53-1003140-01
27 June 2014

Fabric OS

Message Reference

Supporting Fabric OS 7.3.0

BROCADE

Brocade Communications Systems, Incorporated

Corporate and Latin American Headquarters
Brocade Communications Systems, Inc.
130 Holger Way
San Jose, CA 95134
Tel: 1-408-333-8000
Fax: 1-408-333-8101
E-mail: info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems China HK, Ltd.
No. 1 Guanghua Road
Chao Yang District
Units 2718 and 2818
Beijing 100020, China
Tel: +8610 6588 8888
Fax: +8610 6588 9999
E-mail: china-info@brocade.com

European Headquarters
Brocade Communications Switzerland Sàrl
Centre Swissair
Tour B - 4ème étage
29, Route de l'Aéroport
Case Postale 105
CH-1215 Genève 15
Switzerland
Tel: +41 22 799 5640
Fax: +41 22 799 5641
E-mail: emea-info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems Co., Ltd. (Shenzhen WFOE)
Citic Plaza
No. 233 Tian He Road North
Unit 1308 – 13th Floor
Guangzhou, China
Tel: +8620 3891 2000
Fax: +8620 3891 2111
E-mail: china-info@brocade.com

Document History

Title	Publication number	Summary of changes	Date
Diagnostic and System Error Message Reference v3.0, v4.0	53-0000210-02	First release	March 2002
Diagnostic and System Error Message Reference v3.1.0	53-0000511-04	Major content reorganization	June 2003
Diagnostic and System Error Message Reference v4.1.0	54-0000515-02	Major content reorganization	June 2003
Diagnostic and System Error Message Reference v4.1.2	53-0000515-06	Minor editorial changes	October 2003
Diagnostic and System Error Message Reference v4.2.0	53-0000515-07	Added FW and PLATFORM messages	December 2003
Diagnostic and System Error Message Reference v4.2.0	53-0000515-08	Updated software and hardware support	March 2004

Title	Publication number	Summary of changes	Date
Fabric OS System Error Message Reference Manual	53-0000515-09	Updated for v4.4.0, First RASLog release	August 2004
Fabric OS System Error Message Reference Manual	53-0000515-10	Added 22 ZONE messages	April 2005
Fabric OS System Error Message Reference Manual	53-0000515-11	Added FICU-1010, HAMK-1004, and PLAT-1001	July 2005
Fabric OS System Error Message Reference Manual	53-1000046-01	Added BM, FCR, IPS, FCIP, SEC, and ZONE messages	January 2006
Fabric OS System Error Message Reference Manual	53-1000046-02	Minor updates to a few messages.	June 2006
Fabric OS Message Reference	53-1000242-01	Updated for Fabric OS v5.2.0: -Changed doc title and number -Added the following new modules: IBPD, ICPD, ISCSI, ISNSCD. Added Audit messages: AUTH, CONF, HTTP, SEC, SNMP, SULB, ZONE. -Updated Introduction chapter with AUDIT log information. -Updated chapter titles.	September 2006
Fabric OS Message Reference	53-1000437-01	Updated for Fabric OS v5.3.0: -Added new chapters: AG, BKSW, IBD, IPAD, SAS. Revised and added new messages to: AUTH, CDR, CONF, EM, FABR, HAM, ISNS, ISW, PDM,SEC,TS, KTRC.SEC, TS. Revised/updated BL,BLL,FCPD, FICU,FW, HIL,LOG, SNMP, SULB,SWCH,SYSM, TRCE, ZOLB, ZONE. -Deleted USWD chapter. -Updated Introductory chapters. -Updated throughout: rebranding, supported hardware, CLI changes.	June 2007
Fabric OS Message Reference	53-1000600-01	Updated for Fabric OS v6.0.0: -Added new chapters: C2, ESS, FICON -Added new messages to: AG, BL, BM, C2, FCIP, ISW, NS, PLAT, SS, HIL. -Added Audit messages: SEC, SULB -Updated Introductory chapters.	October 2007
Fabric OS Message Reference	53-1000600-02	Updated for Fabric OS v6.1.0: -Revised and added new messages to: AG, BL, C2, EM, FABR, FCR, FCIP, FW, SEC, NS, PDM, PLAT, SULB, SWCH, ZONE, WEBD. -Added new Audit chapter: FW. -Added new Audit messages to: SEC. -Updated Introductory chapters.	Jun 2008
Fabric OS Message Reference	53-1001116-01	Updated for Fabric OS v6.1.1_enc: -Revised and added new messages to AG -Added new chapters: CNM, CTAP, CVLC, CVLM, KAC, RKD, SPC, SPM. -Added new Audit chapters: AG, FCIP, FICU, IPAD, PORT, SWCH, UCST. -Updated Introductory chapters.	Aug 2008

Title	Publication number	Summary of changes	Date
Fabric OS Message Reference	53-1001157-01	Updated for Fabric OS v6.2.0: -Revised and added new messages to FSS, KSWD, CTAP, CNM, CVLM, EM, FABR, FCIP, FW, HIL, FCR, SEC, SWCH, UCST, ZONE. -Added new chapters: CHASSIS, LFM, PMGR, TAPE. -Updated Introductory chapters.	November 2008
Fabric OS Message Reference	53-1001338-01	Updated for Fabric OS v6.3.0: -Modified a message to BKSW, BL, BKSW, BLL, CDR, CEE CONFIG, CONF, EM, FCOE, FCPD, FCPH, FCR, FICON, FICU, FLOD, FSPF, FSSM, FW, HAM,,HAMK, HIL, IPS, ISNS, L2SYS, MFIC, PDM, PLAT, PORT, RCS, RPCD, RTWR, SEC, SNMP, SWCH, TRCE, TRCK, WEBD, ZONE. -Added new messages to AG, AN, AUTH, BLS, C2, CDR, CEE, CONFIG, CHASSIS, CNM, CONF, CTAP, CVLC, CVLM, DAUTH, EM, FABR, FCIP, FCPH, FCR, FICON, FICU, FSPF, FSS, FW, HAM, HSL, KAC, KSWD, LANCE, LFM, MS, NS, NSM, PMGR, PORT, PSWP, RKD, SEC, SPC, SPM, SS, SULB, SWCH, TAPE, UCST, UPTH, XTUN, ZONE. -Added new chapters for LANCE, BLS, AN, CVLM, DAUTH, XTUN. -Updated Introductory chapters.	July 2009
Fabric OS Message Reference	53-1001338-02	Updated for Fabric OS v6.3.0 patch: -Modified a message to BL. -Added new messages to AG, BL, and FCOE. -Added new chapters for Audit CNM, Audit CVLM, and Audit SPM.	November 2009
Fabric OS Message Reference	53-1001767-01	Updated for Fabric OS v6.4.0: -Modified messages to FICU and FW. -Deleted messages to BL, FCOE and FW. -Added new messages to AG, AN, AUTH, BL, C2, CNM, CONF, CVLC, CVLM, FABR, FICU, FW, HAM, HIL, MQ, MS, MSTP, NS, NSM, ONM, PS, PSWP, RKD, SEC, SPM, SS, SSM, SULB, SWCH and ZONE. -Updated Introductory chapters.	March 2010

Title	Publication number	Summary of changes	Date
Fabric OS Message Reference	53-1002149-01	Updated for Fabric OS v7.0.0: -Added new chapters: C3, CAL, MCAST_SS, RTE, and VS. -Added new messages: AG, AN, ANV, BL, C2, CDR, CCFG, ECC, EM, ESS, FABR, FCOE, FCPH, FICN, FICU, FSPF, FW, HIL, IPAD, IPS, KAC, L2SYS, LACP, LOG, MS, NS, NSM, ONM, PDM, PS, RAS, RCS, SCN, SEC, SNMP, SPM, SS, SSM, SULB, SWCH, XTUN, ZEUS, and ZONE. -Modified messages: CDR, EM, FABR, FCOE, FICU, FW, HIL, L2SYS, PMGR, SEC, SPM, SS, and XTUN. -Deleted messages: C2, FCOE, FICU, and NSM. -Added new Audit chapters: ESS, MS, PMGR, and RAS. -Updated Introductory chapter.	April 2011
Fabric OS Message Reference	53-1002448-01	Updated for Fabric OS v7.0.1: -Added new messages: BL, CVLC, FICON, FSPF, and PS -Modified messages: AG, AN, C2, C3, CDR, FABR, FSPF, L2SYS, NSM, RTE, and ZONE. -Deleted messages: EM, FABR, ISCS, SAS, and ZOLB. -Updated Introductory chapter.	December 2011
Fabric OS Message Reference	53-1002749-01	Updated for Fabric OS v7.1.0: - Added new chapters: MM and VDR. - Added new messages: AG, ANV, BL, C2, C3, CDR, CONF, CVLM, EM, FABR, FCR, FSPF, FW, HAM, HIL, KAC, LOG, MS, NBFS, PLAT, PS, RAS, SEC, SS, SWCH, TRCE, VDR, XTUN, ZEUS, and ZONE. - Modified messages: AN, AUTH, BL, C2, C3, CDR, CAL, CNM, DOT1, FABR, FCOE, FCPD, FCR, FICU, FSPF, FSS, HIL, HSL, HTTP, IPS, KTRC, L2SS, LFM, PMGR, PS, RCS, RTWR, SEC, ZONE. - Deleted messages: EM, FCOE, HAM, SNMP, SYSC, UCST, ZONE. - Deleted modules: BLL, CER, FCIP, IBPD, and ICPD. - Updated Introductory chapter.	December 2012
Fabric OS Message Reference	53-1002749-02	Modified C2, C3, and HSL messages.	March 2013
Fabric OS Message Reference	53-1002929-01	Updated for Fabric OS v7.2.0: - Added new chapters: FV and MAPS - Added new messages: AG, C2, C3, FCR, FSPF, KAC, PLAT, PORT, RAS, SEC, SS, SULB, -WEBD, and XTUN. - Modified messages: AG, BL, C2, C3, FCR, FSS, HIL, MM, MQ, SEC, and SULB. - Deleted messages: FW and SULB.	July 2013

Title	Publication number	Summary of changes	Date
Fabric OS Message Reference	53-1003109-01	Updated for Fabric OS v7.2.1: - Added new messages: FCR and PLAT. - Modified messages: BL.	December 2013
Fabric OS Message Reference	53-1003140-01	Updated for Fabric OS v7.3.0: - Added new chapters: BCM, BLZ, and ESM. - Added new messages: AG, AN, AUTH, BL, C2, C3, CVLM, EM, FV, HIL, MAPS, NBFS, NS, RAS, SEC, SNMP, SULB, SWCH, UCST, XTUN, and ZONE. - Modified messages: C3, FABR, FCR, FV, NBFS, SNMP, and XTUN.	June 2014

Contents

About This Document

In this chapter

How this document is organized

This document is organized to help you find the information that you want as quickly and easily as possible.

The document contains the following components:

- Chapter 1, "Introduction to System Messages" provides basic information on system messages.
- Chapter 2, "Audit Messages" includes a lookup list for Audit messages.
- Chapter 3, "FFDC Messages" includes a lookup list for FFDC messages.
- Chapter 4, "Log Messages" includes a lookup list for LOG messages.
- Chapter 5, "Fabric OS System Messages" provides message text, probable cause, recommended action, and severity for each of the messages.

Supported hardware and software

In those instances in which procedures or parts of procedures documented here apply to some switches but not to others, this guide identifies exactly which switches are supported and which are not.

Although many different software and hardware configurations are tested and supported by Brocade Communications Systems, Inc. for Fabric OS v7.3.0, documenting all possible configurations and scenarios is beyond the scope of this document.

The following hardware platforms are supported by this release of Fabric OS:

- Brocade 300
- Brocade 5100
- Brocade 5300
- Brocade 5410
- Brocade 5424
- Brocade 5430
- Brocade 5431
- Brocade 5432
- Brocade 5450
- Brocade 5460
- Brocade 5470
- Brocade 5480
- Brocade 6505
- Brocade M6505
- Brocade 6510
- Brocade 6520
- Brocade 6547
- Brocade 6548
- Brocade 7800 Extension Switch
- Brocade 7840 Extension Switch
- Brocade Encryption Switch
- Brocade DCX Backbone and Brocade DCX-4S Backbone
  - FC8-16 port blade
  - FC8-32 port blade
  - FC8-48 port blade
  - FC8-64 port blade
  - FCOE10-24 DCX Blade
  - FS8-18 Encryption Blade
  - FX8-24 DCX Extension Blade
- Brocade DCX 8510-8 Backbone and Brocade DCX 8510-4 Backbone
  - FC8-32E port blade
  - FC8-48E port blade
  - FC8-64 port blade
  - FC16-32 port blade
  - FC16-48 port blade
  - FC16-64 port blade
  - FCOE10-24 DCX Blade (not supported on Brocade DCX 8510-4)

- FS8-18 Encryption Blade
- FX8-24 DCX Extension Blade

- Brocade VA-40FC

What's new in this document

The following changes have been made since this document was last released:

- New modules added:
  - BCM Messages
  - BLZ Messages
  - ESM Messages
- Information that was added:
  - AG-1046
  - AG-1047
  - AN-1014
  - AUTH-1048
  - AUTH-1049
  - BL-1053
  - BL-1054
  - BL-1055
  - C2-1031
  - C2-1032
  - C3-1032
  - C3-1033
  - C3-1034
  - CVLM-1017
  - EM-1073
  - EM-1134
  - FV-3012
  - FV-3013
  - FV-3014
  - HIL-1512
  - HIL-1614
  - HIL-1615
  - HIL-1651
  - MAPS-1011
  - MAPS-1012
  - NBFS-1005

- NS-1013
- NS-1014
- NS-1015
- RAS-2004
- RAS-2005
- SEC-1341
- SEC-1342
- SEC-1343
- SEC-1344
- SEC-1343
- SNMP-1010
- SULB-1051
- SULB-1052
- SULB-1053
- SULB-1054
- SWCH-1027
- SWCH-1028
- SWCH-1029
- SWCH-1030
- UCST-1028
- UCST-1029
- XTUN-1009
- XTUN-4104
- XTUN-4105
- XTUN-4106
- XTUN-4107
- XTUN-4115
- XTUN-4120
- XTUN-4121
- XTUN-4122
- XTUN-4123
- XTUN-4124
- XTUN-4125
- XTUN-4126
- XTUN-4127
- XTUN-4137
- ZONE-1064
- ZONE-1065
- ZONE-1066

- Information that was changed:
  - C3-1012
  - FABR-1052
  - FCR-1048
  - FV-3006
  - FV-3007
  - FV-3008
  - FV-3009
  - NBFS-1001
  - SNMP-1005
  - XTUN-1000
  - XTUN-1001
  - XTUN-1002
  - XTUN-1003
  - XTUN-1004
  - XTUN-1006
  - XTUN-1007
  - XTUN-1008
  - XTUN-1996
  - XTUN-1997

For further information about new features and documentation updates for this release, refer to the release notes.

Document conventions

This section describes text formatting conventions and important notice formats used in this document.

Text formatting

The narrative-text formatting conventions that are used are as follows:

bold text	Identifies command names Identifies the names of user-manipulated GUI elements Identifies keywords and operands Identifies text to enter at the GUI or CLI
italic text	Provides emphasis Identifies variables Identifies paths and Internet addresses Identifies document titles
`code` text	Identifies CLI output Identifies command syntax examples

For readability, command names in the narrative portions of this guide are presented in mixed lettercase: for example, **switchShow**. In actual examples, command lettercase is all lowercase.

Command syntax conventions

Command syntax in this manual follows these conventions:

command	Commands are printed in bold.
--**option, option**	Command options are printed in bold.
-**argument,** arg	Arguments.
[ ]	Optional element.
variable	Variables are printed in italics. In the help pages, values are underlined or enclosed in angled brackets < >.
...	Repeat the previous element, for example “member[;member...]”
value	Fixed values following arguments are printed in plain font. For example, --**show** WWN
|	Boolean. Elements are exclusive. Example: --**show** -**mode** egress | ingress

Command examples

This book describes how to perform configuration tasks using the Fabric OS command line interface, but does not describe the commands in detail. For complete descriptions of all Fabric OS commands, including syntax, operand description, and sample output, see the *Fabric OS Command Reference*.

Notes, cautions, and warnings

The following notices and statements are used in this manual. They are listed below in order of increasing severity of potential hazards.

NOTE
A note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates potential damage to hardware or data.

CAUTION

A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER

A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Key terms

For definitions specific to Brocade and Fibre Channel, see the technical glossaries on MyBrocade. See "Brocade resources" on page xix for instructions on accessing MyBrocade.

For definitions of SAN-specific terms, visit the Storage Networking Industry Association online dictionary at:

http://www.snia.org/education/dictionary

Notice to the reader

This document may contain references to the trademarks of the following corporations. These trademarks are the properties of their respective companies and corporations.

These references are made for informational purposes only.

Corporation	Referenced Trademarks and Products
Red Hat, Inc.	Red Hat, Red Hat Network, Maximum RPM, Linux Undercover

Additional information

This section lists additional Brocade and industry-specific documentation that you might find helpful.

Brocade resources

To get up-to-the-minute information, go to *http://my.brocade.com* to register at no cost for a user ID and password.

White papers, online demonstrations, and data sheets are available through the Brocade website at:

http://www.brocade.com/products-solutions/products/index.page

For additional Brocade documentation, visit the Brocade website:

http://www.brocade.com

Release notes are available on the MyBrocade website.

Other industry resources

For additional resource information, visit the Technical Committee T11 website. This website provides interface standards for high-performance and mass storage applications for Fibre Channel, storage management, and other applications:

http://www.t11.org

For information about the Fibre Channel industry, visit the Fibre Channel Industry Association website:

http://www.fibrechannel.org

Getting technical help

Contact your switch support supplier for hardware, firmware, and software support, including product repairs and part ordering. To expedite your call, have the following information available:

1. General Information
   - Switch model
   - Switch operating system version
   - Software name and software version, if applicable
   - Error numbers and messages received
   - **supportSave** command output
   - Detailed description of the problem, including the switch or fabric behavior immediately following the problem, and specific questions
   - Description of any troubleshooting steps already performed and the results
   - Serial console and Telnet session logs
   - syslog message logs
2. Switch Serial Number

   The switch serial number and corresponding bar code are provided on the serial number label, as illustrated below.

   FT00X0054E9

   The serial number label is located as follows:

   - *Brocade 300, 5100, 5300, 6505, M6505, 6520, 6547, 6548, 7800, 7840, VA-40FC, and Brocade Encryption Switch*—On the switch ID pull-out tab located inside the chassis on the port side on the left.

- *Brocade 5410, 5424, 5430, 5431, 5432, 5450, 5460, 5470, 5480*—Serial number label attached to the module.
- *Brocade 6510*—On the pull-out tab on the front of the switch
- *Brocade DCX and DCX 8510-8*—On the port side of the chassis, on the lower right side and directly above the cable management comb.
- *Brocade DCX-4S and DCX 8510-4*—On the non-port side of the chassis, on the lower left side.

3. World Wide Name (WWN)

   Use the **licenseIdShow** command to display the WWN of the chassis.

   If you cannot use the **licenseIdShow** command because the switch is inoperable, you can get the WWN from the same place as the serial number, except for the Brocade DCX. For the Brocade DCX, access the numbers on the WWN cards by removing the Brocade logo plate at the top of the non-port side of the chassis.

Document feedback

Quality is our first concern at Brocade and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. Forward your feedback to:

documentation@brocade.com

Provide the title and version number of the document and as much detail as possible about your comment, including the topic heading and page number and your suggestions for improvement.

Chapter

Introduction to System Messages

1

In this chapter

Overview of system messages

This guide supports Fabric OS v7.3.0 and documents system messages that can help you diagnose and fix problems with a switch or fabric. The messages are organized alphabetically by module name. A *module* is a subsystem in the Fabric OS. Each module generates a set of numbered messages. For each message, this guide provides message text, probable cause, recommended action, and severity level. There may be more than one cause and more than one recommended action for any given message. This guide discusses the most probable cause and typical action recommended.

System message types

Fabric OS supports three types of system messages. A system message can be of one or more of the following types:

- RASLog messages
- Audit log messages
- FFDC messages

Fabric OS supports a different methodology for storing and accessing each type of message.

RASLog messages

RASLog messages report significant system events (failure, error, or critical conditions) or information and are also used to show the status of the high-level user-initiated actions. RASLog messages are forwarded to the console, to the configured syslog servers, and to the SNMP management station through the Simple Network Management Protocol (SNMP) traps or informs.

The following is an example of a RASLog system message.

```
2012/10/25-17:51:05, [C3-1001], 937, CHASSIS, ERROR, switch, Port 18 failed due to
SFP validation failure. Check if the SFP is valid for the configuration.
```

For information on displaying and clearing the RASLog messages, refer to "Displaying system message logs and attributes" on page 17.

Audit log messages

Event auditing is designed to support post-event audits and problem determination based on high-frequency events of certain types such as security violations, zoning configuration changes, firmware downloads, and certain types of fabric events. Audit messages flagged only as AUDIT are not saved in the switch error logs. The switch can be configured to stream Audit messages to the switch console and to forward the messages to specified syslog servers. The Audit log messages are not forwarded to an SNMP management station. There is no limit to the number of audit events.

The following is an example of an Audit message.

```
0 AUDIT, 2012/10/14-06:07:33 (UTC), [SULB-1003], INFO, FIRMWARE,
admin/admin/192.0.2.2/telnet/CLI ad_0/switch, , Firmwarecommit has started.
```

For any given event, Audit messages capture the following information:

- User Name - The name of the user who triggered the action.
- User Role - The access level of the user, such as root or admin.
- Event Name - The name of the event that occurred.
- Event Information - Information about the event.

The seven event classes described in Table 1 can be audited.

TABLE 1 Event classes

Operand	Event class	Description
1	Zone	You can audit zone event configuration changes, but not the actual values that were changed. For example, you may receive a message that states "Zone configuration has changed," but the message does not display the actual values that were changed.
2	Security	You can audit any user-initiated security event for all management interfaces. For events that have an impact on the entire fabric, an audit is only generated for the switch from which the event was initiated.
3	Configuration	You can audit configuration downloads of existing SNMP configuration parameters. Configuration uploads are not audited.
4	Firmware	You can audit configuration downloads of existing SNMP configuration parameters. Configuration uploads are not audited.

TABLE 1 Event classes (Continued)

Operand	Event class	Description
5	Fabric	You can audit Administration Domain-related changes.
6	FW	You can audit Fabric Watch (FW)-related changes.
7	LS	You can audit Virtual Fabric (Logical Switch)-related changes.
8	CLI	You can audit the CLI commands executed on the switch.
9	MAPS	You can audit Monitoring and Alerting Policy Suite (MAPS)-related changes.
N/A	RAS	Used to audit or track the RASLog messages or modules that are enabled or disabled using the **rasAdmin** command. **NOTE:** The RAS class is not configurable, and it is always enabled internally.

Fabric OS v7.3.0 generates component-specific Audit messages.

Event auditing is a configurable feature, which is by default disabled. You must enable event auditing using the **auditCfg --enable** command to send the events to a configured remote host. Syslogd must be configured for logging audit messages. You can set up filters to screen out particular classes of events using the **auditCfg** command. The defined set of Audit messages is sent to the configured remote host in the Audit message format, so that they are easily distinguishable from other syslog events that may occur in the network. For details on how to configure event auditing, refer to "Configuring event auditing" on page 15. For more details, refer to "Displaying Audit messages" on page 19 and "Reading an Audit message" on page 24.

FFDC messages

First Failure Data Capture (FFDC) is used to capture failure-specific data when a problem or failure is noted for the first time and before the switch reboots, or trace and log buffer get wrapped. All subsequent iterations of the same error are ignored. This critical debug information is saved in nonvolatile storage and can be retrieved using the **supportSave** command. The FFDC data is used for debugging or analyzing the problem. FFDC is intended for use by Brocade technical support.

FFDC is enabled by default. Execute the **supportFfdc** command to enable or disable FFDC. If FFDC is disabled, the FFDC daemon does not capture any data, even when a message with an FFDC attribute is logged.

The following is an example of the FFDC message.

```
2000/12/17-08:30:13, [SS-1000], 88, SLOT 6 | FFDC | CHASSIS, INFO, DCX,
supportSave has uploaded support information to the host with IP address
192.0.2.2.
```

Message severity levels

Table 2 shows the four levels of severity for system messages, ranging from CRITICAL (1) to INFO (4). In general, the definitions are wide ranging and are to be used as general guidelines for troubleshooting. For all cases, you must look at each specific error message description thoroughly before taking action.

TABLE 2 Severity levels of a message

Severity level	Description
1 = CRITICAL	Critical-level messages indicate that the software has detected serious problems that will cause a partial or complete failure of a subsystem if not corrected immediately; for example, a power supply failure or rise in temperature must receive immediate attention.
2 = ERROR	Error-level messages represent an error condition that does not impact overall system functionality significantly. For example, error-level messages might indicate time-outs on certain operations, failures of certain operations after retries, invalid parameters, or failure to perform a requested operation.
3 = WARNING	Warning-level messages highlight a current operating condition that should be checked or it may lead to a failure in the future. For example, a power supply failure in a redundant system relays a warning that the system is no longer operating in redundant mode unless the failed power supply is replaced or fixed.
4 = INFO	Info-level messages report the current non-error status of the system components: for example, detecting online and offline status of a fabric port.

System error message logging

The RASLog service generates and stores messages related to abnormal or erroneous system behavior. It includes the following features:

- All RASLog error messages are saved to nonvolatile storage by default.
- The system error message log can save a maximum of 1024 messages in random access memory (RAM).
- The system message log is implemented as a circular buffer. When more than the maximum entries are added to the log file, old entries are overwritten by new entries.
- Messages are numbered sequentially from 1 to 2,147,483,647 (0x7fffffff). The sequence number will continue to increase beyond the storage limit of 1024 messages. The sequence number can be reset to 1 using the **errClear** command. The sequence number is persistent across power cycles and switch reboots.
- The message log size is 256.
- Trace dump, FFDC, and core dump files can be uploaded to the FTP server using the **supportSave** command.
- Brocade recommends that you configure the syslogd facility as a management tool for error logs. This is particularly important for dual-domain switches because the syslogd facility saves messages from two logical switches as a single file and in sequential order. For more information, refer to "System logging daemon" on page 5.
- RASLog messages are streamed to the console, and are forwarded to the configured syslog servers and to the SNMP management station through the SNMP traps (in SNMPv1 and SNMPv3) or informs (in SNMPv3). Use the **snmpConfig** command to configure the SNMPv1 and SNMPv3 hosts and their configurations.
- Audit messages are streamed to the switch console, and are forwarded to the configured syslog servers. The Audit log messages are not forwarded to an SNMP management station.

Configuring the syslog message destinations

You can configure the Fabric OS to send the syslog messages to the following output locations: syslog daemon, system console, and SNMP management station.

System logging daemon

The system logging daemon (syslogd) is a process on UNIX, Linux, and some Windows systems that reads and logs messages as specified by the system administrator.

Fabric OS can be configured to use a UNIX-style syslogd process to forward system events and error messages to log files on a remote host system. The host system can be running UNIX, Linux, or any other operating system that supports the standard syslogd functionality. Configuring for syslogd involves configuring the host, enabling syslogd on the Brocade model, and, optionally, setting the facility level.

For the Brocade DCX family of switches, each control processor (CP) has a unique error log, depending on which CP was active when that message was reported. To fully understand message logging, you should enable the syslogd, because the logs on the host computer are maintained in a single merged file for both CPs and are in sequential order. Otherwise, you must examine the error logs in both CPs, particularly for events such as **firmwareDownload** or **haFailover**, for which the active CP changes.

For the Brocade DCX family of switches, any security violations that occur through Telnet, HTTP, or serial connections are not propagated between CPs. Security violations on the active CP are not propagated to the standby CP counters in the event of a failover, nor do security violations on the standby CP get propagated to the active CP counters.

Configuring a syslog server

To configure the switch to forward all system events and error messages to the syslogd of one or more servers, perform the following steps.

1. Log in to the switch as admin.
2. Execute the **syslogdIpAdd** *IP address* command to add a server to which system messages are forwarded.

   ```
   switch:admin> syslogdipadd 192.0.2.2
   ```

   You can configure up to six syslog servers to receive the syslog messages.
3. Execute the **syslogdIpShow** command to verify the syslog configuration on the switch.

   ```
   switch:admin> syslogdipshow
   syslog.1 192.0.2.2
   ```

You can remove a configured syslog server using the **syslogdIpRemove** *IP address* command.

System console

The system console displays RASLog messages, Audit messages (if enabled), and panic dump messages. These messages are mirrored to the system console; they are always saved in one of the system logs.

The system console displays messages only through the serial port. If you log in to a switch through the Ethernet port or modem port, you will not receive system console messages.

You can filter messages that display on the system console by severity using the **errFilterSet** command. All messages are still sent to the system message log and syslogd (if configured).

Setting the system console severity level

You can limit the types of messages that are logged to the console using the **errFilterSet** command. The system messages displayed on the console are filtered up to and include the configured severity level. You can choose one of the following severity levels: INFO, WARNING, ERROR, or CRITICAL.

To set the severity levels for the system console, perform the following steps.

1. Log in to the switch as admin.
2. Execute the **errFilterSet** [-**d console -v** *severity*] command to set the console severity level. The *severity* can be one of the following: INFO, WARNING, ERROR, or CRITICAL. The *severity* values are not case-sensitive.

   For example, to set the filter severity level for the console to ERROR, enter the following command.

   ```
   switch:admin> errfilterset -d console -v error
   ```

3. Execute the **errFilterSet** command to verify the configured filter settings.

   ```
   switch:admin> errfilterset
   console: filter severity = ERROR
   ```

SNMP trap recipient

An unsolicited message that comes to the management station from the SNMP agent on the device is called a *trap*. When an event occurs and if the event severity level is at or below the set severity level, the SNMP trap, swEventTrap, is sent to the configured trap recipients. The VarBind in the Trap Data Unit contains the corresponding instance of the event index, time information, event severity level, the repeat count, and description. The following are the possible severity levels:

- None (0)
- Critical (1)
- Error (2)
- Warning (3)
- Informational (4)
- Debug (5)

By default, the severity level is set to None, implying all traps are filtered and therefore no event traps are received. When the severity level is set to Informational, all traps with the severity level of Informational, Warning, Error, and Critical are received. For more information on changing the severity level of swEventTrap, refer to "Changing the severity level of swEventTrap" on page 11.

NOTE

The Audit messages are not converted into swEventTrap.

The SNMP traps are unreliable because the trap recipient does not send any acknowledgment when it receives a trap. Therefore, the SNMP agent cannot determine if the trap was received.

Brocade switches send traps out on UDP port 162. To receive traps, the management station IP address must be configured on the switch. You can configure the SNMPv1 and SNMPv3 hosts to receive the traps.

For more information on the swEventTrap, refer to the *Fabric OS MIB Reference*.

Configuring the SNMPv1 trap recipient

Use the **snmpConfig --set snmpv1** command to specify the recipient of the SNMP trap. To configure the SNMPv1 host to receive the trap, perform the following steps.

1. Log in to the switch as admin.
2. Execute the **snmpConfig --set snmpv1** command to configure the SNMP trap recipient.

```
switch:admin> snmpconfig --set snmpv1

SNMP community and trap recipient configuration:
Community (rw): [Secret C0de]
Trap Recipient's IP address : [192.0.2.2]
Trap recipient Severity level : (0..5) [4]
Trap recipient Port : (0..65535) [162]
Community (rw): [OrigEquipMfr]
Trap Recipient's IP address : [fec0:60:22bc:200:313:72ff:fe64:78b2]
```

NOTE

To receive the traps, the management station IP address must be configured on the switch.

3. Execute the **snmpConfig --show snmpv1** command to verify the SNMPv1 agent configuration.

```
switch:admin> snmpconfig --show snmpv1

SNMPv1 community and trap recipient configuration:
  Community 1: Secret C0de (rw)
    Trap recipient: 192.0.2.2
    Trap port: 162
    Trap recipient Severity level: 5
  Community 2: OrigEquipMfr (rw)
    Trap recipient: fec0:60:22bc:200:313:72ff:fe64:78b2
    Trap port: 162
    Trap recipient Severity level: 5
  Community 3: private (rw)
    Trap recipient: tools.lab.brocade.com
    Trap port: 162
    Trap recipient Severity level: 5
  Community 4: public (ro)
    Trap recipient: 192.0.10.10
    Trap port: 65530
    Trap recipient Severity level: 1
  Community 5: common (ro)
    Trap recipient: fec0:60:69bc:200:213:72ff:fe64:069f
    Trap port: 11
    Trap recipient Severity level: 2
  Community 6: FibreChannel (ro)
    Trap recipient: WT.org.brocade.com
    Trap port: 65521
```

```
    Trap recipient Severity level: 2
SNMPv1:Enabled
```

Configuring the SNMPv3 trap recipient

To configure the SNMPv3 host to receive the trap, perform the following steps.

1. Log in to the switch as admin.
2. Execute the **snmpConfig** - -**set snmpv3** command to configure the SNMP trap recipient. Ignore the step to enable the SNMP informs "SNMP Informs Enabled".

```
switch:admin> snmpconfig --set snmpv3

SNMP Informs Enabled (true, t, false, f): [false]

SNMPv3 user configuration(snmp user not configured in FOS user database will
have physical AD and admin role as the default):
User (rw): [snmpadmin1]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]):
(2..2) [2]
User (rw): [snmpadmin2]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]):
(2..2) [2]
User (rw): [snmpadmin3]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]):
(2..2) [2]
User (ro): [snmpuser1]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]):
(2..2) [2]
User (ro): [snmpuser2]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]):
(2..2) [2]
User (ro): [snmpuser3]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]):
(2..2) [2]

SNMPv3 trap recipient configuration:
Trap Recipient's IP address : [192.0.2.2]
UserIndex: (1..6) [1]
Trap recipient Severity level : (0..5) [1]
Trap recipient Port : (0..65535) [35432]
Trap Recipient's IP address : [192.0.10.10]
UserIndex: (1..6) [2]
Trap recipient Severity level : (0..5) [5]
Trap recipient Port : (0..65535) [162]
Trap Recipient's IP address : [192.0.20.20]
[...]
```

NOTE

To receive the SNMP traps, the username, the authentication protocol, the UDP port number, and the privacy protocol must match between the switch and the management station.

3. Execute the **snmpConfig --show snmpv3** command to verify the SNMP agent configuration.

```
switch:admin> snmpconfig --show snmpv3
SNMP Informs = 0 (OFF)
SNMPv3 USM configuration:
User 1 (rw): snmpadmin1
Auth Protocol: noAuth
Priv Protocol: noPriv
User 2 (rw): snmpadmin2
Auth Protocol: MD5
Priv Protocol: noPriv
User 3 (rw): snmpadmin3
Auth Protocol: MD5
Priv Protocol: DES
User 4 (ro): snmpuser1
Auth Protocol: noAuth
Priv Protocol: noPriv
User 5 (ro): snmpuser2
Auth Protocol: noAuth
Priv Protocol: noPriv
User 6 (ro): snmpuser3
Auth Protocol: noAuth
Priv Protocol: noPriv
SNMPv3 Trap configuration:
Trap Entry 1: 192.0.2.2
Trap Port: 162
Trap User: snmpadmin1
Trap recipient Severity level: 1
Trap Entry 2: fe80::224:1dff:fef6:0f21
Trap Port: 162
[...]
```

SNMP inform recipient

An SNMP inform is similar to the SNMP trap except that the management station that receives an SNMP inform acknowledges the system message with an SNMP response packet data unit (PDU). If the sender does not receive the SNMP response PDU, the inform request can be sent again. An SNMP inform request is saved in the switch memory until a response is received or the request times out. The informs are more reliable and they consume more resources in the device and in the network. Use SNMP informs only if it is important that the management station receives all event notifications. Otherwise, use the SNMP traps. Brocade devices support SNMPv3 informs.

