for details). If necessary, create a new script file. Unload the old file, and then load the new file.

## 251013

**Error Message** %ACE-3-251013: Could not load script *script-name* - Error getting file size

**Explanation** This message is logged when the ACE is unable to determine the script file size. Before a script file can be loaded, the ACE needs determine its size so the appropriate amount of memory can be allocated.

**Recommended Action** Verify if the file contents are correct. If correct, unload, and then reload the script file (see the *Cisco Application Control Engine Module Server Load-Balancing Configuration Guide* for details). If necessary, create a new script file. Unload the old file, and then load the new file.

## 253001

**Error Message** %ACE-6-253001: Certificate *certificate\_information* expired

**Explanation** This message is logged during the SSL handshake when client authentication is enabled. The ACE determines that the certificate has expired.

**Recommended Action** None required.

## 253002

**Error Message** %ACE-6-253002: Certificate *certificate\_information* not yet valid

**Explanation** This message is logged during the SSL handshake when client authentication is enabled. The ACE determines that the certificate is not currently valid.

**Recommended Action** None required.

## 253003

**Error Message** %ACE-6-253003: Unknown CA *certificate\_information*

**Explanation** This message is logged during the SSL handshake when client authentication is enabled. The ACE determines that the certificate has an unknown certificate authority (CA).

**Recommended Action** None required.

## 253004

**Error Message** %ACE-6-253004: Certificate *certificate\_information* revoked

**Explanation** This message is logged during the SSL handshake when client authentication is enabled. The ACE determines that the certificate has been revoked by the CA.

**Recommended Action** None required.

## 253005

**Error Message** %ACE-6-253005: Signature for *certificate\_information* is invalid

**Explanation** This message is logged during the SSL handshake when client authentication is enabled. The ACE determines that the signature for the certificate is invalid.

**Recommended Action** None required.

## 253006

**Error Message** %ACE-6-253006: Error peer sent invalid or nonexistent certificate

**Explanation** This message is logged during the SSL handshake when client authentication is enabled. The ACE determines a certificate is invalid or nonexistent.

**Recommended Action** None required.

## 253007

**Error Message** %ACE-6-253007: Certificate in file *file\_name* is expired

**Explanation** This message is logged when the ACE attempts to use a certificate that has expired. X509 certificates have a fixed lifetime. If the ACE uses an expired certificate in an SSL handshake, the client may reject the connection. The *file\_name* argument is the name of the file where the certificate resides.

**Recommended Action** Obtain a new certificate and replace the expired one.

## 253008

**Error Message** %ACE-6-253008: CRL *crl\_name* could not be retrieved

**Explanation** This message is logged when the ACE failed to retrieve a CRL. If you define CRL checking for SSL client authentication, the ACE periodically retrieves a CRL. Due to a variety of reasons, these attempts can occasionally fail. The *crl\_name* variable is the name of the CRL as defined by the **crypto crl** command.

**Recommended Action** Check to see if there is a network connectivity problem or if the server location of the CRL has changed.

## 253009

**Error Message** %ACE-6-253009: Certificate in file *file\_name* is not yet valid

**Explanation** X509 certificates have a fixed lifetime. This message is logged when a certificate that is not currently valid is used in an SSL handshake. This event may cause the client to reject the connection. The *file\_name* variable is the name of the file where the certificate resides.

**Recommended Action** Use a certificate that is currently valid.

## 253010

**Error Message** %ACE-3-253010: Configuration failure: Certificate in file *certificate\_name* and key in file *key\_name* do not match

**Explanation** This message is logged when the certificate and key do not match. As a result, the SSL handshake fails and the ACE does not download the unmatched certificate and key in the configuration. Note that a X509 certificate has a matching private key. The *certificate\_name* variable is the name of the certificate file. The *key\_file* variable is the name of the key file.

**Recommended Action** Verify that the correct certificate and key are in use in the SSL-proxy service. If necessary, modify the SSL-proxy service to contain the correct files.

## 253011

**Error Message** %ACE-6-253011: The CRL *crl\_Name* may not be from a trusted source. Signature mismatch detected for CRL.

**Explanation** When the ACE performs signature verification on a CRL with a CA certificate configured with the **crypto crlparams** command, it detects a signature mismatch. Either the CRL (*crl\_name*) download failed or the CRL has been removed from the ACE.

**Recommended Action** Verify the CRL configuration for the **crypto crlparams** command.

## 254001

**Error Message** %ACE-4-254001: ACL resource usage beyond maximum limit for context *context\_id*. Free up some resources.

**Explanation** This message indicates that ACL resources in use for the specified context (*context\_id*) are above the maximum limit allowed by the resource class.

**Recommended Action** Decrease the minimum ACL usage in the specified context to below the maximum limit.

## 254002

**Error Message** %ACE-4-254002: Minimum ACL resources could not be guaranteed for context *context\_id*.

**Explanation** This message indicates that the requested minimum ACL resources could not be guaranteed in the specified context (*context\_id*).

**Recommended Action** Contact the global administrator to request that other context administrators release ACL resources.

## Messages 302022 to 327001

This section contains messages from 302022 to 327001.

### 302022

**Error Message** %ACE-6-302022: Built TCP connection *id* for *interface:real-address/real-port (mapped-address/mapped-port)* to *interface:real-address/real-port (mapped-address/mapped-port)*

**Explanation** This informational message is logged when a TCP connection slot between two hosts is created. This message is formatted by the control plane.

**Recommended Action** None required.

### 302023

**Error Message** %ACE-6-302023: Teardown TCP connection *id* for *interface:real-address/real-port* to *interface:real-address/real-port* duration *hh:mm:ss* bytes *bytes* [*reason*]

**Explanation** This informational message is logged when a TCP connection slot between two hosts is terminated. This message is formatted by the control plane.

The *reason* variable presents the action that causes the connection to terminate. [Table 2-1](#) lists the TCP termination causes.

**Recommended Action** None required.

**Table 2-1** TCP Termination Reasons

Reason	Description
TCP FINs	Normal close down sequence.
TCP Reset	A TCP reset is received.
Idle Timeout	TCP connection is timed out.
FIN Timeout	TCP FIN timeout.
SYN Timeout	TCP SYN timeout.
Exception	Connection setup error.
Policy Close	A policy closes the TCP connection.
Voluntary Close	TCP connection is closed voluntarily by a user.
Rebalance	HTTP rebalance.
Reuse Conn.	Connection is reused.
Reap Conn.	Connection is closed due to control plane reap messages.

**Table 2-1 TCP Termination Reasons (continued)**

Reason	Description
Xlate clear	Connection is closed due to execution of a <b>clear xlate</b> command.
Conn clear	Connection is closed due to execution of a <b>clear conn</b> command.

## 302024

**Error Message** %ACE-6-302024: Built UDP connection *id* for *interface:real-address/real-port (mapped-address/mapped-port)* to *interface:real-address/real-port (mapped-address/mapped-port)*

**Explanation** A UDP connection slot between two hosts was added. This message is formatted by the control plane.

**Recommended Action** None required.

## 302025

**Error Message** %ACE-6-302025: Teardown UDP connection *id* for *interface:real-address/real-port* to *interface:real-address/real-port* duration *hh:mm:ss* bytes *bytes*

**Explanation** A UDP connection slot between two hosts was deleted. This message is formatted by the control plane

**Recommended Action** None required.

## 302026

**Error Message** %ACE-6-302026: Built ICMP connection for *faddr/NATed\_ID* *gaddr/icmp\_type* *laddr/icmpID*

**Explanation** An ICMP session was established.

**Recommended Action** None required.

## 302027

**Error Message** %ACE-6-302027: Teardown ICMP connection for *faddr/NATed ID gaddr/icmp\_type laddr/icmpID*

**Explanation** An ICMP session was removed.

**Recommended Action** None required.

## 302028

**Error Message** %ACE-6-302028: Built TCP connection *id* for *interface: real-address/real-port (mapped-address/mapped-port)* to *interface: real-address/real-port (mapped-address/mapped-port)*

**Explanation** A TCP connection slot between two hosts was created. This message is generated by the data plane.

**Recommended Action** None required.

## 302029

**Error Message** %ACE-6-302029: Teardown TCP connection *id* for *interface: real-address/real-port* to *interface: real-address/real-port* duration *hh:mm:ss* bytes *bytes* [*reason*]

**Explanation** A TCP connection between two hosts was terminated. This message is generated by the data plane.

The *reason* variable presents the action that causes the connection to terminate. [Table 2-1](#) lists the TCP termination causes.

**Recommended Action** None required.

## 302030

**Error Message** %ACE-6-302030: Built UDP connection *id* for *interface: real-address/real-port (mapped-address/mapped-port)* to *interface: real-address/real-port (mapped-address/mapped-port)*

**Explanation** A UDP connection slot between two hosts was added. This message is generated by the data plane.

**Recommended Action** None required.

## 302031

**Error Message** %ACE-6-302031: Teardown UDP connection *id* for *interface: real-address/real-port* to *interface: real-address/real-port* duration *hh:mm:ss* bytes *bytes*

**Explanation** A UDP connection slot between two hosts was deleted. This message is generated by the data plane.

**Recommended Action** None required.

## 303003

**Error Message** %ACE-6-303003: FTP *cmd\_name* command denied - failed strict inspection, terminating connection from *source\_interface:source\_address/source\_port* to *dest\_interface:dest\_address/dest\_port*

**Explanation** The ACE module is using strict inspection on FTP traffic. This message displays if an FTP **request** command is denied by the strict FTP inspection policy from the **ftp-map** command.

**Recommended Action** None required.

## 303004

**Error Message** %ACE-5-303004: FTP *cmd\_string* command unsupported - failed strict inspection, terminating connection from *source\_interface:source\_address/source\_port* to *dest\_interface:dest\_address/dest\_interface*

**Explanation** The ACE module is using strict FTP inspection on FTP traffic. This message displays if an FTP request message contains a command that is not recognized by the device.

**Recommended Action** None required.

## 304001

**Error Message** %ACE-5-304001: user *source\_address* Accessed {*URL*} *dest\_address: url* Connection *connection\_ID*

**Explanation** This is a URL message that is logged when the specified host attempts to access the specified URL.

**Recommended Action** None required.

## 305009

**Error Message** %ACE-6-305009: Built {dynamic|static} translation from *interface\_name* [(*acl-name*)] :*real\_address* to *interface\_name:mapped\_address*

**Explanation** An address translation slot was created. The slot translates the source address from the local side to the global side. In reverse, the slot translates the destination address from the global side to the local side.

**Recommended Action** None required.

## 313004

**Error Message** %ACE-4-313004: Denied ICMP type=*icmp\_type*, from *source\_address* on interface *interface\_name* to *dest\_address*:no matching session

**Explanation** ICMP packets were discarded by the ACE because of security checks added by the stateful ICMP feature. These ICMP packets are discarded for any of the following reasons:

- ICMP echo replies are received without a valid echo request already passed across the ACE
- ICMP error messages are received that are not related to any TCP, UDP, or ICMP session already established in the ACE

**Recommended Action** None required.

## 313006

**Error Message** %ACE-1-313006: ICMP Manager Initialization Failed. Reason : *Variable1*

**Explanation** The ICMP Manager running on the Control Plane of the ACE fails to start.

The possible values of the *Variable1* variable are the following:

- Timer creation failed.
- MTS initialization failed.
- Error while opening system call.
- Error while mapping buffer manager memory.
- Encap/Decap registration failed.

**Recommended Action** The ACE should automatically reboot the card. If not, try rebooting manually. If the problem still exists, contact Cisco TAC and provide them with the output of **show tech-support** command.

## 313007

**Error Message** %ACE-1-313007: ICMP Manager Memory Problem. Reason: *Variable1*

**Explanation** Reports ICMP-related memory failures.

The possible values of the *Variable1* variable are the following:

- No memory available to create ping free list.
- No memory from buffer manager. Cannot send packet.
- No memory available for ping block.
- Possible memory corruption.

**Recommended Action** Reboot the ACE (see the *Cisco Application Control Engine Module Administration Guide* for details). If the problem persists, contact Cisco TAC and provide them with the following command output:

- If the “No memory from buffer manager. Cannot send packet.” message appears, provide the output generated from the **show buffer usage** and **show buffer stats** commands.
- If any other message is returned, provide the output generated from the **show process cpu memory** command.