Configuring the SNMPv3 inform recipient

To configure the SNMPv3 host to receive the SNMP informs, perform the following steps.

1. Log in to the switch as admin.
2. Execute the **snmpConfig --set snmpv3** command to configure the inform recipient. When prompted to enable the SNMP informs, enter **true** or **t**. Informs are disabled by default.

```
switch:admin> snmpconfig --set snmpv3

SNMP Informs Enabled (true, t, false, f): [false] t

SNMPv3 user configuration(snmp user not configured in FOS user database will
have physical AD and admin role as the default):
User (rw): [snmpadmin1]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
```

```
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]):
(2..2) [2]
Engine ID: [0:0:0:0:0:0:0:0:0]
User (rw): [snmpadmin2]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3] 1
New Auth Passwd:
Verify Auth Passwd:
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]):
(1..6) [2] 1
New Priv Passwd:
Verify Priv Passwd:
Engine ID: [0:0:0:0:0:0:0:0:0] 80:00:05:23:01:0A:23:34:1B
User (rw): [snmpadmin3]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]):
(2..2) [2]
Engine ID: [0:0:0:0:0:0:0:0:0]
User (ro): [snmpuser1]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]):
(2..2) [2]
Engine ID: [0:0:0:0:0:0:0:0:0]
User (ro): [snmpuser2]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]):
(2..2) [2]
Engine ID: [0:0:0:0:0:0:0:0:0]
User (ro): [snmpuser3]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]):
(2..2) [2]
Engine ID: [0:0:0:0:0:0:0:0:0]
SNMPv3 trap recipient configuration:
Trap Recipient's IP address : [0.0.0.0] 192.0.2.2
UserIndex: (1..6) [1]
Trap recipient Severity level : (0..5) [0] 4
Trap recipient Port : (0..65535) [162]
Trap Recipient's IP address : [0.0.0.0] 192.0.10.10
UserIndex: (1..6) [2]
Trap recipient Severity level : (0..5) [0] 4
Trap recipient Port : (0..65535) [162]
Trap Recipient's IP address : [0.0.0.0]
Trap Recipient's IP address : [0.0.0.0]
Trap Recipient's IP address : [0.0.0.0]
Trap Recipient's IP address : [0.0.0.0]
Committing configuration.....done.
```

NOTE

To receive the SNMP informs, the username, the authentication protocol, the privacy protocol, the UDP port number, and the engine ID must match between the switch and the management station.

3. Execute the **snmpConfig --show snmpv3** command to verify the SNMP agent configuration.

```
switch:admin> snmpconfig --show snmpv3
SNMP Informs = 1 (ON)
SNMPv3 USM configuration:
User 1 (rw): snmpadmin1
Auth Protocol: noAuth
```

```
Priv Protocol: noPriv
Engine ID: 80:00:05:23:01:0a:23:34:21
User 2 (rw): snmpadmin2
Auth Protocol: MD5
Priv Protocol: DES
Engine ID: 80:00:05:23:01:0a:23:34:1b
User 3 (rw): snmpadmin3
Auth Protocol: noAuth
Priv Protocol: noPriv
Engine ID: 00:00:00:00:00:00:00:00:00
User 4 (ro): snmpuser1
Auth Protocol: noAuth
Priv Protocol: noPriv
Engine ID: 00:00:00:00:00:00:00:00:00
User 5 (ro): snmpuser2
Auth Protocol: noAuth
Priv Protocol: noPriv
Engine ID: 00:00:00:00:00:00:00:00:00
User 6 (ro): snmpuser3
Auth Protocol: noAuth
Priv Protocol: noPriv
Engine ID: 00:00:00:00:00:00:00:00:00
SNMPv3 Trap configuration:
Trap Entry 1: 192.0.2.2
Trap Port: 162
Trap User: snmpadmin1
Trap recipient Severity level: 4
Trap Entry 2: 192.0.10.10
Trap Port: 162
Trap User: snmpadmin2
Trap recipient Severity level: 4
Trap Entry 3: No trap recipient configured yet
Trap Entry 4: No trap recipient configured yet
Trap Entry 5: No trap recipient configured yet
```

Port logs

The Fabric OS maintains an internal log of all port activity. Each switch or logical switch maintains a log file for each port. Port logs are circular buffers that can save up to 8000 entries per logical switch. When the log is full, the newest log entries overwrite the oldest log entries. Port logs capture switch-to-device, device-to-switch, switch-to-switch, some device A-to-device B, and control information. Port logs are not persistent and are lost over power cycles and reboots.

Execute the **portLogShow** command to display the port logs for a particular port.

Execute the **portLogEventShow** command to display the specific events reported for each port.

Port log functionality is completely separate from the system message log. Port logs are typically used to troubleshoot device connections.

Changing the severity level of swEventTrap

When an event occurs and if the event severity level is at or below the set severity level, the SNMP trap, swEventTrap, is sent to the configured trap recipients. By default, the severity level is set at 0 (None), implying that all the event traps are sent. Use the **snmpConfig --set mibCapability** command to modify the severity level of swEventTrap.

To change the severity level of swEventTrap, perform the following steps.

1. Log in to the switch as admin.
2. Execute the **snmpConfig --set mibCapability** command to configure MIBs interactively. All the supported MIBs and associated traps are displayed. You can change the DesiredSeverity for swEventTrap to 1 (Critical), 2 (Error), 3 (Warning), or 4 (Informational). The default value is 0.

```
switch:admin> snmpconfig --set mibcapability
FE-MIB: YES
SW-MIB: YES
FA-MIB: YES
FICON-MIB: YES
HA-MIB: YES
FCIP-MIB: YES
ISCSI-MIB: YES
IF-MIB: YES
BD-MIB: YES
SW-TRAP: YES
                swFault: YES
                swSensorScn: YES
                swFCPortScn: YES
                swEventTrap: YES
                                DesiredSeverity:Informational
                swFabricWatchTrap: YES
                                DesiredSeverity:None
                swTrackChangesTrap: YES
                swIPv6ChangeTrap: YES
                swPmgrEventTrap: YES
                swFabricReconfigTrap: YES
                swFabricSegmentTrap: YES
                swExtTrap: NO
                swStateChangeTrap: NO
                swPortMoveTrap: NO
                swBrcdGenericTrap: YES

... <lines omitted for brevity>

SW-TRAP (yes, y, no, n): [yes]
                swFault (yes, y, no, n): [yes]
                swSensorScn (yes, y, no, n): [yes]
                swFCPortScn (yes, y, no, n): [yes]
                swEventTrap (yes, y, no, n): [yes]
                                DesiredSeverity: (0..4) [4] 3
                swFabricWatchTrap (yes, y, no, n): [yes]
                                DesiredSeverity: (0..4) [0] 2
                swTrackChangesTrap (yes, y, no, n): [yes]
                swIPv6ChangeTrap (yes, y, no, n): [yes]
                swPmgrEventTrap (yes, y, no, n): [yes]
[...]
```

3. Execute the **snmpConfig --show mibCapability** command to verify the severity level of swEventTrap.

```
switch:admin> snmpconfig --show mibcapability
FE-MIB: YES
SW-MIB: YES
FA-MIB: YES
FICON-MIB: YES
HA-MIB: YES
FCIP-MIB: YES
ISCSI-MIB: YES
```

```
IF-MIB: YES
BD-MIB: YES
SW-TRAP: YES
           swFault: YES
           swSensorScn: YES
           swFCPortScn: YES
           swEventTrap: YES
                            DesiredSeverity:Informational
           swFabricWatchTrap: YES
                            DesiredSeverity:Critical
           swTrackChangesTrap: YES
           swIPv6ChangeTrap: YES
           swPmgrEventTrap: YES
           swFabricReconfigTrap: YES
[...]
```

Commands for displaying and configuring the system message logs

Table 3 describes commands that you can use to view or configure the system message logs. Most commands require the admin access level. For detailed information on required access levels and commands, refer to the *Fabric OS Command Reference*.

TABLE 3 Commands for viewing or configuring the system parameters and message logs

Command	Description
auditCfg	Configures the audit message log.
auditDump	Displays or clears the audit log.
errClear	Clears all error log messages for all switch instances on this control processor (CP).
errDelimiterSet	Sets the error log start and end delimiter for messages pushed to the console.
errDump	Displays the entire error log, without page breaks. Use the -r option to show the messages in reverse order, from newest to oldest.
errFilterSet	Sets an error severity filter for the system console.
errModuleShow	Displays all the defined error log modules.
errShow	Displays the entire error log, with page breaks. Use the -r option to show the messages in reverse order, from newest to oldest.
pdShow	Displays the contents of the panic dump and core dump files.
portErrShow	Displays the port error summary.
portLogClear	Clears the port log. If the port log is disabled, this command enables it.
portLogDisable	Disables the port log facility.
portLogDump	Displays the port log, without page breaks.
portLogDumpPort	Displays the port log of the specified port, without page breaks.
portLogEnable	Enables the port log facility.
portLogEventShow	Displays which port log events are currently being reported.
portLoginShow	Displays port logins.
portLogPdisc	Sets or clears the debug pdisc_flag.
portLogReset	Enables the port log facility.

TABLE 3 Commands for viewing or configuring the system parameters and message logs (Continued)

Command	Description
portLogResize	Resizes the port log to the specified number of entries.
portLogShow	Displays the port log, with page breaks.
portLogShowPort	Displays the port log of the specified port, with page breaks.
portLogTypeDisable	Disables an event from reporting to the port log. Port log events are described by the **portLogEventShow** command.
portLogTypeEnable	Enables an event to report to the port log. Port log events are described by the **portLogEventShow** command.
rasAdmin	Used to enable or disable logging for selected messages or modules, to change the default severity level for a specified message, and to display configured RASLog message settings.
rasMan	Displays message documentation on switch.
setVerbose	Sets the verbose level of a particular module within the Fabric OS.
snmpConfig	Manages the SNMP agent configuration.
supportFfdc	Enables and disables FFDC.
supportFtp	Sets, clears, or displays support FTP parameters or a time interval to check the FTP server.
supportSave	Collects RASLog, trace files, and **supportShow** (active CP only) information for the local CP and then transfers the files to an FTP server. The operation can take several minutes.
supportShow	Executes a list of diagnostic and error display commands. This output is used by your switch service provider to diagnose and correct problems with the switch. The output from this command is very long. Refer to the following related commands: • **supportShowCfgShow** - Displays the groups of commands enabled for display by the **supportShow** command. • **supportShowCfgEnable** - Enables a group of commands to be displayed under the **supportShow** command. • **supportShowCfgDisable** - Disables a group of commands under the **supportShow** command.
syslogdFacility	Changes the syslogd facility.
syslogdIpAdd	Adds an IP address as a recipient of system messages.
syslogdIpRemove	Removes an IP address as a recipient of system messages.
syslogdIpShow	Views the currently configured IP addresses that are recipients of system messages.
traceDump	Displays, initiates, or removes a Fabric OS module trace dump.

Displaying message content on switch

You can view the message documentation such as the message text, message type, class (for audit messages), message severity, cause, and action on the switch console by using the **rasMan** *message_ID* command.

To display the message documentation on switch, perform the following steps.

1. Log in to the switch as admin.
2. Use the **rasMan** *message_ID* command to display the documentation of a message. The *message_ID* values are case-sensitive.

   For example, execute the following command to display the documentation for PS-1007.

```
switch:admin> rasman PS-1007
Log Messages                                        PS-1007(7m)


MESSAGE
     PS-1007  -  Failed  to  add   Fabricmode   Top   Talker   on
     domain=<domain id>. <function name>.

MESSAGE TYPE
     LOG

SEVERITY
     WARNING

PROBABLE CAUSE
     Indicates that FC Routing (FCR) is enabled on the  specified
     fabric.

RECOMMENDED ACTION
     Top Talker cannot be installed on a fabric with FCR  service
     enabled.  In  case Top Talker must be installed on a fabric,
     disable FCR using the fosconfig --disable fcr command.
```

Configuring system messages and attributes

This section provides information on configuring the system message logs and its attributes. All admin-level commands mentioned in this section are used to enable or disable only the external messages.

Configuring event auditing

To configure event auditing, perform the following steps.

1. Log in to the switch as admin.
2. Execute the **auditCfg** --**enable** command to enable the audit feature.

```
switch:admin> auditcfg --enable
Audit filter is enabled.
```

3. Execute the **auditCfg** --**class** command to configure the event classes you want to audit.

```
switch:admin> auditcfg --class 1,2,3,4,5,6,7,8,9
Audit filter is configured.
```

   NOTE
   The RAS audit class is not configurable, and it is always enabled internally.

4. Execute the **auditCfg** --**severity** *severity level* command if you want to set the Audit severity level. By default, all messages are logged. When the severity is set, only messages with the configured severity and higher are displayed. Valid values for *severity level* are INFO, WARNING, ERROR, and CRITICAL

```
switch:admin> auditcfg --severity ERROR
```

5. Execute the **auditCfg** - -**show** command to verify the configuration.

```
switch:admin> auditcfg --show
Audit filter is enabled.
1-ZONE
2-SECURITY
3-CONFIGURATION
4-FIRMWARE
5-FABRIC
6-FW
7-LS
8-CLI
9-MAPS
Severity level: ERROR
```

You must configure the syslog daemon to send the Audit events to a configured remote host using the **syslogdIpAdd** command. For more information on configuring the syslog server, refer to "Configuring a syslog server" on page 5.

Disabling a RASLog message or module

To disable a single RASLog message or all messages in a module, perform the following steps.

1. Log in to the switch as admin.
2. Use the following commands to disable a single RASLog message or all messages that belong to a module:
   - Execute the **rasadmin** --**disable -log** *messgae_ID* command to disable a RASLog message. For example, execute the following command to disable the BL-1001 message.

     ```
     switch:admin> rasadmin --disable -log BL-1001
     2012/07/20-13:30:41, [LOG-1005], 378, SLOT 4 | CHASSIS, INFO, switch, Log
     message NSM-1009 has been disabled.
     ```

     Use the **rasadmin** --**show -log** *messgae_ID* command to verify the status of the message.
   - Execute the **rasadmin** --**disable -module** *module_ID* command to disable all messages in a module. For example, execute the following command to disable all messages that belong to the BL module.

     ```
     switch:admin> rasadmin --disable -module BL
     2012/07/20-13:28:37, [LOG-1007], 375, SLOT 4 | CHASSIS, INFO, switch, Log
     Module BL has been disabled.
     ```

     Use the **rasadmin** --**show -module** *module_ID* command to verify the status of the messages that belong to a module.

NOTE

You cannot disable Audit and FFDC messages using the **rasAdmin** command.

Enabling a RASLog message or module

To enable a single RASLog message or all messages in a module that were previously disabled, perform the following steps.

1. Log in to the switch as admin.
2. Use the following commands to enable a single RASLog message or all messages that belong to a module:
   - Execute the **rasadmin --enable -log** *messgae_ID* command to enable a single RASLog message that has been disabled.

     For example, execute the following command to enable BL-1001 message that was previously disabled.

     ```
     switch:admin> rasadmin --enable -log BL-1001
     2012/10/15-13:24:30, [LOG-1006], 373, SLOT 4 | CHASSIS, INFO, switch, Log
     message BL-1001 has been enabled.
     ```

     Use the **rasadmin --show -log** *messgae_ID* command to verify the status of the message.
   - Execute the **rasadmin --enable -module** *module_ID* command to enable all messages in a module. For example, execute the following command to enable to all previously disabled BL messages.

     ```
     switch:admin> rasadmin --enable -module BL
     2012/10/15-13:28:37, [LOG-1007], 375, SLOT 4 | CHASSIS, INFO, switch, Log
     Module BL has been enabled.
     ```

     Use the **rasadmin --show -module** *module_ID* command to verify the status of the messages that belong to a module.

Setting the severity level of a RASLog message

To change the default severity level of a RASLog message, perform the following steps.

1. Log in to the switch as admin.
2. Use the **rasadmin --set -log** *message_ID* **-severity** [**DEFAULT** | **INFO** | **WARNING** | **ERROR** | **CRITICAL**] to change the severity level of a message. For example, execute the following command to change the severity level of C2-1004 message to WARNING.

   ```
   switch:admin> rasadmin --set -log C2-1004 -severity WARNING
   ```
3. Use the **rasadmin --show -severity** *message_ID* command to verify the severity of the message.

   ```
   switch:admin> rasadmin --show -severity C2-1004
   Message       Severity
    C2-1004 :   WARNING
   ```

Displaying system message logs and attributes

This section provides information on displaying the system message logs. These procedures are valid for all the supported platforms.

Displaying RASLog messages

To display the system message log on a switch with no page breaks, perform the following steps. You can display the messages in reverse order using the **reverse** option. To display message logs in all switches (logical switches), use the **all** option.

1. Log in to the switch as admin.
2. Enter the **errDump** command at the command line.

```
switch:admin> errdump
Version: v7.2.0

2000/12/17-05:54:30, [HAM-1004], 1, CHASSIS, INFO, switch, Processor rebooted
- Reset

2000/12/17-05:55:04, [ZONE-1034], 2, FID 128, INFO, switch, A new zone
database file is created.

2000/12/17-05:55:04, [FCR-1069], 3, FID 128, INFO, switch, The FC Routing
service is enabled.

2000/12/17-05:55:04, [FCR-1068], 4, FID 128, INFO, switch, The FC Routing
service is disabled.

2000/12/17-05:55:11, [EM-1034], 5, CHASSIS, ERROR, switch, PS 2 set to faulty,
rc=2000e.
[...]
```

Displaying RASLog messages one message at a time

To display the system message log one message at a time, perform the following steps.

1. Log in to the switch as admin.
2. Enter the **errShow** command at the command line.

```
switch:admin> errshow
Version: v7.2.0

2011/11/11-05:54:30, [HAM-1004], 1, CHASSIS, INFO, switch, Processor rebooted
- Reset

Type <CR> to continue, Q<CR> to stop:

2011/11/11-05:55:04, [ZONE-1034], 2, FID 128, INFO, switch, A new zone
database file is created.

Type <CR> to continue, Q<CR> to stop:

2011/11/11-05:55:04, [FCR-1069], 3, FID 128, INFO, switch, The FC Routing
service is enabled.

Type <CR> to continue, Q<CR> to stop:
[...]
```

Displaying Audit messages

To display the Audit messages, perform the following steps. Beginning with Fabric OS v7.1.0 release, the RAS-3005 message is generated for each CLI command executed on switch and is saved in the Audit message log.

1. Log in to the switch as admin.
2. Enter the **auditDump -s** command at the command line.

```
switch:admin> auditdump -s

0 AUDIT, 2011/01/14-06:06:49 (UTC), [RAS-2001], INFO, SYSTEM,
admin/admin/192.0.2.2/telnet/CLI, ad_0/switch/FID 128, , Audit message log is
enabled.

2 AUDIT, 2011/01/14-06:07:03 (UTC), [SEC-3020], INFO, SECURITY,
admin/admin/192.0.2.2/telnet/CLI ad_0/switch, , Event: login, Status: success,
Info: Successful login attempt via SERIAL.

3 AUDIT, 2011/01/14-06:07:33 (UTC), [SULB-1003], INFO, FIRMWARE,
admin/admin/192.0.2.2/telnet/CLI ad_0/switch, , Firmwarecommit has started.

4 AUDIT, 2011/12/11-10:08:58 (UTC), [SULB-1004], INFO, FIRMWARE,
admin/admin/192.0.2.2/telnet/CLI ad_0/switch, , Firmwarecommit has completed.

5 AUDIT, 2012/05/23-03:45:15 (UTC), [RAS-3005], INFO, CLI,
admin/admin/NONE/console/CLI, ad_0/switch/CHASSIS, , CLI: clihistory --all

6 AUDIT, 2012/05/23-04:12:04 (UTC), [RAS-3005], INFO, CLI,
admin/admin/NONE/console/CLI, ad_0/switch/CHASSIS, , CLI: auditdump -s
[...]
```

Displaying FFDC messages

To display the saved FFDC messages, perform the following steps.

1. Log in to the switch as admin.
2. Enter the **errDump --attribute FFDC** command at the command line.

```
switch:admin> errDump --attribute FFDC
Fabric OS: v7.2.0

2012/10/15-10:39:02, [LOG-1002], 4496, FFDC, WARNING, switch, A log
message was not recorded.

2012/10/15-10:39:18, [RAS-1001], 4496, FFDC, WARNING, switch, First
failure data capture (FFDC) event occurred.
[...]
```

Displaying status of the system messages

To display the status of the system message, perform the following steps.

1. Log in to the switch as admin.
2. Use the following commands to display the status of all messages in the log, a single message, or all messages that belong to a module:
   - Execute the **rasadmin --show -all** command to the status of all RASLog messages in the system log.

     ```
     switch:admin> rasadmin --show -all
     Message      Status    Default Severity    Current Severity
      FCIP-1000   ENABLED   CRITICAL            CRITICAL
      FCIP-1001   ENABLED   INFO                ERROR
      FCIP-1002   ENABLED   INFO                INFO
     [...]
     ```

   - Execute the **rasadmin --show -log** *message_ID* command to display the status of a single RASLog message.

     ```
     switch:admin> rasadmin --show -log IPAD-1002
     Message      Status     Default Severity    Current Severity
      IPAD-1002   DISABLED   INFO                INFO
     ```

   - Execute the **rasadmin --show -module** *module_ID* command to display the status of all messages that belong to the module.

     ```
     switch:admin> rasadmin --show -module ECC
     Message    Status    Default Severity    Current Severity
      ECC-1000  ENABLED   ERROR               ERROR
      ECC-1001  DISABLED  ERROR               WARNING
     ```

   - Execute the **rasadmin --show -disabled** command to display the list of all RASLog messages that are disabled.

     ```
     switch:admin> rasadmin --show -disabled
     Message                  Status
      CDR-1001       :        DISABLED
      CDR-1003       :        DISABLED
      CDR-1004       :        DISABLED
      ECC-1001       :        DISABLED
      IPAD-1002      :        DISABLED
     ```

Displaying the severity level of RASLog messages

To display the severity level of a RASLog message, perform the following steps.

1. Log in to the switch as admin.
2. Use the **rasadmin --show -severity** *message_ID* command to display the severity level of a RASLog message. For example, execute the following command to display the status of the SEC-1203 message.

   ```
   switch:admin> rasadmin --show -severity SEC-1203
   Message        Severity
   SEC-1203 :     WARNING
   ```

Displaying RASLog messages by severity level

To display the RASLog messages based on the severity level, perform the following steps.

1. Log in to the switch as admin.
2. Execute the **errdump** --**severity** [**DEFAULT** | **INFO** | **WARNING** | **ERROR** | **CRITICAL**] command. For more information on message severity levels, refer to "Message severity levels" on page 3. You can set the count of messages to display using the **count** option. The following example filters messages by severity level of ERROR.

```
switch:admin> errdump --count 4 --severity ERROR
Fabric OS: v7.2.0
2012/10/24-11:23:24, [C3-1001], 12, CHASSIS, ERROR, switch, Port 4 failed due
to SFP validation failure. Check if the SFP is valid for the configuration.

2012/10/24-11:23:24, [C3-1001], 13, CHASSIS, ERROR, switch, Port 5 failed due
to SFP validation failure. Check if the SFP is valid for the configuration.

2012/10/24-11:23:25, [C3-1001], 14, CHASSIS, ERROR, switch, Port 18 failed due
to SFP validation failure. Check if the SFP is valid for the configuration.

2012/10/24-11:46:14, [C3-1001], 27, CHASSIS, ERROR, switch, Port 4 failed due
to SFP validation failure. Check if the SFP is valid for the configuration.
```

Displaying RASLog messages by message ID

To display the RASLog messages based on the message ID, perform the following steps.

1. Log in to the switch as admin.
2. Execute the **errdump** --**message** *message_ID* command. The following example displays all instances of the message HAM-1004.

```
switch:admin> errdump --message HAM-1004
Fabric OS: v7.2.0
2012/11/27-16:18:38, [HAM-1004], 1, CHASSIS, INFO, switch, Processor rebooted
- Reset.

2012/11/27-17:26:44, [HAM-1004], 90, CHASSIS, INFO, switch, Processor rebooted
- FirmwareDownload.

2012/11/27-21:06:25, [HAM-1004], 201, CHASSIS, INFO, switch, Processor
rebooted - FirmwareDownload.
[...]
```

Displaying messages on a slot

To display the saved messages for a specific slot, perform the following steps.

1. Log in to the switch as admin.
2. Execute the **errdump** --**slot** *slot_num* command.

```
switch:admin> errdump --slot 4
Fabric OS: v7.2.0

2012/06/19-03:26:44, [HAM-1004], 31, SLOT 4 | CHASSIS, INFO, switch, Processor
rebooted - Reboot.
```

```
2012/06/19-03:26:44, [SULB-1003], 32, SLOT 4 | CHASSIS, INFO, switch,
Firmwarecommit has started.

2012/06/19-03:26:44, [IPAD-1001], 33, SLOT 4 | CHASSIS, INFO, switch, CP/1
IPv6 manual fe80::224:38ff:fe1b:4400 DHCP Off.

2012/06/19-03:29:15, [IPAD-1000], 48, SLOT 4 | CHASSIS, INFO, switch, CP/0
Ether/0 IPv6 autoconf fd00:60:69bc:816:205:1eff:fe84:3f49/64 tentative DHCP
Off.
[...]
```

NOTE

The **slot** option is not supported on the non-bladed systems.

Viewing RASLog messages from Web Tools

To view the system message log for a switch from Web Tools, perform the following steps.

1. Launch Web Tools.
2. Select the desired switch from the Fabric Tree. The Switch View displays.
3. Click the **Switch Events** tab. You can view the switch events and messages in the Switch Events Report displayed.

In dual-domain switches, an **Event** button exists for each logical switch. Only messages relating to that switch (and chassis) will be displayed.

Clearing the system message logs

This section provides information on clearing the system message logs. These procedures are valid for all the supported platforms.

Clearing the system message log

To clear the system message log for a particular switch instance, perform the following steps.

1. Log in to the switch as admin.
2. Execute the **errClear** command to clear all messages from memory.

NOTE

For products that have a single processor, all error log messages are cleared. For products that have multiple processors, this command only clears the error logs of the processor from which it is executed.

Clearing the Audit message log

To clear the Audit message log for a particular switch instance, perform the following steps.

1. Log in to the switch as admin.
2. Execute the **auditDump -c** command to clear all Audit messages from memory.

Reading the system messages

This section provides information about reading the RASLog and Audit messages.

Reading a RAS system message

This section provides information about reading system messages.

The following example shows the format of a RAS system error message.

```
<timestamp>, [<Event ID>], <Sequence Number>, <Flags>, <Severity>, <Switch name>,
<Event-specific information>
```

The following example shows a sample message from the error log.

```
2011/02/10-14:18:04, [SS-1000], 88, SLOT 6 | FFDC | CHASSIS, INFO, ESNSVT_DCX,
supportSave has uploaded support information to the host with IP address
192.0.2.2.
```

```
2011/02/10-14:13:34, [SS-1001], 87, SLOT 6/1 | FFDC | CHASSIS, WARNING,
ESNSVT_DCX, supportSave's upload operation to host IP address aborted.
```

```
2011/02/10-15:44:51, [SEC-1203], 89, SLOT 6 | FFDC | FID 128, INFO, ESNSVT_DCX,
Login information: Login successful via TELNET/SSH/RSH. IP Addr:192.0.2.2.
```

NOTE

Any reference to slot 0 in a system message is a reference to the blade within the switch platform, for example, Brocade DCX contains FC8-48 blade, FC8-32 blade, FC8-16 blade, and so on.

The fields in the error message are described in Table 4.

TABLE 4 System message field description

Variable name	Description
Time Stamp	The system time (UTC) when the message was generated on the switch. The RASLog subsystem supports an internationalized time stamp format based on the “LOCAL” setting.
Event ID	The message module and number. These values uniquely identify each message in the Fabric OS and reference the cause and actions recommended in this manual. Note that not all message numbers are used; there can be gaps in the numeric message sequence.

TABLE 4 System message field description (Continued)

Variable name	Description
Sequence Number	The error message position in the log. When a new message is added to the log, this number is incremented by 1. The message sequence number starts at 1 after a **firmwareDownload** and will increase up to a value of 2,147,483,647 (0x7ffffff). The sequence number continues to increase after the message log wraps around, i.e. the oldest message in the log is deleted when a new message is added. The sequence number can be reset to 1 using the **errClear** command. The sequence number is persistent across power cycles and switch reboots.
Flags	For most messages, this field contains a space character (null value) indicating that the message is neither an AUDIT or FFDC message. Messages may contain the following values: • FFDC – Indicates that additional first failure data capture information has also been generated for this event. • FID – The Fabric ID that can range from 0 to 128. FID 128 means the message was generated by the default switch instance. • CHASSIS – The message that was generated by the chassis instance. • SLOT number – Indicates the message was generated from slot # blade main CPU. • SLOT #/1 – Indicates the message was generated from slot # blade Co-CPU.
Severity Level	The severity of the error, which can be one of the following: • 1 – CRITICAL • 2 – ERROR • 3 – WARNING • 4 – INFO
Switch name	The defined switch name or the chassis name of the switch depending on the action; for example, high availability (HA) messages typically show the chassis name, and login failures show the logical switch name. This value is truncated if it exceeds 16 characters in length. Run either the **chassisName** command to name the chassis or the **switchName** command to rename the logical switch.
Event-specific information	A text string explaining the error encountered and providing parameters supplied by the software at runtime.

Reading an Audit message

Compared to RASLog error messages, messages flagged as AUDIT provide additional user and system-related information of interest for post-event auditing and troubleshooting the problem.

The following example shows the format of the Audit event message.

```
<Sequence Number> AUDIT, <timestamp>, [<Event ID>], <Severity>, <Event Class>,
<User ID>/<Role>/<IP address>/<Interface>/<Application Name>, <Admin
Domain>/<Switch name>, <Reserved field for future expansion>, <Event-specific
information>
```

For the syslog audit messages, the Fabric OS version and 6 reserved fields will be displayed in the message.

The following is a sample Audit event message.

```
0 AUDIT, 2005/12/10-09:54:03, [SEC-1000], WARNING, SECURITY,
JohnSmith/root/192.0.2.2/Telnet/CLI, Domain A/JohnsSwitch, , Incorrect password
during login attempt.
```

The fields in the error message are described in Table 5.

TABLE 5 Audit message field description

Variable name	Description
Sequence Number	The error message position in the log.
Audit flag	Identifies the message as an Audit message.
Time Stamp	The system time (UTC) when the message was generated on the switch. The RASLog subsystem will support an internationalized time stamp format based on the "LOCAL" setting.
Event ID	The message module and number. These values uniquely identify each message in the Fabric OS and reference the cause and actions recommended in this manual. Note that not all message numbers are used; there can be gaps in the numeric message sequence.
Severity	The severity of the error, which can be one of the following: • 1 – CRITICAL • 2 – ERROR • 3 – WARNING • 4 – INFO
Event Class	The event class, which can be one of the following: • CFG • CLI • FABRIC • FIRMWARE • FW • LS • MAPS • RAS • SECURITY • ZONE
User ID	The user ID.
Role	The role of the user ID.
IP address	The IP address.
Interface	The interface being used.
Application Name	The application name being used on the interface.
Admin Domain	The Admin Domain, if there is one.
Switch name	The defined switch name or the chassis name of the switch depending on the action; for example, HA messages typically show the chassis name and login failures show the logical switch name. This value is truncated if it is over 16 characters in length. Execute the **chassisName** command to name the chassis or the **switchName** command to rename the logical switch.

TABLE 5 Audit message field description (Continued)

Variable name	Description
Reserved field for future expansion	This field is reserved for future use and contains a space character (null value).
Event-specific information	A text string explaining the error encountered and providing parameters supplied by the software at runtime.

Responding to a system message

This section provides procedures on gathering information on system messages.

Looking up a system message

Messages in this manual are arranged alphabetically by Module ID, and then numerically within a given module. To look up a message, copy down the module (see Table 6) and the error code and compare this with the Table of Contents or look up lists to determine the location of the information for that message.

The following information is provided for each message:

- Module and code name for the error
- Message text
- Message type
- Class (for Audit messages only)
- Message severity
- Probable cause
- Recommended action

Gathering information about the problem

Questions to ask yourself when troubleshooting a system message are as follows:

- What is the current Fabric OS level?
- What is the switch hardware version?
- Is the switch operational?
- Assess impact and urgency:
  - Is the switch down?
  - Is it a standalone switch?
  - How large is the fabric?
  - Is the fabric redundant?
- Execute the **errDump** command on each logical switch.
- Execute the **supportFtp** command (as needed) to set up automatic FTP transfers, and then run the **supportSave** command.

- Document the sequence of events by answering the following questions:
  - What happened just prior to the problem?
  - Is the problem repeatable?
  - If so, what are the steps to produce the problem?
  - What configuration was in place when the problem occurred?
- Did a failover occur?
- Was security enabled?
- Was POST enabled?
- Are serial port (console) logs available?
- Which CP was master?
- What and when were the last actions or changes made to the system?

Common steps to be followed when troubleshooting a system message are as follows:

- Execute the **errDump** command on each logical switch.
- Execute the **supportFtp** command (as needed) to set up automatic FTP transfers, and then execute the **supportSave** command.

Support

Fabric OS creates a number of files that can help support personnel troubleshoot and diagnose a problem. This section describes those files and how to access or save the information for support personnel.

Panic dump and core dump files

The Fabric OS creates panic dump files and core files when there are problems in the Fabric OS kernel. You can view panic dump files using the **pdShow** command. These files can build up in the kernel partition (typically because of failovers) and might need to be periodically deleted or downloaded using the **supportSave** command.

The software watchdog process (SWD) is responsible for monitoring daemons critical to the function of a healthy switch. The SWD holds a list of critical daemons that ping the SWD periodically at a predetermined interval defined for each daemon. The ping interval is set at 133 seconds, with the exception of the Fabric Watch daemon and the IP storage demon, which ping the SWD every 333 seconds. (For a complete listing of daemons, refer to the KSWD entry in Table 6.)

If a daemon fails to ping the SWD within the defined interval, or if the daemon terminates unexpectedly, then the SWD dumps information to the panic dump files, which helps to diagnose the root cause of the unexpected failure.

Execute the **pdShow** command to view these files or the **supportSave** command to send them to a host workstation using FTP. The panic dump files and core files are intended for support personnel use only.

Trace dumps

The Fabric OS produces trace dumps when problems are encountered within Fabric OS modules. The Fabric OS trace dump files are intended for support personnel use only. You can use the **supportSave** or **supportFTP** commands to collect trace dump files to a specified remote location to provide to support when requested. Trace dump must be enabled and set up on the switch to detect the first event. Note that there is only one trace buffer on a switch.

supportSave command

The **supportSave** command can be used to send the output of the system messages (RASLog), the trace files, and the output of the **supportShow** command to an off-switch storage location through FTP. Prior to running the **supportSave** command, you can optionally set up the FTP parameters using the **supportFtp** command. The **supportShow** command runs a large number of dump and show commands to provide a global output of the status of the switch. After the supportsave operation is completed, you must execute the **supportSave -R** command to remove all unwanted files. Refer to the *Fabric OS Command Reference* for more information on these commands.

System module descriptions

Table 6 provides a summary of the system modules for which messages are documented in this guide; the system modules are listed alphabetically by name. A module is a subsystem in the Fabric OS. Each module generates a set of numbered messages.

TABLE 6 System module descriptions

System module	Description
AG	Access Gateway (AG) allows multiple hosts (or HBAs) to access the fabric using fewer physical ports. Access Gateway mode transforms the Brocade switches as well as embedded switches into a device management tool that is compatible with different types of fabrics, including Brocade-, Cisco-, and McDATA-based fabrics.
AN	Error or warning messages from the Bottleneck Detection module, including notification of detected bottlenecks.
ANV	ANV error messages indicate problems with the driver that deal with the ENET application-specific integrated circuits (ASICs) on the Fabric OS. They can be software- or hardware-related errors.
AUTH	Authentication error messages indicate problems with the authentication module of the Fabric OS.
BKSW	BKSW messages are generated by the Fabric OS blade kernel software watchdog module.
BL	BL error messages are a result of faulty hardware, transient out-of-memory conditions, ASIC errors, or inconsistencies in the software state between a blade and the environment monitor (EM) module.
BLS	Fibre Channel over IP port configuration messages over the Brocade 7800 and FX8-24 blade.
BM	Blade management error messages are a result of autoleveling firmware upgrades performed by the control processor (CP).
C2	C2 error messages indicate problems with the 8 Gbps-capable FC module of the Fabric OS.
C3	C3 error messages indicate problems with the 16 Gbps-capable FC module of the Fabric OS.
CAL	Common Access Layer (CAL) provides XML interface for configuring switch parameters in an object model.

TABLE 6 System module descriptions (Continued)

System module	Description
CCFG	CCFG error messages indicate problems with the Converged Enhanced Ethernet (CEE) configuration module of the Fabric OS.
CDR	Driver error messages.
CHS	Error messages reporting the problems in the management of the blades in the different slots of the chassis.
CNM	Cluster Node Manager (CNM) is a software daemon module of the Fabric OS. The messages from CNM are problems encountered by CNM, warnings, or information to the user of events.
CONF	Status messages for **configUpload** and **configDownload** operations.
CTAP	A user-space daemon that forwards non-performance-critical messages from the TAPE driver to the Crypto Virtual LUN Controller (CVLC) and Security Processor (SP), and vice versa. This module also maintains a cache of recently acquired keys, reducing requests to the key vault itself.
CVLC	Crypto Virtual LUN Controller (CVLC) is a software module running on blade FOS (BFOS). The messages of CVLC are problems encountered by CVLC, warnings to alert the user, or information to the user.
CVLM	Crypto Virtual LUN Manager (CVLM) is a software module of the Fabric OS. The messages of CVLM are problems encountered by CVLM, warnings to alert the user, or information to the user.
DOT1	DOT1 error messages indicate problems with the 802.1x authentication module of the Fabric OS.
ECC	Error Checking and Correction (ECC) error messages indicate single-bit and multiple-bit errors in the Dynamic Random Access Memory (DRAM) devices. ECC is a technology that helps to correct memory errors.
EM	The environmental monitor (EM) manages and monitors the various field-replaceable units (FRUs), including the port cards, control processor (CP) blades, blower assemblies, power supplies, and World Wide Name (WWN) cards. EM controls the state of the FRUs during system startup, hot-plug sequences, and fault recovery. EM provides access to and monitors the sensor and status data from the FRUs and maintains the integrity of the system using the environmental and power policies. EM reflects system status by CLI commands, system light emitting diodes (LEDs), and status and alarm messages. EM also manages some component-related data.
ESS	Exchange Switch Support (ESS) error messages indicate problems with the ESS module of the Fabric OS. ESS is an SW_ILS mechanism utilized by switches to exchange vendor and support information.
ESW	ESW error messages indicate problems with the Ethernet switch module of Fabric OS.
EVMD	EVMD is the event management module.
FABR	FABRIC refers to a network of Fibre Channel switches. The FABR error messages come from the fabric daemon. The fabric daemon follows the FC-SW-3 standard for the fabric initialization process, such as determining the E_Ports, assigning unique domain IDs to switches, creating a spanning tree, throttling the trunking process, and distributing the domain and alias lists to all switches in the fabric.
FABS	Fabric OS system driver module.
FBC	Firmware blade compatibility errors with the control processor (CP).
FCMC	Fibre Channel miscellaneous messages relate to problems with the physical layer used to send Fibre Channel traffic to and from the switch.
FCOE	FCoE error messages indicate problems with the FCoE module of the Fabric OS.

TABLE 6 System module descriptions (Continued)

System module	Description
FCPD	The Fibre Channel Protocol daemon is responsible for probing the devices attached to the loop port. Probing is a process the switch uses to find the devices attached to the loop ports and to update the Name Server with the information.
FCPH	The Fibre Channel Physical Layer is used to send Fibre Channel traffic to and from the switch.
FCR	Fibre Channel router-related traffic and activity on the fabric or back-end fabric.
FICN	The FICN messages are generated during FICON emulation processing on an FCIP Tunnel.
FICU	The FICON-CUP daemon handles communication with fibre connectivity (FICON) on IBM FICON storage devices. Errors to this module are usually initiation errors or indications that FICON-CUP prerequisites have not been met, such as a license key, core process ID (PID), and secure mode on the fabric.
FKLB	Fabric OS I/O kernel library module.
FLOD	FLOD is a part of the Fabric Shortest Path First (FSPF) protocol that handles synchronization of the link state database (LSDB) and propagation of the link state records (LSRs).
FSPF	Fabric Shortest Path First (FSPF) is a link state routing protocol that is used to determine how frames should be routed. These messages are about protocol errors.
FSS	The Fabric OS state synchronization framework provides facilities by which the active control processor (CP) can synchronize with the standby CP, enabling the standby CP to take control of the switch nondisruptively during failures and software upgrades. These facilities include version negotiation, state information transfer, and internal synchronization functions, enabling the transition from standby to active operation. FSS is defined both as a component and a service. A *component* is a module in the Fabric OS, implementing a related set of functionality. A *service* is a collection of components grouped together to achieve a modular software architecture.
FSSM	The Fabric OS state synchronization management module is defined both as a component and a service. A *component* is a module in Fabric OS, implementing a related set of functionality. A *service* is a collection of components grouped together to achieve a modular software architecture.
FV	Flow Vision is a network diagnostic tool that allows you to simulate, monitor, and capture the network traffic pattern to validate the connectivity, performance, and hardware components. FV messages indicate operations associated with a flow in Flow Vision.
FW	FW is the Fabric Watch module. This module monitors thresholds for many switch subsystems; for example, temperature, voltage, fan speed, and switch status. Any changes that cross a specified threshold are reported to the system message log.
HAM	HAM is a user-space daemon responsible for high availability management.
HAMK	This is the kernel module for the high availability management (HAM) daemon.
HIL	Hardware independent layer.
HLO	HLO is a part of the Fabric Shortest Path First (FSPF) protocol that handles the HELLO protocol between adjacent switches. The HELLO protocol is used to establish connectivity with a neighbor switch, to establish the identity of the neighbor switch, and to exchange FSPF parameters and capabilities.
HMON	Health monitor.
HSL	HSL error messages indicate problems with the Hardware Subsystem Layer of the Fabric OS.
HTTP	HTTP error messages.
IBD	IBD generates messages related to port restart failure.

TABLE 6 System module descriptions (Continued)

System module	Description
IPAD	System messages generated by the IP admin demon.
IPS	Fibre Channel over IP license, tunneling, and port-related messages.
ISNS	ISNS server and client status messages.
KAC	KAC error messages indicate problems associated with Fabric OS and the external key vaults.

TABLE 6 System module descriptions (Continued)

System module	Description
KSWD	The kernel software watchdog (KSWD) watches daemons for unexpected terminations and “hang” conditions and informs the HAM module to take corrective actions such as failover or reboot. The following daemons are monitored by KSWD: • Access Gateway daemon (agd) • Alias Server daemon (asd) • ARR daemon (arrd) • Authentication daemon (authd) • Blade Manager daemon (bmd) • Cluster Node Manager daemon (cnmd) • Common Access Layer daemon (cald) • DAUTH daemon (dauthd) • Diagnostics daemon (diagd) • Environment Monitor daemon (emd) • Event Manager daemon (evmd) • Exchange Switch Support daemon (essd) • FA-API rpc daemon (rpcd) • Fabric daemon (fabricd) • Fabric Device Management Interface daemon (fdmid) • Fabric Watch daemon (fwd) • FCoE daemon (fcoed) • Fibre Channel Protocol daemon (fcpd) • FICON CUP daemon (ficud) • FSPF daemon (fspfd) • IGMP daemon (igmpd) • IMI daemon (imid) • Inter-fabric Routing daemon (iswitchd) • IP Storage daemon (ipsd) • ISNS client daemon on CP (isnscd) • KAC daemon (kacd) • Layer 2 System daemon (l2sysd) • LFM daemon (lfmd) • Link Aggregation Control Protocol daemon (lacpd) • Management Server daemon (msd) • MM daemon (mmd) • Multicast Sub-System daemon (mcast_ssd) • Multiple Spanning Tree Protocol daemon (mstpd) • Name Server daemon (nsd) • NSM daemon (nsmd) • ONM daemon (onmd) • Parity data manager daemon (pdmd) • Proxy daemon (proxyd) • PS daemon (psd) • RASLOG daemon (raslogd) • RCS daemon (rcsd) • RM daemon (rmd) • RMON daemon (rmond) • Security daemon (secd) • Sigma daemon (sigmad) • SNMP daemon (snmpd) • SP management daemon (spmd) • SVP daemon (svpd)

TABLE 6 System module descriptions (Continued)

System module	Description
KSWD (continued)	• System services module daemon (ssmd) • Time Service daemon (tsd) • TRACE daemon (traced) • Traffic daemon (trafd) • VS daemon (vsd) • Web linker daemon (weblinkerd) • Web Tools daemon (webd) • ZONE daemon (zoned)
KTRC	Kernel RAS trace module.
L2SS	L2SYS error messages indicate problems with the Layer 2 System manager that controls the Layer 2 forwarding engine and controls the learning/aging/forwarding functionality.
LACP	LACP error messages indicate problems with the Link Aggregation Control Protocol module of the Fabric OS.
LANCE	LANCE error messages indicate problems with the LANCE module of the Fabric OS.
LFM	LFM error messages indicate problems with the logical fabric manager module that is responsible for making a logical switch use XISLs. This involves creating and managing LISLs in a logical fabric.
LOG	RASLog subsystem.
LSDB	The link state database is a part of the FSPF protocol that maintains records on the status of port links. This database is used to route frames.
MCAST_SS	The Multicast Sub-System messages indicate any problems associated with the Layer 2 and Layer 3 Multicast platform support, including allocation of global platform resources such as MGIDs, hardware acceleration resources for Multicast, and route programming into the hardware (Layer 2 EXM for IGMP Snooping).
MAPS	The MAPS module identifies and reports anomalies associated with the various error counters, thresholds, and resources monitored on the switch.
MFIC	MS-FICON messages relate to Fibre Connection (FICON) installations. Fibre Connection control unit port (FICON-CUP) messages are displayed under the FICU module.
MM	MM message indicate problems with the management modules.
MPTH	Multicast path uses the shortest path first (SPF) algorithm to dynamically compute a broadcast tree.
MQ	Message queues are used for interprocess communication. Message queues allow many messages, each of variable length, to be queued. Any process or interrupt service routine (ISR) can write messages to a message queue. Any process can read messages from a message queue.
MS	The Management Service enables the user to obtain information about the Fibre Channel fabric topology and attributes by providing a single management access point. MS provides for both monitoring and control of the following areas: • **Fabric Configuration Server**: Provides for the configuration management of the fabric. • **Unzoned Name Server**: Provides access to Name Server information that is not subject to zone constraints. • **Fabric Zone Server**: Provides access to and control of zone information.
MSTP	MSTP error messages indicate problems with Multiple Spanning Tree Protocol modules of the Fabric OS.

TABLE 6 System module descriptions (Continued)

System module	Description
NBFS	NBFSM is a part of the Fabric Shortest Path First (FSPF) protocol that handles a neighboring or adjacent switch's finite state machine (FSM). Input to the FSM changes the local switch from one state to another, based on specific events. For example, when two switches are connected to each other using an interswitch link (ISL) cable, they are in the Init state. After both switches receive HELLO messages, they move to the Database Exchange state, and so on. NBFSM states are Down (0), Init (1), Database Exchange (2), Database Acknowledge Wait (3), Database Wait (4), and Full (5).
NS	Indicates problems with the simple Name Server module.
NSM	NSM error messages indicate problems with the Interface Management and VLAN Management module of the Fabric OS.
ONMD	ONMD error messages indicate problems with the Operation, Administration and Maintenance module of the Fabric OS.
PDM	Parity data manager (PDM) is a user-space daemon responsible for the replication of persistent configuration files from the primary partition to the secondary partition and from the active CP blade to the standby CP blade.
PDTR	PDTR messages indicate panic dump trace files have been created.
PLAT	PLAT messages indicate hardware problems.
PMGR	A group of messages relating to logical switch creation, deletion, and configuration.
PORT	PORT error messages refer to the front-end user ports on the switch. Front-end user ports are directly accessible by users to connect end devices or connect to other switches.
PS	The performance server daemon measures the amount of traffic between endpoints or traffic with particular frame formats, such as SCSI frames, IP frames, and customer-defined frames.
PSWP	The portswap feature and associated commands generate these error messages.
RAS	Informational messages when first failure data capture (FFDC) events are logged to the FFDC log and size or roll-over warning.
RCS	The reliable commit service daemon generates log entries when it receives a request from the zoning, security, or management server for passing data messages to switches in the fabric. RCS then requests reliable transport write and read (RTWR) to deliver the message. RCS also acts as a gatekeeper, limiting the number of outstanding requests for the Zoning, Security, or Management Server modules.
RKD	These messages are either error or informational messages pertaining to the re-key daemon of the Fabric OS.
RMON	RMON messages are error or informational messages pertaining to the RMOND daemon.
RPCD	The remote procedure call daemon (RPCD) is used by Fabric Access for API-related tasks.
RTE	RTE is responsible for determining the correct paths for each ingress frame and populating the routing tables in the ASICs with this information. The ASIC then uses the information available in the routing tables to determine the path a particular ingress frame needs to take before it exits the switch.
RTWR	The reliable transport write and read daemon helps deliver data messages either to specific switches in the fabric or to all of the switches in the fabric. For example, if some of the switches are not reachable or are offline, RTWR returns an "unreachable" message to the caller, allowing the caller to take the appropriate action. If a switch is not responding, RTWR retries 100 times.
SCN	The internal state change notification daemon is used for state change notifications from the kernel to the daemons within Fabric OS.

TABLE 6 System module descriptions (Continued)

System module	Description
SEC	The security daemon generates security errors, warnings, or information during security-related data management or fabric merge operations. Administrators should watch for these messages to distinguish between internal switch and fabric operation errors and external attacks.
SFLO	sFlow is a standard-based sampling technology embedded within switches and routers, which is used to monitor high-speed network traffic for Data Center Ethernet (DCE) and Converged Enhanced Ethernet (CEE) platforms. sFlow uses two types of sampling: • Statistical packet-based sampling of switched or routed packet flows. • Time-based sampling of interface counters. SFLO messages indicate errors or information related to the sflowd daemon.
SNMP	Simple Network Management Protocol (SNMP) is a universally supported low-level protocol that allows simple get, get next, and set requests to go to the switch (acting as an SNMP agent). It also allows the switch to send traps to the defined and configured management station. Brocade switches support six management entities that can be configured to receive these traps.
SPC	SPC messages indicate problems and informational updates associated with the security processor. These messages could be triggered by the following three modules: Security processor controller, SP system controller, and SP Keyapp.
SPM	Error messages indicating problems either with key or SP management.
SS	The **supportSave** command generates these error messages if problems are encountered.
SSMD	SSMD error messages indicate problems with the System Services Module of the Fabric OS.
SULB	The software upgrade library provides the **firmwareDownload** command capability, which enables firmware upgrades to both CP blades with a single command, as well as nondisruptive code load to all Fabric OS switches. These messages might display if there are any problems during the **firmwareDownload** procedure. Most messages are informational only and are generated even during successful firmware download. For additional information, refer to the *Fabric OS Administrator's Guide*.
SWCH	These messages are generated by the switch driver module that manages a Fibre Channel switch instance.
SYSC	System controller is a daemon that starts up and shuts down all Fabric OS modules in the proper sequence.
SYSM	General system messages.
TAPE	A kernel-space driver that handles all I/O operations aimed at Tape containers.
TRCE	RAS TRACE error messages.
TRCK	The track change feature tracks the following events: • Turning on or off the track change feature • CONFIG_CHANGE • LOGIN • LOGOUT • FAILED_LOGIN If any of these events occur, a message is sent to the system message log. Additionally, if the SNMP trap option is enabled, an SNMP trap is also sent. For information on configuring the track change feature, refer to the *Fabric OS Command Reference* or the *Fabric OS Administrator's Guide*.
TS	Time Service provides fabric time-synchronization by synchronizing all clocks in the fabric to the clock time on the principal switch.

TABLE 6 System module descriptions (Continued)

System module	Description
UCST	UCST is a part of the Fabric Shortest Path First (FSPF) protocol that manages the Unicast routing table.
UPTH	UPATH is a part of the FSPF protocol that uses the SPF algorithm to dynamically compute a Unicast tree.
VDR	VDR messages indicate Field-Programmable Gate Array (FPGA) parity errors.
VS	The VS module messages indicate any problems or information associated with the Dynamic Fabric Provisioning feature, including commands associated with the **fapwwn** command and configurations.
WEBD	Indicates problems with the Web Tools module.
XTUN	XTUN messages are generated by the FCIP Tunnel implementation. These messages indicate status of FCIP tunnels, FCIP emulation events for FCP traffic, or FCIP debug information (FTRACE buffer status changes).
ZEUS	Zeus error messages indicate problems with the Zeus driver module.
ZONE	The zone module messages indicate any problems associated with the zoning features, including commands associated with aliases, zones, and configurations.

Chapter 2

Audit Messages

AG Messages

AN Messages

AUTH Messages

BCM Messages

BLS Messages

BLZ Messages

CCFG Messages

CNM Messages

CONF Messages

CVLM Messages

ESS Messages

FICU Messages

FV Messages

FW Messages

HAM Messages

HTTP Messages

IPAD Messages

LOG Messages

MAPS Messages

MS Messages

PMGR Messages

PORT Messages

RAS Messages

SEC Messages

SNMP Messages

SPM Messages

SULB Messages

SWCH Messages

UCST Messages

ZONE Messages

Chapter 3

FFDC Messages

ANV Messages

AUTH Messages

BCM Messages

BKSW Messages

BL Messages

BLS Messages

BLZ Messages

BM Messages

C2 Messages

C3 Messages

CDR Messages

CHS Messages

EM Messages

FABR Messages

FABS Messages

FCMC Messages

FCPH Messages

FCR Messages

FLOD Messages

FSS Messages

HAM Messages

HAMK Messages

HIL Messages

HLO Messages

HMON Messages

KSWD Messages

LFM Messages

LOG Messages

LSDB Messages

MPTH Messages

MQ Messages

NBFS Messages

PDM Messages

PLAT Messages

PS Messages

RAS Messages

RCS Messages

SCN Messages

SNMP Messages

SULB Messages

SYSC Messages

SYSM Messages

TRCE Messages

UCST Messages

WEBD Messages

ZEUS Messages

Chapter 4

Log Messages

AG Messages

AN Messages

ANV Messages

AUTH Messages

BCM Messages

BKSW Messages

BL Messages

BLS Messages

BLZ Messages

BM Messages

C2 Messages

C3 Messages

CAL Messages

CCFG Messages

CDR Messages

CHS Messages

CNM Messages

CONF Messages

CTAP Messages

CVLC Messages

CVLM Messages

DOT1 Messages

ECC Messages

EM Messages

ESM Messages

ESS Messages

ESW Messages

EVMD Messages

FABR Messages

FABS Messages

FBC Messages

FCMC Messages

FCOE Messages

FCPD Messages

FCPH Messages

FCR Messages

FICN Messages

FICU Messages

FKLB Messages

FLOD Messages

FSPF Messages

FSS Messages

FSSM Messages

FV Messages

FW Messages

HAM Messages

HAMK Messages

HIL Messages

HLO Messages

HMON Messages

HSL Messages

HTTP Messages

IBD Messages

IPAD Messages

IPS Messages

ISNS Messages

KAC Messages

KSWD Messages

KTRC Messages

L2SS Messages

L3SS Messages

LACP Messages

LANCE Messages

LFM Messages

LOG Messages

LSDB Messages

MAPS Messages

MCAST_SS Messages

MFIC Messages

MM Messages

MPTH Messages

MQ Messages

MS Messages

MSTP Messages

NBFS Messages

NS Messages

NSM Messages

ONMD Messages

PDM Messages

PDTR Messages

PLAT Messages

PMGR Messages

PORT Messages

PS Messages

PSWP Messages

RAS Messages

RCS Messages

RKD Messages

RMON Messages

RPCD Messages

RTE Messages

RTWR Messages

SCN Messages

SEC Messages

SFLO Messages

SNMP Messages

SPC Messages

SPM Messages

SS Messages

SSMD Messages

SULB Messages

SWCH Messages

SYSC Messages

SYSM Messages

TAPE Messages

TRCE Messages

TRCK Messages

TS Messages

UCST Messages

UPTH Messages

VDR Messages

VS Messages

WEBD Messages

XTUN Messages

ZEUS Messages

ZONE Messages

Chapter 5

Fabric OS System Messages

AG Messages

AG-1001

Message `N_Port ID virtualization (NPIV) is not supported by fabric port connected to port <port number>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the N_Port ID virtualization (NPIV) capability is not supported by the fabric port to which the Access Gateway is connected.

Recommended Action

- Execute the **portCfgNpivPort** command to enable NPIV capability on the port connected to the Access Gateway.
- Some blades and ports in a switch may not support NPIV. NPIV functionality cannot be enabled on such ports and they will not respond to NPIV requests. Refer to the *Access Gateway Administrator's Guide* for specific AG-compatibility requirements.
- On non-Brocade switches, refer to the manufacturer's documentation to determine whether the switch supports NPIV and how to enable NPIV on these types of switches.

AG-1002

Message `Unable to find alternate N_Port during failover for N_Port <port number>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that no other N_Port is configured or the fabric was unstable during failover.

Recommended Action

Check whether an alternate N_Port is configured using the **portCfgShow** command.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AG-1003

Message `Unable to failover N_Port <port number>. Failover across different fabric is not supported.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the failover does not get blocked between two fabrics, although it is not a supported configuration.

Recommended Action Configure two or more N_Ports to connect to the same fabric; then execute the **ag --failoverenable** command to enable failover on these N_Ports.

AG-1004

Message `Invalid response to fabric login (FLOGI) request from the fabric for N_Port <port number>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the fabric sent an invalid response to the FLOGI Extended Link Service (ELS) for the specified N_Port.

Recommended Action Check the configuration of the fabric switch.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AG-1005

Message `FDISC response was dropped because F_Port <port number> is offline.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the F_Port connected to the host is offline, which caused the Fabric Discovery (FDISC) response to drop.

Recommended Action Check the configuration of the host connected to the specified F_Port.

AG-1006

Message `Access Gateway mode has been <message>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Access Gateway mode has been enabled or disabled.

Recommended Action Execute the **ag --modeshow** command to verify the current status of the Access Gateway mode.

AG-1007

Message `FLOGI response not received for the N_Port <port number> connected to the fabric.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the N_Port connected to the fabric switch is not online. The specified N_Port has been disabled.

Recommended Action Check the connectivity between the Access Gateway N_Port and the fabric switch port.

AG-1008

Message `Invalid Port Login (PLOGI) response from the fabric on the N_Port <port number>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the fabric switch management server did not accept the N_Port Login (PLOGI) request sent by the Access Gateway.

Recommended Action Check the configuration of the fabric switch connected to the Access Gateway.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AG-1009

Message `Sending FLOGI failed on N_Port <port number>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that there was a failure sending a Fabric Login (FLOGI) request from the Access Gateway to the fabric switch.

Recommended Action Check the configuration of the fabric switch connected to the Access Gateway.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AG-1010

Message `Sending PLOGI failed on N_Port <port number>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that there was a failure sending an N_Port Login (PLOGI) request from the Access Gateway to the fabric switch.

Recommended Action Check the configuration of the fabric switch connected to the Access Gateway.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AG-1011

Message `Sending FDISC failed on N_Port <port number>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that there was a failure sending a discover F_Port service parameter request from the Access Gateway to the fabric switch.

Recommended Action Check the configuration of the fabric switch connected to the Access Gateway.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AG-1012

Message `Sending logout (LOGO) request failed on N_Port <port number>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that there was a failure sending an N_Port logout request from the Access Gateway to the fabric switch.

Recommended Action Check the configuration of the fabric switch connected to the Access Gateway.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AG-1013

Message `F_Ports mapped to N_Port <port number> failed over to other N_Port(s).`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified N_Port is failing over to other N_Ports connected to the same fabric.

Recommended Action Execute the **ag --mapshow** command to display updated F_Port-to-N_Port mapping.

AG-1014

Message `Failing back F_Ports mapped to N_Port <port number>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified N_Port is failing back F_Ports mapped to it.

Recommended Action Execute the **ag --mapshow** command to display updated F_Port-to-N_Port mapping.

AG-1015

Message `Unable to find online N_Ports to connect to the fabric.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that no other N_Port is configured or all N_Ports are currently offline.

Recommended Action Check whether any other N_Port is configured using the **portCfgShow** command.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AG-1016

Message `Failing over F_Ports mapped to N_Port <port number> to other N_Port(s).`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified N_Port has failed to come online. All F_Ports mapped to this N_Port are being failed over to other active N_Ports.

Recommended Action Execute the **ag --mapshow** command to display updated F_Port-to-N_Port mapping.

AG-1017

Message `No N_Port(s) are currently Online.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that no N_Ports are currently configured in the system or all configured N_Ports have failed to come online.

Recommended Action Execute the **switchShow** command to display the status of all ports in the system. Execute the **portCfgShow** command to display the list of ports currently configured as N_Ports.

AG-1018

Message `Host port should not be connected to port <port number> which is configured as N_Port.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that an initiator or target port is erroneously connected to a port configured for N_Port operation.

Recommended Action Execute the **switchShow** command to display the status of all ports in the system. Execute the **portCfgShow** command to display the list of ports currently configured as N_Ports. Make sure the host is connected to an F_Port.

AG-1019

Message `Unable to failover N_Port <port number>. No other N_Port in port group:<pgid> is online.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that failover across port groups is not supported.

Recommended Action Check whether an alternate N_Port is configured in the specified port group using the **ag --pgshow** command.

AG-1020

Message `F_Ports to N_Ports route/mapping has been changed.`

Message Type LOG

Severity INFO

Probable Cause Indicates that F_Port-to-N_Port mapping has been changed because the switch has come online or some new N_Ports or F_Ports have come online.

Recommended Action Execute the **ag --mapshow** command to display the updated F_Port-to-N_Port mapping.

AG-1021

Message `Unable to do Preferred-Failover of F_Port <port number>. Failover across different fabric is not supported.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that failover across N_Ports connected to different fabrics is not supported.

Recommended Action Change the preferred N_Port settings of the specified F_Port using the **ag --prefset** command.

Choose the preferred N_Port so that it is in the same fabric as the primary N_Port of this F_Port. Execute the **ag --show** command to check the fabric connectivity of the N_Ports.

AG-1022

Message `F_Port <f_port> is failed over to its preferred N_Port <n_port>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the specified F_Port is failing over to its preferred N_Port.

Recommended Action Execute the **ag --mapshow** command to display the updated F_Port-to-N_Port mapping.

AG-1023

Message `F_Port <f_port> mapped to offline N_Port <n_port> is failed over to its preferred N_Port <preferred port>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified N_Port has failed to come online. The F_Port mapped to this N_Port had its preferred set and is online.

Recommended Action Execute the **ag --mapshow** command to display updated F_Port-to-N_Port mapping.

AG-1024

Message `F_Port <f_port> is failed back to its preferred N_Port <n_port>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified N_Port is failing back F_Ports, which are failed over to some other N_Port.

Recommended Action Execute the **ag --mapshow** command to display the updated F_Port-to-N_Port mapping.

AG-1025

Message `Port group of Slave N_Port <port number> is different than its Master N_Port <n_port>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the port groups of the Master and Slave N_Ports are different, while the trunk area assigned to the attached F_Ports on the edge switch is the same.

Recommended Action Execute the **porttrunkarea --show** command on the attached switch to verify that the trunk area is assigned to all ports in the system, and execute the **porttrunkarea --enable** command to reconfigure the trunk area.

AG-1026

Message `Unable to handle the login request on port <port number> due to insufficient resources.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that there are insufficient resources to accept the login request.

Recommended Action Execute the **configure** command on the Access Gateway switch and increase the number of allowed logins on the specified port.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AG-1027

Message `Unable to handle this login request on port <port number> because NPIV capability is not enabled on this port.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that N_Port ID virtualization (NPIV) is not enabled on the specified port.

Recommended Action Execute the **portCfgNpivPort** command on the Access Gateway switch to enable the NPIV capability on the port.

AG-1028

Message `Device with Port WWN <port_name> tried to perform fabric login through port <f_port>, without having access permission.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the device does not have login access for the specified port as per Advanced Device Security (ADS) policy set by the user.

Recommended Action Add the device to the ADS allow list for the specified port using the **ag --adsadd** command.

AG-1029

Message `Port Group (ID: <pgid>) has ports going to different fabrics.`

Message Type LOG

Severity WARNING

Probable Cause Indicates a misconfiguration.

Recommended Action Connect all ports in the port group to the same fabric.

AG-1030

Message `N_Port (ID: <port number>) has been determined to be unreliable.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the port goes online and offline often and therefore the port is marked as unreliable.

Recommended Action No action is required. The port will automatically be marked as reliable after a certain interval of time, if the port toggling remains within the threshold limit.

AG-1031

Message `Loop Detected for device with Port WWN <port_name> connected to port <port number>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a routing loop is detected for the device connected to the specified port.

Recommended Action Check the device configuration.

AG-1032

Message `N_Port (ID: <port number>) has recovered from an unreliable state.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the port state has been stable for the last five minutes.

Recommended Action No action is required.

AG-1033

Message `F_Port to N_Port mapping has been updated for N_Port (<n_port>).`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates that the F_Ports mapped to an N_Port have changed and the configuration file has been updated.

Recommended Action No action is required.

AG-1034

Message `F_Port cannot accept any more logins (<f_port>).`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates that the F_Port has already logged in the maximum number of devices.

Recommended Action No action is required.

AG-1035

Message `Device cannot login as ALPA value is not available (<alpa>).`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates that a device has already used the specified arbitrated loop physical address (ALPA) value.

Recommended Action No action is required.

AG-1036

Message `Port <port number> is connected to a non-Brocade fabric with Persistent ALPA enabled. Check the admin guide for supported configuration.`

Message Type AUDIT | LOG

Class CFG

Severity WARNING

Probable Cause Indicates that one of the ports is connected to a non-Brocade fabric.

Recommended Action Refer to the *Access Gateway Administrator's Guide* for the supported configuration.

AG-1037

Message `Trunked N_Port (<n_port>) going offline. If switchshow CLI for the connected fabric switch port displays Persistently disabled: Area has been acquired, then check cabling: all trunked ports should be in same ASIC Port Group.`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates an incorrect cabling.

Recommended Action If the **switchShow** command on the connected fabric switch port displays "Persistently disabled: Area has been acquired", then check cabling on the Access Gateway. All trunked ports in a single trunk must belong to the same application-specific integrated circuit (ASIC) port group.

AG-1038

Message `Brocade 8000 ports are going to different fabrics, check N_Port (<n_port>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates a misconfiguration.

Recommended Action Connect all ports in the port group to the same fabric.

AG-1039

Message `F_Port <Port that was reset> was reset because a WWN mapped device using it, through N_Port <Port who's state change caused the reset>, went offline.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified F_Port was reset because an N_Port went offline and the changes need to be propagated to all involved devices.

Recommended Action No action is required. This port reset was not an error.

AG-1040

Message `PID of the devices connected to Port <port number> may have changed, as the port was toggled. Check EE monitor <Truncated message>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that N_Port ID virtualization (NPIV) assigns a new port ID (PID) each time the same port is disabled and then re-enabled. As the PID has changed, the end-to-end (EE) monitors installed with the previous PID stops functioning.

Recommended Action Install new EE monitors with the new PID of the port to be monitored by using the **perfAddEEMonitor** command.

AG-1041

Message `Static F_Ports mapped to N_Port <port number> are disabled as Trunking is enabled on the N_Port.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a trunk is enabled on the specified N_Port, and therefore the F_Port static mapping is disabled.

Recommended Action Delete static mapping on the Access Gateway using the **ag --staticdel** command or disable the trunk on the N_Port using the **switchCfgTrunkPort** command.

AG-1042

Message `Sending ELS_PORT_OPEN failed on N_Port <port number>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates there was a failure sending an ELS_PORT_OPEN request from the Access Gateway to the fabric switch.

Recommended Action Check the configuration of the fabric switch connected to the Access Gateway.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AG-1043

Message `Authentication cannot be negotiated with the connected switch/HBA and therefore disabling the Port <port number>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that authentication has failed on the specified port. A possible reason could be that the edge switch connected to Access Gateway is using firmware earlier than Fabric OS v7.1.0.

Recommended Action Check the authentication configuration of the edge switch using the **authutil --show** command.

AG-1044

Message `Port <Port Number> has been disabled because switch requires authentication when device authentication policy is set to ON.`

Message Type LOG

Severity WARNING

Probable Cause Indicates a device that does not support authentication has tried to log in to the switch when the device authentication policy is in ON status on the switch.

Recommended Action Enable the authentication on the device or set the device authentication status to PASSIVE/OFF on the switch if it is not mandatory. Use the **authUtil** command to change the device authentication policy.

AG-1045

Message `New port <nport> has same Port WWN as old port <fport> as part of duplicate Port WWN detection policy.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the specified new port has the same Port World Wide Name (PWWN) as the old port.

Recommended Action No action is required.

AG-1046

Message `D_Port test will not start due to error in removing mapping for the F_Port <port>. Retry after sometime.`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates that there is an error in removing mapping for the specified port and due this there was a failure in starting the D_Port test.

Recommended Action Retry the D_Port test after sometime.

AG-1047

Message `Error in restoring one or all the mappings for the F_Port <port>. Add the mappings manually. Configured <Cofigured N-port>, Static <Static N-port> and Preffered <Preferred N-port>.`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates that there is an error in restoring the mapping for the specified port.

Recommended Action Add the mappings to the port manually.

AN Messages

AN-1001

Message `Failed to allocate memory: (<function name>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified function has failed to allocate memory.

Recommended Action Check memory usage on the switch using the **memShow** command. Restart or power cycle the switch.

AN-1002

Message `Failed to initialize; rc = <error>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the initialization of the "trafd" daemon has failed.

Recommended Action Download a new firmware version using the **firmwareDownload** command.

AN-1003

Message

```
Latency bottleneck on port <slot number>/<port number within slot number>.
<percentage of seconds affected by latency bottlenecking> pct. of <observation
period over which the percentage of affected seconds is reported> secs. affected.
Avg. delay <observed average time between frames during affected seconds> us. Avg.
slowdown <observed throughput drop factor during affected seconds>.
```

Message Type LOG | AUDIT

Class FABRIC

Severity WARNING

Probable Cause For an F_Port, indicates that the attached device is slow in responding to frames going out of the specified port. This latency may be inherent in the device or due to heavy workload on the device.