## 314001

**Error Message** %ACE-6-314001: Pre-allocate RTSP UDP backconnection for foreign\_address outside\_address/outside\_port to local\_address inside\_address/inside\_port

**Explanation** The Cisco ASA opened an RTSP connection for the specified IP addresses and ports.

**Recommended Action** None required.

## 322001

**Error Message** %ACE-3-322001: Deny MAC address *MAC\_address*, possible spoof attempt on interface *interface*

**Explanation** The ACE received a packet from the offending MAC address on the specified interface, but the source MAC address in the packet is statically bound to another interface in your configuration. This situation can be caused by either a MAC-spoofing attack or a misconfiguration.

**Recommended Action** Check the configuration and take appropriate action by either finding the offending host or by reconfiguring the ACE.

## 322002

**Error Message** %ACE-3-322002: ARP inspection check failed for arp {request|response} received from host *MAC\_address* on interface *interface*. This host is advertising MAC Address *MAC\_address\_1* for IP Address *IP\_address*, which is {statically|dynamically} bound to MAC Address *MAC\_address\_2*.

**Explanation** If ARP inspection is enabled, the ACE checks whether a new ARP entry advertised in the packet conforms to the statically configured or dynamically learned IP-MAC address binding before forwarding ARP packets. If this check fails, the ACE drops the ARP packet and generates this message. This situation can be caused by either ARP spoofing attacks in the network or an invalid configuration (IP-MAC binding).

**Recommended Action** If the cause is an attack, deny the host by using an ACL. If the cause is an invalid configuration, correct the binding (see the *Cisco Application Control Engine Module Routing and Bridging Configuration Guide* for details).

## 322003

**Error Message** %ACE-3-322003: ARP inspection check failed for arp {request|response} received from host *MAC\_address* on interface *interface*. This host is advertising MAC Address *MAC\_address\_1* for IP Address *IP\_address*, which is not bound to any MAC Address.

**Explanation** If ARP inspection is enabled, the ACE checks whether a new ARP entry advertised in the packet conforms to the statically configured IP-MAC address binding before forwarding ARP packets. If this check fails, the ACE drops the ARP packet and generates this message. This situation may be caused by either ARP spoofing attacks in the network or an invalid configuration (IP-MAC binding).

**Recommended Action** If the cause is an attack, deny the host by using an ACL. If the cause is an invalid configuration, correct the binding (see the *Cisco Application Control Engine Module Routing and Bridging Configuration Guide* for details).

## 327001

**Error Message** %ACE-3-327001: Detected Encap table Full when allocating encap entry for *IP* interface *interface\_name*

**Explanation** The Encap table size is limited to 32,000 entries. This message is logged when trying to allocate an encap entry after the limit is reached.

**Recommended Action** Use the **clear arp** command to remove any unused or invalid table entries.

## Messages 40000 to 444007

This section contains messages from 40000 to 444007.

### 400000

**Error Message** %ACE-4-400000: IDS:1000 IP Option Bad Option List from *IP\_address* to *IP\_address* on interface *interface\_name*

**Explanation** Cisco Intrusion Detection System signature message. The ACE does not support IP options. This IDS message is generated whenever the ACE detects IP options in a packet.

**Recommended Action** See the *Cisco Intrusion Detection System User Guide*.

### 405001

**Error Message** %ACE-4-405001: Received ARP {request | response} collision from *IP\_address/mac\_address* on interface *interface\_name*

**Explanation** The ACE received an ARP packet, and the MAC address in the packet differs from the ARP cache entry.

**Recommended Action** This traffic may be legitimate, or it may indicate that an ARP poisoning attack is in progress. Check the source MAC address to determine where the packets are coming from and determine if the host is valid.

### 405201

**Error Message** %ACE-4-405201: ILS *ctxid* from *vlan x:src\_ip/srcprt* to *vlan y:dst\_ip/dstprt* has wrong embedded address *embedded addr* in ILS payload

**Explanation** The embedded IP address in the ILS packet payload is not same as the source IP address of the IP packet header.

**Recommended Action** Check the host with the specified source IP address to determine why it sent an ILS packet with an incorrect embedded IP address.

## 406001

**Error Message** %ACE-4-406001: FTP port command low port: *IP\_address/port* to *IP\_address* on interface *interface\_name*

**Explanation** A client issued an FTP **port** command with a port number less than 1024; in the well-known port range, this number is typically devoted to server ports. This error message indicates an attempt to avert the site security policy. The Cisco ASA drops the packet, terminates the connection, and logs the event.

**Recommended Action** None required.

## 406002

**Error Message** %ACE-4-406002: FTP port command different address: *IP\_address(IP\_address)* to *IP\_address* on interface *interface\_name*

**Explanation** A client issued an FTP **port** command with an address other than the address used in the connection. This error message indicates that an attempt was made to avert the site security policy. The address in parentheses is the address from the **port** command. For example, an attacker may attempt to hijack an FTP session by changing the transmitted packet and putting different source information instead of the correct source information. The security appliance drops the packet, terminates the connection, and logs the event.

**Recommended Action** None required.

## 410001

**Error Message** %ACE-4-410001: Dropped UDP DNS *packet\_type* from *source\_interface:source\_address/source\_port* to *dest\_interface:dest\_address/dest\_port*; *error\_length\_type* length *length* bytes exceeds *max\_length\_type* limit of *maximum\_length* bytes.

**Explanation** The domain-name length exceeds 255 bytes in a UDP DNS packet. (See RFC 1035 section 3.1.)

**Recommended Action** None required.

## 411001

**Error Message** %ACE-4-411001: Line protocol on interface *interface\_name* changed state to up

**Explanation** The status of the line protocol has changed from down to up.

**Recommended Action** None required.

## 411002

**Error Message** %ACE-4-411002: Line protocol on interface *interface\_name* changed state to down

**Explanation** The status of the line protocol has changed from up to down.

**Recommended Action** If this is an unexpected event on the interface, check the line.

## 411003

**Error Message** %ACE-4-411003: Configuration status on interface *interface\_name* changed state to up

**Explanation** The configuration status of the interface has changed from down to up.

**Recommended Action** If this is an unexpected event on the interface, check the line.

## 411004

**Error Message** %ACE-4-411004: Configuration status on interface *interface\_name* changed state to down

**Explanation** The configuration status of the interface has changed from up to down.

**Recommended Action** None required.

## 412001

**Error Message** %ACE-4-412001: MAC *MAC\_address* moved from *interface\_1* to *interface\_2*

**Explanation** The ACE detects that a host was moved from one module interface to another. In a transparent ACE, mapping between the host (MAC) and the ACE port is maintained in a Layer 2 forwarding table. The table dynamically binds packet source MAC addresses to an ACE port. When movement of a host from one interface to another interface is detected during this binding process, this error message is generated.

**Recommended Action** The host move may be valid or the host move may be an attempt to spoof host MACs on other interfaces. You can take one of these actions:

- If it is a genuine host move, no action is required.
- If it is a MAC spoof attempt, you can either locate vulnerable hosts on your network and remove them or configure static MAC entries. Configuring static MAC entries will not allow MAC address and port binding to change.

## 415004

**Error Message** %ACE-5-415004:HTTP - matched *mime\_type* in policy-map *policy\_map\_name*, content-type verification failed from *source\_address* to *dest\_address/port\_num*  
Connection *connection\_ID*

**Explanation** The **match content-type-verification** command is configured and a MIME type in the content-type HTTP header field is found in the list of policies of allowed types. However, the expected number in the body of the message is not the correct number to identify a file of that type. This behavior is unusual and could indicate an attempt to smuggle contraband data over the connection.

**Recommended Action** None required.

## 415006

**Error Message** %ACE-5-415006: HTTP - matched *class\_map\_name* in *policy\_map\_name*, URI matched *connection\_action* from *source\_address/port\_num* to *dest\_address/port\_num*  
Connection *connection\_ID*

**Explanation** The URI matches the regular expression that the user configured.

**Recommended Action** None required.

## 415007

**Error Message** %ACE-5-415007: HTTP - matched *class\_map\_name* in policy-map *policy\_map\_name*, Body matched *connection\_action* from *IP\_address/port\_num* to *IP\_address/port\_num*  
Connection *connection\_ID*

**Explanation** The body matches the regular expression that the user configured.

**Recommended Action** None required.

## 415008

**Error Message** %ACE-5-415008: HTTP - matched *class\_map\_name* in policy-map *policy\_map\_name*, Header matched *connection\_action* from *IP\_address/port\_num* to *IP\_address/port\_num*  
Connection *connection\_ID*

**Explanation** The header matches the regular expression that the user configured.

**Recommended Action** None required.

## 415009

**Error Message** %ACE-5-415009: HTTP - matched *class\_map\_name* in policy-map *policy\_map\_name*, method matched - *connection\_action* from *IP\_address/port\_num* to *IP\_address/port\_num* Connection *connection\_ID*

**Explanation** The request method matches the regular expression that the user configured.

**Recommended Action** None required.

## 415010

**Error Message** %ACE-5-415010: HTTP - matched *class\_map\_name* in policy-map *policy\_map\_name*, transfer encoding matched *connection\_action* from *IP\_address/port\_num* to *IP\_address/port\_num* Connection *connection\_ID*

**Explanation** The transfer or content encoding matches the regular expression that the user configured.

**Recommended Action** None required.

## 415011

**Error Message** %ACE-5-415011: HTTP - policy-map *policy\_map\_name*:Protocol violation *connection\_action* from *IP\_address/port\_num* to *IP\_address/port\_num* Connection *connection\_ID*

**Explanation** The HTTP parser cannot detect a valid HTTP message in the first few bytes of an HTTP message. A user may be running a protocol over the port for HTTP transactions. This action violates the user-configured policy.

**Recommended Action** None required.

## 415021

**Error Message** %ACE-5-415021: HTTP - matched *class\_map\_name* in policy-map *policy\_map\_name*, URI length range matched *connection\_action* from *source\_address/port\_num* to *dest\_address/port\_num* Connection *connection\_ID*

**Explanation** The URI length is within the range that the user configured.

**Recommended Action** None required.

## 415022

**Error Message** %ACE-5-415022: HTTP - matched *class\_map\_name* in *policy\_map\_name*, Header length range matched *connection\_action* from *source\_address/port\_num* to *dest\_address/port\_num* Connection *connection\_ID*

**Explanation** The header length is within the range that the user configured.

**Recommended Action** None required.

## 415023

**Error Message** %ACE-5-415023: HTTP - matched *class\_map\_name* in *policy-map policy\_map\_name*, body length range matched *connection\_action* from *source\_interface:source\_address/port\_num* to *dest\_interface:dest\_address/port\_num* Connection *connection\_ID*

**Explanation** The body length is within the range that the user configured.

**Recommended Action** None required.

## 415024

**Error Message** %ACE-5-415024:HTTP - matched *class\_map\_name* in *policy-map policy\_map\_name*, Header content type matched *connection\_action* from *IP\_address/port\_num* to *IP\_address/port\_num* Connection *connection\_ID*

**Explanation** The header content type matches the regular expression that the user configured.

**Recommended Action** None required.

## 415025

**Error Message** %ACE-5-415025: HTTP *policy\_map\_name* - Tunnel detected - *connection\_action* from *IP\_address/port\_num* to *IP\_address/port\_num* connection *connection\_ID*

**Explanation** A tunneling protocol is detected in the HTTP content. A user may be running a tunneling protocol using HTTP as the transport. This action violates the user-configured policy.

**Recommended Action** None required.

## 415026

**Error Message** %ACE-5-415026: HTTP *policy\_map\_name*: Instant Messenger detected *connection\_action* from *IP\_address/port\_num* to *IP\_address/port\_num* connection *connection\_ID*

**Explanation** An instant messenger protocol is detected in the HTTP content. A user may be running an instant messenger protocol using HTTP as the transport. This action violates the user-configured policy.

**Explanation** None required.

## 415027

**Error Message** %ACE-5-415027: HTTP *policy\_map\_name*: Peer-to-Peer detected *connection\_action* from *IP\_address/port\_num* to *IP\_address/port\_num* connection *connection\_ID*

**Explanation** A peer-to-peer protocol is detected in the HTTP content. A user may be running a peer-to-peer protocol using HTTP as the transport. This action violates the user-configured policy.