For a long-distance E_Port, may indicate too few credits for the distance. For a non-long-distance E_Port, indicates latency produced by a device downstream of the E_Port and is an indication of back-pressure produced by that latency.

Recommended Action If the port is an F_Port, examine the connected device for the source of the latency. If the port is a long-distance E_Port, make sure that there are enough buffer credits to service the link distance.

AN-1004

Message

```
Congestion bottleneck on port <slot number>/<port number within slot number>.
<percentage of seconds affected by congestion bottlenecking> pct. of <observation
period over which the percentage of affected seconds is reported> secs. affected.
```

Message Type LOG | AUDIT

Class FABRIC

Severity WARNING

Probable Cause Indicates that the volume of outgoing traffic at the specified port is too high for the capacity of the link.

Recommended Action Add more capacity on the path, using trunk links if possible.

AN-1005

Message

```
Slot <slot number>, port <port number within slot number> has <bottleneck type>
bottleneck cleared.
```

Message Type LOG | AUDIT

Class FABRIC

Severity INFO

Probable Cause Indicates that the bottleneck condition on the specified port has cleared.

Recommended Action No action is required.

AN-1006

Message

```
Bottleneck detection configuration is successfully changed.
```

Message Type AUDIT

Class FABRIC

Severity INFO

Probable Cause Indicates that the bottleneck detection configuration has been changed.

Recommended Action No action is required.

AN-1010

Message `Severe latency bottleneck detected at slot <slot number> port <port number within slot number>.`

Message Type LOG | AUDIT

Class FABRIC

Severity WARNING

Probable Cause Indicates credit loss at the specified port, a downstream port, or a very high latency device at the edge of the fabric.

Recommended Action Contact your switch service provider for assistance.

AN-1011

Message `Could not distinguish between primary and dependent severe latency bottleneck on slot <slot number> port <port number within slot number> because port mirroring is enabled on this port.`

Message Type LOG | AUDIT

Class FABRIC

Severity WARNING

Probable Cause Indicates that resources that are needed to determine whether there is complete credit loss on a virtual channel (VC) at the specified port are used by port mirroring.

Recommended Action Contact your switch service provider for assistance.

AN-1012

Message `Credits did not return from other end. Complete loss of credits on a VC on slot <slot number> port <port number within slot number>.`

Message Type LOG | AUDIT

Class FABRIC

Severity WARNING

Probable Cause Indicates a credit loss.

Recommended Action If this message is not followed by the AN-1013 message, contact your switch service provider for assistance.

AN-1013

Message `Performed link reset to recover the port credits on slot <slot number> port <port number within slot number>.`

Message Type LOG | AUDIT

Class FABRIC

Severity INFO

Probable Cause Indicates a credit loss.

Recommended Action The port is recovered. No action is required.

AN-1014

Message `Frame <frametype> detected, tx port <tx port>, rx port <rx port>, sid <sid>, did <did>, timestamp <timestamp>.`

Message Type AUDIT

Class FABRIC

Severity INFO

Probable Cause Indicates C3 discard frame.

Recommended Action Check the *Fabric OS Troubleshooting and Diagnostics Guide* for troubleshooting information or contact your switch service provider if the message persists.

ANV Messages

ANV-1001

Message `Port <port number> port fault. Change the SFP or check the cable.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a deteriorated small form-factor pluggable (SFP) transceiver, an incompatible SFP transceiver pair, or a faulty cable between the peer ports.

Recommended Action Verify that compatible SFP transceivers are used on the peer ports, the SFP transceivers have not deteriorated, and the Fibre Channel cable is not faulty. Replace the SFP transceivers or the cable, if necessary.

ANV-1002

Message `Port <port number> chip faulted due to an internal error.`

Message Type LOG | FFDC

Severity ERROR

Probable Cause Indicates an internal error. All the ports on the chip will be disrupted.

Recommended Action To recover a bladed system, execute the **slotPowerOff** and **slotPowerOn** commands on the blade. To recover a non-bladed system, execute the **fastBoot** command on the switch.

ANV-1003

Message
```
S<slot number>,C<chip index>: HW ASIC Chip error. Type = 0x<chip error type>,
Error = <chip error string>.
```

Message Type LOG

Severity CRITICAL

Probable Cause Indicates an internal error in the application-specific integrated circuit (ASIC) hardware that may degrade the data traffic.

Recommended Action Restart the system at the next maintenance window. If the problem persists, replace the blade.

ANV-1004

Message

```
S<slot number>,C<chip index>: Invalid DMA ch pointer, chan:<Channel number>,
good_addr:0x<Good address> bad_addr:0x<Bad address>.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates an internal error in the application-specific integrated circuit (ASIC) hardware that may degrade the data traffic.

Recommended Action

Restart the system at the next maintenance window. If the problem persists, replace the blade.

ANV-1005

Message

```
S<slot number>,C<chip index>,A<anvil id>: Memory allocation failed.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates memory allocation failure in the software.

Recommended Action

Restart the system at the next maintenance window. If the problem persists, replace the switch or contact your switch service provider.

ANV-1006

Message

```
S<slot number>,C<chip index>: HW ASIC Chip fault. Type = 0x<chip error type>,
Error = <chip error string>.
```

Message Type

LOG

Severity

CRITICAL

Probable Cause

Indicates an internal error in the application-specific integrated circuit (ASIC) hardware that renders the chip as not operational.

Recommended Action

Restart the system at the next maintenance window. If the problem persists, replace the blade.

ANV-1007

Message `S<slot number>,C<chip index>: ANVIL PASS 1 low buff pool fault: <chip regval field> 0x<chip error type>.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that Anvil Pass 1 is running out of free buffers, which may cause chip fault.

Recommended Action When this error is observed persistently, power cycle the specified blade using the **slotPowerOff** and **slotPowerOn** commands. If the problem persists, replace the blade.

ANV-1008

Message `S<slot number>,C<chip index>: MAC-VID classifier table is full. No space for new entry.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the Media Access Control (MAC) VLAN ID (VID) classifier table is full and no more entries can be added.

Recommended Action Delete some of the existing unused rules using the **portcfg arp** command and then add new entries.

ANV-1015

Message `Port reinitialized due to Link Reset failure on internal port S<slot number>,P<port number>(<blade port number>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the specified port is re-initialized due to link reset failure.

Recommended Action When this error is observed persistently, power cycle the specified blade using the **slotPowerOff** and **slotPowerOn** commands. If the problem persists, replace the blade.

ANV-1016

Message `Port is faulted due to port reinitialization failure on internal port S<slot number>,P<port number>(<blade port number>) with reason <port fault reason>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the specified port is faulted due to port re-initialization failure.

Recommended Action When this error is observed persistently, power cycle the specified blade using the **slotPowerOff** and **slotPowerOn** commands. If the problem persists, replace the blade.

ANV-1028

Message `Detected excessive Link resets on the port in a second. Slot <slot number>, Port <port number>(<blade port number>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the port received excessive link resets from peer port within 1 second and that exceeded threshold.

Recommended Action When this error is observed persistently, change the small form-factor pluggable (SFP) transceiver or the cable on the peer port to which this port is connected.

AUTH Messages

AUTH-1001

Message `<Operation type> has been successfully completed.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the secret database operation has been updated using the **secAuthSecret** command. The values for *Operation type* can be "set" or "remove".

Recommended Action No action is required.

AUTH-1002

Message `<Operation type> has failed.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified action has failed to update the secret database using the **secAuthSecret** command. The values for *Operation type* can be "set" or "remove".

Recommended Action Execute the **secAuthSecret** command again.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-1003

Message `<data type> type has been successfully set to <setting value>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that an authentication configuration value was set to a specified value. The *data type* is authentication type, DH group type, hash type, or policy type.

Recommended Action No action is required.

AUTH-1004

Message `Failed to set <data type> type to <setting value>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the **authUtil** command has failed to set the authentication configuration value. The *data type* can be authentication type, DH group type, hash type, or policy type.

Recommended Action Execute the **authUtil** command again.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-1005

Message `Authentication file does not exist: <error code>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates an authentication file corruption.

Recommended Action Execute the **firmwareDownload** command to reinstall the firmware.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-1006

Message `Failed to open authentication configuration file.`

Message Type LOG

Severity WARNING

Probable Cause Indicates an internal problem with the Secure Fabric OS.

Recommended Action Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-1007

Message `The proposed authentication protocol(s) are not supported: port <port number>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the proposed authentication protocol types are not supported by the specified local port.

Recommended Action Execute the **authUtil** command to make sure the local switch supports the Fibre Channel Authentication Protocol (FCAP) or Diffie Hellman - Channel Authentication Protocol (DH-CHAP) protocols.

AUTH-1008

Message `No security license, operation failed.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the switch does not have a security license.

Recommended Action Verify that the security license is installed using the **licenseShow** command. If necessary, reinstall the license using the **licenseAdd** command.

AUTH-1010

Message `Failed to initialize security policy: switch <switch number>, error <error code>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates an internal problem with the Secure Fabric OS.

Recommended Action Reboot or power cycle the switch.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-1011

Message `Failed to register for failover operation: switch <switch number> error <error code>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates an internal problem with the Secure Fabric OS.

Recommended Action Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-1012

Message `Authentication <code> is rejected: port <port number> explain <explain code> reason <reason code>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the specified authentication is rejected because the remote entity does not support authentication.

Recommended Action Verify the hash type, protocol, group, and authentication policy using the **authutil --show** command.

AUTH-1013

Message `Cannot perform authentication request message: port <port number>, message code <message code>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the system is running low on resources when receiving an authentication request. Usually this problem is transient. The authentication may fail.

Recommended Action Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-1014

Message `Invalid port value to <operation>: port <port number>.`

Message Type LOG | FFDC

Severity ERROR

Probable Cause Indicates an internal problem with the Secure Fabric OS.

Recommended Action Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-1016

Message `Invalid value to start HBA authentication port: <port number>, pid <pid>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates an internal failure.

Recommended Action Copy the message and collect the switch information using the **supportShow** command, and contact your switch service provider.

AUTH-1017

Message `Invalid value to start authentication request: port <port number>, operation code <operation code>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates an internal problem with the Secure Fabric OS.

Recommended Action Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-1018

Message `Invalid value to check protocol type: port <port number>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates an internal problem with the Secure Fabric OS.

Recommended Action Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-1020

Message `Failed to create timer for authentication: port <port number>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that an authentication message timer was not created. Usually this problem is transient. The authentication may fail.

Recommended Action Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-1022

Message `Failed to extract <data type> from <message> payload: port <port number>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the authentication process failed to extract a particular value from the receiving payload. Usually this problem is transient. The authentication may fail.

Recommended Action Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-1023

Message `Failed to <operation type> during <authentication phase>: port <port number>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates an authentication operation failed for a certain authentication phase. The *Operation type* varies depending on authentication type:

- Some operations for Switch Link Authentication Protocol (SLAP): certificate retrieve, certificate verification, signature verification, or nonce signing.
- Some operations for Fibre Channel Authentication Protocol (FCAP): certificate retrieve, certificate verification, signature verification, or nonce signing.
- Some operations for Diffie Hellman - Challenge Handshake Authentication Protocol (DH-CHAP): response calculation, challenge generation, or secret retrieve.

The *authentication phase* specifies which phase of a particular authentication protocol failed.

A nonce is a single-use, usually random value used in authentication protocols to prevent replay attacks.

Recommended Action The error may indicate that an invalid entity tried to connect to the switch. Check the connection port for a possible unauthorized access attack.

It may indicate that the public key infrastructure (PKI) object for SLAP or FCAP or the secret value for DH-CHAP on the local entity is not set up properly. Reinstall all PKI objects or reset the secret value for DH-CHAP properly.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-1025

Message `Failed to get <data type> during <authentication phase>: port <port number>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the authentication process failed to get expected information during the specified authentication phase. Usually this problem is transient. The authentication may fail.

Recommended Action Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-1026

Message `Failed to <Device information> during negotiation phase: port <port number>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the authentication failed to get device or Host Bus Adapter (HBA) information due to an internal failure. Usually this problem is transient. If the authentication failed, retry the login.

Recommended Action Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-1027

Message `Failed to select <authentication value> during <authentication phase>: value <value> port <port number>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the authentication process failed to select an authentication value (DH Group, hash value, or protocol type) from a receiving payload for a particular authentication phase. This indicates that the local switch does not support the specified authentication value.

Recommended Action Check the authentication configuration and reset the supported value if needed using the **authUtil** command.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-1028

Message `Failed to allocate <data type> for <operation phase>: port <port number>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the authentication process failed because the system is low on memory. Usually this problem is transient. The authentication may fail.

The *Data type* is the payload or structure that failed to get memory. The *Operation phase* specifies which operation of a particular authentication phase failed.

Recommended Action Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-1029

Message `Failed to get <data type> for <message phase> message: port <port number>, retval <error code>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the authentication process failed to get a particular authentication value at a certain phase. Usually this problem is transient. The authentication may fail.

The *Data type* is the payload or structure that failed to get memory.

Recommended Action Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-1030

Message `Invalid message code for <message phase> message: port <port number>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the receiving payload does not have a valid message code for a particular authentication phase. Usually this problem is transient. The authentication may fail.

Recommended Action Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-1031

Message `Failed to retrieve secret value: port <port number>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the secret value was not set properly for the authenticated entity.

Recommended Action

Reset the secret value using the **secAuthSecret** command.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-1032

Message

```
Failed to generate <data type> for <message payload> payload: length <data
length>, error code <error code>, port <port number>.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that the authentication process failed to generate specific data (challenge, nonce, or response data) for an authentication payload. This usually relates to internal failure.

A nonce is a single-use, usually random value used in authentication protocols to prevent replay attacks.

Usually this problem is transient. The authentication may fail.

Recommended Action

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-1033

Message

```
Disable port <port number> due to unauthorized switch <switch WWN value>.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that an entity was not configured in the Switch Connection Control (SCC) policy and tried to connect to the port.

Recommended Action

Add World Wide Name (WWN) of the entity to the SCC policy and reinitialize authentication by using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

AUTH-1034

Message

```
Failed to validate name <entity name> in <authentication message>: port <port
number>.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that the specified entity name in the payload is not in the correct format.

Recommended Action Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-1035

Message `Invalid <data type> length in <message phase> message: length <data length>, port <port number>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that a particular data field in the authentication message has an invalid length field. This error usually relates to internal failure. Usually this problem is transient. The authentication may fail.

Recommended Action Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-1036

Message `Invalid state <state value> for <authentication phase>: port <port number>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the switch received an unexpected authentication message. Usually this problem is transient. The authentication may fail.

Recommended Action Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-1037

Message

```
Failed to <operation type> response for <authentication message>: init_len <data
length>, resp_len <data length>, port <port number>.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that a Diffie Hellman - Challenge Handshake Authentication Protocol (DH-CHAP) authentication operation failed on the specified port due to mismatched response values between two entities.

The error may indicate that an invalid entity tried to connect to the switch. Check the connection port for a possible security attack.

Recommended Action

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-1038

Message

```
Failed to retrieve certificate during <authentication phase>: port <port number>.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that the public key infrastructure (PKI) certificate is not installed properly.

Recommended Action

Reinstall the PKI certificate using the **secCertUtil** command.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-1039

Message

```
Neighboring switch has conflicting authentication policy: Port <Port Number>
disabled.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that the neighboring switch has a conflicting authentication policy enabled. The E_Port has been disabled because the neighboring switch has rejected the authentication negotiation, and the local switch has a strict switch authentication policy.

Recommended Action Correct the switch policy configuration on either of the switches using the **authUtil** command, and then enable the port using the **portEnable** command.

AUTH-1040

Message

```
Reject authentication on port <Port Number>, because switch authentication policy
is set to OFF.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the local switch has rejected the authentication because the switch policy is turned off. If the neighboring switch has a strict (ON) switch policy, the port will be disabled due to conflicting configuration settings. Otherwise, the E_Port will form without authentication.

Recommended Action If the port is disabled, correct the switch policy configuration on either of the switches using the **authUtil** command, and then enable the port on the neighboring switch using the **portEnable** command. If the E_Port has formed, no action is required.

AUTH-1041

Message

```
Port <port number> has been disabled, because an authentication-reject was
received with code '<Reason String>' and explanation '<Explanation String>'.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified port has been disabled because it received an authentication-reject response from the connected switch or device. The error may indicate that an invalid entity tried to connect to the switch.

Recommended Action

Check the connection port for a possible security attack.

Check the shared secrets using the **secAuthSecret** command and reinitialize authentication using the **portDisable** and **portEnable** commands.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-1042

Message

```
Port <port number> has been disabled, because authentication failed with code
'<Reason String>' and explanation '<Explanation String>'.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified port has been disabled because the connecting switch or device failed to authenticate. The error may indicate that an invalid entity attempted to connect to the switch.

Recommended Action

Check the connection port for a possible security attack.

Check the shared secrets using the **secAuthSecret** command and reinitialize authentication using the **portDisable** and **portEnable** commands.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-1043

Message

```
Failed to enforce device authentication mode:<Device Auth Policy>(error: <Reason
Code>).
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that the Kernel mode setting for F_Port authentication failed. Device authentication will be defaulted to OFF, and the switch will not participate in Diffie Hellman - Challenge Handshake Authentication Protocol (DH-CHAP) authentication with other devices.

Recommended Action

Set the device authentication policy manually using the **authUtil** command.

AUTH-1044

Message

```
Authentication <Reason for disabling the port>. Disabling the port <port number>.
```

Message Type

LOG | FFDC

Severity

ERROR

Probable Cause

Indicates that authentication has timed out after multiple retries. The specified port has been disabled as a result. This problem may be transient due to the system CPU load. In addition, a defective small form-factor pluggable (SFP) transceiver or faulty cable may have caused the failure.

Recommended Action

Check the SFP transceiver and the cable; then enable the port using the **portEnable** command.

AUTH-1045

Message

```
Certificate not present in this switch in <authentication phase> port <port
number>.
```

Message Type

AUDIT | LOG

Class

SECURITY

Severity

ERROR

Probable Cause

Indicates that the public key infrastructure (PKI) certificate is not installed in this switch.

Recommended Action

Check the certificate availability using the **secCertUtil show -fcapall** command.

Install the certificate and reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-1046

Message

`<Operation type> has been successfully completed.`

Message Type

AUDIT | LOG

Class

SECURITY

Severity

INFO

Probable Cause

Indicates that the certificate database operation has been updated using the **secAuthCertificate** command. The values for *Operation type* can be "set" or "remove".

Recommended Action

No action is required.

AUTH-1047

Message

`<Operation type> has failed.`

Message Type

AUDIT | LOG

Class

SECURITY

Severity

ERROR

Probable Cause

Indicates that the specified action has failed to update the certificate database using the **secAuthCertificate** command. The values for *Operation type* can be "set" or "remove".

Recommended Action

Execute the **secAuthCertificate** command again.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-1048

Message

```
Stopping synchronization of the system due to <Operation type> incompatibility
with standby CP.
```

Message Type

AUDIT | LOG

Class

SECURITY

Severity

ERROR

Probable Cause

Indicates that the software version on the standby control processor (CP) is incompatible with this software feature enabled in this Fabric OS firmware version because the in-flight encryption feature supports both DH-CHAP and FCAP protocols.

Recommended Action

Upgrade the software on the standby CP or disable the software feature on this CP.

To allow standby synchronization, use the DH-CHAP protocol only for in-flight encryption and disable FCAP protocol in authutil. Use the **authutil --set -a "protocol type"** command to configure the DH-CHAP protocol.

AUTH-1049

Message

```
Slave port <Slave port number> has been disabled, as Master port <Master port
number> was disabled because of authentication failure/rejection.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that the specified slave port has been disabled because it received an authentication-reject response from the connected switch or device. The error informs that the slave port is disabled due to master port authentication failure or rejection.

Recommended Action

Check the connection port for a possible security attack.

Check the shared secrets using the **secAuthSecret** command or check certificates using the **secCertUtil** command, and reinitialize authentication using the **authutil --authinit** command.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-3001

Message `Event: <Event Name>, Status: success, Info: <Data type> type has been changed from [<Old value>] to [<New value>].`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that an authentication configuration value was set to a specified value. The *Data type* can be authentication type, DH group type, hash type, or policy type.

Recommended Action No action is required.

AUTH-3002

Message `Event: <Event Name>, Status: success, Info: <Event Related Info>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the secret database operation has been updated using the **secAuthSecret** command.

Recommended Action No action is required.

AUTH-3003

Message `Event: <Event Name>, Status: success, Info: <Operation type> the PKI objects.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the public key infrastructure (PKI) objects were created using the **secCertUtil** command or that the PKI objects were removed using the **secCertUtil delete -fcapall** command. Operation type can be either "Created" or "Removed".

Recommended Action No action is required.

AUTH-3004

Message `Event: <Event Name>, Status: failed, Info: Neighboring switch has a conflicting authentication policy; Port <Port Number> disabled.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the specified E_Port was disabled because the neighboring switch rejected the authentication negotiation, and the local switch has a strict switch authentication policy.

Recommended Action Correct the switch policy configuration on either of the switches using the **authUtil** command, and then enable the port using the **portEnable** command.

AUTH-3005

Message `Event: <Event Name>, Status: failed, Info: Rejecting authentication request on port <Port Number> because switch policy is turned OFF.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the local switch has rejected the authentication request, because the switch policy is turned off. If the neighboring switch has a strict (ON) switch policy, the port will be disabled due to conflicting configuration settings. Otherwise, the E_Port will form without authentication.

Recommended Action If the specified port is disabled, correct the switch policy configuration on either of the switches using the **authUtil** command, and then enable the port on the neighboring switch using the **portEnable** command. If the E_Port formed, no action is required.

AUTH-3006

Message `Event: <Event Name>, Status: failed, Info: Authentication failed on port <port number> due to mismatch of DH-CHAP shared secrets.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that a Diffie Hellman - Challenge Handshake Authentication Protocol (DH-CHAP) authentication operation failed on the specified port due to mismatched response values between two entities.

The error may indicate that an invalid entity tried to connect to the switch.

Recommended Action

Check the connection port for a possible security attack.

Check the shared secrets using the **secAuthSecret** command and reinitialize authentication using the **portDisable** and **portEnable** commands.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-3007

Message

```
Event: <Event Name>, Status: failed, Info: Port <port number> disabled due to
receiving an authentication reject with code '<Reason String>' and Explanation
'<Explanation String>'.
```

Message Type

AUDIT

Class

SECURITY

Severity

INFO

Probable Cause

Indicates that the specified port was disabled because it received an authentication-reject response from the connected switch or device.

The error may indicate that an invalid entity tried to connect to the switch.

Recommended Action

Check the connection port for a possible security attack.

Check the shared secrets using the **secAuthSecret** command and reinitialize authentication using the **portDisable** and **portEnable** commands.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

AUTH-3008

Message

```
Event: <Event Name>, Status: failed, Info: Port <port number> has been disabled
due to authentication failure with code '<Reason String>' and explanation
'<Explanation String>'.
```

Message Type

AUDIT

Class

SECURITY

Severity

INFO

Probable Cause

Indicates that the specified port has been disabled because the connecting switch or device failed to authenticate.

The error may indicate that an invalid entity tried to connect to the switch.

Recommended Action

Check the connection port for a possible security attack.

Check the shared secrets using the **secAuthSecret** command and reinitialize authentication using the **portDisable** and **portEnable** commands.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

BCM Messages

BCM-1000

Message `<command name> of GE <port number> failed. Please retry the command. Data: inst=<ASIC instance> st=<ASIC initializing state> rsn=<reason code> fn=<message function> oid=<ASIC ID>.`

Message Type LOG | FFDC

Severity ERROR

Probable Cause Indicates that the hardware is not responding to a command request, possibly because it is busy.

Recommended Action Retry the command.

BCM-1001

Message `FIPS <FIPS Test Name> failed; algo=<algorithm code> type=<algorithm type> slot=<Slot Number>.`

Message Type LOG | FFDC

Severity CRITICAL

Probable Cause Indicates that a Federal Information Protection Standard (FIPS) failure has occurred and requires faulting the blade or switch.

Recommended Action Retry the command.

BCM-1002

Message `An IPsec/IKE policy was added.`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates that an Internet Protocol Security (IPsec) or Internet Key Exchange (IKE) policy was added and the configuration file was updated.

Recommended Action No action is required.

BCM-1003

Message `An IPsec/IKE policy was deleted.`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates that an Internet Protocol Security (IPsec) or Internet Key Exchange (IKE) policy was deleted and the configuration file was updated.

Recommended Action No action is required.

BCM-1004

Message `Tape Read Pipelining is being disabled slot (<slot number>) port (<user port index>) tunnel (<The configured tunnel ID (0-7)>).`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Fabric OS version on the remote end of the tunnel does not support Tape Read Pipelining.

Recommended Action No action is required.

BCM-1005

Message `S<slot number>,P<user port index>(<blade index>) [OID 0x<port OID>]: <string name of ge>: port faulted due to SFP validation failure. Please check if the SFP is valid for the configuration.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a deteriorated small form-factor pluggable (SFP) transceiver, an incompatible SFP transceiver pair, or a faulty cable between the peer ports.

Recommended Action Verify that compatible SFP transceivers are used on the peer ports (execute the **sfpShow** command on each side to verify matched pair), the SFP transceivers have not deteriorated, and the Fibre Channel cable is not faulty. Replace the SFP transceivers or the cable if necessary.

BKSW Messages

BKSW-1003

Message `kSWD: <Warning message>.`

Message Type FFDC | LOG

Severity WARNING

Probable Cause Indicates a warning state within the system.

A critical application error was reported in the watchdog subsystem. This message is used to convey information regarding the state of the system. The switch will reboot (on single-CP switches) or fail over (on dual-CP switches).

The *Warning message* variable will be one of the following:

- Detected unexpected termination of: *daemon name* - One of the critical daemons ended unexpectedly.
- *daemon name* failed to refresh SWD*** Sending SIGABRT to PID *process id number* - One of the critical daemons is found to be nonresponsive; sending signal abort (SIGABRT).

Recommended Action Execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

BL Messages

BL-1000

Message `Initializing ports...`

Message Type LOG

Severity INFO

Probable Cause Indicates that the switch has started initializing the ports.

Recommended Action No action is required.

BL-1001

Message `Port initialization completed.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the switch has completed initializing the ports.

Recommended Action No action is required.

BL-1002

Message

```
Init Failed: slot <slot number> DISABLED because internal ports were not ONLINE,
<list of internal port number not ONLINE>.
```

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the blade initiation failed because one or more of the internal ports was not online. The blade is faulted.

Recommended Action

Make sure that the blade is seated correctly.

If the blade is seated correctly, execute the **diagPost** command to make sure that Power-On Self-Test (POST) is enabled; then power cycle the blade using the **slotPowerOff** and **slotPowerOn** commands or have the blade's ejector switch cycled to run POST and verify that the blade does not have any hardware problems.

Additional blade fault messages precede and follow this error, providing more information. Refer to other error messages for recommended action.

If the message persists, replace the blade.

BL-1003

Message `Faulting blade in slot <slot number>.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates a faulty blade in the specified slot.

Recommended Action Make sure that the blade is seated correctly.

If the blade is seated correctly, execute the **diagPost** command to make sure that Power-On Self-Test (POST) is enabled; then power cycle the blade using the **slotPowerOff** and **slotPowerOn** commands or have the blade's ejector switch cycled to run POST and verify that the blade does not have any hardware problems.

If the message persists, replace the blade.

BL-1004

Message `Suppressing blade fault in slot <slot number>.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the specified blade experienced a failure but was not faulted due to a user setting.

Recommended Action Execute the **diagPost** command to make sure that Power-On Self-Test (POST) is enabled; then power cycle the blade using the **slotPowerOff** and **slotPowerOn** commands or have the blade's ejector switch cycled to run POST and verify that the blade does not have any hardware problems.

If the message persists, replace the blade.

BL-1006

Message `Blade <slot number> NOT faulted. Peer blade <slot number> experienced abrupt failure.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the errors (mostly synchronization errors) on the specified blade are harmless. Probably, the standby control processor (CP) blade connected to the active CP blade has experienced transitory problems.

Recommended Action Execute the **haShow** command to verify that the standby CP is healthy. If the problem persists, remove and reinstall the faulty blade.

If the standby CP was removed or faulted by user intervention, no action is required.

BL-1007

Message `blade #<blade number>: blade state is inconsistent with EM. bl_cflags 0x<blade control flags>, slot_on <slot_on flag>, slot_off <slot_off flag>, faulty <faulty flag>, status <blade status>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a failover occurred while a blade was initializing on the previously active control processor (CP).

Recommended Action No action is required. The blade is reinitialized. Because reinitializing a blade is a disruptive operation and can stop I/O traffic, you may need to stop and restart the traffic during this process.

BL-1008

Message `Slot <slot number> control-plane failure. Expected value: 0x<value 1>, Actual: 0x<value 2>.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the blade has experienced a hardware failure or was removed without following the recommended removal procedure.

Recommended Action Make sure that the blade is seated correctly.

If the blade is seated correctly, execute the **diagPost** command to make sure that Power-On Self-Test (POST) is enabled; then power cycle the blade using the **slotPowerOff** and **slotPowerOn** commands or have the blade's ejector switch cycled to run POST and verify that the blade does not have any hardware problems.

If the message persists, replace the blade.

BL-1009

Message `Blade in slot <slot number> timed out initializing the chips.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the blade has failed to initialize the application-specific integrated circuit (ASIC) chips.

Recommended Action

Make sure that the blade is seated correctly.

If the blade is seated correctly, execute the **diagPost** command to make sure that Power-On Self-Test (POST) is enabled; then power cycle the blade using the **slotPowerOff** and **slotPowerOn** commands or have the blade's ejector switch cycled to run POST and verify that the blade does not have any hardware problems.

If the message persists, replace the blade.

BL-1010

Message

```
Blade in slot <slot number> inconsistent with the hardware settings.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that a failover occurred while some hardware changes (such as changing the domain ID) were being made on the previously active control processor (CP).

Recommended Action

No action is required. This blade has been reinitialized. Because reinitializing a blade is a disruptive operation and can stop I/O traffic, you may need to stop and restart the traffic during this process.

BL-1011

Message

```
Busy with emb-port int. for chip <chip number> in minis <minis number> on blade
<slot number>, chip int. is disabled. interrupt status=0x<interrupt status>.
```

Message Type

FFDC | LOG

Severity

CRITICAL

Probable Cause

Indicates that too many interrupts in the embedded port caused the specified chip to be disabled. The probable cause is too many abnormal frames; the chip is disabled to prevent the control processor (CP) from becoming too busy.

Recommended Action

Make sure to capture the console output during this process.

Check for a faulty cable, small form-factor pluggable (SFP) transceiver, or device attached to the specified port.

On a bladed switch, execute the **diagPost** command to make sure that Power-On Self-Test (POST) is enabled; then power cycle the blade using the **slotPowerOff** and **slotPowerOn** commands or have the blade's ejector switch cycled to run POST and verify that the blade does not have any hardware problems.

On a non-bladed switch, reboot or power cycle the switch.

If the message persists, replace the blade or the (non-bladed) switch.

BL-1012

Message

```
bport <port number> port int. is disabled. status=0x<interrupt status> Port <port
number> will be re-enabled in 1 minute.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that the port generated an excessive number of interrupts that may prove unrecoverable to the switch operation. The port is disabled to prevent the control processor (CP) from becoming too busy. The bport is the blade port; this number may not correspond to a user port number.

Recommended Action

Make sure to capture the console output during this process.

Check for a faulty cable, small form-factor pluggable (SFP) transceiver, or device attached to the specified port.

On a bladed switch, run the **slotPowerOff** and **slotPowerOn** commands to power cycle the blade.

On a non-bladed switch, reboot or power cycle the switch.

If the message persists, replace the blade or the (non-bladed) switch.

BL-1013

Message

```
bport <port number> port is faulted. status=0x<interrupt status> Port <port
number> will be re-enabled in 1 minute.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that the port generated an excessive number of interrupts that may prove fatal to the switch operation. The port is disabled to prevent the control processor (CP) from becoming too busy. The *bport* number displayed in the message is the blade port; this number may not correspond to a user port number.

Recommended Action

Make sure to capture the console output during this process.

Check for a faulty cable, small form-factor pluggable (SFP) transceiver, or device attached to the specified port.

On a bladed switch, run the **slotPowerOff** and **slotPowerOn** commands to power cycle the blade.

On a non-bladed switch, reboot or power cycle the switch.

If the message persists, replace the blade.

BL-1014

Message

```
bport <port number> port int. is disabled. status=0x<interrupt status>.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that the port generated an excessive number of interrupts that may prove fatal to the switch operation. The port is disabled to prevent the control processor (CP) from becoming too busy. The *bport* number displayed in the message is the blade port; this number may not correspond to a user port number.

Recommended Action

Make sure to capture the console output during this process.

On a bladed switch, execute the **diagPost** command to make sure that Power-On Self-Test (POST) is enabled; then power cycle the blade using the **slotPowerOff** and **slotPowerOn** commands or have the blade's ejector switch cycled to run POST and verify that the blade does not have any hardware problems.

On a non-bladed switch, execute the **reboot** command to restart the switch.

If there is a hardware error, the **slotPowerOff** or **slotPowerOn** fails on the bladed switch, or errors are encountered again, replace the blade or the (non-bladed) switch.

BL-1015

Message

```
bport <port number> port is faulted. status=0x<interrupt status>.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that the port generated an excessive number of interrupts that may prove fatal to the switch operation. The port is disabled to prevent the control processor (CP) from becoming too busy. The *bport* number displayed in the message is the blade port; this number may not correspond to a user port number.

Recommended Action

Make sure to capture the console output during this process.

On a bladed switch, execute the **diagPost** command to make sure that Power-On Self-Test (POST) is enabled; then power cycle the blade using the **slotPowerOff** and **slotPowerOn** commands or have the blade's ejector switch cycled to run POST and verify that the blade does not have any hardware problems.

On a non-bladed switch, execute the **reboot** command to restart the switch.

If there is a hardware error, the **slotPowerOff** or **slotPowerOn** fails on the bladed switch, or errors are encountered again, replace the blade or the (non-bladed) switch.

BL-1016

Message `Blade port <port number> in slot <slot number> failed to enable.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the specified blade port could not be enabled.

Recommended Action Make sure that the blade is seated correctly.

If the blade is seated correctly, execute the **diagPost** command to make sure that Power-On Self-Test (POST) is enabled; then power cycle the blade using the **slotPowerOff** and **slotPowerOn** commands or have the blade's ejector switch cycled to run POST and verify that the blade does not have any hardware problems.

If the message persists, replace the blade.

BL-1017

Message `Slot <slot number> Initializing...`

Message Type LOG

Severity INFO

Probable Cause Indicates that the slot has started initializing the ports.

Recommended Action No action is required.

BL-1018

Message `Slot <slot number> Initialization completed.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the slot has completed initializing the ports.

Recommended Action No action is required.

BL-1019

Message `Slot <Slot number>, retry <Retry Number>, internal port retry initialization, <List of internal ports retrying initialization>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the slot had internal ports that are not online. Initiated a retry on ports that failed to go online.

Recommended Action No action is required.

BL-1020

Message `Switch timed out initializing the chips.`

Message Type LOG | FFDC

Severity CRITICAL

Probable Cause Indicates that the switch has failed to initialize the application-specific integrated circuit (ASIC) chips.

Recommended Action Reboot or power cycle the switch. If the message persists, replace the switch.

BL-1021

Message `Retry <Retry Number>, internal port retry initialization, <List of internal ports retrying initialization>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the switch had internal ports that are not online. Initiated a retry on ports that failed to go online.

Recommended Action No action is required.

BL-1022

Message

```
Init Failed: Switch DISABLED because internal ports were not ONLINE, <list of
internal port number not ONLINE>.
```

Message Type

LOG

Severity

CRITICAL

Probable Cause

Indicates that the switch initiation failed because one or more of the internal ports was not online. The switch is faulted.

Recommended Action

Reboot or power cycle the switch.

Additional fault messages precede and follow this error providing more information. Refer to other error messages for recommended action.

If the message persists, replace the switch.

BL-1023

Message

```
Blade in slot <slot number> was reset before blade init completed. As a result the
blade is faulted.
```

Message Type

LOG

Severity

CRITICAL

Probable Cause

Indicates that the blade was reset before the initialization completed.

Recommended Action

Reboot or power cycle the blade using the **slotPowerOff** and **slotPowerOn** commands.

If the message persists, replace the blade.

BL-1024

Message

```
All ports on the blade in slot <slot number> will be reset as part of the firmware
upgrade.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that a recent firmware upgrade caused the blade firmware to be upgraded and resulted in the cold upgrade. As part of the upgrade, all datapath elements were reset.

Recommended Action

No action is required.

BL-1025

Message `All GigE/FCIP/Virtualization/FC Fastwrite ports on the blade in slot <slot number> will be reset as part of the firmware upgrade.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a recent firmware upgrade caused the blade's firmware to be upgraded and resulted in the cold upgrade. As part of the upgrade, all the Gigabit Ethernet, Fibre Channel over IP (FCIP), virtualization data elements, and FC Fastwrite ports were reset.

Recommended Action No action is required.

BL-1026

Message `Internal port offline during warm recovery, state <port state> (0x<port ID>).`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that an internal port went offline during warm recovery of the switch. The switch will reboot and start cold recovery.

Recommended Action Execute the **supportSave** command and then reboot switch. If the problem persists, replace the switch.

BL-1027

Message `Blade in slot <slot number> faulted, boot failed; status 0x<boot status> 0x<1250 0 boot status> 0x<1250 1 boot status>.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that the blade failed to boot properly.

Recommended Action Reboot or power cycle the blade using the **slotPowerOff** and **slotPowerOn** commands.

If the message persists, replace the blade.

BL-1028

Message `Switch faulted; internal processor was reset before switch init completed.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that the switch internal processor was reset before the initialization completed.

Recommended Action Reboot or power cycle the switch using the **slotPowerOff** and **slotPowerOn** commands.

If the message persists, replace the switch.

BL-1029

Message `All ports on the switch will be reset as part of the firmware upgrade.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a recent firmware upgrade caused the switch internal processor firmware to be upgraded and resulted in a cold upgrade. As part of the upgrade, all the datapath elements were reset.

Recommended Action No action is required.

BL-1030

Message `All GigE/FCIP/Virtualization/FC Fastwrite ports on the switch will be reset as part of the firmware upgrade.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a recent firmware upgrade caused the switch internal processor firmware to be upgraded and resulted in the cold upgrade. As part of the upgrade, all Gigabit Ethernet, Fibre Channel over IP (FCIP), virtualization data elements, and FC Fastwrite ports were reset.

Recommended Action No action is required.

BL-1031

Message

```
Link timeout in internal port (slot <slot number>, port <port number>) resulted in
blade fault. Use slotpoweroff/slotpoweron to recover the blade.
```

Message Type

LOG

Severity

CRITICAL

Probable Cause

Indicates that link timeout occurred in one of the back-end internal ports.

Recommended Action

Power cycle the blade using the **slotPowerOff** and **slotPowerOn** commands.

BL-1032

Message

```
(slot <slot number>,bitmap 0x<object control flags(bitmap)>) ports never came up
ONLINE (reason <reason for port disable>, state <status of the blade>). Disabling
slot.
```

Message Type

LOG

Severity

CRITICAL

Probable Cause

Indicates that back-end (non-user) ports have not come online within the time limit.

Recommended Action

Execute the **diagPost** command to make sure that Power-On Self-Test (POST) is enabled; then power cycle the blade using the **slotPowerOff** and **slotPowerOn** commands or have the blade's ejector switch cycled to run POST and verify that the blade does not have any hardware problems.

If the message persists, replace the blade.

BL-1033

Message

```
(slot <slot number>,bitmap 0x<object control flags(bitmap)>) No disable
acknowledgment from ports (state <status of the blade>). Disabling slot.
```

Message Type

LOG

Severity

CRITICAL

Probable Cause

Indicates that the system has timed out waiting for the disable messages from the user ports after disabling the ports.

Recommended Action

Execute the **diagPost** command to make sure that Power-On Self-Test (POST) is enabled; then power cycle the blade using the **slotPowerOff** and **slotPowerOn** commands or have the blade's ejector switch cycled to run POST and verify that the blade does not have any hardware problems.

If the message persists, replace the blade.

BL-1034

Message `Slot <slot number> FC Initialization completed.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the slot has completed initializing the Fibre Channel (FC) ports.

Recommended Action No action is required.

BL-1035

Message `Slot <slot number> iSCSI port <iscsi port number> Initialization completed.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the slot has completed initializing the specified iSCSI port.

Recommended Action No action is required.

BL-1036

Message
```
Faulting 8G blade in slot = <slot number> due to incompatible stag mode. All
EX/VEX ports must be disabled in order to enable the 8G blade in the chassis.
```

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that the 8 Gbps blade with legacy mode (EX_port having stag) will be disabled.

Recommended Action Disable all EX_Ports and VEX_Ports and execute the **slotPowerOff** or **slotPowerOn** commands on the 8 Gbps blade. All EX_Ports and VEX_Ports can be re-enabled.

BL-1037

Message

```
Faulting chip in slot = <slot number>, miniS = <miniS number>,port = <port number>
due to BE/BI port fault.
```

Message Type

LOG

Severity

CRITICAL

Probable Cause

Indicates that all ports on the chip have been disabled due to a fault on the chip.

Recommended Action

Make sure that the blade is seated correctly.

If the blade is seated correctly, execute the **diagPost** command to make sure that Power-On Self-Test (POST) is enabled; then power cycle the blade using the **slotPowerOff** and **slotPowerOn** commands or have the blade's ejector switch cycled to run POST and verify that the blade does not have any hardware problems.

Additional blade fault messages precede and follow this error, providing more information. Refer to other error messages for recommended action.

If the message persists, replace the blade.

BL-1038

Message

```
Inconsistent FPGA image version detected, please reboot the switch for recovery.
```

Message Type

LOG

Severity

CRITICAL

Probable Cause

Indicates that the field-programmable gate array (FPGA) image version is incompatible with the software version.

Recommended Action

Reboot the switch. If the message persists, replace the switch.

BL-1039

Message

```
Inconsistent FPGA image version detected, faulting the blade in slot <slot
number>.
```

Message Type

LOG

Severity

CRITICAL

Probable Cause

Indicates that the field-programmable gate array (FPGA) image version is incompatible with the software version.

Recommended Action

Power cycle the blade using the **slotPowerOff** and **slotPowerOn** commands.

If the message persists, replace the blade.

BL-1041

Message `Dynamic area mode is enabled on default switch, Faulting the blade w/ ID <Blade ID of blade that has the mini SFP+ that does not support it> in slot <slot number> as it does not support this mode.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that the blade does not support dynamic area mode on the default switch.

Recommended Action Turn off the dynamic area mode using the **configure** command.

BL-1045

Message `mini SFP+ (SN: <mini SFP+ serial number>) is only supported in certain high port count blades, not blade in slot <slot number of blade that has the mini SFP+> w/ ID <Blade ID of blade that has the mini SFP+ that does not support it>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that mini-SFP+ is supported only by a certain type of blade (FC8-64), but it can be inserted in other blades.

Recommended Action Replace the mini-SFP+ with an SFP or SFP+.

BL-1046

Message `<Slot number of blade that has the SFP> error on SFP in Slot <Port number into which the SFP is inserted>/Port <The type of error "checksum" or "data access" for general problems accessing the i2c accessible data> (<A detailed error code>). Try reseating or replacing it.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the checksum in an area on the small form-factor pluggable (SFP) transceiver does not match with the computed value, or there is problem accessing the data.

Recommended Action Reseat the SFP transceiver. If problem persists, replace the SFP transceiver.

BL-1047

Message `Buffer optimized mode is turned <buffer optimized mode> for slot <slot number>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the buffer optimized mode is changed for the specified slot.

Recommended Action No action is required.

BL-1048

Message `FCoE Blade in slot <Slot> failed because the Interop mode is enabled on the switch.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the interop mode is turned on in the default switch while powering on the FCoE blade.

Recommended Action Disable the interop mode using the **interopmode** command; then execute the **slotPowerOff** and **slotPowerOn** commands on the FCoE blade.

BL-1049

Message `Serdestunemode: <serdestuning mode>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the SerDes tuning mode is changed for the slot.

Recommended Action No action is required.

BL-1050

Message `Incompatible Blade Processor FPGA version with current FOS firmware in slot=<slot number> on FX8-24. Contact support for upgrade instructions.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the blade processor field-programmable gate array (FPGA) version with current Fabric OS firmware is incompatible on the FX8-24 blade.

Recommended Action Contact your switch service provider for upgrade instructions.

BL-1051

Message `Incompatible Blade Processor FPGA version with current FOS firmware on 7800. Contact support for upgrade instructions.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the blade processor field-programmable gate array (FPGA) version with current Fabric OS firmware is incompatible on the Brocade 7800 switch.

Recommended Action Contact your switch service provider for upgrade instructions.

BL-1052

Message `Link Reset threshold exceeded in the internal port (slot <slot number>, port <port number>). No core blade has been faulted because it has only one active core blade.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the internal port in the core blade exceeded the link reset threshold level. Faulting the peer edge blade because there is only one active core blade.

Recommended Action Replace the core blade.

BL-1053

Message `Invalid E_Port credits <credits> configured for slot <slot number>, port <port number>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that invalid E_Port credits are configured. The old credit model will be retained.

Recommended Action Disable the E_Port credits using the **portcfgeportcredits --disable** command.

BL-1054

Message `QSFP (SN: <QSFP serial number>) is not supported on blade in slot <slot number of blade that has the QSFP> with ID <Blade ID of blade that has the QSFP that does not support it>. Check for compatibility of QSFP with this core or port blade.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the current quad small form-factor pluggable (QSFP) is not supported by this particular type of blade (core or port), but it can be inserted in other blades. Core blades and port blades have their own supported versions of QSFPs.

Recommended Action Replace QSFP that is compatible with the blade.

BL-1055

Message `The octet mode of user port (<Port Number>) in slot:<Slot Number of blade that has the QSFP>, blade ID <Blade ID of blade that has the QSFP that does not support it> is not supported.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that quad small form-factor pluggables (QSFPs) supports only the octet combo 1. If the port is configured in the other 2 modes (2 and 3), there is a mismatch in capabilities.

Recommended Action Set the correct octet combo by using the **portCfgOctetSpeedCombo** command.

BLS Messages

BLS-1000

Message `<command name> of GE <port number> failed. Please retry the command. Data: inst=<ASIC instance> st=<ASIC initializing state> rsn=<reason code> fn=<message function> oid=<ASIC ID>.`

Message Type LOG | FFDC

Severity ERROR

Probable Cause Indicates that the hardware is not responding to a command request, possibly because it is busy.

Recommended Action Retry the command.

BLS-1001

Message `FIPS <FIPS Test Name> failed; algo=<algorithm code> type=<algorithm type> slot=<Slot Number>.`

Message Type LOG | FFDC

Severity CRITICAL

Probable Cause Indicates that a Federal Information Protection Standard (FIPS) failure has occurred and requires faulting the blade or switch.

Recommended Action Retry the command.

BLS-1002

Message `An IPsec/IKE policy was added.`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates that an Internet Protocol Security (IPsec) or Internet Key Exchange (IKE) policy was added and the configuration file was updated.

Recommended Action No action is required.

BLS-1003

Message `An IPsec/IKE policy was deleted.`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates that an Internet Protocol Security (IPsec) or Internet Key Exchange (IKE) policy was deleted and the configuration file was updated.

Recommended Action No action is required.

BLS-1004

Message `Tape Read Pipelining is being disabled slot (<slot number>) port (<user port index>) tunnel (<The configured tunnel ID (0-7)>).`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Fabric OS version on the remote end of the tunnel does not support Tape Read Pipelining.

Recommended Action No action is required.

BLS-1005

Message `S<slot number>,P<user port index>(<blade index>) [OID 0x<port OID>]: <string name of ge>: port faulted due to SFP validation failure. Please check if the SFP is valid for the configuration.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a deteriorated small form-factor pluggable (SFP) transceiver, an incompatible SFP transceiver pair, or a faulty cable between the peer ports.

Recommended Action Verify that compatible SFP transceivers are used on the peer ports, the SFP transceivers have not deteriorated, and the Fibre Channel cable is not faulty. Replace the SFP transceivers or the cable if necessary.

BLZ Messages

BLZ-1000

Message `<command name> of GE <port number> failed. Please retry the command. Data: inst=<ASIC instance> st=<ASIC initializing state> rsn=<reason code> fn=<message function> oid=<ASIC ID>.`

Message Type LOG | FFDC

Severity ERROR

Probable Cause Indicates that the hardware is not responding to a command request, possibly because it is busy.

Recommended Action Retry the command.

BLZ-1001

Message `FIPS <FIPS Test Name> failed; algo=<algorithm code> type=<algorithm type> slot=<Slot Number>.`

Message Type LOG | FFDC

Severity CRITICAL

Probable Cause Indicates that a Federal Information Protection Standard (FIPS) failure has occurred and requires faulting the blade or switch.

Recommended Action Retry the command.

BLZ-1002

Message `An IPsec/IKE policy was added.`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates that an Internet Protocol Security (IPsec) or Internet Key Exchange (IKE) policy was added and the configuration file was updated.

Recommended Action No action is required.

BLZ-1003

Message `An IPsec/IKE policy was deleted.`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates that an Internet Protocol Security (IPsec) or Internet Key Exchange (IKE) policy was deleted and the configuration file was updated.

Recommended Action No action is required.

BLZ-1004

Message `Tape Read Pipelining is being disabled slot (<slot number>) port (<user port index>) tunnel (<The configured tunnel ID (0-7)>).`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Fabric OS version on the remote end of the tunnel does not support Tape Read Pipelining.

Recommended Action No action is required.

BLZ-1005

Message `Datapath Slot:<slot number> Chip:<Chip number> reset during HAreboot.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that datapath chip reset happened during high availability (HA) reboot. Traffic may be disrupted.

Recommended Action Reboot to recover.

BM Messages

BM-1001

Message `BM protocol version <Protocol version> in slot <Slot number>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the firmware running on the control processor (CP) cannot communicate with the application processor (AP) blade in the indicated slot and determine the AP blade's firmware version. The reason can be one of the following:

- The CP blade is running a later version of firmware than the AP blade.
- The CP blade is running an earlier version of firmware than the AP blade.

Recommended Action The problem can be corrected by changing the firmware version on either the CP or on the AP blade. You can modify the firmware version on the CP blade by using the **firmwareDownload** command. Refer to the release notes to determine whether a non-disruptive firmware download is supported between the revisions. Because the AP and CP blades cannot communicate, it is not possible to load new firmware on the AP blade. If necessary, send the AP blade back to the factory for a firmware update.

BM-1002

Message `Connection established between CP and blade in slot <Slot number>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the control processor (CP) has established a connection to the blade processor (BP) and can communicate.

Recommended Action No action is required.

BM-1003

Message
```
Failed to establish connection between CP and blade in slot <Slot number>.
Faulting blade.
```

Message Type LOG | FFDC

Severity WARNING

Probable Cause Indicates that the control processor (CP) could not establish a connection to the blade processor (BP) to communicate.

Recommended Action Execute the **slotPowerOff** and **slotPowerOn** commands or reseat the affected blade.

BM-1004

Message

```
Blade firmware <Blade firmware> on slot <Slot> is not consistent with system
firmware <System firmware>. Auto-leveling blade firmware to match system firmware.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the policy of the specified blade is to auto-level the blade firmware to the system firmware. This may be due to one of the following reasons:

- Blade firmware was detected to be different from the control processor (CP) firmware due to a firmware upgrade.
- The blade was recently inserted and had a different version of the firmware loaded.

Recommended Action No action is required. The blade will automatically download the updated firmware.

BM-1005

Message

```
Firmwaredownload timed-out for blade in slot <Slot>. Faulting blade.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that the **firmwareDownload** command failed for the blade in the specified slot.

Recommended Action Execute the **slotPowerOff** and **slotPowerOn** commands or reseat the affected blade.

BM-1006

Message

```
Blade is not configured. Persistently disabling all ports for blade in slot <Slot
number>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the policy of the specified blade is set to persistently disable all ports the first time the blade is detected. The message indicates either of the following:

- The blade was detected in this slot for the first time.
- The blade was configured under a different mode.

Recommended Action Configure the blade so that it will persistently enable the ports.

BM-1007

Message `If set, clear EX/VEX/FC Fastwrite configuration for all ports for blade in slot <Slot number>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the specified blade was detected for the first time after an FR4-18i was previously configured in the same slot. The new blade requires the specified port configurations to be cleared.

Recommended Action No action is required. The blade ports are cleared automatically.

BM-1008

Message `Download of blade firmware failed for blade in slot <slot>. Reissue firmwaredownload to recover.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the automatic firmware upgrade on the blade failed because the blade firmware version was detected to be different from the control processor (CP) firmware version.

Recommended Action Execute the **firmwareDownload** command to recover the blade.

BM-1009

Message `Firmwaredownload timed-out for application processor. Faulting switch.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the firmware download on the application processor (AP) blade failed.

Recommended Action Execute the **slotPowerOff** and **slotPowerOn** commands or reseat the affected blade.

BM-1010

Message `Resetting port configuration and linkcost for all ports for blade in slot <Slot number>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the specified blade was detected for the first time after an FC10-6 was previously configured in the same slot. The new blade requires resetting the port configuration and linkcost.

Recommended Action No action is required. The blade ports are cleared automatically.

BM-1053

Message `Failed to establish connection between CP and Application Processor. Faulting switch.`

Message Type LOG | FFDC

Severity WARNING

Probable Cause Indicates that the control processor (CP) could not establish a connection with the application processor (AP) to communicate.

Recommended Action Execute the **slotPowerOff** and **slotPowerOn** commands or reseat the affected blade.

BM-1054

Message `AP firmware <Blade firmware> is not consistent with system firmware <System firmware>. Auto-leveling AP firmware to match system firmware.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the policy of the specified blade is set to auto-level the blade firmware to the system firmware. This may be due to one of the following reasons:

- Blade firmware was detected to be different from the control processor (CP) firmware due to a firmware upgrade.
- The blade was recently inserted and had a different version of the firmware loaded.

Recommended Action No action is required. The blade will automatically download the updated firmware.

BM-1055

Message `Firmwaredownload timed-out for AP. Faulting switch.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that firmware download on the application processor (AP) blade has failed.

Recommended Action Execute the **slotPowerOff** and **slotPowerOn** commands or reseat the affected blade.

BM-1056

Message `AP is not configured. Persistently disabling all ports on the switch.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the policy of the specified switch is to persistently disable all ports the first time the AP is detected. This may be caused by one of the following reasons:

- The AP was detected for the first time on this switch.
- The switch was configured under a different mode.

Recommended Action Configure the switch to persistently enable all ports.

BM-1058

Message `Download of AP firmware failed for the switch. Reissue firmwaredownload to recover.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the automatic firmware upgrade on the application processor (AP) failed because the firmware version running on the AP was detected to be different from the system firmware.

Recommended Action Execute the **firmwareDownload** command to recover the AP.

C2 Messages

C2-1001

Message `S<slot number>,P<port number>(Bp<blade port number>) user_idx:<User port index> [PID 0x<24 bit FC address>] faulted due to SFP validation failure. Check if the SFP is valid for the configuration.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a deteriorated small form-factor pluggable (SFP) transceiver, an incompatible SFP transceiver pair, or a faulty cable between the peer ports.

Recommended Action Verify that compatible SFP transceivers are used on the peer ports, the SFP transceivers have not deteriorated, and the Fibre Channel cable is not faulty. Replace the SFP transceivers or the cable if necessary.

C2-1002

Message `Port <port number> chip faulted due to an internal error.`

Message Type LOG | FFDC

Severity ERROR

Probable Cause Indicates an internal error. All the ports on the blade or switch will be disrupted.

Recommended Action To recover a bladed system, execute the **slotPowerOff** and **slotPowerOn** commands on the blade. To recover a non-bladed system, execute the **fastBoot** command on the switch.

C2-1004

Message `S<slot number>,C<chip index>: Invalid DMA ch pointer, chan:<Channel number>, good_addr:0x<Good address> bad_addr:0x<Bad address>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates an internal error in the application-specific integrated circuit (ASIC) hardware that may degrade the data traffic.

Recommended Action Restart the system at the next maintenance window. If the problem persists, replace the blade.

C2-1006

Message

```
S<slot number>,C<chip index>: Internal link errors reported, no hardware faults
identified, continuing monitoring: fault1:0x<fault1_cnt>, fault2:0x<fault2_cnt>
thresh1:0x<threshold_used>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that some internal link errors have been detected. These errors can be normal in an active running system.

The system automatically starts a more detailed monitoring of the errors reported in the internal hardware. There is no action required by the user at this time. If any actual hardware failures are detected, the C2-1010 message will be generated identifying the failing field-replaceable unit (FRU).

Recommended Action No action is required.

C2-1007

Message

```
S<slot number>,P<port number>(<blade port number>): best effort QoS will be turned
off at next port state change as it is not supported under this configuration
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that quality of service (QoS) will be turned off automatically at the next port state change because best effort QoS is no longer supported on 4 Gbps or 8 Gbps platform long distance ports.

Recommended Action No action is required.

C2-1008

Message

```
S<slot number>,P<port number>(<blade port number>): QoS overwrites
portcfglongdistance vc_translation_link_init. ARB will be used on the link.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that quality of service (QoS) has overwritten the fill word IDLE used on the long distance links. Arbitrated loop (ARB) will be used on the link.

Recommended Action No action is required.

C2-1009

Message

```
S<slot number>,P<port number>(<blade port number>): portcfglongdistance
vc_translation_link_init = 1 overwrites fill word IDLE. ARB will be used on the
link.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the **portcfglongdistance vc_translation_link_init 1** command has overwritten the fill word IDLE. Arbitrated loop (ARB) will be used on the link.

Recommended Action

No action is required.

C2-1010

Message

```
S<slot number>,C<chip index>: Internal monitoring has identified suspect
hardware, blade may need to be reset or replaced: fau1:0x<fault1_cnt>,
fau2:0x<fault2_cnt> th2:0x<threshold_used>.
```

Message Type

LOG

Severity

CRITICAL

Probable Cause

Indicates that above-normal errors were observed in hardware that may or may not impact the data traffic.

Recommended Action

When this error is observed persistently, power cycle the specified blade using the **slotPowerOff** and **slotPowerOn** commands. If the problem persists, replace the blade.

C2-1012

Message

```
S<slot number>,P<port number>(<blade port number>): Link Timeout on internal port
ftx=<frame transmitted> tov=<real timeout value> (><expected timeout value>)
vc_no=<vc number> crd(s)lost=<Credit(s) lost> complete_loss:<complete credit
loss>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that one or more credits have been lost on a back-end port, and there is no traffic on that port for two seconds.

Recommended Action

Turn on the back-end credit recovery to reset the link and recover the lost credits. If credit recovery has already been turned on, the link will be reset to recover the credits and no action is required.

C2-1013

Message `S<slot number>,P<port number>(<blade port number>): Duplicate rte_tbl_select detected.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the selected table is corrupted.

Recommended Action This message must have a matching message for the other duplicate table. Reset both the specified ports. If it is a trunk, reset the entire trunk.

C2-1014

Message `Link Reset on Port S<slot number>,P<port number>(<blade port number>) vc_no=<vc number> crd(s)lost=<Credit(s) lost> <Source of link reset > trigger.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that one or more credits are lost and the link is reset.

Recommended Action When this error is observed persistently, power cycle the specified blade using the **slotPowerOff** and **slotPowerOn** commands. If the problem persists, replace the blade.

C2-1015

Message `Port re-initialized due to Link Reset failure on internal Port S<slot number>,P<port number>(<blade port number>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the specified port is re-initialized due to link reset failure.

Recommended Action When this error is observed persistently, power cycle the specified blade using the **slotPowerOff** and **slotPowerOn** commands. If the problem persists, replace the blade.

C2-1016

Message `Port is faulted due to port re-initialization failure on internal Port S<slot number>,P<port number>(<blade port number>) with reason <port fault reason>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified port failed due to port re-initialization failure.

Recommended Action When this error is observed persistently, power cycle the specified blade using the **slotPowerOff** and **slotPowerOn** commands. If the problem persists, replace the blade.

C2-1017

Message `Blade in Slot <slot number> failed due to unavailability of ports in the internal trunk.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified blade failed because of the unavailability of the ports in the internal trunk.

Recommended Action When this error is observed persistently, power cycle the specified blade using the **slotPowerOff** and **slotPowerOn** commands. If the problem persists, replace the blade.

C2-1018

Message `Link reset threshold value exceeded in the link S<slot number>,P<port number>(<blade port number>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified blade is faulted because the link reset threshold value has exceeded.

Recommended Action When this error is observed persistently, power cycle the specified blade using the **slotPowerOff** and **slotPowerOn** commands. If the problem persists, replace the blade.

C2-1019

Message `S<slot number>,C<chip index>: HW ASIC Chip TXQ FID parity error threshold reached type = 0x<chip error type>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that an internal error is observed in the application-specific integrated circuit (ASIC) hardware that may degrade the data traffic.

Recommended Action Restart the system at the next maintenance window.

C2-1020

Message `S<slot number>,P<port number>(<blade port number>): Internal CRC with good EOF errors were observed, continuing monitoring. current:0x<last_crc_good_eof_cnt>, last:0x<total_crc_good_eof_cnt> thresh1:0x<threshold_used>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates some CRC errors detected on backend link by hardware, typically applications are not affected at this low count.

Recommended Action No action is required.

C2-1025

Message `S<slot number>,P<port number>(<blade port number>): Extra credit on F_port:ftx=<ftx> curr_cred=<current credits> actual_cred=<actual credits>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the device is returning the wrong number of receiver-ready (R_RDY) frames.

Recommended Action When this error is observed persistently, replace the device.

C2-1026

Message `S<slot number>,P<port number>(<blade port number>): Faulting F_port due to extra credit detected:ftx=<ftx> curr_cred=<current credits> actual_cred=<actual credits>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the device is returning the wrong number of receiver-ready (R_RDY) frames.

Recommended Action When this error is observed persistently, replace the device.

C2-1027

Message `Detected credit loss on Peer internal Port of Slot <slot number>, Port <port number>(<blade port number>) vc_no=<vc number> crd(s)lost=<Credit(s) lost> complete_loss:<complete credit loss>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that credit loss was detected on the peer port.

Recommended Action When this error is observed persistently, power cycle the specified blade using the **slotPowerOff** and **slotPowerOn** commands. If the problem persists, replace the blade.

C2-1028

Message `Detected excessive Link resets on the port in a second. Slot <slot number>, Port <port number>(<blade port number>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the port received excessive link resets from peer port within 1 second and that exceeded threshold.

Recommended Action When this error is observed persistently, change the small form-factor pluggable (SFP) transceiver or the cable on the peer port to which this port is connected.

C2-1029

Message `Detected credit loss on Port of Slot <slot number>, Port <port number>(<blade port number>) vc_no=<vc number> crd(s)lost=<Credit(s) lost> complete_loss:<complete credit loss>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that credit loss was detected on the port.

Recommended Action When this error is observed persistently, power cycle the specified blade using the **slotPowerOff** and **slotPowerOn** commands. If the problem persists, replace the blade.

C2-1030

Message `S<slot number>,P<port number>(<blade port number>): Internal CRC with good EOF errors exceeded threshold, tuning is required. current:0x<last_crc_good_eof_cnt>, last:0x<total_crc_good_eof_cnt> thresh2:0x<threshold_used>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates some CRC errors detected on backend link by hardware, applications may be affected.

Recommended Action If core blade reset, auto tuning or manual tuning did not resolve the issue, replace the blade.

C2-1031

Message `Loss of Sync occured on Slot <slot number>, Port <port number>(<blade port number>).`

Message Type LOG

Severity INFO

Probable Cause Indicates that loss of synchronization has occurred on the BE port and link reset was invoked on this port by the blade driver.

Recommended Action No action is required.

C2-1032

Message

```
S<slot number>,P<port number>(<blade port number>): Required buffer unavailable
for the port. req_buf:<required buffer> port_buf:<port buffer> unused_buf:<Unused
buffer> est_buf:<Estimated buffer>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that free buffers in the chip are not sufficient to bring the port online in fully operational mode. The port may not come online or may operate in a degraded buffer mode.

Recommended Action

If one or more ports that are configured as long distance in the chip are unused, reset these ports to normal distance. If the problem persists, move the affected port to a different blade or chip.

C3 Messages

C3-1001

Message `S<slot number>,P<port number>(Bp<blade port number>) user_idx:<User port index> [PID 0x<24 bit FC address>] faulted due to SFP validation failure. Check if the SFP is valid for the configuration.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a deteriorated small form-factor pluggable (SFP) transceiver, an incompatible SFP transceiver pair, or a faulty cable between the peer ports.

Recommended Action Verify that compatible SFP transceivers are used on the peer ports, the SFP transceivers have not deteriorated, and the Fibre Channel cable is not faulty. Replace the SFP transceivers or the cable if necessary.

C3-1002

Message `Port <port number> chip failed due to an internal error.`

Message Type LOG | FFDC

Severity ERROR

Probable Cause Indicates an internal error. All the ports on the blade or switch will be disrupted.

Recommended Action To recover a bladed system, execute the **slotPowerOff** and **slotPowerOn** commands on the blade. To recover a non-bladed system, execute the **fastBoot** command on the switch.

C3-1004

Message `S<slot number>,C<chip index>: Invalid DMA ch pointer, chan:<Channel number>, good_addr:0x<Good address> bad_addr:0x<Bad address>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates an internal error in the application-specific integrated circuit (ASIC) hardware that may degrade the data traffic.

Recommended Action Reboot the system at the next maintenance window. If the problem persists, replace the blade.

C3-1006

Message `S<slot number>,C<chip index>: Various non-critical hardware errors were observed: fault1:0x<fault1_cnt>, fault2:0x<fault2_cnt> thresh1:0x<threshold_used>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that some errors were found in hardware that may or may not impact the data traffic.

Recommended Action No action is required. Usually these errors are transient.

C3-1007

Message `S<slot number>,P<port number>(<blade port number>): best effort QoS will be turned off at next port state change as it is not supported under this configuration.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that quality of service (QoS) will be turned off automatically at the next port state change because best effort QoS is no longer supported on 4 Gbps or 8 Gbps platform long distance ports.

Recommended Action No action is required.

C3-1008

Message `S<slot number>,P<port number>(<blade port number>): QoS overwrites portcfglongdistance vc_translation_link_init. ARB will be used on the link.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that quality of service (QoS) has overwritten the fill word IDLE used on the long distance links. Arbitrated loop (ARB) will be used on the link.

Recommended Action No action is required.

C3-1009

Message `S<slot number>,P<port number>(<blade port number>): portcfglongdistance vc_translation_link_init = 1 overwrites fill word IDLE. ARB will be used on the link.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the **portcfglongdistance vc_translation_link_init 1** command has overwritten the fill word IDLE. Arbitrated loop (ARB) will be used on the link.

Recommended Action No action is required.

C3-1010

Message `S<slot number>,C<chip index>: Above normal hardware errors were observed: fault1:0x<fault1_cnt>, fault2:0x<fault2_cnt> thresh2:0x<threshold_used>.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that above-normal errors were observed in hardware that may or may not impact the data traffic.

Recommended Action When this error is observed persistently, power cycle the specified blade using the **slotPowerOff** and **slotPowerOn** commands. If the problem persists, replace the blade.

C3-1011

Message `Detected a complete loss of credit on internal back-end VC: Slot <slot number>, Port <port number>(<blade port number>) vc_no=<vc number> crd(s)lost=<Credit(s) lost>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that all credits have been lost on the specified virtual channel (VC) and port.

Recommended Action Turn on the back-end credit recovery to reset the link and recover the lost credits. If credit recovery has already been turned on, the link will be reset to recover the credits and no action is required.

C3-1012

Message

```
S<slot number>,P<port number>(<blade port number>): Link Timeout on internal port
ftx=<frame transmitted> tov=<real timeout value> (><expected timeout value>)
vc_no=<vc number> crd(s)lost=<Credit(s) lost> complete_loss:<Compless credit
loss>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that one or more credits have been lost on a back-end port, and there is no traffic on that port for two seconds.

Recommended Action Turn on the back-end credit recovery to reset the link and recover the lost credits. If credit recovery has already been turned on, the link will be reset to recover the credits and no action is required.

C3-1013

Message

```
Multi RDY/Frame Loss detected on Slot <slot number>, Port <port number>(<blade
port number>) m_rdy(0x<Multiple Credit(s) Lost>)/m_frame(0x<Multiple Frame(s)
Lost>).
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that wait cycles to recover the lost frame or credit are exceeded on the specified port.

Recommended Action Turn on the back-end credit recovery to reset the link and recover the lost credits. If credit recovery has already been turned on, the link will be reset to recover the credits and no action is required.

C3-1014

Message

```
Link Reset on Port S<slot number>,P<port number>(<blade port number>) vc_no=<vc
number> crd(s)lost=<Credit(s) lost> <Source of link reset > trigger.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that one or more credits were lost and the link is reset.

Recommended Action When this error is observed persistently, power cycle the specified blade using the **slotPowerOff** and **slotPowerOn** commands. If the problem persists, replace the blade.

C3-1015

Message `Port re-initialized due to Link Reset failure on internal Port S<slot number>,P<port number>(<blade port number>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the specified port is re-initialized due to link reset failure.

Recommended Action When this error is observed persistently, power cycle the specified blade using the **slotPowerOff** and **slotPowerOn** commands. If the problem persists, replace the blade.

C3-1016

Message `Port is faulted due to port re-initialization failure on internal Port S<slot number>,P<port number>(<blade port number>) with reason <port fault reason>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified port failed due to port re-initialization failure.

Recommended Action When this error is observed persistently, power cycle the specified blade using the **slotPowerOff** and **slotPowerOn** commands. If the problem persists, replace the blade.

C3-1017

Message `Blade in Slot-<slot number> failed due to unavailability of ports in the internal trunk.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified blade failed because of the unavailability of the ports in the internal trunk.

Recommended Action When this error is observed persistently, power cycle the specified blade using the **slotPowerOff** and **slotPowerOn** commands. If the problem persists, replace the blade.

C3-1018

Message `Link reset threshold value exceeded in the link S<slot number>,P<port number>(<blade port number>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified blade is faulted because the link reset threshold value has exceeded.

Recommended Action When this error is observed persistently, power cycle the specified blade using the **slotPowerOff** and **slotPowerOn** commands. If the problem persists, replace the blade.

C3-1019

Message `S<slot number>,C<chip index>: HW ASIC Chip TXQ FID parity error threshold reached type = 0x<chip error type>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that an internal error is observed in the application-specific integrated circuit (ASIC) hardware that may degrade the data traffic.

Recommended Action Restart the system at the next maintenance window.

C3-1020

Message `S<slot number>,P<port number>(<blade port number>): Internal CRC with good EOF errors were observed, continuing monitoring. current:0x<last_crc_good_eof_cnt>, last:0x<total_crc_good_eof_cnt> thresh1:0x<threshold_used>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates some CRC errors detected on backend link by hardware, typically applications are not affected at this low count.

Recommended Action No action is required.

C3-1021

Message `S<slot number>,P<port number>(<blade port number>): Port is offline due to Encryption Compression Block error.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that an internal error is observed in the application-specific integrated circuit (ASIC) hardware that may degrade the data traffic.

Recommended Action When this error occurs, the software will automatically recover from the error and no action is required. However, if the problem persists, replace the blade.

C3-1023

Message `Single RDY/Frame Loss detected and recovered on Slot <slot number>,Port <port number>(<blade port number>) rdy(0x<Credit Lost>)/frame(0x<Frame Lost>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that above-normal errors are observed in hardware that may or may not impact the data traffic.

Recommended Action When this error is observed persistently, power cycle the specified blade using the **slotPowerOff** and **slotPowerOn** commands. If the problem persists, replace the blade.

C3-1025

Message `S<slot number>,P<port number>(<blade port number>): Extra credit on F_port:ftx=<ftx> curr_cred=<current credits> actual_cred=<actual credits>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the device is returning the wrong number of receiver-ready (R_RDY) frames.

Recommended Action When this error is observed persistently, replace the device.

C3-1026

Message

```
S<slot number>,P<port number>(<blade port number>): Faulting F_port due to extra
credit detected:ftx=<ftx> curr_cred=<current credits> actual_cred=<actual
credits>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that the device is returning the wrong number of receiver-ready (R_RDY) frames.