**Recommended Action** None required.

## 440002

**Error Message** %ACE-3-440002: Addition failed for *variable 1*

**Explanation** An error occurred for the SNMP Shadow Table Addition. SNMP Get/Get-Next requests may fail on the table name specified by *variable 1*.

**Recommended Action** Check the memory-related information in the system. Enter the **show processes cpu memory** command and locate the MemAlloc column in the output.

## 440003

**Error Message** %ACE-3-440003: Deletion failed for *variable 2*

**Explanation** An error occurred for the SNMP Shadow Table Deletion. Deletion failure may result in a memory leak or wrong or non-existent values being returned for subsequent Get/Get-Next requests on the table name specified by *variable 2*.

**Recommended Action** Check the Memory related information in the system. Execute the **show processes cpu memory** command and locate the MemAlloc column in the output.

## 441001

**Error Message** %ACE-5-441001: Serverfarm *name* failed over to backup. Number of failovers = *count1*, number of times back in service = *count2*

**Explanation** A serverfarm failover event has occurred. The *name* variable is the name of the serverfarm. The *count1* variable is the number of times that the primary serverfarm failed over to the backup serverfarm. The *count2* variable is the number of times the primary serverfarm returned to service.

**Recommended Action** None required.

## 441002

**Error Message** %ACE-5-441002: Serverfarm *name* is back in service. Number of failovers = *count1*, number of times back in service = *count2*

**Explanation** A serverfarm in service event has occurred. The *name* variable is the name of the serverfarm. The *count1* variable is the number of times that the primary serverfarm failed over to the backup serverfarm. The *count2* variable is the number of times the primary serverfarm returned to service.

**Recommended Action** None required.

## 442001

**Error Message** %ACE-4-442001: Health probe *probe name* detected *real\_server\_name* (interface *interface\_name*) in serverfarm *sfarm\_name* changed state to UP

**Explanation** The state of a real server changed from down to up in the specified server farm.

**Recommended Action** None required.

## 442002

**Error Message** %ACE-4-442002: Health probe *probe name* detected *real\_server\_name* (interface *interface\_name*) in serverfarm *sfarm\_name* changed state to DOWN

**Explanation** The state of a real server changed from up to down in the specified server farm.

**Recommended Action** None required.

## 442003

**Error Message** %ACE-4-442003: Real Server *real\_server\_name* in serverfarm *sfarm\_name* changed state to *new state*

**Explanation** This message reports a real server state change.

The *new state* variable can be one of the following:

- outOfService since max connection reached
- outOfService since retcode threshold reached
- outOfService in normal scenarios

**Recommended Action** None required.

## 442004

**Error Message** %ACE-4-442004: Health probe *probe name* detected *real\_server\_name* (interface *interface\_name*) changed state to UP

**Explanation** The state of a real server changed from down to up.

**Recommended Action** None required.

## 442005

**Error Message** %ACE-4-442005: Health probe *probe name* detected *real\_server\_name* (interface *interface\_name*) changed state to DOWN

**Explanation** The state of a real server changed from up to down.

**Recommended Action** None required.

## 442006

**Error Message** %ACE-4-442006: Real Server *Real Server name* changed state to inService/outOfService

**Explanation** Whenever a real server is manually placed in service or taken out of service, this syslog is generated. Also, this syslog is generated if there is an indication from the data plane about the state change of the real server.

**Recommended Action** No action is required. This syslog is for informational purposes only.

## 443001

**Error Message** %ACE-2-443001: System experienced fatal failure. *Char*, reloading system

**Explanation** If the ACE encounters a fatal error and reloads, it displays the module or service name and reboots. The *Char* variable can be one of the following:

- tar system call failed
- Sysmgr core not present
- Service name:Sysmgr(1234) has terminated on receiving signal 11

**Recommended Action** Check the core file. The **show version** command output displays the reason for the failure in the last boot reason field.

## 444001

**Error Message** %ACE-2-444001: License checkout failure for feature *feature\_name* *reason*

**Explanation** A license checkout error has occurred for a specified feature due to the reported reason.

**Recommended Action** Contact Cisco TAC.

## 444002

**Error Message** %ACE-5-444002: Installed license file *license\_file\_name*

**Explanation** The license installation completed for the specified license filename.

**Recommended Action** Use the **show license usage** command to verify that this license installed.

## 444003

**Error Message** %ACE-5-444003: Uninstalled license file *license\_file\_name*

**Explanation** The license uninstall completed for the specified license filename.

**Recommended Action** Use the **show license usage** command to verify that the license uninstalled.

## 444004

**Error Message** %ACE-2-444004: Evaluation license expired for feature *feature\_name*

**Explanation** The license for the specified feature has exceeded the evaluation time period. All the licensed feature specific configurations are removed.

**Recommended Action** Install a new license for this feature to use it.

## 444005

**Error Message** %ACE-4-444005: Evaluation license for feature *feature\_name* will expire in *num\_days* days *num\_hours* hours

**Explanation** The specified license will exceed its evaluation time period after specified duration as designated in the days and hours remaining. All the licensed feature specific configurations will be removed after the license expires.

**Recommended Action** Install new license to continue to use the feature without any interruption.

## 444006

**Error Message** %ACE-1-444006: License manager exiting: *reason*

**Explanation** The license manager exits due to the reported reason.

**Recommended Action** Contact Cisco TAC.

## 444007

**Error Message** %ACE-4-444007: Installed *feature\_name* license on Revision 6 or older hardware, will not take effect until next reboot.

**Explanation** The installed 16G throughput license on Revision 6 or older hardware does not take effect until the next ACE reboot.

**Recommended Action** Reboot the ACE after saving the current running configuration.

## Messages 504001 to 504002

This section contains messages from 504001 to 504002.

### 504001

**Error Message** %ACE-5-504001: Security context *context-name* was added to the system

**Explanation** A security context was successfully added to the system.

**Recommended Action** None required.

### 504002

**Error Message** %ACE-5-504002: Security context *context-name* was successfully removed from the system

**Explanation** A security context was successfully removed from the system.

**Recommended Action** None required.

## Messages 607001 to 615004

This section contains messages from 607001 to 615004.

### 607001

**Error Message** %ACE-6-6-7001: Pre-allocate SIP media secondary channel for *source\_interface:source\_address/source\_port* to *destination\_interface:destination\_address/destination\_port* from *message\_id* message

**Explanation** This message is generated when a connection is preallocated to allow media streams negotiated on a Session Initiation Protocol (SIP) session.

**Recommended Action** None required.

## 607003

**Error Message** %ACE-6-6-7003: SIP Classification: *Action\_type* and log SIP *message\_id* from *source\_interface:source\_address/source\_port* to *destination\_interface:destination\_address/destination\_port*

**Explanation** This message is generated when the ACE permits or drops a SIP packet or resets the SIP control connection (if it is over TCP), and a log action is configured.

**Recommended Action** None required.

## 608001

**Error Message** %ACE-6-608001: Pre-allocate Skinny connection\_type secondary channel for *source\_interface:source\_address/source\_port* to *destination\_interface:destination\_address/destination\_port* from *message\_id* message

**Explanation** This message is generated when a connection is preallocated to allow media streams negotiated on a Skinny Client Control Protocol (SCCP) session.

**Recommended Action** None required.

## 608002

**Error Message** %ACE-4-608002: Dropping Skinny message for *source\_interface:source\_address/source\_port* to *destination\_interface:destination\_address/destination\_port*, SCCPPrefix length *prefix\_length* too small

**Explanation** This message appears when using SCCP inspection on SCCP traffic. It is displayed if a SCCP message is too small to carry the SCCP payload.

**Recommended Action** None required.

## 608003

**Error Message** %ACE-4-608003: Dropping Skinny message for *source\_interface:source\_address/source\_port* to *destination\_interface:destination\_address/destination\_port*, SCCPPrefix length *prefix\_length* too large

**Explanation** This message appears when using SCCP inspection on SCCP traffic. It is displayed if a SCCP message is larger than the maximum configured size.

**Recommended Action** None required.

## 608004

**Error Message** %ACE-4-608004: Dropping Skinny message for *source\_interface:source\_address/source\_port* to *destination\_interface:destination\_address/destination\_port*, message id *message\_id* not allowed

**Explanation** This message is generated when using inspection on SCCP traffic. It is displayed if a Skinny command is denied by the SCCP inspection policy.

**Recommended Action** None required.

## 608005

**Error Message** %ACE-4-608005: Dropping Skinny message for *source\_interface:source\_address/source\_port* to *destination\_interface:destination\_address/destination\_port*, message id *message\_id* registration not complete

**Explanation** This message is generated when using inspection on SCCP traffic. It is displayed if a Skinny command that is not allowed before registration is seen before the IP phone has successfully registered with the Cisco Call Manager (CCM).

**Recommended Action** None required.

## 615003

**Error Message** %ACE-6-615003: VLAN *VLAN-number* not available for configuring an interface

**Explanation** The specified VLAN number is no longer assigned to the ACE. If an interface is configured with that VLAN number on the module, it will be kept in a shutdown state. If an interface is already configured with that VLAN and is up, it will change the state to shutdown.

**Recommended Action** If the VLAN specified in the log message is not required for the ACE, delete all interfaces that use this VLAN from the module configuration.

## 615004

**Error Message** %ACE-6-615004: VLAN *VLAN-number* available for configuring an interface

**Explanation** The specified VLAN number is now assigned to the ACE. The module can use that VLAN to configure an interface and receive traffic on it.

**Recommended Action** To use the new VLAN, configure interfaces on the ACE using the new VLAN.

# Messages 727001 to 750002

This section contains messages from 727001 to 750002.

## 727001

**Error Message** %ACE-1-727001: HA: Peer IP address is not reachable. Error: *error str*.

**Explanation** An active or standby device cannot reach its redundant peer. This message is displayed on both devices and causes a switchover on the standby device. After the switchover occurs, both devices are no longer redundant. The *error str* value can be one of the following:

- Heartbeat stopped. Ping on alternate interface failed.
- Heartbeat stopped. No alternate interface configured.

**Recommended Action** Verify connectivity between the peers. If a peer device is physically up but connectivity is the problem, you may end up with two active devices. If connectivity is lost due to the peer going down, reboot the peer to restore redundancy between the two devices.

## 727002

**Error Message** %ACE-1-727002: HA: FT interface *interface name* to reach peer IP address is down. Error: *error str*

**Explanation** A peer device is not reachable on an FT interface. In this situation the standby device does not switchover to active, which prevents two actives in the network. The *error str* value can be one of the following:

- Heartbeats stopped. Peer is reachable via alternate interface.
- Heartbeats are up but cannot use the Telnet connection to the peer device.

**Recommended Action** Verify connectivity between the two devices over the FT interface. Ping or use Telnet to the peer IP address to confirm connectivity.

## 727003

**Error Message** %ACE-1-727003: HA: Mismatch in context names detected for FT group *FTgroupID*. Cannot be redundant.

**Explanation** Redundancy is enabled for a particular context, but both devices are unable to become active or standby because of a mismatch in context names.

**Recommended Action** Check the FT group configuration on both devices. Make sure that both devices are associated with the same context.

## 727004

**Error Message** %ACE-1-727004: HA: Two actives have been detected for FT group *FTgroupID*.

**Explanation** Both devices were detected to be active for the same FT group. At this point, one of the two devices automatically relinquishes control and switches over to standby.

**Recommended Action** None required.

## 727005

**Error Message** %ACE-1-727005: HA: Config replication failed for context *ctx name*.  
Error : *error str*

**Explanation** A configuration could not be synchronized to the peer device due to the error condition returned by the *error str* value. The *error str* value can be one of the following:

- Error on Standby device when applying Configuration file replicated from Active.
- Failed to transfer Configuration file to standby. TFTP Failed.
- Failed to generate Running Configuration for peer device. “show running peer” failed.
- Failed to convert Configuration to peer version. Flip of peer addresses failed.
- Failed to retrieve Context Information.
- Failed to rollback Running Configuration on Standby device.
- Failed to sync Running Configuration to Standby device.
- Failed to sync Startup Configuration to Standby device.
- Failed to send MTS message to peer to communicate config status.

**Recommended Action** Check the running and startup configurations on both devices. To recover, disable configuration synchronization, and then manually apply the configuration on each device.

## 727006

**Error Message** %ACE-1-727006: HA: Peer is incompatible due to *error str*. Cannot be Redundant.

**Explanation** A peer device failed to become compatible. This can be a result of Software Relationship Graph (SRG) version inconsistency or a mismatch in licenses between the devices. The error string indicates the reason for the failure.

The *error str* value can be one of the following:

- License Compatibility Mismatch.
- SRG Compatibility Mismatch.

**Recommended Action** Verify version and license compatibility on both the devices.

## 727007

**Error Message** %ACE-1-727007: HA: Module Initialization failure - Error *Error str*.

**Explanation** An initialization error occurred for one of the redundant modules. The *Error str* variable indicates the reason for the failure.

The *Error str* variable can be one of the following:

- MTS Init Failure
- TNRPC Failure
- Select Call Failure
- Timer Creation Failure

**Recommended Action** Contact Cisco TAC.

## 727008

**Error Message** %ACE-1-727008: HA: Failed to send heartbeats to peer. Internal error: *Error str*

**Explanation** The device is unable to send heartbeats to its peer due to an internal error. The error string indicates the reason for the failure.

The *Error str* variable can be one of the following:

- Failed to setup UDP Connection to Peer for Heartbeats.
- Failed to create Encap for Peer.
- Failed to communicate to IXP.

**Recommended Action** Contact Cisco TAC.

## 727009

**Error Message** %ACE-1-727009: HA: Communication failure for Peer *Peer id* Event: *error str*

**Explanation** The device is unable to establish a TCP connection to the peer. The *error str* variable is “Failed to establish TCP connection to Peer device.”

**Recommended Action** Contact Cisco TAC.

## 727010

**Error Message** %ACE-2-727010: HA: Data replication failed for context *ctx name*. Error code *error str*

**Explanation** Data replication fails and data could not be successfully synchronized to the peer device. The next periodic synchronization will correct the failure and update the lost records. The *error str* variable indicates the reason for the failure.

The *error str* variable can be one of the following:

- Failed to bulk sync Connection Records.
- Failed to bulk sync Load Balancer Records.

**Recommended Action** None required.

## 727011

**Error Message** %ACE-2-727011: HA: Configuration replication for context *ctx name* will not happen. Error: *Error str*

**Explanation** The configuration synchronization does not occur for a context. The error string indicates the reason for the failure.

The *Error str* value can be one of the following:

- Failed to open Startup Configuration File. It does not exist.
- HA election timed out.
- Configuration sync to peer not initiated because Peer doesn't exist.
- HA has not been configured for context.

**Recommended Action** None required.

## 727012

**Error Message** %ACE-2-727012: HA: FT Group *group ID* changed state to *NewState*. Reason: *reason str*.

**Explanation** This message displays the state transitions made by an HA state (redundancy) device for a context.

[Table 2-2](#) lists the values for the *NewState* variable.

**Table 2-2** *NewState Values and Descriptions*

<b>NewState Value</b>	<b>Description</b>
FSM_FT_STATE_INIT	The initial state. Visible only when the configuration for the FT group exists but it is not in service.
FSM_FT_STATE_ELECT	After you enter the <b>inservice</b> command when you are configuring an FT group, the ACE enters the ELECT state. The redundancy state machine negotiates with its peer context in the FT group to determine the redundancy role (active or standby).
FSM_FT_STATE_ACTIVE	The active member of the FT group.
FSM_FT_STATE_STANDBY_COLD	This state can be entered if one of the following actions occur: <ul style="list-style-type: none"> <li>• FT VLAN is down but the peer device is still alive.</li> <li>• Configuration or application state synchronization failure have occurred.</li> </ul>
FSM_FT_STATE_STANDBY_CONFIG	The standby context is waiting to receive configuration information. Upon entering this state, the active context will be notified to send a copy of the running configuration.
FSM_FT_STATE_STANDBY_BULK	The standby context is waiting to receive state information. Upon entering this state, the active context will be notified to send a copy of the current states information for all applications.
FSM_FT_STATE_STANDBY_HOT	The standby context is ready to become active in a failover situation.

Values returned for the *reason str* variable can be one of the following:

- FSM\_FT\_EV\_PEER\_DOWN
- FSM\_FT\_EV\_PEER\_FT\_VLAN\_DOWN
- FSM\_FT\_EV\_PEER\_SOFT\_RESET
- FSM\_FT\_EV\_STATE
- FSM\_FT\_EV\_TIMEOUT
- FSM\_FT\_EV\_CFG\_SYNC\_STATUS
- FSM\_FT\_EV\_BULK\_SYNC\_STATUS
- FSM\_FT\_EV\_COUP
- FSM\_FT\_EV\_RELINQUISH
- FSM\_FT\_EV\_TRACK\_STATUS
- FSM\_FT\_EV\_UPDATE
- FSM\_FT\_EV\_ENABLE\_INSERVICE
- FSM\_FT\_EV\_DISABLE\_INSERVICE
- FSM\_FT\_EV\_SWITCHOVER
- FSM\_FT\_EV\_PEER\_COMPATIBLE
- FSM\_FT\_EV\_MAINT\_MODE\_OFF

- FSM\_FT\_EV\_MAINT\_MODE\_PARTIAL
- FSM\_FT\_EV\_MAINT\_MODE\_FULL

**Recommended Action** None required.

## 727013

**Error Message** %ACE-2-727013: HA: Peer *Peer #* is UP and reachable.

**Explanation** The peer is now reachable. Heartbeats are flowing successfully between the two peers.

**Recommended Action** None required.

## 727014

**Error Message** %ACE-2-727014: HA: Heartbeats from Peer *Peer id* have become unidirectional.

**Explanation** Redundancy heartbeats from a peer have become unidirectional. That is, the peer cannot receive (only send) heartbeats. This problem occurs if one of the network processors has a problem.

**Recommended Action** Collect network processor drop counters, and then contact Cisco TAC.

## 727015

**Error Message** %ACE-2-727015: HA: Detected mismatch in heartbeat interval from Peer *peer id*. Modified interval to *interval*.

**Explanation** The redundancy heartbeat received from one peer differs from the value of the second peer. This condition can occur when you choose to dynamically change the heartbeat interval. The modified heartbeat interval that is displayed shows the adjusted interval. This value is the greater of the two values.

**Recommended Action** None required.

## 727016

**Error Message** %ACE-2-727016: HA: Replication for context *ctx name* has started. Status - *status*.

The replication is being carried out to a peer. The *status* variable indicates the synchronization status.

Values for the *status* variable can be one of the following:

- Running Configuration sync has started to peer.

- Startup Configuration sync has started to peer.
- Startup Configuration sync has completed to peer.
- Running Configuration sync has completed to peer.
- Data Replication has completed to peer.
- Startup configuration has been applied successfully for context.

**Recommended Action** None required.

## 727017

**Error Message** %ACE-2-727017: HA: FT Track *track type track name* is UP.

**Explanation** The FT track is up.

The *track type* variable can be one of the following:

- Interface
- HSRP
- Host

**Recommended Action** None required.

## 727018

**Error Message** %ACE-2-727018: HA: FT Track *track type track name* is DOWN.

**Explanation** The FT track is down.

The *track type* variable can be one of the following:

- Interface
- HSRP
- Host

**Recommended Action** None required.

## 727019

**Error Message** %ACE-5-727019: HA: Started alternate ping to IP address *ip addr*

**Explanation** ICMP pings have started on the alternate interface to check the health of the peer. This process starts when heartbeats from the peer are no longer received. The standby device issues an alternate ping to the peer to determine whether the peer is still alive. If it is alive, it does not switchover, which prevents two active states on the network.

**Recommended Action** None required.

## 727020

**Error Message** %ACE-5-727020: HA: Stopped alternate ping to IP address *ip addr*.

**Explanation** ICMP pings have stopped on the alternate interface. This occurs when heartbeats from the peer are received and the peer is up and reachable.

**Recommended Action** None required.

## 727021

**Error Message** %ACE-5-727021: HA: Peer is compatible.

**Explanation** The two devices are in a compatible state and can be configured for redundancy.

**Recommended Action** None required.

## 727022

**Error Message** %ACE-5-727022: HA: Started sending heartbeats to peer *Peer id* interval *value* and count *cnt*

**Explanation** The redundancy connections to the peer have been successfully established and heartbeats have been started to the peer with the configured interval and count.

The interval variable specifies interval in milliseconds. The count variable specifies the number of missed heartbeat intervals before the peer is declared down.

**Recommended Action** None required.

## 727023

**Error Message** %ACE-5-727023: HA: Stopped sending heartbeats to peer *Peer id*.

**Explanation** Redundancy heartbeats to the peer have been stopped. This can occur if you unconfigure redundancy or make changes to basic connection parameters such as the peer IP address.

**Recommended Action** None required.

## 728001

**Error Message** %ACE-1-728001: Initialization failure (general) type *variable1*

**Explanation** Initialization of the ACE load-balancing process is aborted due to a failure of a general nature (for example, lack of memory, failure to spawn threads, failure to establish a communication channel, and so on).

*variable1* specifies the exact failure location in the codebase.

**Recommended Action** Document the syslog message, and then reboot the ACE (see the *Cisco Application Control Engine Module Administration Guide* for details). Contact Cisco TAC with the documented message text.

## 728002

**Error Message** %ACE-1-728002: Initialization failure (sticky) type *variable1*

**Explanation** Initialization of the ACE load-balancing process is aborted because of a failure in the sticky subsystem (for example, memory alignment failure, failure to spawn threads, failure to establish communication channel).

*variable1* specifies the exact failure location in the codebase.

**Recommended Action** Document the syslog message, and then reboot the ACE (see the *Cisco Application Control Engine Module Administration Guide* for details). Contact Cisco TAC with the documented message text.

## 728003

**Error Message** %ACE-1-728003: Initialization failure (sticky hash) *variable1* entries, *variable2* min, *variable3* max type *variable4*

**Explanation** Initialization of the ACE load-balancing process is aborted because of a failure when allocating entries for the sticky database (for example, the database is not allocated).

The variables displayed in this message represent the following:

- *variable1*—Specifies the requested number of sticky entries.
- *variable2*—Specifies the minimum number of sticky entries required for successful operation of the hash algorithm.
- *variable3*—Specifies the maximum number of entries that can be allocated.
- *variable4*—Specifies the exact failure location in the codebase.

**Recommended Action** Document the syslog message, and then reboot the ACE (see the *Cisco Application Control Engine Module Administration Guide* for details). Contact Cisco TAC with the documented message text.

## 728004

**Error Message** %ACE-5-728004: Internal communications notice (general) type *variable1*

**Explanation** The ACE load-balancing process detects a spurious or unintelligible internal message that cannot be dispatched. Under high load, message loss may occur.

*variable1* specifies the exact failure location in the codebase.

**Recommended Action** If this message occurs frequently, or in conjunction with problems in load balancing under normal system load, contact Cisco TAC.

## 728005

**Error Message** %ACE-3-728005: Failed to transmit *variable1* decision for connection from client *variable2* type *variable3*

**Explanation** A load-balancing decision was lost internally. No server connection can be initiated, and the identified client connection is reset. At this point, the client can attempt reconnection.

*variable1* specifies the connection type. Possible values are as follows:

- destination (determined by load balancer)
- drop (connection discarded)
- forwarded (not load balanced)

*variable2* specifies the address of client from whom the connection originated.

*variable3* specifies the unique identifier for the line of code where the error was logged.

**Recommended Action** If this message occurs frequently, document the syslog message, and then contact Cisco TAC.

## 728006

**Error Message** %ACE-5-728006: Internal communications error (messaging) msg subType *variable1* -- type *variable2*

During load balancing, the ACE received an internal message that cannot be identified. This message is discarded without processing.

The variables displayed in this message represent the following:

- *variable1*—Specifies the message type (decimal) that could not be processed.
- *variable2*—Specifies the unique identifier for the line of code where the error was logged.

**Recommended Action** If this message occurs frequently, document the syslog message, and then contact Cisco TAC.

## 728007

**Error Message** %ACE-3-728007: Internal configuration communications error (sticky) type *variable1*

**Explanation** During load balancing, the ACE received a configuration request for sticky database resources that cannot be honored. The resources may exceed the permitted amounts or the resources cannot be located.

*variable1* specifies the unique identifier for the line of code where the error was logged.

**Recommended Action** Verify that the requested resources are available within the chosen context. If the requested resources are available and are allowed by the configuration, an internal error exists. Contact Cisco TAC.