Recommended Action When this error is observed persistently, replace the device.

C3-1027

Message

```
Detected credit loss on Peer internal Port of Slot <slot number>, Port <port
number>(<blade port number>) vc_no=<vc number> crd(s)lost=<Credit(s) lost>
complete_loss:<complete credit loss>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that credit loss was detected on the peer port.

Recommended Action When this error is observed persistently, power cycle the specified blade using the **slotPowerOff** and **slotPowerOn** commands. If the problem persists, replace the blade.

C3-1028

Message

```
Detected excessive Link resets on the port in a second. Slot <slot number>, Port
<port number>(<blade port number>).
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that the port received excessive link resets from peer port within 1 second and that exceeded the threshold.

Recommended Action When this error is observed persistently, change the small form-factor pluggable (SFP) transceiver or the cable on the peer port to which this port is connected.

C3-1030

Message `S<slot number>,P<port number>(<blade port number>): Internal CRC with good EOF errors exceeded threshold, tuning is required. current:0x<last_crc_good_eof_cnt>, last:0x<total_crc_good_eof_cnt> thresh2:0x<threshold_used>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates some CRC errors detected on backend link by hardware, applications may be affected.

Recommended Action If core blade reset, auto tuning or manual tuning did not resolve the issue, replace the blade.

C3-1032

Message `S<slot number>,P<port number>(<blade port number>): Required buffer unavailable for the port. req_buf:<required buffer> port_buf:<port buffer> unused_buf:<Unused buffer> est_buf:<Estimated buffer>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that free buffers in the chip are not sufficient to bring the port online in fully operational mode. The port may not come online or may operate in a degraded buffer mode.

Recommended Action If one or more ports that are configured as long distance in the chip are unused, reset these ports to normal distance. If the problem persists, move the affected port to a different blade or chip.

C3-1033

Message `S<slot number>,P<port number>(<blade port number>): FEC TTS is only supported on F_Port.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that Forward Error Correction (FEC) TTS is enabled on the specified port. The FEC TTS option is supported only on F_Ports.

Recommended Action Disable the FEC TTS option using the **portcfgfec --disable -TTS** command.

C3-1034

Message

```
S<slot number>,P<port number>(<blade port number>): FEC is Enabled but FEC is
Inactive. Check peer port's FEC configurations.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that Forward Error Correction (FEC) is enabled but is inactive on the specified port.

Recommended Action

Check local and peer port's FEC configurations using the **portcfgfec --show** command.

CAL Messages

CAL-1001

Message `Switch offline requested by remote domain <domain number>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified remote domain requested the local domain to be disabled.

Recommended Action Check the error message log on the remote domain using the **errShow** command to find the reason.

CCFG Messages

CCFG-1001

Message `Failed to initialize <module>, rc = <error>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the initialization of a module within the Converged Enhanced Ethernet (CEE) configuration management daemon has failed.

Recommended Action Download a new firmware version using the **firmwareDownload** command.

CCFG-1002

Message `Started loading CEE system configuration.`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates that the Converged Enhanced Ethernet (CEE) system configuration has started loading.

Recommended Action No action is required.

CCFG-1003

Message `System is ready to accept CEE user commands.`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates that the Converged Enhanced Ethernet (CEE) shell is ready to accept configuration commands.

Recommended Action No action is required.

CCFG-1004

Message `Configuration replay failed due to missing system startup configuration file.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the startup configuration file has been moved or deleted and therefore replaying the system configuration has failed.

Recommended Action Execute the **copy file startup-config** command to restore the startup configuration file from any backup retrieved on the server.

CCFG-1005

Message `Startup configuration file is updated.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the startup configuration file has been updated.

Recommended Action No action is required.

CCFG-1006

Message `Current system running configuration file is updated.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the current running configuration file has been updated.

Recommended Action No action is required.

CCFG-1007

Message `Startup configuration is deleted.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the startup configuration file has been moved or deleted.

Recommended Action No action is required.

CCFG-1008

Message `CMSH init failed: <msg>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the CEE Management Shell (CMSH) initialization has failed.

Recommended Action No action is required.

CCFG-1009

Message `Successfully copied to <destination>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a configuration file has been copied to the specified destination.

Recommended Action No action is required.

CCFG-1010

Message `Current system running configuration file is updated partially.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the current running configuration file has been updated partially.

Recommended Action No action is required.

CCFG-1011

Message `Linecard configuration mismatch on slot <slot>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the inserted line card is different from the pre-configured line card on the specified slot.

Recommended Action Execute the **no linecard** command to remove the line card configuration.

CCFG-1012

Message `Blade in slot <slot> failed to reach ONLINE state within <timeout> seconds after receiving system ready.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the blade in the specified slot has failed to come online within the specified timeout interval after receiving the system ready event.

Recommended Action Execute the **slotPowerOff** and **slotPowerOn** commands on the specified slot to bring the blade online.

CCFG-1013

Message `<mode_command>.`

Message Type AUDIT

Class CFG

Severity INFO

Probable Cause Indicates that the switch state has changed.

Recommended Action No action is required.

CDR Messages

CDR-1001

Message `Port <port number> port fault. Change the SFP or check cable.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a deteriorated small form-factor pluggable (SFP) transceiver, an incompatible SFP transceiver pair, a faulty cable between the peer ports, or the port speed configuration does not match the capability of the SFP transceiver.

Recommended Action Verify that compatible SFP transceivers are used on the peer ports, the SFP transceivers have not deteriorated, and the Fibre Channel cable is not faulty. Replace the SFP transceivers or the cable if necessary.

CDR-1002

Message `Port <port number> chip faulted due to internal error.`

Message Type LOG | FFDC

Severity ERROR

Probable Cause Indicates an internal error. All the ports on the blade or switch will be disrupted.

Recommended Action To recover a bladed system, execute the **slotPowerOff** and **slotPowerOn** commands on the blade. To recover a non-bladed system, execute the **fastBoot** command on the switch.

CDR-1003

Message `S<slot number>,C<chip index>: HW ASIC Chip error type = 0x<chip error type>. If the problem persists, blade may need to be reset or replaced.`

Message Type LOG

Severity WARNING

Probable Cause Indicates an internal error in the application-specific integrated circuit (ASIC) hardware that may degrade the data traffic.

Recommended Action Restart the system at the next maintenance window. If the problem persists, replace the blade.

CDR-1004

Message `S<slot number>,C<chip index>: Invalid DMA ch pointer, chan:<Channel number>, good_addr:0x<Good address> bad_addr:0x<Bad address>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates an internal error in the application-specific integrated circuit (ASIC) hardware that may degrade the data traffic.

Recommended Action Restart the system at the next maintenance window. If the problem persists, replace the blade.

CDR-1005

Message `S<slot number>,P<port number>(<blade port number>): best effort QoS will be turned off at next port state change as it is not supported under this configuration.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that quality of service (QoS) will be turned off automatically at the next port state change because best effort QoS is no longer supported on 4 Gbps or 8 Gbps platform long distance ports.

Recommended Action No action is required.

CDR-1006

Message `S<slot number>,P<port number>(<blade port number>): QoS overwrites portcfglongdistance vc_translation_link_init. ARB will be used on the link.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that quality of service (QoS) has overwritten the fill word IDLE used on the long distance links. Arbitrated loop (ARB) will be used on the link.

Recommended Action No action is required.

CDR-1007

Message `S<slot number>,C<chip index>: Internal link errors have been reported, no hardware faults identified, continuing to monitor for errors: flt1:0x<fault1_cnt>, flt2:0x<fault2_cnt> thresh1:0x<threshold_used>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that some errors were found in hardware that may or may not impact the data traffic.

Recommended Action No action is required.

CDR-1008

Message `S<slot number>,C<chip index>: HW ASIC Chip warning Level 1 type = 0x<chip error type>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates an internal error in the application-specific integrated circuit (ASIC) hardware that may or may not degrade the data traffic.

Recommended Action Restart the system at the next maintenance window.

CDR-1009

Message `S<slot number>,C<chip index>: HW ASIC Chip warning Level 2 type = 0x<chip error type>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates an internal error in the application-specific integrated circuit (ASIC) hardware that may or may not degrade the data traffic.

Recommended Action Restart the system at the next maintenance window.

CDR-1010

Message `S<slot number>,C<chip index>: Internal monitoring of faults has identified suspect hardware, blade may need to be reset or replaced: fault1:0x<fault1_cnt>, fault2:0x<fault2_cnt> thresh2:0x<threshold_used>.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that above-normal errors observed in hardware that may or may not impact the data traffic.

Recommended Action When this error is observed persistently, power cycle the specified blade using the **slotPowerOff** and **slotPowerOn** commands. If the problem persists, replace the blade.

CDR-1011

Message `S<slot number>,P<port number>(<blade port number>): Link Timeout on internal port ftx=<frame transmitted> tov=<real timeout value> (><expected timeout value>) vc_no=<vc number> crd(s)lost=<Credit(s) lost> complete_loss:<complete credit loss>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that one or more credits have been lost on a back-end port, and there is no traffic on that port for two seconds.

Recommended Action Turn on the back-end credit recovery to reset the link and recover the lost credits. If credit recovery has already been turned on, the link will be reset to recover the credits and no action is required.

CDR-1012

Message `S<slot number>,P<port number>(<blade port number>): Port Fault: Hard <Hard fault>(<Fault reason>) fault1=<Fault1 count> fault2=<Fault2 count> (0x<LIP and LLI fault count> 0x<RX_FIFO and HSS fault count> 0x<BWAIT fault count>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the specified port has failed. Port initialization will be retried.

Recommended Action Replace the SFP transceiver and the cable and then re-enable the port.

CDR-1014

Message `Link Reset on Internal Port S<slot number>,P<port number>(<blade port number>) vc_no=<vc number> crd(s)lost=<Credit(s) lost>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that one or more credits were lost and the link is reset.

Recommended Action When this error is observed persistently, power cycle the specified blade using the **slotPowerOff** and **slotPowerOn** commands. If the problem persists, replace the blade.

CDR-1015

Message `Port re-initialized due to Link Reset failure on internal Port S<slot number>,P<port number>(<blade port number>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that specified port got re-initialized due to link reset failure.

Recommended Action When this error is observed persistently, power cycle the specified blade using the **slotPowerOff** and **slotPowerOn** commands. If the problem persists, replace the blade.

CDR-1016

Message `Port is faulted due to port re-initialization failure on internal Port S<slot number>,P<port number>(<blade port number>) with reason <port fault reason>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified port is faulted due to port re-initialization failure.

Recommended Action When this error is observed persistently, power cycle the specified blade using the **slotPowerOff** and **slotPowerOn** commands. If the problem persists, replace the blade.

CDR-1017

Message `Blade in Slot <slot number> faulted due to unavailable ports in internal Trunk.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified blade is faulted due to unavailable ports in internal trunk.

Recommended Action When this error is observed persistently, power cycle the specified blade using the **slotPowerOff** and **slotPowerOn** commands. If the problem persists, replace the blade.

CDR-1018

Message `Blade in Slot <slot number> faulted due to Link reset threshold value exceeded.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified blade is faulted because the link reset threshold is exceeded.

Recommended Action When this error is observed persistently, power cycle the specified blade using the **slotPowerOff** and **slotPowerOn** commands. If the problem persists, replace the blade.

CDR-1019

Message
```
S<slot number>,C<chip index>: HW ASIC Chip TXQ FID parity error threshold reached
type = 0x<chip error type>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that an internal error is observed in the application-specific integrated circuit (ASIC) hardware that may degrade the data traffic.

Recommended Action Restart the system at the next maintenance window.

CDR-1022

Message

```
S<slot number>,P<port number>(<blade port number>): Link Timeout on External port,
ftx=<frame transmitted> tov=<real timeout value> (><expected timeout value>)
vc_no=<vc number> crd(s)lost=<Credit(s) lost>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that above-normal errors are observed in hardware that may or may not impact the data traffic.

Recommended Action

When this error is observed persistently, power cycle the specified blade using the **slotPowerOff** and **slotPowerOn** commands. If the problem persists, replace the blade.

CDR-1028

Message

```
Detected excessive Link resets on the port in a second. Slot <slot number>, Port
<port number>(<blade port number>).
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the port received excessive link resets from peer port within 1 second and that exceeded threshold.

Recommended Action

When this error is observed persistently, change the small form-factor pluggable (SFP) transceiver or the cable on the peer port to which this port is connected.

CHS Messages

CHS-1002

Message `ki_gd_register_action failed with rc = <return val>.`

Message Type LOG | FFDC

Severity ERROR

Probable Cause Indicates an internal error.

Recommended Action To recover a bladed system, execute the **slotPowerOff** and **slotPowerOn** commands on the blade. To recover a non-bladed system, execute the **fastBoot** command on the switch.

CHS-1003

Message `Slot ENABLED but Not Ready during recovery, disabling slot = <slot number> rval = <return value>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the slot state has been detected as inconsistent during failover or recovery.

Recommended Action For a bladed switch, execute the **slotPowerOff** and **slotPowerOn** commands to power cycle the blade.

For a non-bladed switch, restart or power cycle the switch.

CHS-1004

Message `Blade attach failed during recovery, disabling slot = <slot number>, rval = <return value>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified blade has failed during failover or recovery.

Recommended Action For a bladed switch, execute the **slotPowerOff** and **slotPowerOn** commands to power cycle the blade.

For a non-bladed switch, restart or power cycle the switch.

CHS-1005

Message `Diag attach failed during recovery, disabling slot = <slot number>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the diagnostic blade attach operation has failed during failover or recovery.

Recommended Action For a bladed switch, execute the **slotPowerOff** and **slotPowerOn** commands to power cycle the blade.

For a non-bladed switch, restart or power cycle the switch.

CNM Messages

CNM-1001

Message `Failed to allocate memory: (<function name>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified function has failed to allocate memory.

Recommended Action Check memory usage on the switch using the **memShow** command.
Restart or power cycle the switch.

CNM-1002

Message `Failed to initialize <module> rc = <error>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the initialization of a module within the Cluster Node Manager (CNM) has failed.

Recommended Action Download a new firmware version using the **firmwareDownload** command.

CNM-1003

Message `Crypto device cfg between local switch (<local domain id>) and peer (<peer domain id>) out of sync. New encryption session not allowed.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the encryption engine nodes in the cluster encryption group have different configurations.

Recommended Action Synchronize the configuration in the cluster group using the **cryptocfg** command.

CNM-1004

Message `iSCSI service is <status> on the switch.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the crypto service is enabled or disabled on the switch.

Recommended Action No action is required.

CNM-1005

Message `Posting event CNM_EVT_GRP_LEADER_ELECTED Name [<nodeName>], WWN [<WWN>].`

Message Type LOG

Severity INFO

Probable Cause Indicates that the cluster Encryption Group (EG) leader is elected.

Recommended Action No action is required.

CNM-1006

Message `Posting event CNM_EVT_NODE_JOIN nodeName [<nodeName>], WWN [<WWN>], ipaddress [<IP address>].`

Message Type LOG

Severity INFO

Probable Cause Indicates that the member node has joined.

Recommended Action No action is required.

CNM-1007

Message `Posting event CNM_EVT_GRP_LEADER_FAILED Name [<nodeName>]`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Encryption Group (EG) leader has failed.

Recommended Action No action is required.

CNM-1008

Message `Posting event CNM_EVT_NODE_EJECT nodeName [<nodeName>], WWN [<WWN>].`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified node is ejected from the Encryption Group (EG).

Recommended Action No action is required.

CNM-1009

Message `Posting event CNM_EVT_STANDALONE_MODE.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the node is in standalone mode.

Recommended Action No action is required.

CNM-1010

Message `Posting event CNM_EVT_CLUSTER_UDATA_UPDATE cid [<client id>], ulen [<udata len>].`

Message Type LOG

Severity INFO

Probable Cause Indicates the client data update.

Recommended Action No action is required.

CNM-1011

Message `Posting event CNM_EVT_NODE_JOIN_TIMEOUT nodeName [<nodeName>], WWN [<wwn>], ipaddress [<ipAddr>].`

Message Type LOG

Severity INFO

Probable Cause Indicates the node join timeout.

Recommended Action Take the peer node offline, and rejoin the node to Encryption Group (EG).

CNM-1012

Message `Posting event CNM_EVT_EG_DELETED.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Encryption Group (EG) is deleted.

Recommended Action No action is required.

CNM-1013

Message `Posting event GL Node Split condition, isolating peer GL node <nodeName>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Encryption Group (EG) is split.

Recommended Action No action is required.

CNM-1014

Message `Posting event Node Admission Control passed, admitting node [<nodeName>].`

Message Type LOG

Severity INFO

Probable Cause Indicates that the node admission control was successful.

Recommended Action No action is required.

CNM-1015

Message `Posting event Potential Cluster Split condition.`

Message Type LOG

Severity INFO

Probable Cause Indicates a Potential Cluster Split condition.

Recommended Action No action is required.

CNM-1016

Message `Posting event Detected a EG degrade condition.`

Message Type LOG

Severity INFO

Probable Cause Indicates an Encryption Group (EG) degrade condition.

Recommended Action No action is required.

CNM-1017

Message `Got JOIN REQUEST from un-recognized GL node [<rxglname>], configured GL node is [<glname>].`

Message Type LOG

Severity INFO

Probable Cause Indicates a join request was received from an invalid group leader (GL) node.

Recommended Action No action is required.

CNM-1018

Message `Got CNM_FSM_EVT_JOIN_REQ when already a member, My assigned name [<nodename>], dropping request.`

Message Type LOG

Severity INFO

Probable Cause Indicates the node is already a member of the Encryption Group (EG).

Recommended Action No action is required.

CNM-1019

Message `Join Rejected by GL node, fix certificate and later add member node from GL node, or reboot the member node.`

Message Type LOG

Severity INFO

Probable Cause Indicates an invalid member node certificate.

Recommended Action Install a valid certificate and add member node to the group leader (GL) node, or reboot the member node.

CNM-1020

Message `Node Admission Control failed due to mismatch in certificates, rejecting node [<nodename>].`

Message Type LOG

Severity INFO

Probable Cause Indicates that node admission control has failed.

Recommended Action No action is required.

CNM-1021

Message `Failed to sign the node authentication message, admission control might fail.`

Message Type LOG

Severity INFO

Probable Cause Indicates that node admission control has failed.

Recommended Action No action is required.

CNM-1022

Message `Operation not allowed on GL Node.`

Message Type LOG

Severity INFO

Probable Cause Indicates an operation is not allowed on a group leader (GL) node.

Recommended Action No action is required.

CNM-1023

Message `Group Leader node eject is not allowed.`

Message Type LOG

Severity INFO

Probable Cause Indicates an eject operation is not allowed in group leader (GL) node.

Recommended Action No action is required.

CNM-1024

Message `Operation not required on GL node.`

Message Type LOG

Severity INFO

Probable Cause Indicates an operation is not required on a group leader (GL) node.

Recommended Action No action is required.

CNM-1025

Message `Operation not allowed, as member is active with the Cluster. Eject member node and retry.`

Message Type LOG

Severity INFO

Probable Cause Indicates an operation is not allowed on a member node.

Recommended Action Eject member node and retry the operation.

CNM-1026

Message `Recvd HBT Msg with version mismatch, Recvd Hdr version 0x<received hardware version> Exp Hdr version 0x<expected hardware version> Node <WWN>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a version mismatch has occurred.

Recommended Action Upgrade the firmware or delete the node from the Encryption Group (EG).

CNM-1027

Message `Received HBT from non-Group Member Node [<WWN>].`

Message Type LOG

Severity INFO

Probable Cause Indicates an operation is not allowed on a non-group member node.

Recommended Action No action is required.

CNM-1028

Message `Certfile <certificate file name> already exists. No need to sync up.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the certificate file for the node already exists.

Recommended Action No action is required.

CNM-1029

Message `Certfile <certificate file name> content does not match the cert sent by GL.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the contents of the node's certificate file is different from the certificate file sent by the group leader (GL) node.

Recommended Action No action is required.

CNM-1030

Message `Certfile <certificate file name> read less number of bytes <nbytes>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the read operation of the certificate file returned a fewer number of bytes than expected.

Recommended Action No action is required.

CNM-1031

Message `Certfile <certificate file name> open failed with errno <error num>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that an attempt to open the certificate file has failed.

Recommended Action No action is required.

CNM-1032

Message `Certfile <certificate file name> size <file size> does not match cert file size <length> sent by GL.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that there is a size mismatch between a node's certificate file and the certificate file received from the group leader (GL).

Recommended Action No action is required.

CNM-1033

Message `Some of the defined nodes in the Encryption Group are not ONLINE. Encryption Group is in degraded state.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the cluster is in a degraded state.

Recommended Action No action is required.

CNM-1034

Message `All the defined nodes in the Encryption Group are ONLINE. Cluster is in converged state.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the cluster is in a converged state.

Recommended Action No action is required.

CNM-1035

Message `Cluster is in degraded state. Posting degrade event.`

Message Type LOG

Severity WARNING

Probable Cause Indicates an event is being posted to specify the cluster is in a degraded state.

Recommended Action No action is required.

CNM-1036

Message `All the active nodes of the cluster are in ONLINE state. Posting converged event.`

Message Type LOG

Severity INFO

Probable Cause Indicates an event is being posted to specify the cluster is in a converged state.

Recommended Action No action is required.

CNM-1037

Message `Split-Brain Arbitration lost, minority GL Node, remote:local [<remote_count>:<local_gl_ncount>].`

Message Type LOG

Severity INFO

Probable Cause Indicates that split-brain arbitration is lost.

Recommended Action No action is required.

CNM-1038

Message `Split-Brain Arbitration won, majority GL Node, remote:local [<remote_count>:<local_gl_ncount>].`

Message Type LOG

Severity INFO

Probable Cause Indicates that split-brain arbitration is won.

Recommended Action No action is required.

CNM-1039

Message `Split-Brain Arbitration lost, Minority WWN/GL Node, remote_WWN:local_WWN <wbuf>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that split-brain arbitration is lost.

Recommended Action No action is required.

CNM-1040

Message `Split-Brain Arbitration won, Majority WWN/GL Node, remote_WWN:local_WWN <WWN>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that split-brain arbitration is won.

Recommended Action No action is required.

CNM-1041

Message `Updating persistent Cluster DB, please avoid powering off the switch.`

Message Type LOG

Severity INFO

Probable Cause Indicates the system is updating the persistent database.

Recommended Action No action is required.

CNM-1042

Message `Completed updating persistent Cluster DB.`

Message Type LOG

Severity INFO

Probable Cause Indicates the persistent database update is complete.

Recommended Action No action is required.

CNM-1043

Message `Received HBT from undefined node IpAddress [<ip>], WWN [<wwn>]. Possible configuration error.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the remote node's WWN may be changed.

Recommended Action No action is required.

CNM-1044

Message `Cluster Create Failed as the Certificate files not found, Please do the initnode.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the initnode is not invoked.

Recommended Action Execute the **cryptocfg --initnode** command.

CNM-1045

Message `Member node [<wwn>] is having dual IP stack.Registering member node with dual IP in an EG with only IPv6 is not allowed.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the member node with dual IP stack was registered with the IPv6 Encryption Group (EG).

Recommended Action No action is required.

CNM-1046

Message `Posting event CNM_EVT_NODE_LEAVE nodeName [<nodeName>], WWN [<wwn>].`

Message Type LOG

Severity INFO

Probable Cause Indicates that the node has decided to leave the Encryption Group (EG).

Recommended Action No action is required.

CNM-1047

Message `Network Interface to Remote Node [<ip>] is [<string>].`

Message Type LOG

Severity INFO

Probable Cause Indicates that the status of the network interface is up or down.

Recommended Action No action is required.

CNM-1048

Message `Posting <string>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the event that is posted.

Recommended Action No action is required.

CNM-1049

Message `Failed to define node, Node Name [<string>].`

Message Type LOG

Severity ERROR

Probable Cause Indicates the failure to define the node object.

Recommended Action No action is required.

CNM-1050

Message `Node Admission Control failed due to mismatch in Access Gateway Daemon (AGD) mode settings, rejecting node [<nodename>].`

Message Type LOG

Severity ERROR

Probable Cause Indicates mode mismatch between the switches, such as the Access Gateway mode mismatch.

Recommended Action No action is required.

CNM-1051

Message `Join Rejected by GL Node due to Access Gateway Daemon mode mismatch, ensure mode settings are same across all nodes in EG.`

Message Type LOG

Severity ERROR

Probable Cause Indicates mode mismatch between the switches, such as the Access Gateway mode mismatch.

Recommended Action No action is required.

CNM-1052

Message `Member node registered with another Encryption Group. To proceed eject the member node [<nodename>] from other EG.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the member node is registered with another Encryption Group (EG).

Recommended Action No action is required.

CNM-1053

Message `Node is already a registered member of another EG. First eject the current node [<nodename>] from the existing EG and then try.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the node is already a registered member of another Encryption Group (EG).

Recommended Action Eject the specified node from EG and retry the operation.

CNM-1054

Message `Encryption Group database state [<state>] with node IP [<node>], WWN [<wwn>].`

Message Type LOG

Severity INFO

Probable Cause Indicates the status of the cluster database.

Recommended Action No action is required.

CNM-1055

Message `Got CNM_FSM_EVT_JOIN_REQ when already a member from same GL node, rejoining EG with GL [<glname>].`

Message Type LOG

Severity INFO

Probable Cause Indicates the node is rejoining the Encryption Group (EG).

Recommended Action No action is required.

CNM-1056

Message `Posting event CNM_EVT_EE_INITIALIZING Slot [<slot>], WWN [<wwn>], IP [<ip>], flags [<flags>].`

Message Type LOG

Severity INFO

Probable Cause Indicates that the encryption engine is added into the Encryption Group (EG).

Recommended Action No action is required.

CNM-1057

Message `Posting event CNM_EVT_ONLINE Slot [<slot>], WWN [<wwn>], IP [<ip>], flags [<flags>].`

Message Type LOG

Severity INFO

Probable Cause Indicates that the encryption engine is online in the Encryption Group (EG).

Recommended Action No action is required.

CNM-1058

Message `Posting event CNM_EVT_OFFLINE Slot [<slot>], WWN [<wwn>], IP [<ip>], flags [<flags>].`

Message Type LOG

Severity INFO

Probable Cause Indicates that the encryption engine is removed from the Encryption Group (EG).

Recommended Action No action is required.

CNM-1059

Message `Local Node CP certificate pair mismatch detected, re-initialize the node.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the certificate pair is mismatched.

Recommended Action No action is required.

CNM-1060

Message `Local Node CP certificate pair match detected.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the certificate pair is matched.

Recommended Action No action is required.

CNM-1061

Message `IP of the switch changed from [<old_ip_address>] to [<new_ip_address>].`

Message Type LOG

Severity INFO

Probable Cause Indicates that the switch IP address has changed.

Recommended Action No action is required.

CNM-1062

Message `Copied certificate to [<ofname>] due to change in IP.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the certificate was copied to the file with new IP name.

Recommended Action No action is required.

CNM-3001

Message

```
Event: cryptocfg Status: success, Info: encryption group
\"<encryption_group_name>\" created.
```

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the specified encryption group was created.

Recommended Action No action is required.

CNM-3002

Message `Event: cryptocfg Status: success, Info: encryption group deleted.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates an encryption group was deleted.

Recommended Action No action is required.

CNM-3003

Message `Event: cryptocfg Status: success, Info: Membernode \"<member_node_WWN>\" added to encryption group.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the specified member node was added to an encryption group.

Recommended Action No action is required.

CNM-3004

Message `Event: cryptocfg Status: success, Info: Membernode \"<member_node_WWN>\" ejected from encryption group.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the specified member node was ejected from an encryption group.

Recommended Action No action is required.

CNM-3005

Message `Event: cryptocfg Status: success, Info: Membernode \"<member_node_WWN>\" left encryption group.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the specified member node left an encryption group.

Recommended Action No action is required.

CNM-3006

Message `Event: cryptocfg Status: success, Info: Heartbeat miss count set to <heartbeat_misses>.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the heartbeat miss value was set.

Recommended Action No action is required.

CNM-3007

Message `Event: cryptocfg Status: success, Info: Heartbeat timeout set to <heartbeat_timeout>.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the heartbeat timeout value was set.

Recommended Action No action is required.

CNM-3008

Message `Event: cryptocfg Status: success, Info: Routing mode of EE in slot <slot> set to <routingmode>.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the encryption engine routing mode was set.

Recommended Action No action is required.

CNM-3009

Message `Event: cryptocfg Status: success, Info: <nodeType> <nodeWWN> registered.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the specified member node was registered.

Recommended Action No action is required.

CNM-3010

Message `Event: cryptocfg Status: success, Info: Membernode <membernodeWWN> unregistered.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the specified member node was unregistered.

Recommended Action No action is required.

CNM-3011

Message `Event: cryptocfg Status: success, Info: Encryption group synchronized.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates an encryption group was synchronized.

Recommended Action No action is required.

CNM-3012

Message `Deleteing an EG with LUNs setup for encryption can lead to LUNs being disabled if Encryption Group name is not preserved (<egName>).`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the Encryption Group (EG) was deleted. Recreate EG with the same name if LUNs are set up for encryption.

Recommended Action Preserve the EG name when EG is recreated if LUNs are set up for encryption.

CONF Messages

CONF-1000

Message `configDownload completed successfully <Info about the parameters and AD.>.`

Message Type LOG | AUDIT

Class CFG

Severity INFO

Probable Cause Indicates that the **configDownload** operation was initiated and completed successfully. The *Info about the parameters and AD* variable is the description of the classes of configuration parameters that were downloaded. If Admin Domain (AD) is enabled, the AD number is specified in the description.

Recommended Action No action is required.

CONF-1001

Message `configUpload completed successfully <Info about the parameters and AD>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the **configUpload** operation was initiated and completed successfully. The *Info about the parameters and AD* variable is the description of the classes of configuration parameters that were uploaded. If Admin Domain (AD) is enabled, the AD number is specified in the description.

Recommended Action No action is required.

CONF-1020

Message `configDownload not permitted <AD Number if AD is configured on the system>.`

Message Type AUDIT

Class CFG

Severity INFO

Probable Cause Indicates that a **configDownload** operation is not permitted. There are many possible causes.

Recommended Action Execute the **errShow** command to view the error log. Correct the error and execute the **configDownload** command again.

CONF-1021

Message `configUpload not permitted <AD Number if AD is configured on the system>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a **configUpload** operation is not permitted. There are many possible causes.

Recommended Action Execute the **errShow** command to view the error log. Correct the error and execute the **configUpload** command again.

CONF-1022

Message `Downloading configuration without disabling the switch was unsuccessful.`

Message Type AUDIT

Class CFG

Severity WARNING

Probable Cause Indicates an attempt to download the configuration without disabling the switch was unsuccessful because there are one or more parameters that require the switch to be disabled.

Recommended Action Disable the switch using the **switchDisable** command and download the configuration.

CONF-1023

Message `configDownload failed <Message>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a **configDownload** operation has failed.

Recommended Action Execute the **errShow** command to view the error log. Correct the error and execute the **configDownload** command again.

CONF-1024

Message `configUpload failed <Message>.`

Message Type LOG

Severity INFO

Probable Cause Indicates a **configUpload** operation has failed.

Recommended Action Execute the **errShow** command to view the error log. Correct the error and execute the **configUpload** command again.

CONF-1030

Message `Configuration database full, data not committed (key: <Key of failed configuration data>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the previous configuration commands have resulted in a database full condition.Configuration changes associated with the specified key was not applied.

Recommended Action Use **configure** command and various other commands to erase configuration parameters that are no longer required. As a last resort, execute the **configDefault** command and reconfigure the system.

CONF-1031

Message `configDefault completed successfully <Message>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the **configDefault** command was initiated and completed successfully.

Recommended Action No action is required.

CONF-1032

Message `configRemove completed successfully <Message>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the **configRemove** command was initiated and completed successfully.

Recommended Action No action is required.

CONF-1040

Message `configDefault Failed. <Message>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that an error occurred while executing the **configDefault** command.

Recommended Action Execute the **errShow** command to view the error log. Correct the error and execute the **configDefault** command again.

CONF-1041

Message `configRemove Failed. <Message>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that an error occurred while executing the **configRemove** command.

Recommended Action Execute the **errShow** command to view the error log. Correct the error and execute the **configRemove** command again.

CONF-1042

Message `Fabric Configuration Parameter <Parameter> changed to <Value>`

Message Type LOG | AUDIT

Class CFG

Severity INFO

Probable Cause Indicates that the fabric configuration parameter value has been changed.

Recommended Action No action is required.

CONF-1043

Message `Fabric Configuration Parameter <Parameter> changed to <Value>`

Message Type LOG | AUDIT

Class CFG

Severity INFO

Probable Cause Indicates that the fabric configuration parameter value has been changed.

Recommended Action No action is required.

CONF-1044

Message `Fabric Configuration Parameter <Parameter> changed from <Old_Location> to <New_Location>`

Message Type LOG | AUDIT

Class CFG

Severity INFO

Probable Cause Indicates that the fabric configuration parameter value has been changed by a user.

Recommended Action No action is required.

CTAP Messages

CTAP-1001

Message `Key acquisition for <Pool or Container> <Begins or Complete>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a change in the tape pool database has triggered the key acquisition process for each pool.

Recommended Action Do not start tape backup or restore operations involving tape pools until the process is complete.

CVLC Messages

CVLC-1001

Message
```
<Re-key type (First time encryption/Key expired/Manual)> re-key <Re-key action
(started/completed/failed/cancelled)>, LUN SN: <LUN serial number>. Container:
<Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the first-time encryption, key expired, or manual re-key operation is performed. The operation has been started, completed, failed, or cancelled.

Recommended Action No action is required.

CVLC-1002

Message
```
Tape session <Re-key action (started/cancelled/failed)>. Container: <Target
container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that a tape session was started, failed, or cancelled.

Recommended Action No action is required.