## 728008

**Error Message** %ACE-3-728008: Internal communications error (sticky) /source processor *variable1* destination processor *variable2* -- type *variable3*

**Explanation** During load balancing, the ACE detected an error in communication between the two network processors. As a result, sticky load balancing may not occur for some client connections.

The variables displayed in this message represent the following:

- *variable1*—Specifies the received decimal identifier of source processor.
- *variable2*—Specifies the received decimal identifier of destination processor.
- *variable3*—Specifies the unique identifier for the line of code where the error was logged.

**Recommended Action** Contact Cisco TAC.

## 728009

**Error Message** %ACE-3-728009: Context ID *variable1* requested *variable2* of *variable3* sticky entries. No action taken. -- type *variable4*

**Explanation** This message is reported from the Admin context. A configuration request from the context identified by *variable1* cannot be responded to because it exceeds the permitted resources for the sticky entries.

The variables displayed in this message represent the following:

- *variable1*—Specifies the context requesting the sticky entry action.
- *variable2*—Specifies the requested action.
- *variable3*—Specifies the number of sticky entries requested.
- *variable4*—Specifies the unique identifier for the line of code where the error was logged.

**Recommended Action** Contact Cisco TAC.

## 728011

**Error Message** %ACE-4-728011: Context ID *variable1* being *variable2* should not have *variable3* associated sticky groups -- type *variable4*

**Explanation** This message is reported from the Admin context and appears when adding or removing a context that has associated sticky groups. When this condition exists and the error message is logged, the addition or removal of the context still occurs.

- *variable1*—specifies the context identifier to be added or removed.
- *variable2*—specifies the requested action. Possible values are added or removed.
- *variable3*—specifies the number of associated sticky groups detected.
- *variable4*—specifies the unique identifier for the line of code where the error was logged.

**Recommended Action** Before adding or removing a context, make sure there are no sticky groups associated with that context.

## 728012

**Error Message** %ACE-5-728012: Context ID *variable1* failed to receive return data -- type *variable2*

**Explanation** Data collected in response to a **show** command at the CLI was not successfully returned from the network processor to the CLI.

The variables displayed in this message represent the following:

- *variable1*—Specifies the context identifier for the context that made the request.
- *variable2*—Specifies the unique identifier for the line of code where the error was logged.

**Recommended Action** Reenter the **show** command. If the problem persists, contact Cisco TAC.

## 728013

**Error Message** %ACE-4-728013: A cache alignment error *variable1* was detected during initialization -- type *variable2*

**Explanation** A cache alignment error was detected during the load-balancing initialization. This may impact performance, but load balancing will still be correctly performed.

The variables displayed in this message represent the following:

- *variable1* specifies the cache alignment return code.
- *variable2* specifies the unique identifier for the line of code where the error was logged.

**Recommended Action** If you see this error message frequently, contact Cisco TAC.

## 728014

**Error Message** %ACE-3-728014: Internal cross-processor communications error (sticky) type *variable1*

**Explanation** During load-balancing, the ACE could not parse a message from the second network processor on the ACE. This can result in the loss of sticky information between the two processors, resulting in a sticky server-connection loss for some clients.

*variable1* specifies the unique identifier for the line of code where the error was logged.

**Recommended Action** Contact Cisco TAC.

## 728015

**Error Message** %ACE-3-728015: Internal channel communications error (sticky) type *variable1*

**Explanation** During load-balancing operations, the ACE was unable to open or use an internal communications channel to process a load-balancing configuration or a display directive. The specific directive on which the failure occurred is not be completed (although it may be retried).

*variable1* specifies the unique identifier for the line of code where the error was logged.

**Recommended Action** Contact Cisco TAC.

## 728016

**Error Message** %ACE-4-728016: HA data receive failure (type *variable1*)

**Explanation** This message is logged when a redundancy message received from the redundant peer cannot be understood and is subsequently discarded.

*variable1* specifies the unique identifier for the line of code where the error was logged.

**Recommended Action** Use the **show ft stats group\_id** command to display load-balancing statistics for the FT group:

- If the type variable returned a value of 90 (decimal), then monitor the “Number of Sticky Entries Dropped” value. Contact Cisco TAC if the values continue to increase over time.
- If the type variable returned a value of 99 (decimal), then monitor the “Number of Receive Failures” value. Contact Cisco TAC if the values continue to increase over time.

## 728017

**Error Message** %ACE-3-728017: Internal communications error (ha) -- type *variable1*

**Explanation** This message is reported from the current context. An attempt to send a redundancy message to the redundant peer was unsuccessful because the message could not be sent.

*variable1* specifies the unique identifier for the line of code where the error was logged.

**Recommended Action** Use the **show ft stats group\_id** command to display load-balancing statistics for the FT group. Monitor the “Number of Send Failures” value. Contact Cisco TAC if the problem persists.

## 728018

**Error Message** %ACE-5-728018: Proxy connection *variable1* rebalanced to server *variable2*

**Explanation** The ACE has determined that the server side of a connection should be rebalanced to another server. This is an informational message issued in the context in which the rebalance occurs.

The variables displayed in this message represent the following:

- *variable1* specifies the identifier of the proxy connection.
- *variable2* specifies the index of the realServer to which the connection was rebalanced.

**Recommended Action** None required.

## 728019

**Error Message** %ACE-4-728019: Sticky resources were not *variable1* for this context -- type *variable2*

**Explanation** A sticky request (lookup, configure, or delete a sticky entry) was not honored because the sticky group could not locate any configured sticky entries. This is not the result of exceeding the configuration limits, but indicates an unexpected sticky group lookup result.

*variable1* specifies the requested sticky action. Possible values are as follows:

- detected
- inserted
- removed

*variable2* specifies the unique identifier for the line of code where the error was logged.

**Recommended Action** Contact Cisco TAC.

## 728020

**Error Message** %ACE-6-728020: LB is configured to consume *variable1* bytes of memory.

**Explanation** The message indicates the amount of physical memory that is mapped by the ACE during load-balancing initialization and indicates that the mapping was successful.

*variable1* specifies the bytes of mapped physical memory.

**Recommended Action** None required.

## 728021

**Error Message** %ACE-6-728021: Found inconsistent sticky entry. Terminating *variable1*.

**Explanation** Various commands processed by the ACE during load balancing require searching the sticky database to find all relevant sticky entries. An unexpected finding of no further sticky entries generates this message. This message is useful in troubleshooting sticky issues. The indicated action is terminated, but further requests of the same type (or of other types) are completed.

*variable1* specifies the terminated action. Possible values are as follows:

- show screen (user request)
- resetting timestamps (aging sticky entries)
- HA share (updating database with entries learned via HA)

**Recommended Action** None required.

## 728022

**Error Message** %ACE-6-728022: Invalid hash table index (*variable1*) used for *variable2*

**Explanation** The specified action was aborted because of an invalid hash index.

*variable1* specifies the value of the invalid hash table index.

*variable2* specifies the index table use. Possible values are as follows:

- LookupRealServerId
- InsertNewEntry

**Recommended Action** None required.

## 728023

**Error Message** %ACE-6-728023: *variable1 variable2* sticky entries from ContextId *variable3*.

**Explanation** Sticky entries have been added or removed from a context as a result of a resource limit change.

*variable1* specifies the action. Possible values are as follows:

- Added
- Removed

*variable2* specifies the number of sticky entries moved.

*variable3* specifies the context ID from which the entries were added or removed.

**Recommended Action** None required.

## 728024

**Error Message** %ACE-4-728024: Received an unknown *variable1* type message (*variable2*) for Sticky from remote IXP *variable3*!

**Explanation** A request or reply from the second network processor indicates an unknown operation type. The request or reply is not responded to and is discarded. This message is useful when troubleshooting sticky database synchronization problems with the network processors.

*variable1* specifies the message class. Possible values are as follows:

- request
- reply

*variable2* specifies the numerical value of the operation type that could not be identified.

*variable3* specifies the identifier of the IXP (network processor) that sent the message.

**Recommended Action** No action required.

## 728025

**Error Message** %ACE-6-728025: Dropped *variable1* '*variable2*' messages (*variable3* total) from IXP *variable4* to IXP *variable5*!

**Explanation** Sticky messages between network processors (sticky insert, sticky lookup, or sticky connection close) were lost. This information may be useful when troubleshooting problems with sticky functionality.

*variable1* specifies the number of lost messages.

*variable2* specifies the message type. Possible values are as follows:

- request
- response

*variable3* specifies the total number of messages discarded (includes both lost messages and messages which were discarded because they could not be sent).

*variable4* specifies the source network processor identifier.

*variable5* specifies the destination network processor identifier.

**Recommended Action** None required.

## 728026

**Error Message** %ACE-6-728026: Attempting to use invalid lookup key for *variable1* processing.

**Explanation** The message indicates that a connection close notification was not sent to the remote network processor because of an invalid key. *Variable1* specifies the type of processing (connection close). This information may be useful when troubleshooting problems with sticky functionality.

**Recommended Action** None required.

## 728027

**Error Message** %ACE-3-728027: Received unhandled message of type *variable1* from CP SrcSAP *variable2*.

**Explanation** An unrecognized message was received from the control processor (CP) during load-balancing operations. The message is discarded. This message is useful when troubleshooting commands or configuration directives from the control processor that are ignored by the ACE.

The variables displayed in this message represent the following:

- *variable1*—Specifies the raw (decimal) unrecognized message type that is received.
- *variable2*—Specifies the (decimal) source SAP on the CP from which this message was sent.

**Recommended Action** No action required.

## 728028

**Error Message** %ACE-5-728028: Sticky mapping failed: *variable1* *variable2*

**Explanation** Information received from an redundant peer cannot be mapped locally. The associated sticky entry information is discarded.

*variable1* specifies the reason for the mapping failure. Possible values are as follows:

- Invalid sticky group id
- Invalid real server id
- Sticky group not active

*variable2* specifies the (decimal) identifier of the invalid entity. If the entry is an “invalid real server id,” the value of the real server ID is displayed. Otherwise, the invalid or inactive sticky group ID is displayed.

**Recommended Action** Use the **show ft stats group\_id** command to display load-balancing statistics for the FT group. Monitor the “Number of Sticky Entries Dropped” value. Contact Cisco TAC if the values continue to increase over time.

## 728029

**Error Message** %ACE-6-728029: HA state for FtGroup *variable1* changed from *variable2* to *variable3* State *variable4*.

**Explanation** This message tracks state changes received from the redundant peer. Events that are not relevant to load balancing are ignored. This message is useful when tracking redundancy state changes to troubleshoot redundant peer synchronization problems.

*variable1* specifies the (decimal) fault tolerant group ID.

*variable2* and *variable3* specify the previous and current state change event. Possible values are as follows:

- Active
- StartCfgSync
- StartBulkSync
- StartPeriodicSync
- StopSync
- Stdbycfg
- StdbyBulk
- StdbyHot
- StdbyCold
- BulkSyncDone
- NonRedundant
- None
- "???" (specifies an unidentified event)

*variable4* specifies the state change action. Possible values are as follows:

- handled
- ignored

**Recommended Action** No action required.

## 728030

**Error Message** %ACE-6-728030: Silently discarding HA data: *variable1*

**Explanation** Redundancy data must be discarded during load-balancing operations because the ACE could not process the data. The discarding of the data could affect seamless failover. This message is useful when troubleshooting redundant peer problems

*variable1* specifies the reason for discarding data from the redundant peer. Possible values are as follows:

- Received unknown message type
- Received data packet in wrong HA state

**Recommended Action** No action required.

## 728031

**Error Message** %ACE-3-728031: Memory mapping for debug logging failed.

**Explanation** Memory mapping fails during initialization for debug logging. Load balancing continues, but no debug logging will occur, even if invoked from the command line.

**Recommended Action** Reboot the ACE to reinitialize the debug logging component (see the *Cisco Application Control Engine Module Administration Guide* for details). Rebooting may correct a transient mapping issue. If this error persists, contact Cisco TAC.

## 728032

**Error Message** %ACE-LB\_General-4-728032: Real Server *variable1* in Serverfarm *variable2* has reached configured threshold for HTTP retcode *variable3*

**Explanation** HTTP return codes were configured on a server farm and a specific real server has reached the configured return code threshold.

The variables displayed in this message represent the following:

- *variable1*—Specifies the name of the real server within the server farm.
- *variable2*—Specifies the name of the server farm.
- *variable3*—Specifies the HTTP return code value returned by the server which caused this message to be logged.

**Recommended Action** Review the types of client HTTP requests that cause these server return code responses. Look for return codes that indicate possible problems, for example, missing content or incorrect search paths.

## 729001

**Error Message** %ACE-3-729001: Regular expression config download failed due to out of memory. No regexp rules are currently applied on class-map *map\_name* in service-policy *policy\_name*. Manual roll back to a previous regexp configuration on this service-policy is needed.

**Explanation** The regular expression table compilation process has run out of memory or encountered an error, causing inability to apply new rules to the specified service policy. The regular expression configuration downloaded in hardware for the service policy may not be in a known state due to this failure.

**Recommended Action** Remove some regular expressions or allocate more regular expression resources.

## 729002

**Error Message** %ACE-4-729002: Regex resource usage beyond maximum limit for context *context\_id*. Free up some resources.

**Explanation** This syslog message indicates that regex resources in use for the specified context (*context\_id*) are above the maximum limit allowed by the resource class.

**Recommended Action** Decrease the minimum regex usage in the specified context to below the maximum limit.

## 729003

**Error Message** %ACE-4-729003: Minimum regex resources could not be guaranteed for context *context\_id*.

**Explanation** This syslog message indicates that the requested minimum regex resources could not be guaranteed in the specified context (*context\_id*).

**Recommended Action** Contact the global administrator to request that other context administrators release regex resources.

## 750001

**Error Message** %ACE-4-750001: Sticky resource usage beyond maximum limit for context *ctx id*

**Explanation** The sticky resources in use for the context have exceeded the configured limit for that context.

**Recommended Action** Free up resources in the context to keep them within the configured limit. For details about managing resources, see the *Cisco Application Control Engine Module Virtualization Configuration Guide*.

## 750002

**Error Message** %ACE-4-750002: Minimum sticky resources could not be guaranteed for context *ctx id*

**Explanation** .When configuring a sticky resource limit for a particular context, the ACE was not able to guarantee the resource limit.

**Recommended Action** Free up resources in all other contexts that have exceeded their configured limits. For details about managing resources, see the *Cisco Application Control Engine Module Virtualization Configuration Guide*.





## CHAPTER 3

# Messages Listed by Severity Level

---

This chapter contains the following sections:

- [Alert Messages, Severity Level 1](#)
- [Critical Messages, Severity Level 2](#)
- [Error Messages, Severity Level 3](#)
- [Warning Messages, Severity Level 4](#)
- [Notification Messages, Severity Level 5](#)
- [Informational Messages, Severity Level 6](#)
- [Debugging Messages, Severity Level 7](#)



**Note**

The ACE does not send severity 0, emergency messages to syslog. These are comparable to a UNIX panic message and indicate an unstable system.

---

## Alert Messages, Severity Level 1

The following messages appear at severity level 1, alerts:

- **Error Message** %ACE-1-106021: Deny protocol reverse path check from source\_address to dest\_address on interface interface\_name
- **Error Message** %ACE-1-106028: String Incomplete rule is currently applied on interface interface-name. Manual rollback to a previous access rule configuration on this interface is needed.
- **Error Message** %ACE-1-313006: ICMP Manager Initialization Failed. Reason : Variable1
- **Error Message** %ACE-1-313007: ICMP Manager Memory Problem. Reason: Variable1
- **Error Message** %ACE-1-444006: License manager exiting: reason
- **Error Message** %ACE-1-727001: HA: Peer IP address is not reachable. Error: error str.
- **Error Message** %ACE-1-727002: HA: FT interface interface name to reach peer IP address is down. Error: error str
- **Error Message** %ACE-1-727003: HA: Mismatch in context names detected for FT group FTgroupID. Cannot be redundant.
- **Error Message** %ACE-1-727004: HA: Two actives have been detected for FT group FTgroupID.

- Error Message %ACE-1-727005: HA: Config replication failed for context ctx name. Error : error str
- Error Message %ACE-1-727006: HA: Peer is incompatible due to error str. Cannot be Redundant.
- Error Message %ACE-1-727007: HA: Module Initialization failure - Error Error str.
- Error Message %ACE-1-727008: HA: Failed to send heartbeats to peer. Internal error: Error str
- Error Message %ACE-1-727009: HA: Communication failure for Peer Peer id Event: error str
- Error Message %ACE-1-728001: Initialization failure (general) type variable1
- Error Message %ACE-1-728002: Initialization failure (sticky) type variable1
- Error Message %ACE-1-728003: Initialization failure (sticky hash) variable1 entries, variable2 min, variable3 max type variable4

## Critical Messages, Severity Level 2

The following messages appear at severity level 2, critical:

- Error Message %ACE-2-100001: EOL function chars from library chars exited due to Signal dec
- Error Message %ACE-2-199006 : Orderly reload started at when by whom. Reload reason: reason
- Error Message %ACE-2-212007: SNMPD initialization failed while Variable1
- Error Message %ACE-2-443001: System experienced fatal failure. Char, reloading system
- Error Message %ACE-2-444001: License checkout failure for feature feature\_name reason
- Error Message %ACE-2-444004: Evaluation license expired for feature feature\_name
- Error Message %ACE-2-727010: HA: Data replication failed for context ctx name. Error code error str
- Error Message %ACE-2-727011: HA: Configuration replication for context ctx name will not happen. Error: Error str
- Error Message %ACE-2-727012: HA: FT Group group ID changed state to NewState. Reason: reason str.
- Error Message %ACE-2-727013: HA: Peer Peer # is UP and reachable.
- Error Message %ACE-2-727014: HA: Heartbeats from Peer Peer id have become unidirectional.
- Error Message %ACE-2-727015: HA: Detected mismatch in heartbeat interval from Peer peer id. Modified interval to interval.
- Error Message %ACE-2-727016: HA: Replication for context ctx name has started. Status - status.
- Error Message %ACE-2-727017: HA: FT Track track type track name is UP.
- Error Message %ACE-2-727018: HA: FT Track track type track name is DOWN.

## Error Messages, Severity Level 3

The following messages appear at severity level 3, errors:

- Error Message %ACE-3-211001: Memory allocation Error
- Error Message %ACE-3-212008: Failed while allocating memory in snmpd

- Error Message %ACE-3-251001: Probe configuration error, memory allocation failure.
- Error Message %ACE-3-251003: Could not load script script-name - File not found
- Error Message %ACE-3-251004: Could not load script script-name - memory allocation failure
- Error Message %ACE-3-251006: Health probe failed for server A.B.C.D on port P, internal error: error message
- Error Message %ACE-3-251007: ICMP health probe failed for server A.B.C.D, internal error: error message
- Error Message %ACE-3-251008: Health probe failed for server A.B.C.D on port P, connectivity error: server open timeout (no SYN ACK)
- Error Message %ACE-3-251009: ICMP health probe failed for server A.B.C.D, connectivity error: error message
- Error Message %ACE-3-251010: Health probe failed for server A.B.C.D on port P, error message
- Error Message %ACE-3-251011: ICMP health probe failed for server A.B.C.D, error message.
- Error Message %ACE-3-251012: Could not load script script-name - Error reading script-file
- Error Message %ACE-3-251013: Could not load script script-name - Error getting file size
- Error Message %ACE-3-322001: Deny MAC address MAC\_address, possible spoof attempt on interface interface
- Error Message %ACE-3-322002: ARP inspection check failed for arp {request|response} received from host MAC\_address on interface interface. This host is advertising MAC Address MAC\_address\_1 for IP Address IP\_address, which is {statically|dynamically} bound to MAC Address MAC\_address\_2.
- Error Message %ACE-3-322003: ARP inspection check failed for arp {request|response} received from host MAC\_address on interface interface. This host is advertising MAC Address MAC\_address\_1 for IP Address IP\_address, which is not bound to any MAC Address.
- Error Message %ACE-3-327001: Detected Encap table Full when allocating encap entry for IP interface interface\_name
- Error Message %ACE-3-440002: Addition failed for variable 1
- Error Message %ACE-3-440003: Deletion failed for variable 2
- Error Message %ACE-3-728005: Failed to transmit variable1 decision for connection from client variable2 type variable3
- Error Message %ACE-3-728007: Internal configuration communications error (sticky) type variable 1
- Error Message %ACE-3-728008: Internal communications error (sticky) /source processor variable1 destination processor variable2 -- type variable3
- Error Message %ACE-3-728009: Context ID variable1 requested variable2 of variable3 sticky entries. No action taken. -- type variable4
- Error Message %ACE-3-728014: Internal cross-processor communications error (sticky) type variable 1
- Error Message %ACE-3-728015: Internal channel communications error (sticky) type variable1
- Error Message %ACE-3-728017: Internal communications error (ha) -- type variable1
- Error Message %ACE-3-728027: Received unhandled message of type variable1 from CP SrcSAP variable2.
- Error Message %ACE-3-728031: Memory mapping for debug logging failed.

- Error Message %ACE-3-729001: Regular expression config download failed due to out of memory. No regexp rules are currently applied on class-map map\_name in service-policy policy\_name. Manual roll back to a previous regexp configuration on this service-policy is needed.

## Warning Messages, Severity Level 4

The following messages appear at severity level 4, warning:

- Error Message %ACE-4-106023: Deny protocol number | name src incoming-interface:src-ip dst outgoing-interface:dst-ip by access-group "acl-name" (hash 1, hash 2)
- Error Message %ACE-4-251002: The configured health probe script script-name for server A.B.C.D on port P is empty
- Error Message %ACE-4-251005: Could not unload script script-name
- Error Message %ACE-4-254001: ACL resource usage beyond maximum limit for context context\_id. Free up some resources.
- Error Message %ACE-4-254002: Minimum ACL resources could not be guaranteed for context context\_id.
- Error Message %ACE-4-313004: Denied ICMP type=icmp\_type, from source\_address on interface interface\_name to dest\_address:no matching session
- Error Message %ACE-4-400000: IDS:1000 IP Option Bad Option List from IP\_address to IP\_address on interface interface\_name
- Error Message %ACE-4-405001: Received ARP {request | response} collision from IP\_address/mac\_address on interface interface\_name
- Error Message %ACE-4-405201: ILS ctxid from vlan x:src\_ip/src\_prt to vlan y:dst\_ip/dst\_prt has wrong embedded address embedded\_addr in ILS payload
- Error Message %ACE-4-406001: FTP port command low port: IP\_address/port to IP\_address on interface interface\_name
- Error Message %ACE-4-406002: FTP port command different address: IP\_address(IP\_address) to IP\_address on interface interface\_name
- Error Message %ACE-4-410001: Dropped UDP DNS packet\_type from source\_interface:source\_address/source\_port to dest\_interface:dest\_address/dest\_port; error\_length\_type length length bytes exceeds max\_length\_type limit of maximum\_length bytes.
- Error Message %ACE-4-411001: Line protocol on interface interface\_name changed state to up
- Error Message %ACE-4-411002: Line protocol on interface interface\_name changed state to down
- Error Message %ACE-4-411003: Configuration status on interface interface\_name changed state to up
- Error Message %ACE-4-411004: Configuration status on interface interface\_name changed state to down
- Error Message %ACE-4-412001: MAC MAC\_address moved from interface\_1 to interface\_2
- Error Message %ACE-4-442001: Health probe probe\_name detected real\_server\_name (interface interface\_name) in serverfarm sfarm\_name changed state to UP
- Error Message %ACE-4-442002: Health probe probe\_name detected real\_server\_name (interface interface\_name) in serverfarm sfarm\_name changed state to DOWN