CVLC-1003

Message
```
Forceful LUN policy change to clear text while re-key session is still active.
Container: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID:
<LUN ID>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the encryption LUN policy was forcefully changed while a re-key session was still active.

Recommended Action No action is required.

CVLC-1004

Message `Forceful encryption LUN removal while re-key session is still active. Container: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the encryption LUN was forcefully removed while a re-key session was still active.

Recommended Action No action is required.

CVLC-1005

Message `There are no LUNs found from the target. Container: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that there are no LUNs found from the target-initiator pair.

Recommended Action No action is required.

CVLC-1006

Message `Duplicate LUN serial number <LUN SN> found. Container: <Target container name>, Initiator: <Initiator physical WWN>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that there is more than one LUN serial number discovered from the same target. Therefore, encryption on this target is disabled.

Recommended Action No action is required.

CVLC-1007

Message

```
Removal of encryption LUN is not allowed when decrypt of existing data is enabled.
Container: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID:
<LUN ID>.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that there has been an attempt to remove the encryption LUN while decryption of existing data is still enabled.

Recommended Action

To preserve the user data, execute the **cryptocfg --modify -LUN -cleartext** command to convert to cleartext LUN.

Use the **cryptocfg --modify -LUN -cleartext** command to disable decryption of existing data.

Then try to delete the LUN again.

CVLC-1008

Message

```
LUN discovery failure: <Discovery state>, Container: <Target container name>,
Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that LUN discovery failed.

Recommended Action

No action is required.

CVLC-1009

Message

```
Wrong device type: should be <Expected device type (Disk/Tape)>, found <Discovered
device type (Disk/Tape)>. Container: <Target container name>, Initiator:
<Initiator physical WWN>, LUN ID: <LUN ID>.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that LUN discovery failed.

Recommended Action

No action is required.

CVLC-1010

Message `Tape license is required for tape container: <Target container name>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the tape container is configured with non-Brocade mode but there is no valid license.

Recommended Action Obtain a license for non-Brocade mode.

CVLC-1011

Message `Third party license is required for encryption LUN in third party mode. Container: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the encryption LUN is configured with non-Brocade mode but there is no valid license.

Recommended Action Obtain a license for non-Brocade mode.

CVLC-1012

Message `Disk metadata is in wrong format (<Metadata format found (Brocade/Third party)>). Container: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the metadata found on the disk LUN is in the wrong format.

Recommended Action Use the **cryptoCfg** command to change the metadata mode of the LUN.

CVLC-1013

Message `Unable to retrieve key record from the key archive. Container: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the encryption engine is unable to retrieve the key record base on the key ID found in the metadata.

Recommended Action No action is required.

CVLC-1014

Message `Missing Key ID from user input. Container: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the data state in the LUN configuration is in the encrypted state without a key ID and there is no metadata found on the LUN.

Recommended Action Use the **cryptoCfg** command to add the key ID, if available.

CVLC-1015

Message `LUN is set to read only mode. Reason: <Reason for LUN is set to read only mode>. Container: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the LUN is set to read-only mode because there is a conflict in the configuration.

Recommended Action No action is required.

CVLC-1016

Message `LUN is out of read only mode. Reason: <Reason for LUN is out of read only mode>. Container: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the LUN is set to read/write mode.

Recommended Action No action is required.

CVLC-1017

Message `Event: <Description of the event>. Container: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a warning or an error event.

Recommended Action No action is required.

CVLC-1018

Message `Event: <Description of the event>. Container: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Message Type LOG

Severity INFO

Probable Cause Indicates an informational event.

Recommended Action No action is required.

CVLC-1019

Message `Metadata exists while data state is clear text. Container: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the data state in the LUN configuration is cleartext, but metadata exists on the LUN.

Recommended Action Use the **cryptoCfg** command to confirm the configuration.

CVLC-1020

Message `Metadata exists while LUN is clear text. Container: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that metadata exists on the LUN that is in cleartext state.

Recommended Action Use the **cryptoCfg** command to confirm the configuration.

CVLC-1021

Message `User provided key ID <Key ID provided by the user> is ignored while metadata <Key ID from metadata> exists. Container: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the key ID provided is ignored because metadata exists on the LUN.

Recommended Action No action is required.

CVLC-1022

Message `User provided key ID <Key ID provided by the user> is ignored while data state is clear text. Container: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the key ID provided is ignored because the data state is cleartext.

Recommended Action No action is required.

CVLC-1023

Message `Rebalance recommended on EE: <EE name>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that due to container configuration changes, weights are not balanced on OB1s.

Recommended Action Run the **cryptocfg --rebalance** command to increase system performance.

CVLC-1024

Message `Device Decommission operation <Decommission state (succeeded/failed)>. Container: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the device decommission process has either succeeded or failed.

Recommended Action No action is required.

CVLC-1025

Message `Secondary Metadata exists for encrypted LUN not configured with -newLUN option. Container: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the secondary metadata exists on the LUN that is not configured with the **-newLUN** option.

Recommended Action Use the **cryptoCfg** command to remove and add the LUN with the **-newLUN** option.

CVLC-1026

Message `Some secondary metadata missing for encrypted LUN configured with -newLUN option. Container: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the secondary metadata does not exist on all logical block addresses (LBAs) for a LUN that is configured with the **-newLUN** option.

Recommended Action No action is required.

CVLC-1027

Message `Encrypted LUN configured with -newLUN option does not contain any metadata. Container: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the metadata was corrupted.

Recommended Action No action is required.

CVLC-1028

Message `Not starting auto rekey on LUN with uncompressible blocks 1-16. Container: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates a warning event.

Recommended Action Perform a manual re-key on this LUN.

CVLC-1029

Message `Mirror LUN is disabled as primary LUN is being rekeyed without splitting the mirror. Container: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that performing first-time encryption or manual re-key of primary LUN without splitting the mirror.

Recommended Action Break the mirror and re-establish the mirror after re-key on primary LUN is complete.

CVLC-1030

Message `Primary LUN may be out of sync with mirror LUN. Container: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the manual re-key was completed on primary LUN.

Recommended Action Perform the following steps.

1. Make the target ports of the mirror LUN offline to hosts.
2. Re-establish the mirror.
3. After the mirror is in sync, split the mirror.
4. Bring back the target ports of the mirror LUN online.

CVLC-1031

Message

```
Primary LUN is restored from mirror LUN. LUN in read-only mode. Container: <Target
container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that a re-keyed primary LUN may have been restored from a mirror LUN without synchronizing.

Recommended Action

Perform the following steps.

1. Create a new primary LUN.
2. Add the new primary LUN to its container with the **-newLUN** option.
3. Using host-based migration application, copy data from the old to the new primary LUN.

CVLC-1032

Message

```
Secondary metadata for LUN has been restored. Container: <Target container name>,
Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates the host I/Os to secondary metadata region.

Recommended Action

No action is required.

CVLC-1033

Message

```
Rebalance completed for EE: <EE name>. Device login in progress.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that a rebalance operation was performed.

Recommended Action

No action is required.

CVLC-1034

Message `Rekey failed on Container: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID> because <Failure reason>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the first-time encryption, key expired, or manual re-key operation failed.

Recommended Action No action is required.

CVLC-1035

Message `A decommissioned LUN has been added back as encrypted LUN. Container: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that a decommissioned LUN has been added as an encrypted LUN.

Recommended Action Perform the following steps.

1. Remove the LUN from the container.
2. Add the LUN back as a cleartext LUN.
3. Modify the LUN policy to encrypt.

CVLC-1039

Message `Refresh DEK operation <Refresh DEK status (SUCCEEDED/FAILED)>. Container: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the status of the refresh DEK operation.

Recommended Action No action is required.

CVLC-1041

Message `<Host IO to secondary meta-data block rejected>. Container: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the host write operation on secondary metadata block region failed.

Recommended Action Disable the initiator port.

CVLM Messages

CVLM-1001

Message `Failed to allocate memory: (<function name>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified function has failed to allocate memory.

Recommended Action Check the memory usage on the switch using the **memShow** command.

Restart or power cycle the switch.

CVLM-1002

Message `Failed to initialize <module> rc = <error>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the initialization of a module within the Crypto Virtual LUN Manager (CVLM) daemon has failed.

Recommended Action Download a new firmware version using the **firmwareDownload** command.

CVLM-1003

Message `Crypto device configuration has been committed by switch (<Switch WWN>).`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified switch has committed a crypto device configuration.

Recommended Action No action is required.

CVLM-1004

Message `Crypto device configuration between local switch (<local switch WWN>) and peer (<peer switch WWN>) is out of sync. New encryption session is not allowed.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that encryption engine nodes in the cluster encryption group have different configurations.

Recommended Action Synchronize the configuration in the cluster group using the **cryptocfg --commit** command.

CVLM-1005

Message `Crypto service is <status> on the switch.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the crypto service is enabled or disabled on the switch.

Recommended Action No action is required.

CVLM-1006

Message `Crypto device <device WWN> in target container <container name> is not in AD0.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the crypto device in the crypto target container is not in root zone database (AD0).

Recommended Action Use the **ad** command to move the crypto device into AD0.

CVLM-1007

Message `Redirect zone update failure. Status is <status>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the redirect zone update has failed.

Recommended Action Run the **cryptocfg --commit** command again.

CVLM-1008

Message `The member (<EE node WWN> <EE slot num>) of HAC (<HAC name>) is not in the fabric.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the member of the HA cluster (HAC) is not in the fabric.

Recommended Action Check the inter-switch link (ISL) port connected to the fabric.

CVLM-1009

Message `The member (<EE node WWN> <EE slot num>) of HAC (<HAC name>) is in the fabric.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the member of the HA cluster (HAC) is found in the fabric.

Recommended Action No action is required.

CVLM-1010

Message `The IP address of EE (<EE node WWN> <EE slot num>) IO link is not configured.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the IP address of the encryption engine IO link is not configured.

Recommended Action Configure the encryption engine IO link IP address using the **ipAddrSet** command.

CVLM-1011

Message `The HAC failover occurs at EE (<EE node WWN> <EE slot num>).`

Message Type LOG

Severity INFO

Probable Cause Indicates that the HA cluster (HAC) failover occurs at the encryption engine.

Recommended Action No action is required.

CVLM-1012

Message `The HAC failback occurs at EE (<EE node WWN> <EE slot num>).`

Message Type LOG

Severity INFO

Probable Cause Indicates that the HA cluster (HAC) failback occurs at the encryption engine.

Recommended Action No action is required.

CVLM-1013

Message
```
Redirect zone create failed because no Host/Target
(<HostPortWWN>/<TargetPortWWN>) L2 zone exists.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates that creation of the redirect zone has failed.

Recommended Action Create the Layer 2 zone for host and target and run the **cryptocfg --commit** command again.

CVLM-1014

Message `RD zone getting deleted for which there is no Host/Target (<HostPortWWN>/<TargetPortWWN>) L2 zone exists in effective configuration.`

Message Type LOG

Severity ERROR

Probable Cause Indicates deletion of Frame Redirect (RD) zone and there is no corresponding Layer 2 zone present, but IT pair is in crypto configuration.

Recommended Action Disable the target access to the host, recreate the Layer 2 zone for host and target, and run the **cryptocfg --commit** command again to recreate the RD zone.

CVLM-1015

Message `Unable to read basewwn from blade in slot <Slot>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a failure to read the base WWN programmed on SEEPROM from this blade. Probably, SEEPROM is not programmed properly.

Recommended Action WWN allocation is not possible from this blade, but the blade can be used for crypto operations. SEEPROM needs to be reprogrammed on this blade.

CVLM-1016

Message `Invalid base WWN (<BaseWWN>) and/or page index (<Page>) received from the blade in slot <Slot>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that invalid base WWN and index are read from SEEPROM on this blade. Probably, SEEPROM is not programmed properly.

Recommended Action WWN allocation is not possible from this blade, but the blade can be used for crypto operations. SEEPROM needs to be reprogrammed on this blade.

CVLM-1017

Message `Detected mismatch in EG names (Old EG: <OldEGName>, New EG: <NewEGName>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates that reclaim cleanup was not executed to clean up the cryptodb configuration pertaining to the older Encryption Group (EG).

Recommended Action To cleanup cryptodb configuration, de-register the node and execute the **cryptocfg --reclaim -cleanup** command.

CVLM-3001

Message `Event: cryptocfg Status: success, Info: Failback mode set to <failbackmode>.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the failback mode was set.

Recommended Action No action is required.

CVLM-3002

Message `Event: cryptocfg Status: success, Info: HA cluster \"<HAClusterName>\" created.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the specified HA cluster was created.

Recommended Action No action is required.

CVLM-3003

Message `Event: cryptocfg Status: success, Info: HA cluster \"<HAClusterName>\" deleted.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the specified HA cluster was deleted.

Recommended Action No action is required.

CVLM-3004

Message `Event: cryptocfg Status: success, Info: Cluster member added to HA cluster \"<HAClusterName>\".`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that an HA cluster member was added.

Recommended Action No action is required.

CVLM-3005

Message `Event: cryptocfg Status: success, Info: Cluster member removed from HA cluster \"<HAClusterName>\".`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that an HA cluster member was removed.

Recommended Action No action is required.

CVLM-3006

Message
```
Event: cryptocfg Status: success, Info: Current node WWN/slot <CurrentWWN> /
<CurrentSlot> replaced with new node WWN/slot: <NewWWN> / <NewSlot>.
```

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that an HA cluster member was replaced.

Recommended Action No action is required.

CVLM-3007

Message
```
Event: cryptocfg Status: success, Info: <diskOrTape> container
\"<containerName>\" created.
```

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the specified crypto-target container was created.

Recommended Action No action is required.

CVLM-3008

Message
```
Event: cryptocfg Status: success, Info: Container \"<containerName>\" deleted.
```

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the specified crypto-target container was deleted.

Recommended Action No action is required.

CVLM-3009

Message

```
Event: cryptocfg Status: success, Info: Manual failback from EE
<currentnodeWWN>/<currentSlot> to EE <newnodeWWN>/<newnodeSlot>.
```

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that a manual failback was performed to an encryption engine.

Recommended Action No action is required.

CVLM-3010

Message

```
Event: cryptocfg Status: success, Info: Move crypto target container
\"<cryptoTargetContainer>\" to EE <newEEWWN>/<newEESlot>.
```

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the specified crypto-target container was moved to another encryption engine.

Recommended Action No action is required.

CVLM-3011

Message

```
Event: cryptocfg Status: success, Info: Initiator PWWN \"<initiatorPWWN>\"
Initiator NWWN \"<initiatorNWWN>\" added to crypto target container
\"<cryptoTargetContainer>\".
```

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that an initiator was added to a crypto-target container.

Recommended Action No action is required.

CVLM-3012

Message `Event: cryptocfg Status: success, Info: Initiator \"<initiator>\" removed from crypto target container \"<cryptoTargetContainer>\".`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the specified initiator was removed from the crypto-target container.

Recommended Action No action is required.

CVLM-3013

Message `Event: cryptocfg Status: success, Info: LUN <LUNSpec>, attached through Initiator \"<Initiator>\", added to crypto target container \"<cryptoTargetContainer>\".`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that a LUN was added to a crypto-target container.

Recommended Action No action is required.

CVLM-3014

Message `Event: cryptocfg Status: success, Info: LUN <LUN Number>, attached through Initiator \"<Initiator>\" in crypto target container \"<cryptoTargetContainer>\", modified.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the specified LUN in the crypto-target container was modified.

Recommended Action No action is required.

CVLM-3015

Message

```
Event: cryptocfg Status: success, Info: LUN <LUN Number>, attached through
initiator \"<Initiator>\", removed from crypto target container
\"<cryptoTargetContainer>\".
```

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the specified LUN was removed from the crypto-target container.

Recommended Action No action is required.

CVLM-3016

Message

```
Event: cryptocfg Status: success, Info: LUN <LUN Number>, attached through
Initiator \"<Initiator>\" in crypto target container \"<cryptoTargetContainer>\",
enabled.
```

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the specified LUN in a crypto-target container was enabled.

Recommended Action No action is required.

CVLM-3017

Message

```
Event: cryptocfg Status: success, Info: Tape pool \"<tapepoolLabelOrNum>\"
created.
```

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the specified tape pool was created.

Recommended Action No action is required.

CVLM-3018

Message
```
Event: cryptocfg Status: success, Info: Tape pool \"<tapepoolLabelOrNum>\"
deleted.
```

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the specified tape pool was deleted.

Recommended Action No action is required.

CVLM-3019

Message
```
Event: cryptocfg Status: success, Info: Tapepool \"<tapepoolLabelOrNum>\"
modified.
```

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the specified tape pool was modified.

Recommended Action No action is required.

CVLM-3020

Message
```
Event: cryptocfg Status: success, Info: Manual rekey of LUN <LUNSpec> attached
through Initiator \"<Initiator>\" in crypto tgt container
\"<cryptoTargetContainer>\".
```

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that a manual re-key of a LUN was performed.

Recommended Action No action is required.

CVLM-3021

Message `Event: cryptocfg Status: success, Info: Manual rekey all performed.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that a complete manual re-key was performed.

Recommended Action No action is required.

CVLM-3022

Message

```
Event: cryptocfg Status: success, Info: Resume rekey of LUN <LUNSpec> attached
through Initiator \"<Initiator>\" in crypto tgt container
\"<cryptoTargetContainer>\".
```

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that a resume re-key was performed.

Recommended Action No action is required.

CVLM-3023

Message `Event: cryptocfg Status: success, Info: Transaction committed.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that a transaction commit operation was performed.

Recommended Action No action is required.

CVLM-3024

Message `Event: cryptocfg Status: success, Info: Transaction <transactionID> aborted.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that a transaction abort operation was performed.

Recommended Action No action is required.

CVLM-3025

Message
```
Event: cryptocfg Status: started, Info: Decommission of device (container
<cryptoTargetContainer> initiator <Initiator>, LUN <LUN>).
```

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the decommission operation has started.

Recommended Action No action is required.

CVLM-3026

Message
```
Event: cryptocfg Status: Failed, Info : Decommission of device (container
<cryptoTargetContainer>, Initiator <Initiator>, LUN <LUN>).
```

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the decommission operation has failed for the device.

Recommended Action Run the **cryptocfg --decommission** command.

CVLM-3027

Message `Event: cryptocfg Status: success, Info: Decommission of device (container <cryptoTargetContainer>, initiator <Initiator>, LUN <LUN>).`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the decommission operation has been completed for the device.

Recommended Action No action is required.

CVLM-3028

Message `Event: cryptocfg Status: success, Info: SRDF mode set to <srdfmode>.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the Symmetrix Remote Data Facility (SRDF) mode was set.

Recommended Action No action is required.

DOT1 Messages

DOT1-1001

Message `802.1X is enabled globally.`

Message Type LOG

Severity INFO

Probable Cause Indicates that 802.1X is enabled globally.

Recommended Action No action is required.

DOT1-1002

Message `802.1X is disabled globally.`

Message Type LOG

Severity INFO

Probable Cause Indicates that 802.1X is disabled globally.

Recommended Action No action is required.

DOT1-1003

Message `802.1X is enabled for port <port_name>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that 802.1X is enabled on the specified port.

Recommended Action No action is required.

DOT1-1004

Message `Port <port_name> is forcefully unauthorized.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified port has been unauthorized forcefully using the **dot1x port-control force-unauthorized** command.

Recommended Action No action is required.

DOT1-1005

Message `802.1X authentication is successful on port <port_name>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that 802.1X authentication has succeeded on the specified port.

Recommended Action No action is required.

DOT1-1006

Message `802.1X authentication has failed on port <port_name>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that 802.1X authentication has failed on the specified port due to incorrect credentials or the remote authentication dial-in user service (RADIUS) server is not functioning properly.

Recommended Action Check the credentials configured with the supplicant and the RADIUS server.

DOT1-1007

Message `No RADIUS server available for authentication.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that there is no remote authentication dial-in user service (RADIUS) server available for authentication.

Recommended Action Execute the **aaaConfig --show** command to verify that the configured RADIUS servers are reachable and functioning.

DOT1-1008

Message `Port <port_name> is forcefully authorized.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified port has been authorized forcefully using the **dot1x port-control forced-authorized** command.

Recommended Action No action is required.

DOT1-1009

Message `802.1X is disabled for port <port_name>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that 802.1X is disabled on the specified port.

Recommended Action No action is required.

DOT1-1010

Message `Port <port_name> is set in auto mode.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified port is set to auto mode.

Recommended Action No action is required.

ECC Messages

ECC-1000

Message

```
ECC Error <Multiple or single occurrence of errors of a given type detected>
occurrence of <Automatic calibration error detected><Multiple bit error
detected><Single bit error detected><Memory select error detected>.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that the processor memory controller has detected one of the several types of double data rate (DDR) memory errors. Single bit errors are corrected, but other errors indicate either software errors or problems with the target system DRAM. Single bit errors can be expected to occur infrequently and can be caused by uncontrollable external events like cosmic rays, but frequent single bit errors can be indications of a degrading DRAM device.

Recommended Action

Frequent single bit errors and all other error types should be reported to technical support for further action.

ECC-1001

Message

```
ECC Error <Multiple or single occurrence of multiple bit ECC error
detected><Multiple or single occurrence of single bit ECC error detected><Multiple
of single occurrence of access outside the defined physical memory space detected>
detected.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that the processor memory controller has detected one of the several types of double data rate (DDR) memory errors. Single bit errors are corrected, but other errors indicate either software errors or problems with the target system DRAM. Single bit errors can be expected to occur infrequently and can be caused by uncontrollable external events like cosmic rays, but frequent single bit errors can be indications of a degrading DRAM device.

Recommended Action

Frequent single bit errors and all other error types should be reported to technical support for further action.

EM Messages

EM-1001

Message `<FRU ID> is overheating: Shutting down.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the specified field-replaceable unit (FRU) is shutting down due to overheating. This event is typically due to a faulty fan and can also be caused by the switch environment.

Recommended Action Verify that the location temperature is within the operational range of the switch. Refer to the *Hardware Reference Manual* for the environmental temperature range of your switch.

Execute the **fanShow** command to verify that all fans are running at normal speeds. If any fans are missing or not performing at high enough speed, they should be replaced.

EM-1002

Message `System fan(s) status <fan FRU>.`

Message Type LOG | FFDC

Severity INFO

Probable Cause Indicates that a non-bladed system has overheated and may shutdown. All fan speeds are dumped to the console.

Recommended Action Verify that the location temperature is within the operational range of the switch. Refer to the *Hardware Reference Manual* for the environmental temperature range of your switch.

Execute the **fanShow** command to verify that all fans are running at normal speeds. If any fans are missing or are not performing at a high enough speed, they should be replaced.

EM-1003

Message `<FRU ID> has unknown hardware identifier: FRU faulted.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that a field-replaceable unit (FRU) header could not be read or is not valid. The FRU is faulted.

Recommended Action Execute the **diagPost** command to make sure that Power-On Self-Test (POST) is enabled; then power cycle the blade by using the **slotPowerOff** and **slotPowerOn** commands or have the blade's ejector switch cycled to run POST and verify that the blade does not have any hardware problems.

For the Brocade 300 and 6510, replace the switch.

EM-1004

Message `<FRU ID> failed to power on.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the specified field-replaceable unit (FRU) failed to power on and is not being used.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port.

The Brocade 300 switch has 4 fans and 1 power supply, but these parts cannot be replaced: the entire switch is a FRU.

Recommended Action Reseat the FRU. If the problem persists, replace the FRU.

EM-1005

Message `<FRU Id> has faulted. Sensor(s) above maximum limits.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that a blade in the specified slot or the switch (for non-bladed switches) is shutdown for environmental reasons; its temperature or voltage is out of range.

Recommended Action Check the environment and make sure the room temperature is within the operational range of the switch. Execute the **fanShow** command to verify fans are operating properly. Make sure there are no blockages of the airflow around the chassis. If the temperature problem is isolated to the blade itself, replace the blade.

Voltage problems on a blade are likely a hardware problem on the blade itself; replace the blade.

EM-1006

Message `<FRU Id> has faulted. Sensor(s) below minimum limits.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the voltage on a switch is below minimum limits. The switch or specified blade is being shutdown for environmental reasons; the voltage is too low.

Recommended Action If this problem occurs on a blade, it usually indicates a hardware problem on the blade; replace the blade.

If this problem occurs on a switch, it usually indicates a hardware problem on the main board; replace the switch.

EM-1008

Message `Unit in <Slot number or Switch> with ID <FRU Id> is faulted, it is incompatible with the <type of incompatibility> configuration, check FOS firmware version as a possible cause.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that a blade inserted in the specified slot or the switch (for non-bladed switches) is not compatible with the platform configuration (includes the firmware version) or the switch configuration. The blade is faulted.

Recommended Action If the blade is incompatible, upgrade the firmware or replace the blade and make sure the replacement blade is compatible with your control processor (CP) type and firmware.

If the incompatibility is with the logical switch configuration, change the configuration by using the **lscfg** command to be consistent with the blade type, or remove the blade.

EM-1009

Message `<FRU Id> powered down unexpectedly.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the environmental monitor (EM) received an unexpected power-down notification from the specified field-replaceable unit (FRU). This may indicate a hardware malfunction in the FRU.

Recommended Action Reseat the FRU. If the problem persists, replace the FRU.

EM-1010

Message `Received unexpected power down for <FRU Id> But <FRU Id> still has power.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the environmental monitor (EM) received an unexpected power-down notification from the specified field-replaceable unit (FRU). However, the specified FRU still appears to be powered up after four seconds.

Recommended Action Reseat the blade. If the problem persists, replace the blade.

EM-1011

Message `Received unexpected power down for <FRU Id>, but cannot determine if it has power.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the environmental monitor (EM) received an unexpected power-down notification from the specified field-replaceable unit (FRU). However, after four seconds, it cannot be determined if it has powered down or not.

Recommended Action Reseat the blade. If the problem persists, replace the blade.

EM-1012

Message `<FRU Id> failed <state> state transition, unit faulted.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that a switch blade or non-bladed switch failed to transition from one state to another. It is faulted. The specific failed target state is displayed in the message. There are serious internal Fabric OS configuration or hardware problems on the switch.

Recommended Action Reseat the specified field-replaceable unit (FRU).

If the problem persists, restart or power cycle the switch.

Execute the **diagPost** command to make sure that Power-On Self-Test (POST) is enabled; then power cycle the blade by using the **slotPowerOff** and **slotPowerOn** commands or have the blade's ejector switch cycled to run POST and verify that the blade does not have any hardware problems.

If the problem still persists, replace the FRU.

EM-1013

Message `Failed to update FRU information for <FRU Id>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the environmental monitor (EM) was unable to update the time alive or original equipment manufacturer (OEM) data in the memory of a field-replaceable unit (FRU).

Recommended Action If you executed the **fruInfoSet** command, execute the command again; otherwise, the update is automatically attempted again. If it continues to fail, reseat the FRU.

If the problem persists, replace the FRU.

EM-1014

Message `Unable to read sensor on <FRU Id> (<Return code>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the environmental monitor (EM) was unable to access the sensors on the specified field-replaceable unit (FRU).

Recommended Action Reseat the FRU. If the problem persists, replace the FRU.

EM-1015

Message `Warm recovery failed (<Return code>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a problem was discovered when performing consistency checks during a warm boot.

Recommended Action Monitor the switch. If the problem persists, restart or power cycle the switch.

EM-1016

Message `Cold recovery failed (<Return code>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a problem was discovered when performing consistency checks during a cold boot.

Recommended Action Monitor the switch.

If the problem persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

EM-1017

Message `Uncommitted WWN change detected. Cold reboot required.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a user did not commit a changed World Wide Name (WWN) value before performing a system restart, power cycle, or firmware download operation.

Recommended Action Change and commit the new WWN value.

EM-1018

Message `CP blade in slot <slot number> failed to retrieve current chassis type (<return code>/<error code>/0x<unit number>).`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that there was a failure to read the chassis type from the system.

Recommended Action Verify that the control processor (CP) blade is operational and is properly seated in its slot.

EM-1019

Message `Current chassis configuration option (<Chassis config option currently in effect>) is not compatible with standby firmware version (Pre 4.4), cannot allow HA Sync.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the current chassis configuration option is not supported by the firmware on the standby control processor (CP). This is true even if the standby CP comes up and is operational. High availability (HA) synchronization of the CPs will not be allowed.

Recommended Action Change the chassis configuration option to 1 using the **chassisConfig** command, or upgrade the firmware on the standby CP to the version running on the active CP.

EM-1020

Message

```
Unit in <Slot number> with ID <FRU Id> is faulted, it's an FCoE blade and the
Ethernet switch service is not enabled. Please run <fosconfig --enable ethsw>.
```

Message Type

FFDC | LOG

Severity

ERROR

Probable Cause

Indicates that a blade inserted in the specified slot requires the Ethernet switch service, which is not enabled. The blade is faulted.

Recommended Action

Execute the **fosconfig --enable ethsw** command to enable the Ethernet switch service. Note that this is a disruptive command, which requires the system to be restarted. Otherwise, remove the blade.

EM-1028

Message

```
HIL Error: <function> failed to access history log for FRU: <FRU Id> (rc=<return
code>).
```

Message Type

FFDC | LOG

Severity

WARNING

Probable Cause

Indicates a problem accessing the data on the World Wide Name (WWN) card field-replaceable unit (FRU) or the WWN card storage area on the main logic board.

The problems were encountered when the software attempted to write to the history log storage to record an event for the specified FRU. The return code is for internal use only. This can indicate a significant hardware problem.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port.

Recommended Action

If the problem persists, restart or power cycle the switch.

If the problem still persists, replace the WWN card, or the switch (for non-bladed switches).

EM-1029

Message

```
<FRU Id>, a problem occurred accessing a device on the I2C bus (<error code>).
Operational status (<state of the FRU when the error occurred>) not changed,
access is being retried.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the Inter-Integrated Circuit (I2C) bus had problems and a timeout occurred.

Recommended Action This is often a transient error.

Watch for the EM-1048 message, which indicates that the problem has been resolved.

If the problem persists, check for loose or dirty connections. Remove all dust and debris before reseating the field-replaceable unit (FRU). If it continues to fail, replace the FRU.

EM-1031

Message `<FRU Id> ejector not closed.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the environmental monitor (EM) has found a switch blade that is inserted, but at least one ejector switch is not latched. The blade in the specified slot is treated as not inserted.

Recommended Action Close the ejector switch (raise the slider in most blades or completely screw in the upper thumbscrew) if the field-replaceable unit (FRU) is intended for use. Refer to the appropriate *Hardware Reference Manual* for instructions on inserting the switch blades.

EM-1033

Message `CP in <FRU Id> set to faulty because CP ERROR asserted.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the standby control processor (CP) has been detected as faulty. The high availability (HA) feature will not be available. This message occurs every time the other CP restarts, even as part of a clean warm failover. In most situations, this message is followed by the EM-1047 message, and no action is required for the standby CP; however, find the reason for failover.

Recommended Action If the standby CP was restarted, wait for the error to clear (execute the **slotShow** command to determine if it has cleared). Watch for the EM-1047 message to verify that this error has cleared.

If the standby CP continues to be faulty or if it was not intentionally restarted, check the error logs on the other CP (using the **errDump** command) to determine the cause of the error state.

Reseat the field-replaceable unit (FRU). If the problem persists, replace the FRU.

EM-1034

Message `<FRU Id> set to faulty, rc=<return code>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified field-replaceable unit (FRU) has been marked as faulty for the specified reason.

Recommended Action

Reseat the FRU.

Execute the **diagPost** command to make sure that Power-On Self-Test (POST) is enabled; then power cycle the blade by using the **slotPowerOff** and **slotPowerOn** commands or have the blade's ejector switch cycled to run POST and verify that the blade does not have any hardware problems.

If the problem persists, replace the FRU.

EM-1035

Message

```
2 circuit paired Power Supplies are faulty, please check the <Switch side> AC main
switch/circuit to see if it has power.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that both power supplies associated with one of the two main circuits are present but faulty, the circuit's switch may have been turned off, or the AC power source has been interrupted for that circuit.

The *Switch side* value designates the circuit switch facing the cable side of the chassis, and is one of the following values:

- left - Controls the odd-numbered power supply units.
- right - Controls the even-numbered power supply units.

Recommended Action

Verify that the identified AC circuit switch is turned on, the power cord is properly attached and undamaged, and the power source is operating properly.