- Error Message %ACE-4-442003: Real Server real\_server\_name in serverfarm sfarm\_name changed state to new state
- Error Message %ACE-4-442004: Health probe probe name detected real\_server\_name (interface interface\_name) changed state to UP
- Error Message %ACE-4-442005: Health probe probe name detected real\_server\_name (interface interface\_name) changed state to DOWN
- Error Message %ACE-4-442006: Real Server Real Server name changed state to inService/outOfService
- Error Message %ACE-4-444005: Evaluation license for feature feature\_name will expire in num\_days days num\_hours hours
- Error Message %ACE-4-444007: Installed feature\_name license on Revision 6 or older hardware, will not take effect until next reboot.
- Error Message %ACE-4-608002: Dropping Skinny message for source\_interface:source\_address/source\_port to destination\_interface:destination\_address/destination\_port, SCCPPrefix length prefix\_length too small
- Error Message %ACE-4-608003: Dropping Skinny message for source\_interface:source\_address/source\_port to destination\_interface:destination\_address/destination\_port, SCCPPrefix length prefix\_length too large
- Error Message %ACE-4-608004: Dropping Skinny message for source\_interface:source\_address/source\_port to destination\_interface:destination\_address/destination\_port, message id message\_id not allowed
- Error Message %ACE-4-608005: Dropping Skinny message for source\_interface:source\_address/source\_port to destination\_interface:destination\_address/destination\_port, message id message\_id registration not complete
- Error Message %ACE-4-728011: Context ID variable1 being variable2 should not have variable3 associated sticky groups -- type variable4
- Error Message %ACE-4-728013: A cache alignment error variable1 was detected during initialization -- type variable2
- Error Message %ACE-4-728016: HA data receive failure (type variable1)
- Error Message %ACE-4-728019: Sticky resources were not variable1 for this context -- type variable2
- Error Message %ACE-4-728024: Received an unknown variable1 type message (variable2) for Sticky from remote IXP variable3!
- Error Message %ACE-LB\_General-4-728032: Real Server variable1 in Serverfarm variable2 has reached configured threshold for HTTP retcode variable3
- Error Message %ACE-4-729002: Regex resource usage beyond maximum limit for context context\_id. Free up some resources.
- Error Message %ACE-4-729003: Minimum regex resources could not be guaranteed for context context\_id.
- Error Message %ACE-4-750001: Sticky resource usage beyond maximum limit for context ctx id
- Error Message %ACE-4-750002: Minimum sticky resources could not be guaranteed for context ctx id

## Notification Messages, Severity Level 5

The following messages appear at severity level 5, notifications:

- Error Message %ACE-5-111008: User user executed the command string
- Error Message %ACE-5-303004: FTP cmd\_string command unsupported - failed strict inspection, terminating connection from source\_interface:source\_address/source\_port to dest\_interface:dest\_address/dest\_interface
- Error Message %ACE-5-304001: user source\_address Accessed {URL} dest\_address: url Connection connection\_ID
- Error Message %ACE-5-415004:HTTP - matched mime\_type in policy-map policy\_map\_name, content-type verification failed from source\_address to dest\_address/port\_num Connection connection\_ID
- Error Message %ACE-5-415006: HTTP - matched class\_map\_name in policy\_map\_name, URI matched connection\_action from source\_address/port\_num to dest\_address/port\_num Connection connection\_ID
- Error Message %ACE-5-415007: HTTP - matched class\_map\_name in policy-map policy\_map\_name, Body matched connection\_action from IP\_address/port\_num to IP\_address/port\_num Connection connection\_ID
- Error Message %ACE-5-415008: HTTP - matched class\_map\_name in policy-map policy\_map\_name, Header matched connection\_action from IP\_address/port\_num to IP\_address/port\_num Connection connection\_ID
- Error Message %ACE-5-415009: HTTP - matched class\_map\_name in policy-map policy\_map\_name, method matched - connection\_action from IP\_address/port\_num to IP\_address/port\_num Connection connection\_ID
- Error Message %ACE-5-415010: HTTP - matched class\_map\_name in policy-map policy\_map\_name, transfer encoding matched connection\_action from IP\_address/port\_num to IP\_address/port\_num Connection connection\_ID
- Error Message %ACE-5-415011: HTTP - policy-map policy\_map\_name:Protocol violation connection\_action from IP\_address/port\_num to IP\_address/port\_num Connection connection\_ID
- Error Message %ACE-5-415021: HTTP - matched class\_map\_name in policy-map policy\_map\_name, URI length range matched connection\_action from source\_address/port\_num to dest\_address/port\_num Connection connection\_ID
- Error Message %ACE-5-415022: HTTP - matched class\_map\_name in policy\_map\_name, Header length range matched connection\_action from source\_address/port\_num to dest\_address/port\_num Connection connection\_ID
- Error Message %ACE-5-415023: HTTP - matched class\_map\_name in policy-map policy\_map\_name, body length range matched connection\_action from source\_interface:source\_address/port\_num to dest\_interface:dest\_address/port\_num Connection connection\_ID
- Error Message %ACE-5-415024:HTTP - matched class\_map\_name in policy-map policy\_map\_name, Header content type matched connection\_action from IP\_address/port\_num to IP\_address/port\_num Connection connection\_ID
- Error Message %ACE-5-415025: HTTP policy\_map\_name - Tunnel detected - connection\_action from IP\_address/port\_num to IP\_address/port\_num connection connection\_ID
- Error Message %ACE-5-415026: HTTP policy\_map\_name: Instant Messenger detected connection\_action from IP\_address/port\_num to IP\_address/port\_num connection connection\_ID

- Error Message %ACE-5-415027: HTTP policy\_map\_name: Peer-to-Peer detected connection\_action from IP\_address/port\_num to IP\_address/port\_num connection connection\_ID
- Error Message %ACE-5-441001: Serverfarm name failed over to backup. Number of failovers = count1, number of times back in service = count2
- Error Message %ACE-5-441002: Serverfarm name is back in service. Number of failovers = count1, number of times back in service = count2
- Error Message %ACE-5-444002: Installed license file license\_file\_name
- Error Message %ACE-5-444003: Uninstalled license file license\_file\_name
- Error Message %ACE-4-444007: Installed feature\_name license on Revision 6 or older hardware, will not take effect until next reboot.
- Error Message %ACE-5-504001: Security context context-name was added to the system
- Error Message %ACE-5-504002: Security context context-name was successfully removed from the system
- Error Message %ACE-5-727019: HA: Started alternate ping to IP address ip addr
- Error Message %ACE-5-727020: HA: Stopped alternate ping to IP address ip addr.
- Error Message %ACE-5-727021: HA: Peer is compatible.
- Error Message %ACE-5-727022: HA: Started sending heartbeats to peer Peer id interval value and count cnt
- Error Message %ACE-5-727023: HA: Stopped sending heartbeats to peer Peer id.
- Error Message %ACE-5-728004: Internal communications notice (general) type variable1
- Error Message %ACE-5-728006: Internal communications error (messaging) msg subType variable1 -- type variable2
- Error Message %ACE-5-728012: Context ID variable1 failed to receive return data -- type variable2
- Error Message %ACE-5-728018: Proxy connection variable1 rebalanced to server variable2
- Error Message %ACE-5-728028: Sticky mapping failed: variable1 variable2

## Informational Messages, Severity Level 6

The following messages appear at severity level 6, informational:

- Error Message %ACE-6-253001: Certificate certificate\_information expired
- Error Message %ACE-6-253002: Certificate certificate\_information not yet valid
- Error Message %ACE-6-253003: Unknown CA certificate\_information
- Error Message %ACE-6-253004: Certificate certificate\_information revoked
- Error Message %ACE-6-253005: Signature for certificate\_information is invalid
- Error Message %ACE-6-253006: Error peer sent invalid or nonexistent certificate
- Error Message %ACE-6-253007: Certificate in file file\_name is expired
- Error Message %ACE-6-253008: CRL crl\_name could not be retrieved
- Error Message %ACE-6-253009: Certificate in file file\_name is not yet valid
- Error Message %ACE-6-253011: The CRL crl\_Name may not be from a trusted source. Signature mismatch detected for CRL.

- Error Message %ACE-6-302022: Built TCP connection id for interface:real-address/real-port (mapped-address/mapped-port) to interface:real-address/real-port (mapped-address/mapped-port)
- Error Message %ACE-6-302023: Teardown TCP connection id for interface:real-address/real-port to interface:real-address/real-port duration hh:mm:ss bytes bytes [reason]
- Error Message %ACE-6-302024: Built UDP connection id for interface:real-address/real-port (mapped-address/mapped-port) to interface:real-address/real-port (mapped-address/mapped-port)
- Error Message %ACE-6-302025: Teardown UDP connection id for interface:real-address/real-port to interface:real-address/real-port duration hh:mm:ss bytes bytes
- Error Message %ACE-6-302026: Built ICMP connection for faddr/NATed\_ID gaddr/icmp\_type laddr/icmpID
- Error Message %ACE-6-302027: Teardown ICMP connection for faddr/NATed ID gaddr/icmp\_type laddr/icmpID
- Error Message %ACE-6-302028: Built TCP connection id for interface: real-address/real-port (mapped-address/mapped-port) to interface: real-address/real-port (mapped-address/mapped-port)
- Error Message %ACE-6-302029: Teardown TCP connection id for interface: real-address/real-port to interface: real-address/real-port duration hh:mm:ss bytes bytes [reason]
- Error Message %ACE-6-302030: Built UDP connection id for interface: real-address/real-port (mapped-address/mapped-port) to interface: real-address/real-port (mapped-address/mapped-port)
- Error Message %ACE-6-302031: Teardown UDP connection id for interface: real-address/real-port to interface: real-address/real-port duration hh:mm:ss bytes bytes
- Error Message %ACE-6-303003: FTP cmd\_name command denied - failed strict inspection, terminating connection from source\_interface:source\_address/source\_port to dest\_interface:dest\_address/dest\_port
- Error Message %ACE-6-305009: Built {dynamiclstatic} translation from interface\_name [(acl-name)]:real\_address to interface\_name:mapped\_address
- Error Message %ACE-6-314001: Pre-allocate RTSP UDP backconnection for foreign\_address outside\_address/outside\_port to local\_address inside\_address/inside\_port
- Error Message %ACE-6-608001: Pre-allocate Skinny connection\_type secondary channel for source\_interface:source\_address/source\_port to destination\_interface:destination\_address/destination\_port from message\_id message
- Error Message %ACE-6-615003: VLAN VLAN-number not available for configuring an interface
- Error Message %ACE-6-615004: VLAN VLAN-number available for configuring an interface
- Error Message %ACE-6-728020: LB is configured to consume variable1 bytes of memory.
- Error Message %ACE-6-728021: Found inconsistent sticky entry. Terminating variable1.
- Error Message %ACE-6-728022: Invalid hash table index (variable1) used for variable2
- Error Message %ACE-6-728023: variable1 variable2 sticky entries from ContextId variable3.
- Error Message %ACE-6-728025: Dropped variable1 'variable2' messages (variable3 total) from IXP variable4 to IXP variable5!
- Error Message %ACE-6-728026: Attempting to use invalid lookup key for variable1 processing.
- Error Message %ACE-6-728029: HA state for FtGroup variable1 changed from variable2 to variable3 State variable4.
- Error Message %ACE-6-728030: Silently discarding HA data: variable1

# Debugging Messages, Severity Level 7

- Error Message `%ACE-7-111009: User user executed cmd:string`



## INDEX

---

### A

#### ACE

- initialization failure [2-43](#)
- logging, enabling [1-20](#)
- logging, rejecting new connections [1-21](#)
- logging levels [1-4](#)
- logging overview [1-2](#)
- log message format [1-3](#)
- network processor error [2-50](#)
- physical memory for load-balancing [2-49](#)
- severity levels [1-4](#)
- subsystem levels [1-4](#)

#### ACL resources

- minimum not guaranteed [2-13](#)
- usage beyond limit [2-13](#)

#### ACLs

- compilation process out of memory [2-3](#)

#### address translation slot

- created [2-18](#)

#### alert messages [3-1](#)

#### ARP

- collision [2-21](#)
- inspection check failure [2-20](#)
- poisoning [2-21](#)

#### attacks

- ARP poisoning [2-21](#)
- spoofing [2-2, 2-19, 2-20, 2-23](#)

---

### B

- buffer, logging to [1-9](#)

---

### C

- cache alignment error [2-47](#)
- clearing log messages [1-22](#)
- configuration, modified by command, system message [2-4](#)
- configuration files
  - replication failure [2-36](#)
- configuration modified by command message [2-2, 2-3](#)
- console
  - logging to [1-11](#)
- content type verification
  - failed, unexpected number in message body [2-24](#)
- context
  - adding context with an associated sticky group [2-46](#)
  - associated sticky group [2-46](#)
  - configuration synchronization failure [2-38](#)
  - removing with an associated sticky group [2-46](#)
  - show command failure [2-47](#)
  - state change [2-38](#)
  - sticky entry request [2-46](#)
- control processor, unrecognized message [2-51](#)
- critical messages [3-2](#)

---

### D

- debugging messages [3-9](#)
- debug logging failure [2-53](#)
- DNS
  - packet message [2-22](#)

---

**E**

EMBLEM-format logging [1-12](#)  
 Encap table full [2-20](#)  
 error messages [3-2](#)

---

**F**

facility, changing [1-17](#)  
 fault tolerance  
     See HA  
 Flash memory  
     logging to [1-14](#)  
 FT group  
     context name mismatch [2-35](#)  
     peer state change [2-52](#)  
     two active devices detected [2-36](#)  
 FT interface, peer unreachable [2-35](#)  
 FTP port command  
     address other than the address used in the  
     connection [2-22](#)  
     low port number [2-22](#)  
 FTP traffic  
     strict inspection policy denies request command [2-17](#)  
     unrecognized command in request message when  
     using strict inspection policy [2-17](#)  
 FT track state change [2-41](#)

---

**H**

HA  
     alternate pings [2-41, 2-42](#)  
     communication failure [2-37](#)  
     configuration replication failure [2-38](#)  
     context name mismatch [2-35](#)  
     context state change [2-38](#)  
     data dropped [2-53](#)  
     FT track state change [2-41](#)  
     heartbeat interval mismatch [2-40](#)

    heartbeats unidirectional [2-40](#)  
     initialization failure [2-37](#)  
     internal error [2-37](#)  
     mapping failure [2-52](#)  
     module [2-37](#)  
     peer compatibility [2-42](#)  
     peer incompatibility [2-36](#)  
     peer reachable [2-40, 2-42](#)  
     peer state change [2-52](#)  
     peer unreachable [2-35, 2-48](#)  
     receive error [2-48](#)  
     redundancy heartbeat stopped [2-42](#)  
     replication failure [2-36, 2-38](#)  
     replication in process [2-40](#)  
     state transitions [2-38](#)  
     two active devices detected [2-36](#)

hash table, invalid index [2-50](#)

## heartbeat

    interval mismatch [2-40](#)  
     started [2-42](#)  
     stopped [2-35, 2-41, 2-42](#)  
     unidirectional [2-40](#)

## High Availability

    See HA

## HTTP

    body length within configured range [2-26](#)  
     body matches regular expression [2-24](#)  
     header length within configured range [2-26](#)  
     parser unable to detect valid message [2-25](#)  
     request method matches regular expression [2-25](#)  
     return code, threshold reached [2-53](#)  
     transfer/content encoding matches regular  
     expression [2-25](#)  
     URI length within configured range [2-25](#)  
     URI matches regular expression [2-24](#)

## HTTP content

    instant messenger protocol detected [2-27](#)  
     peer-to-peer protocol detected [2-27](#)  
     tunneling protocol detected [2-26](#)

## HTTP header

matches regular expression [2-24, 2-26](#)

## I

## ICMP

health probe error [2-8](#)

initialization failure [2-18](#)

memory failure [2-19](#)

packet denied [2-18](#)

probe error [2-7, 2-8](#)

session established [2-15](#)

session removed [2-16](#)

unexpected server response [2-9](#)

informational messages [3-7](#)

initialization failure [2-37, 2-43](#)

## interface

configuration status change [2-23](#)

configuration status changed [2-23](#)

line protocol change of state [2-22, 2-23](#)

VLAN availability [2-34](#)

invalid lookup key [2-51](#)

IP header option error [2-21](#)

## L

## levels

changing [1-18](#)

overview [1-4](#)

severity listing [1-4](#)

## licenses

16G takes effects after reboot [2-31](#)

evaluation time expired [2-31](#)

evaluation time warning [2-31](#)

failed checkout [2-30](#)

installation completed [2-30](#)

manager exiting [2-31](#)

uninstall completed [2-30](#)

limiting the syslog rate [1-19](#)

line protocol, status change [2-22, 2-23](#)

## load balancing

cache alignment error [2-47](#)

general error [2-44](#)

HA data dropped [2-53](#)

internal channel error [2-47](#)

internal error [2-45](#)

mapped memory [2-49](#)

processor communications error [2-47](#)

sticky database error [2-45, 2-49](#)

sticky entry inconsistency [2-49](#)

sticky error [2-45](#)

transmit failure [2-44](#)

unrecognized message [2-51](#)

log files, logging levels [1-4](#)

## logging

changing message levels [1-7, 1-19](#)

connection setup and teardown syslog messages, enabling [1-22](#)

disabling messages [1-18](#)

EMBLEM-format logging [1-12](#)

enabling [1-8, 1-20](#)

facility, changing [1-17](#)

levels [1-4](#)

log messages, clearing [1-22](#)

message format [1-3](#)

message queue size, changing [1-17](#)

overview [1-2](#)

quick start [1-6](#)

rejecting new connections [1-21](#)

severity level of messages, changing [1-18](#)

severity levels [1-4](#)

syslog output locations, specifying [1-8](#)

syslog rate, limiting [1-19](#)

system message timestamp, enabling [1-15](#)

to buffer [1-9](#)

to console [1-11](#)

to Flash memory [1-14](#)

- to SNMP NMS [1-13](#)
- to SSH session [1-9](#)
- to Supervisor engine [1-13](#)
- to syslog server [1-11](#)
- to Telnet session [1-9](#)
- variables [1-4](#)
- viewing log message information [1-23](#)

logging on the ACE, enabling [1-20](#)

---

## M

MAC addresses

- mapping change [2-23](#)

mapping failure [2-52](#)

memory mapping failure [2-53](#)

messages

- format [1-3](#)
- message queue size, changing [1-17](#)
- severity levels [1-4, 3-1](#)
- timestamp, enabling [1-15](#)
- understanding [1-3](#)
- variables [1-4](#)

---

## N

network processor error, sticky [2-50, 2-51](#)

notification messages [3-6](#)

numerical codes of system messages [2-1](#)

---

## O

output locations

- buffer [1-9](#)
- console [1-11](#)
- Flash memory [1-14](#)
- SNMP [1-13](#)
- SNMP NMS [1-13](#)
- specifying [1-8](#)

- SSH session [1-9](#)
- Supervisor module [1-13](#)
- syslog server [1-11](#)
- Telnet [1-9](#)
- Telnet session [1-9](#)

---

## P

peer

- alternate pings [2-41, 2-42](#)
- communication failure [2-37](#)
- heartbeat interval mismatch [2-40](#)
- heartbeats unidirectional [2-40](#)
- incompatibility [2-36](#)
- mapping failure [2-52](#)
- reachable [2-40, 2-42](#)
- receive error [2-48](#)
- replication failure [2-36, 2-38](#)
- replication in process [2-40](#)
- state change [2-52](#)
- unreachable [2-35, 2-48](#)

probe

- connectivity error [2-8](#)
- connectivity error for ICMP probe [2-8](#)
- empty health probe script [2-6](#)
- failure due to internal error [2-7](#)
- internal error for ICMP probe [2-7, 2-8](#)
- internal error when loading script [2-6](#)
- lost script file [2-6](#)
- memory allocation failure [2-5](#)
- unable to load script [2-6](#)
- unexpected ICMP server response [2-9](#)
- unexpected server response [2-9](#)

processing

- ACL compilation process out of memory [2-3](#)
- invalid lookup key [2-51](#)

proxy connection rebalanced [2-48](#)

**Q**

quick start

logging 1-6

**R**

real servers

HTTP return code threshold 2-53

state change 2-29

state change to down 2-29

state change to down in specified server farm 2-28

state change to up 2-29

state change to up in specified server farm 2-28

regex resources

minimum not guaranteed 2-54

usage beyond limit 2-54

regular expression table compilation process, out of memory 2-54

reload

reasons 2-4

record 2-4

RTSP

connection, opened by ASA for specified IP address and ports 2-19

**S**

SCCP

command denied by inspection policy 2-34

connection preallocated for session-negotiated media streams 2-33

message over configured size dropped 2-33

message that is too small dropped 2-33

registration not completed 2-34

scripts

empty 2-6

error determining size 2-10

error reading 2-10

internal error when loading 2-6

lost file 2-6

memory allocation error 2-6

security context

added to system 2-32

removed from system 2-32

server connection

lost 2-44

rebalanced 2-48

server farms

failover back in service notification 2-28

failover to backup notification 2-28

HTTP return code threshold 2-53

severity codes of system messages 3-1

severity level messages

Level 1 messages 3-1

Level 2 messages 3-2

Level 3 messages 3-2

Level 4 messages 3-4

Level 5 messages 3-6

Level 6 messages 3-7

Level 7 messages 3-9

overview 1-4

severity levels

alerts 3-1

changing 1-18

critical 3-2

debugging 3-9

errors 3-2

informational 3-7

notifications 3-6

of messages 3-1

overview 1-4

warning 3-4

show command

failure 2-47

site security policy, averting 2-22

SNMP

daemon initialization failure 2-5

- memory allocation failure [2-5](#)
- network management station [1-13](#)
- Shadow Table error [2-27](#)
- spoofing attack [2-2, 2-19, 2-20, 2-23](#)
- SSH
  - session, sending syslog messages [1-9](#)
- SSL
  - CRL, failure to retrieve [2-12](#)
- SSL certificate
  - expired [2-10, 2-12](#)
  - invalid or nonexistent [2-11](#)
  - not currently valid [2-10](#)
  - revoked by certificate authority [2-11](#)
  - signature invalid [2-11](#)
  - unknown certificate authority [2-11](#)
- sticky
  - associated group [2-46](#)
  - database error [2-45](#)
  - entries added or removed [2-50](#)
  - entry dropped [2-52](#)
  - entry inconsistency [2-49](#)
  - initialization failure [2-43](#)
  - key, invalid [2-51](#)
  - network processor error [2-51](#)
  - processor error [2-45, 2-50](#)
  - request not responded to [2-49](#)
  - resources exceeded [2-46](#)
  - unexpected sticky group lookup result [2-49](#)
- subsystems [1-4](#)
- supervisor
  - logging to [1-13](#)
- syslog output locations
  - buffer [1-9](#)
  - console [1-11](#)
  - Flash memory [1-14](#)
  - SNMP NMS [1-13](#)
  - specifying [1-8](#)
  - SSH session [1-9](#)
  - Supervisor engine [1-13](#)
  - syslog server [1-11](#)
  - Telnet session [1-9](#)
- syslog rate, limiting [1-19](#)
- syslog server
  - device ID, specifying [1-16](#)
  - EMBLEM-format logging [1-12](#)
  - identifying messages sent [1-15](#)
  - sending syslog messages [1-11](#)
- system message logging
  - connections
    - setup and teardown syslog messages, enabling [1-22](#)
  - disabling messages [1-18](#)
  - EMBLEM-format logging [1-12](#)
  - enabling [1-8, 1-20](#)
  - facility, changing [1-17](#)
  - format [1-3](#)
  - log messages, clearing [1-22](#)
  - overview [1-2](#)
  - queue, changing [1-17](#)
  - quick start [1-6](#)
  - rejecting new connections [1-21](#)
  - severity level, changing [1-18](#)
  - severity levels [1-4](#)
  - syslog output locations, specifying [1-8](#)
  - syslog rate, limiting [1-19](#)
  - to buffer [1-9](#)
  - to console [1-11](#)
  - to Flash memory [1-14](#)
  - to SNMP NMS [1-13](#)
  - to SSH session [1-9](#)
  - to Supervisor engine [1-13](#)
  - to syslog server [1-11](#)
  - to Telnet session [1-9](#)
  - understanding [1-3](#)
  - variables [1-4](#)
  - viewing log message information [1-23](#)
- system messages
  - by numerical code [2-1](#)

by severity code [3-1](#)  
timestamps, enabling [1-15](#)

---

## T

### TCP

connection failure [2-37](#)  
connection slot creation [2-14, 2-16](#)  
connection slot termination [2-14, 2-16](#)  
termination reasons [2-14, 2-16](#)

### Telnet

session, sending syslog messages [1-9](#)

---

## U

### UDP

connection slot creation [2-15, 2-16](#)  
connection slot deletion [2-15, 2-17](#)  
DNS packet [2-22](#)

### URL

host access record [2-17](#)

---

## V

### variables

fields [1-4](#)  
in messages [1-4](#)

viewing log message information [1-23](#)

### VLANs

number availability [2-34](#)

---

## W

warning messages [3-4](#)