EM-1036

Message

```
<FRU Id> is not accessible.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the specified field-replaceable unit (FRU) is not present on the switch.

If the FRU is a World Wide Name (WWN) card, the default WWN and IP addresses are used for the switch.

Recommended Action

Reseat the FRU.

If the problem persists, restart or power cycle the switch.

Execute the **diagPost** command to make sure that Power-On Self-Test (POST) is enabled; then power cycle the blade by using the **slotPowerOff** and **slotPowerOn** commands or have the blade's ejector switch cycled to run POST and verify that the blade does not have any hardware problems.

If the problem still persists, replace the FRU.

EM-1037

Message `<FRU Id> is no longer faulted.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified power supply is no longer marked faulty; probably because its AC power supply has been turned on.

Recommended Action No action is required.

EM-1042

Message `Important FRU header data for <FRU Id> is not valid.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the specified field-replaceable unit (FRU) has an incorrect number of sensors in its FRU header-derived information. This could mean that the FRU header was corrupted or read incorrectly, or corrupted in the object database, which contains information about all FRUs.

Recommended Action Reseat the FRU. If the problem persists, replace the FRU.

EM-1043

Message `Can't power <FRU Id> <state (on or off)>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the specified field-replaceable unit (FRU) cannot be powered on or off.

Recommended Action The specified FRU is not responding to the commands and should be replaced.

EM-1044

Message `Can't power on <FRU Id>, its logical switch is shut down.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the specified field-replaceable unit (FRU) cannot be powered on because the associated logical switch is shutdown.

Recommended Action Execute the **switchStart** command on the associated logical switch.

EM-1045

Message `<FRU Id> is being powered <new state>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that an automatic power adjustment is being made because of the (predicted) failure of a power supply or the insertion or removal of a port blade. The *new state* value can be one of the following values:

- On - A port blade is being powered on because the power is available (a power supply was inserted or a port blade was removed or powered down).
- Off - A port blade has been powered down because of the (predicted) failure of the power supply.
- Down - A newly inserted port blade was not powered on because there was not enough power available.

Recommended Action The Brocade 24000 requires only a single power supply for a fully populated chassis; however, you must always operate the system with at least two power supplies for redundancy.

EM-1046

Message `Error status received for blade ID <id value> for the blade in slot <slot number>, <blade incompatibility type: platform, backplane, or switch configuration>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the specified blade is incompatible.

Recommended Action If the blade ID listed is incorrect, the field-replaceable unit (FRU) header for the blade is corrupted and the blade must be replaced.

If the error is due to the platform, the blade ID listed is not supported for that platform (CP) type. Remove the blade from the chassis.

If the error is due to the backplane, the CP type (CP256) is not supported on that chassis (backplane revision D2). Remove the blade from the chassis.

If the error is due to the switch configuration, the logical switch configuration of the blade is incorrect. Execute the **lscfg** command to correct the switch or port configuration for the ports on the blade.

EM-1047

Message `CP in slot <slot number> not faulty, CP ERROR deasserted.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the control processor (CP) is no longer faulted. This message usually follows the EM-1033 message. The new standby CP is in the process of restarting and has turned off the CP_ERR signal.

Recommended Action No action is required.

EM-1048

Message `<FRU Id> I2C access recovered: state <current state>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Inter-Integrated Circuit (I2C) bus problems have been resolved and I2C access to the field-replaceable unit (FRU) has become available again.

Recommended Action No action is required. The EM-1048 message is displayed when the EM-1029 error is resolved.

EM-1049

Message `FRU <FRU Id> insertion detected.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a field-replaceable unit (FRU) of the type and location specified by the *FRU ID* value was detected as having been inserted into the chassis.

Recommended Action No action is required.

EM-1050

Message `FRU <FRU Id> removal detected.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a field-replaceable unit (FRU) of the type and location specified by the *FRU ID* value was removed from the chassis.

Recommended Action Verify that the FRU was intended to be removed. If not, replace the FRU as soon as possible.

EM-1051

Message `<FRU Id>: Inconsistency detected, FRU reinitialized.`

Message Type LOG

Severity INFO

Probable Cause Indicates that an inconsistent state was found in the field-replaceable unit (FRU). This occurs if the state of the FRU was changing during a failover. The FRU is reinitialized and the traffic may have been disrupted.

Recommended Action No action is required.

EM-1057

Message `Blade:<Slot Id> is getting reset:<Fault reason>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the blade is being automatically reset because of known resetable transient errors such as an application-specific integrated circuit (ASIC) parity error.

Recommended Action No action is required if the switch does not reach the reset threshold for the switch or blade. If the reset threshold is reached on the switch or blade, the switch or blade will be faulted and should be replaced.

EM-1058

Message `Switch gets reset:<Fault reason>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the switch is being automatically reset because of a known resetable transient problem such as an application-specific integrated circuit (ASIC) parity error.

Recommended Action No action is required if the switch does not reach the reset threshold for the switch or blade. If the reset threshold is reached on the switch or blade, the switch or blade will be faulted and should be replaced.

EM-1059

Message `<Slot number or Switch> with ID <Blade Id> may not be supported on this platform, check FOS firmware version as a possible cause.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that a a blade inserted in the specified slot or the switch (for non-bladed switches) is incompatible with the switch configuration software. The blade will not be completely usable.

The blade may only be supported by a later (or earlier) version of the firmware.

Recommended Action Change the control processor (CP) firmware or replace the blade. Make sure the replacement is compatible with your switch type and firmware.

EM-1060

Message `Stopping synchronization of the system due to blade incompatibility with software version on standby CP.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a blade in the system is not supported by the firmware on the standby control processor (CP).

Recommended Action Remove all blades of this type or upgrade the standby CP. After an appropriate action is taken, restart the standby CP or execute the **haSyncStart** command to enable the high availability (HA) state synchronization. Until this is done, the system will remain out of synchronization.

EM-1061

Message `Synchronization halted. Remove all blades of type <Blade Type Id> or upgrade your standby CP, then reboot or run haSyncStart.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the blade in the system is not supported by the firmware on the standby control processor (CP).

Recommended Action Remove all blades of the specified type or upgrade the standby CP. After an appropriate action is taken, restart the standby CP or execute the **haSyncStart** command to enable the high availability (HA) state synchronization. Until this is done, the system will remain out of synchronization.

EM-1062

Message `Blade in slot <Slot Id> faulted as it exceeds the maximum support limit of <Limit> blades with Blade ID <Blade Type Id> in the chassis.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that too many blades of a particular type are in the system.

Recommended Action Remove the faulted blade.

EM-1063

Message `Blade in slot <Slot Id> faulted because it exceeds the maximum support limit of <Limit> blades with Blade IDs <Applicable blade Type IDs> in the chassis.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that too many blades of a set of particular types are in the system.

Recommended Action Remove the faulted blade.

EM-1064

Message `Blade:<Slot Id> is being powered off (based on user configuration) upon receiving a HW ASIC ERROR, reason:<Fault reason>.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that the blade is being powered off because a hardware (HW) application-specific integrated circuit (ASIC) error was detected, and you have selected to power off the problem blade when such a condition occurred.

Recommended Action Contact your switch service provider for assistance.

EM-1065

Message `SAS Virtualization Services are not available due to incompatibility between the FOS and SAS versions<Slot number or blank for single board systems>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the version of the control processor firmware (CFOS) or the blade processor firmware (BFOS) is not compatible with the Storage Application Services (SAS) or other application firmware versions.

Recommended Action Upgrade the Fabric OS firmware or the SAS firmware by using the **firmwareDownload** command. Refer to the release notes for a compatible version of firmware.

EM-1066

Message `SAS Virtualization Services are now available <Slot number or blank for single board systems>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the previously incompatible Fabric OS or Storage Application Services (SAS) firmware has been upgraded and is now compatible.

Recommended Action No action is required.

EM-1067

Message `Stopping synchronization of the system due to <version> incompatibility with standby CP.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the software version on the standby control processor (CP) is incompatible with this software feature enabled on this Fabric OS firmware version.

Recommended Action Upgrade the software on the standby CP or disable the software feature on this CP.

To disable the Ethernet switch service, execute the **fosconfig --disable ethsw** command.

To view the buffer optimization mode for the slots, execute the **bufopmod --showall** command, and then execute the **bufopmode --reset** *slot* command to disable the feature for those slots before downgrading.

To disable FC8-16 Serdes tuning mode, execute the **serdestunemode --reset** command.

EM-1068

Message `High Availability Service Management subsystem failed to respond. A required component is not operating.`

Message Type FFDC | LOG

Severity ERROR

Probable Cause Indicates that the high availability (HA) subsystem has not returned a response within four minutes of the request from the environmental monitor (EM). It usually indicates that some component has not started properly or has terminated. The specific component that has failed may be indicated in other messages or debug data. There are serious internal Fabric OS configuration or hardware problems on the switch.

Recommended Action Restart or power cycle the switch.

If the problem persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

EM-1069

Message `Slot <FRU slot number> is being powered off.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the blade in the specified slot is being intentionally powered off.

Recommended Action No action is required.

EM-1070

Message `Slot <FRU slot number> is being powered on.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the blade in the specified slot is being intentionally powered on.

Recommended Action No action is required.

EM-1071

Message `Unit in <Slot number> with ID <FRU Id> is faulted, it is incompatible with the following blade id(s): <blade incompatibility list>.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that a blade inserted in the specified slot is incompatible with another blade in the system.

Recommended Action Determine which blade is essential to your configuration and remove blades that are incompatible with it.

EM-1072

Message `Chassis cannot become ready since no Core Blades are available.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that all core blades are either missing, faulted, or powered off. There must be at least one core blade in enabled state for the chassis to be considered ready.

Recommended Action Insert and close the ejector switch on missing core blades. Reseat or replace core blades that are faulted or powered off.

EM-1073

Message `Blade devices cannot be accessed. The blade in slot <FRU slot number> is being moved to ABSENT state.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the devices on the blade were not accessible. Blade is being tranisitioned to the ABSENT state.

Recommended Action Reseat or replace the affected blade.

EM-1134

Message `<FRU Id> set to faulty, rc=<return code>.`

Message Type LOG | FFDC

Severity ERROR

Probable Cause Indicates that the specified field-replaceable unit (FRU) has been marked as faulty for the specified reason.

Recommended Action Reseat the FRU.

Execute the **diagPost** command to make sure that Power-On Self-Test (POST) is enabled; then power cycle the blade by using the **slotPowerOff** and **slotPowerOn** commands or have the blade's ejector switch cycled to run POST and verify that the blade does not have any hardware problems.

If the problem persists, replace the FRU.

EM-2003

Message `<Slot Id or Switch for pizza boxes> has failed the POST tests. FRU is being faulted.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that a field-replaceable unit (FRU) has failed the Power-On Self-Test (POST). Refer to the */tmp/post[1/2].slot#.log* file for more information on the faults. To view this log file, you must be logged in at the root level. The ID will be Switch for non-bladed systems.

Recommended Action On bladed systems, reseat the specified FRU.

On non-bladed switches, restart or power cycle the switch.

If the problem persists, perform the following actions:

- Execute the **diagPost** command to make sure that Power-On Self-Test (POST) is enabled; then power cycle the blade by using the **slotPowerOff** and **slotPowerOn** commands or have the blade's ejector switch cycled to run POST and verify that the blade does not have any hardware problems.
- On bladed systems, replace the specified FRU; otherwise, replace the switch.

ESM Messages

ESM-1000

Message `ESMd <Module Name> initialization complete rc:<Return Code>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that ESMd module initialization phase has completed.

Recommended Action No action is required.

ESM-1001

Message `ESMd <Module Name> uninitialization complete rc:<Return Code>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that ESMd module uninitialization phase has completed.

Recommended Action No action is required.

ESM-1002

Message `ESMd initialization done for service <Service Name>:<Instance Number>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that ESMd service has initialized.

Recommended Action No action is required.

ESM-1003

Message `ESMd uninitialization called for service <Service Name>:<Instance Number>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that ESMd service uninitialization phase has completed.

Recommended Action No action is required.

ESM-1004

Message `ESMd failed to initialize <Module Name> rc:<Return Code>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified module has failed to initialize.

Recommended Action If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

ESM-1005

Message `Configuration (<Configuration>) replay failed - <Failure Reason>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the specified configuration failed to be reapplied during config replay.

Recommended Action Use the **portCfg**, **portShow**, and **portCfgShow** commands to correct the cause of the failure.

ESM-1010

Message `DP<DP ID> is OFFLINE.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified Data Processor (DP) has went offline.

Recommended Action If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

ESM-1011

Message `DP<DP ID> is ONLINE.`

Message Type LOG

Severity INFO

Probable Cause Indicates that specified Data Processor (DP) has come online.

Recommended Action No action is required.

ESM-1012

Message `DP<DP ID> Configuration replay has started.`

Message Type LOG

Severity INFO

Probable Cause Indicates that Data Processor (DP) configuration replay has started.

Recommended Action No action is required.

ESM-1013

Message `DP<DP ID> Configuration replay has completed.`

Message Type LOG

Severity INFO

Probable Cause Indicates that Data Processor (DP) configuration replay has completed.

Recommended Action No action is required.

ESM-1100

Message `<Warning message string.>`

Message Type LOG

Severity WARNING

Probable Cause Internal warning occurred as indicated by the warning message.

Recommended Action If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

ESM-1101

Message `<Error message string.>`

Message Type LOG

Severity ERROR

Probable Cause Internal error occurred as indicated by the error message.

Recommended Action If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

ESM-2000

Message

```
IP Interface <GE Port>.dp<DP ID> created <Address>/<Mask> vlan: <Vlan ID> mtu:
<MTU> [<Originator>].
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified IP interface has been added.

Recommended Action No action is required.

ESM-2001

Message `IP Interface <GE Port>.dp<DP ID> deleted <Address>/<Mask> [<Originator>].`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified IP interface has been removed.

Recommended Action No action is required.

ESM-2002

Message

```
IP Interface <GE Port>.dp<DP ID> modified: <Address>/<Mask> vlan: <Vlan ID> mtu:
<MTU> [<Originator>].
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified IP interface has been modified.

Recommended Action No action is required.

ESM-2010

Message

```
IProute <GE Port>.dp<DP ID> create dest:<destination address>/<dest address
prefix> gate:<gateway address> [<Originator>].
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified IP route has been created.

Recommended Action No action is required.

ESM-2011

Message

```
IProute <GE Port>.dp<DP ID> deleted dest:<destination address>/<dest address
prefix> gate:<gateway address> [<Originator>].
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified IP route has been deleted.

Recommended Action No action is required.

ESM-2012

Message `IProute <GE Port>.dp<DP ID> modified dest:<destination address>/<dest address prefix> gate:<gateway address> [<Originator>].`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified IP route has been modified.

Recommended Action No action is required.

ESM-2100

Message `VE tunnel <VE-Port> created [<Originator>].`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified VE tunnel has been created.

Recommended Action No action is required.

ESM-2101

Message `VE tunnel <VE-Port> deleted.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified VE tunnel has been deleted.

Recommended Action No action is required.

ESM-2102

Message `VE tunnel <VE-Port> modified [<Originator>].`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified VE tunnel has been modified.

Recommended Action No action is required.

ESM-2103

Message `VE tunnel <VE-Port> MODATTR (<Attribute change description>).`

Message Type LOG

Severity INFO

Probable Cause Indicates an attribute changed for the specified VE tunnel.

Recommended Action No action is required.

ESM-2104

Message `VE tunnel <VE-Port> is OFFLINE.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the operational status of the specified tunnel is offline.

Recommended Action If the tunnel is not administratively down, a network error or disruption may have occurred.

ESM-2105

Message `VE tunnel <VE-Port> is DEGRADED.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the operational status of the specified tunnel has degraded.

Recommended Action If the tunnel is not administratively down, a network error or disruption may have occurred.

ESM-2106

Message `VE tunnel <VE-Port> is ONLINE.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified VE tunnel is online.

Recommended Action No action is required.

ESM-2200

Message `VE Circuit <VE Port>.<Circuit ID> created [<Originator>].`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified circuit has been created.

Recommended Action No action is required.

ESM-2201

Message `VE Circuit <VE Port>.<Circuit ID> deleted [<Originator>].`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified circuit has been deleted.

Recommended Action No action is required.

ESM-2202

Message `VE Circuit <VE Port>.<Circuit ID> modified [<Originator>].`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified circuit has been modified.

Recommended Action No action is required.

ESM-2203

Message `VE Circuit <VE Port>.<Circuit ID> MODATTR (<Attribute change description>).`

Message Type LOG

Severity INFO

Probable Cause Indicates an attribute changed for the specified VE circuit.

Recommended Action No action is required.

ESM-2300

Message `IPsec policy <Policy Name> added [<Originator>].`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified Internet Protocol security (IPsec) policy has been added.

Recommended Action No action is required.

ESM-2301

Message `IPsec policy <Policy Name> deleted [<Originator>].`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified Internet Protocol security (IPsec) policy has been deleted.

Recommended Action No action is required.

ESM-2302

Message `IPsec policy <Policy Name> modified [<Originator>].`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified Internet Protocol security (IPsec) policy has been modified.

Recommended Action No action is required.

ESM-2303

Message `IPsec policy <Policy Name> MODATTR (<Attribute change description>).`

Message Type LOG

Severity INFO

Probable Cause Indicates an attribute changed for the specified Internet Protocol security (IPsec) policy.

Recommended Action No action is required.

ESM-2310

Message `IKE Session Policy <IPSec Policy Name> dp<DP ID>.<IKE Session ID> created <Local IP Address> - <Remote IP Address>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified Internet Key Exchange (IKE) session has been created for the specified Internet Protocol security (IPsec) policy.

Recommended Action No action is required.

ESM-2311

Message `IKE Session Policy <IPSec Policy Name> dp<DP ID>.<IKE Session ID> deleted <Local IP Address> - <Remote IP Address>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified Internet Key Exchange (IKE) session has been deleted for the specified Internet Protocol security (IPsec) policy.

Recommended Action No action is required.

ESM-3000

Message `<Boot Stage> starting.`

Message Type LOG

Severity INFO

Probable Cause Indicates the specific bootup recovery stage has started.

Recommended Action No action is required.

ESM-3001

Message `<Boot Stage> complete.`

Message Type LOG

Severity INFO

Probable Cause Indicates the specific bootup recovery stage has completed.

Recommended Action No action is required.

ESM-3002

Message `DP<DP ID>-<HA Stage> starting.`

Message Type LOG

Severity INFO

Probable Cause Indicates the specific HA recovery stage has started for the specified Data Processor (DP).

Recommended Action No action is required.

ESM-3003

Message `DP<DP ID>-<HA Stage> ending: <Recovery Status>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the specific HA recovery stage has completed for the specified Data Processor (DP).

Recommended Action No action is required.

ESM-3004

Message `DP<DP ID> VE-<HA Operation> <VE Port> failed (<Reason>). Will retry.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the specific HA operation has failed for the specified VE port but will be retried later.

Recommended Action No action is required.

ESM-3005

Message `DP<DP ID> VE-<HA Operation> <VE Port> failed (<Reason>). Not retriable.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the specific HA operation has failed for the specified VE port and traffic will be disrupted on this port.

Recommended Action No action is required.

ESM-3006

Message `<Boot Stage> failed (<Reason>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates that a critical failure has occurred during the boot process.

Recommended Action If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

ESS Messages

ESS-1001

Message `A few switches in the fabric do not support the Coordinated HotCode protocol.`

Message Type LOG

Severity WARNING

Probable Cause Indicates one or more switches in the fabric do not support the Coordinated HotCode protocol. Continuing with the firmware download may cause data traffic disruption.

Recommended Action Discontinue the firmware download, identify the down-level switch or switches that do not support the Coordinated HotCode protocol, and upgrade the down-level switches. Then, restart the firmware download on this switch. Note that upgrading a down-level Brocade switch in a mixed interop fabric may still cause data traffic disruption.

ESS-1002

Message `The pause message is rejected by the domain <domain id>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that during the Coordinated HotCode protocol, a switch in the fabric has rejected the pause message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been due to the rejected pause message.

Recommended Action No action is required.

ESS-1003

Message `The pause retry count is exhausted for the domain <domain id>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that during the Coordinated HotCode protocol, a switch in the fabric did not accept the pause message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been due to this issue.

Recommended Action No action is required.

ESS-1004

Message `The resume message is rejected by the domain <domain id>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that during the Coordinated HotCode protocol, a switch in the fabric has rejected the resume message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been due to the rejected resume message.

Recommended Action No action is required.

ESS-1005

Message `The resume retry count is exhausted for the domain <domain id>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that during the Coordinated HotCode protocol, a switch in the fabric did not accept the resume message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been due to this issue.

Recommended Action No action is required.

ESS-1008

Message `Fabric Name - <fabric_name> configured (received from domain <domain id>).`

Message Type AUDIT | LOG

Class FABRIC

Severity INFO

Probable Cause Indicates that the fabric name is configured or renamed.

Recommended Action No action is required.

ESS-1009

Message `Fabric Name Mismatch - local(<fabric_name>) remote(<r_fabric_name> - received from domain <domain id>).`

Message Type AUDIT | LOG

Class FABRIC

Severity WARNING

Probable Cause Indicates that the specified fabric name is not unique for this fabric.

Recommended Action Select an appropriate fabric name and set it again from any switch.

ESS-1010

Message `Duplicate Fabric Name - <fabric_name> matching with FID <Fabric ID>.`

Message Type AUDIT | LOG

Class FABRIC

Severity WARNING

Probable Cause Indicates that the configured fabric name is already used for another partition.

Recommended Action Select a different fabric name and reconfigure.

ESW Messages

ESW-1001

Message `Switch is not in ready state - Switch enable failed, switch status= 0x<switch status>, c_flags = 0x<switch control flags>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the switch enable operation has failed.

Recommended Action If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

ESW-1002

Message `Security violation: Unauthorized device <wwn name of device> tries to FLOGI to port <port number>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified device is not present in the authorized profile list.

Recommended Action Verify that the device is authorized to log in to the switch. If the device is authorized, execute the **secPolicyDump** command to verify whether the World Wide Name (WWN) of the specified device is listed. If it is not listed, execute the **secPolicyAdd** command to add this device to an existing policy.

ESW-1003

Message `Slot ENABLED but Not Ready during recovery, disabling slot = <slot number>(<return value>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the slot state has been detected as inconsistent during failover or recovery.

Recommended Action For a bladed switch, execute the **slotPowerOff** and **slotPowerOn** commands to power cycle the blade.

For a non-bladed switch, restart or power cycle the switch.

ESW-1004

Message `Blade attach failed during recovery, disabling slot = <slot number>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified blade has failed during failover or recovery.

Recommended Action For a bladed switch, execute the **slotPowerOff** and **slotPowerOn** commands to power cycle the blade.

For a non-bladed switch, restart or power cycle the switch.

ESW-1005

Message `Diag attach failed during recovery, disabling slot = <slot number>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the diagnostic blade attach operation has failed during failover or recovery.

Recommended Action For a bladed switch, execute the **slotPowerOff** and **slotPowerOn** commands to power cycle the blade.

For a non-bladed switch, restart or power cycle the switch.

ESW-1006

Message

```
HA state out of sync: Standby CP (ver = <standby SWC version>) does not support
NPIV functionality. (active ver = <active SWC version>, NPIV devices = <'1' if
NPIV devices exist; Otherwise '0'>).
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that the standby control processor (CP) does not support N_Port ID Virtualization (NPIV) functionality, but the switch has some NPIV devices logged in to the fabric.

Recommended Action Load a firmware version on the standby CP that supports NPIV functionality using the **firmwareDownload** command.

ESW-1007

Message `Switch port <port number> disabled due to \"<disable reason>\".`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the switch port is disabled due to the reason displayed in the message.

Recommended Action Based on the disable reason displayed, take appropriate action to restore the port.

If the disable reason is "Insufficient frame buffers", reduce the distance or speed settings for the port to reduce the buffer requirement of the link. Alternatively, one or more ports in the port group must be disabled to make more buffers available for the link.

Refer to the *Fabric OS Administrator's Guide* for more information.

ESW-1008

Message `<area string> are port swapped on ports that do not support port swap. Slot <slot number> will be faulted.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the blade is enabled with the port configuration that already has the area swapped.

Recommended Action Replace the blade with ports that support port swap. Then swap ports back to the port's default area.

Refer to the *Fabric OS Administrator's Guide* for more information.

EVMD Messages

EVMD-1001

Message `Event could not be sent to remote proxy = <Remote proxy switch id>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the event could not be sent to remote proxy. This could happen if the remote proxy switch cannot be reached through in-band.

Recommended Action Make sure that the specified remote domain is present in the fabric.

FABR Messages

FABR-1001

Message `port <port number>, <segmentation reason>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the specified switch port is isolated because of a segmentation resulting from mismatched configuration parameters.

Recommended Action Based on the segmentation reason displayed with the message, look for a possible mismatch of relevant configuration parameters in the switches at both ends of the link.

Run the **configure** command to modify the appropriate switch parameters on both the local and remote switch.

FABR-1002

Message `fabGaid: no free multicast alias IDs.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the fabric does not have any available multicast alias IDs to assign to the alias server.

Recommended Action Verify alias IDs using the **fabricShow** command on the principal switch.

FABR-1003

Message `port <port number>: ILS <command> bad size <payload size>, wanted <expected payload size>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that an internal link service (ILS) information unit of invalid size has been received. The neighbor switch has sent a payload with an invalid size.

Recommended Action

Investigate the neighbor switch for problems. Run the **errShow** command on the neighbor switch to view the error log for additional messages.

Check for a faulty cable or deteriorated small form-factor pluggable (SFP). Replace the cable or the SFP if necessary.

Run the **portLogDumpPort** command on both the receiving and transmitting ports.

Run the **fabStatsShow** command on both the receiving and transmitting switches.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

FABR-1004

Message

```
port: <port number>, req iu: 0x<address of IU request sent>, state: 0x<command
sent>, resp iu: 0x<address of response IU received>, state 0x<response IU state>,
<additional description>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the information unit response was invalid for the specified command sent. The fabric received an unknown response. This message is rare and usually indicates a problem with the Fabric OS kernel.

Recommended Action

If this message is due to a one-time event because of the incoming data, the system will discard the frame. If it is due to problems with the kernel, the system will recover by performing a failover.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

FABR-1005

Message

```
<command sent>: port <port number>: status 0x<reason for failure> (<description of
failure reason>) xid = 0x<exchange ID of command>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the application failed to send an async command for the specified port. The message provides additional details regarding the reason for the failure and the exchange ID of the command. This can happen if a port is about to go down.

Recommended Action

No action is required. This message is often transitory.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

FABR-1006

Message `Node free error, caller: <error description>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Fabric OS is trying to free or deallocate memory space that has already been deallocated. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action In case of severe memory corruption, the system may recover by performing an automatic failover.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

FABR-1007

Message `IU free error, caller: <function attempting to de-allocate IU>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a failure occurred when deallocating an information unit. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action In case of severe memory corruption, the system may recover by performing an automatic failover.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

FABR-1008

Message `<error description>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that errors occurred during the request domain ID state; the information unit cannot be allocated or sent. If this message occurs with FABR-1005, the problem is usually transitory. Otherwise, this message is rare and usually indicates a problem with the Fabric OS. The error descriptions are as follows:

- FAB RDI: cannot allocate IU
- FAB RDI: cannot send IU

Recommended Action No action is required if the message appears with the FABR-1005 message.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

FABR-1009

Message `<error description>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that errors were reported during the exchange fabric parameter state; cannot allocate domain list due to a faulty exchange fabric parameter (EFP) type. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action The fabric daemon will discard the EFP. The system will recover through the EFP retrial process.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

FABR-1010

Message `<error description>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that errors occurred while cleaning up the request domain ID (RDI). The error description provides further details. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

FABR-1011

Message `<error description>.`

Message Type LOG | FFDC

Severity ERROR

Probable Cause Indicates that the Fabric OS is unable to inform the Fabric OS State Synchronization Management module (FSSME) that the fabric is stable or unstable. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

FABR-1012

Message

```
<function stream>: no such type, <invalid type>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the fabric is not in the appropriate state for the specified process. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action

The fabric daemon will take proper action to recover from the error.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

FABR-1013

Message

```
No Memory: pid=<fabric process id> file=<source file name> line=<line number
within the source file>.
```

Message Type

FFDC | LOG

Severity

CRITICAL

Probable Cause

Indicates that there is not enough memory in the switch for the fabric module to allocate. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action

The system will recover by failing over to the standby CP.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

FABR-1014

Message

```
Port <port number> Disabled: Insistent Domain ID <Domain ID> could not be
obtained. Principal Assigned Domain ID = <Domain ID>.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that the specified port received a request domain ID (RDI) accept message containing a principal-switch-assigned domain ID that is different from the insistent domain ID (IDID). Fibre connectivity (FICON) mode requires an insistent domain ID. If an RDI response has a different domain ID, then the port is disabled.

Recommended Action

Run the **configShow** command to view the fabric.ididmode. A 0 means the IDID mode is disabled; a 1 means it is enabled.

Set the switch to insistent domain ID mode. This mode is set under the **configure** command or in Web Tools on the **Switch Admin > Configure** window.

FABR-1015

Message `FICON Insistent DID max retry exceeded: All E_Ports will be disabled. Switch is isolated.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the application exceeded request domain ID (RDI) requests for the insistent domain ID. All E_Ports are disabled; isolating the specified switch from the fabric.

Recommended Action Verify that the insistent domain ID is unique in the fabric and then re-enable the E_Ports. Run the **fabricShow** command to view the domain IDs across the fabric and the **configure** command to change the insistent domain ID mode. Refer to the *Fabric OS Command Reference* for more information on these commands.

FABR-1016

Message `ficonMode is enabled.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that FICON mode is enabled on the switch through a user interface command.

Recommended Action No action is required.

FABR-1017

Message `ficonMode is disabled.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that FICON mode is disabled on the switch through a user interface command.

Recommended Action No action is required.

FABR-1018

Message `PSS principal failed (<reason for not becoming the principal switch>: <WWN of new principal switch>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a failure occurred when trying to set the principal switch using the **fabricPrincipal** command. The message notifies you that the switch failed to become the principal switch because of one of the following reasons:

- The switch joined an existing fabric and bypassed the F0 state.
- The fabric already contains a principal switch that has a lower World Wide Name (WWN).

Recommended Action Make sure that no other switch is configured as the principal switch. Force a fabric rebuild by using the **switchDisable** and **switchEnable** commands.

Refer to the *Fabric OS Command Reference* for more information about the **fabricPrincipal** command.

FABR-1019

Message `Critical fabric size (<current domains>) exceeds supported configuration (<supported domains>).`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that this switch is a value-line switch and has exceeded the limited fabric size: that is, a specified limit to the number of domains. This limit is defined by your specific value-line license key. The fabric size has exceeded this specified limit, and the grace period counter has started. If the grace period is complete and the size of the fabric is still outside the specified limit, Web Tools is disabled.

Recommended Action Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your switch provider to obtain a full fabric license.

FABR-1020

Message `Web Tools will be disabled in <days> days <hours> hours and <minutes> minutes.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that this switch has a value-line license and has a limited number of domains. If more than the specified number of domains are in the fabric, a counter is started to disable Web Tools. This message displays the number of days left in the grace period. After this time, Web Tools is disabled.

Recommended Action Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your switch provider to obtain a full fabric license.

FABR-1021

Message `Web Tools is disabled.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that this switch has a value-line license and has a limited number of domains. If more than the specified number of domains are in the fabric, a counter is started to disable Web Tools. This grace period has expired and Web Tools has been disabled.

Recommended Action Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your switch provider to obtain a full fabric license.

FABR-1022

Message `Fabric size (<actual domains>) exceeds supported configuration (<supported domains>). Fabric limit timer (<type>) started from <grace period in seconds>.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the fabric size has exceeded the value-line limit, and the grace period counter has started. If the grace period is complete and the size of the fabric is still outside the specified limit, Web Tools is disabled.

Recommended Action Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your switch provider to obtain a full fabric license.

FABR-1023

Message `Fabric size is within supported configuration (<supporteddomains>). Fabric limit timer (<type>) stopped at <grace period in seconds>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the fabric size is within specified limits. Either a full fabric license was added or the size of the fabric was changed to within the licensed limit.

Recommended Action No action is required.

FABR-1024

Message `Initializing fabric size limit timer <grace period>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the fabric size has exceeded the limit set by your value-line switches. Value-line switches have a limited fabric size (for example, a specified limit on the number of domains). This value is defined by your specific value-line license key. The fabric size has exceeded this specified limit. The grace period timer has been initialized. If the grace period is complete and the size of the fabric is still outside the specified limit, Web Tools is disabled.

Recommended Action Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your switch provider to obtain a full fabric license.

FABR-1029

Message `Port <port number> negotiated <flow control mode description> (mode = <received flow control mode>).`

Message Type LOG

Severity INFO

Probable Cause Indicates that a different flow control mode, as described in the message, is negotiated with the port at the other end of the link. The flow control is a mechanism of throttling the transmitter port to avoid buffer overrun at the receiving port. There are three types of flow control modes:

- VC_RDY mode: Virtual-channel flow control mode. This is a proprietary protocol.
- R_RDY mode: Receiver-ready flow control mode. This is the Fibre Channel standard protocol, that uses R_RDY primitive for flow control.
- DUAL_CR mode: Dual-credit flow control mode. In both of the previous modes, the buffer credits are fixed, based on the port configuration information. In this mode, the buffer credits are negotiated as part of exchange link parameter (ELP) exchange. This mode also uses the R_RDY primitive for flow control.

Recommended Action No action is required.

FABR-1030

Message `fabric: Domain <new domain ID> (was <old domain ID>).`

Message Type LOG

Severity INFO

Probable Cause Indicates that the domain ID has changed.

Recommended Action No action is required.

FABR-1031

Message

```
Maximum number of retries sending ILS from port <port number> exceeded.
```

Message Type LOG | FFDC

Severity WARNING

Probable Cause Indicates the fabric exhausted the maximum number of retries sending internal link service (ILS) to the iswitch daemon on the specified E_Port.

Recommended Action Run the **top** command to see if iswitchd is extremely busy or if another process is using excessive CPU resources.

FABR-1032

Message

```
Remote switch with domain ID <Domain ID> and switchname <Switchname> running an
unsupported FOS version v2.x has joined the fabric.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that a switch with an unsupported Fabric OS version 2.x has joined the fabric.

Recommended Action Remove the switch with the unsupported Fabric OS version 2.x from the fabric

FABR-1034

Message

```
Area <Area that has already been acquired> have been acquired by port <Port that
has already acquired the area>. Persistently disabling port <Port that is being
disabled>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates you must enable Trunk Area on a port for another port to use the same area.

Recommended Action Move the cable to a port area that is not in use, or disable Trunk Area. You must manually enable the port or the port remains disabled forever.

Refer to the *Fabric OS Administrator's Guide* for more information.

FABR-1035

Message

```
Slave area <Area that does not match Master port's area> does not match Master
port <Master port >. Persistently disabling port <Port that is being disabled>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates the Slave port's Trunk Area differs from that of the Master port.

Recommended Action Move the cable to a port to match with the same Master Trunk Area, or disable Trunk Area. You must manually enable the port or the port remains disabled forever.

Refer to the *Fabric OS Administrator's Guide* for more information.

FABR-1036

Message

```
F_Port trunks are only allowed on Trunk Area enabled port. Persistently disabling
port <Port that is being disabled>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates the specified port is being disabled because when the port on a switch is Trunk Area-enabled, it does not allow other devices like Access Gateway (AG) or HBA that are not Trunk Area-enabled.

Recommended Action Move the cable to a port that does not have Trunk Area enabled.

FABR-1037

Message

```
Port configuration incompatible with Trunk Area enabled port. Persistently
disabling port <Port that is being disabled>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates the specified port is being disabled because when the port attempts to go online, the switch finds the Trunk Area enabled is incompatible with port configurations such as long distance, port mirror, fast write, or EX_Port.

Recommended Action Check the port configurations to disable long distance, port mirror, fast write, or EX_Port.

FABR-1038

Message `Trunking license not present with F port trunking enabled. Persistently disabling port <Port that is being disabled>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the specified port is being disabled because F_Port trunking is enabled without a trunking license being present.

Recommended Action Install a trunking license or disable F_Port trunking on the port.

FABR-1039

Message `Invalid domain ID zero received from principal switch(domain id=<Principal domain id>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates an invalid domain ID zero has been received.

Recommended Action Check the principal switch for the invalid domain ID zero.

FABR-1040

Message `Speed is not 2G, 4G, or 8G with F_Port trunking enabled. Persistently disabling port <Port that is being disabled>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the speed is not compatible for F_Port trunks.

Recommended Action Change the speed for the port or disable F_Port trunking on the port.

FABR-1041

Message `Port <Port that is being disabled> is disabled due to trunk protocol error.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a link reset was received before the completion of the trunking protocol on the port.

Recommended Action Enable the port by running the **portEnable** command.

The port may recover by re-initialization of the link.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

FABR-1043

Message `Detected Fabric ID conflict with remote (not neighbor) switch <Switchname> (domain <Domain ID>), FID <Fabric ID>. No local E_Ports disabled.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the remote switch has a Fabric ID (FID) conflict with the local switch. But no ports are disabled because the remote switch is not an adjacent to the local switch.

Recommended Action Make sure that all the switches in the fabric have the same FID or upgrade the switch firmware to a VF-capable firmware.

FABR-1044

Message `Detected Fabric ID conflict with neighbor switch <Switchname> (domain <Domain ID>), FID <Fabric ID>. E_Ports (<Number of E_Ports disabled>) connected to the switch are disabled.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the neighbor switch has a Fabric ID (FID) conflict with the local switch. All E_Ports directly connected to the conflicting switch are disabled.

Recommended Action Make sure that all the switches in the fabric have the same FID or upgrade the switch firmware to a VF-capable firmware.

FABR-1045

Message `Detected Base Switch conflict with remote (not neighbor) switch <Switchname> (domain <Domain ID>), BS <Base Switch Mode>. No local E_Ports disabled.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the remote switch has a Base Switch attribute conflict with the local switch. But no ports are disabled because the remote switch is not an adjacent to the local switch.

Recommended Action Make sure that all the switches in the fabric have the same Base Switch attribute or disable VF mode for the conflicting switch using the **fosConfig** command.

FABR-1046

Message `Detected Base Switch conflict with neighbor switch <Switchname> (domain <Domain ID>), BS <Base Switch Mode>. E_Ports (<Number of E_Ports disabled>) connected to the switch are disabled.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the remote switch has a Base Switch attribute conflict with the local switch. All the E_Ports directly connected to the conflicting switch are disabled.

Recommended Action Make sure that all the switches in the fabric have the same Base Switch attribute or upgrade the switch firmware to a VF-capable firmware.

FABR-1047

Message `Area unavailable to assign to the port. Persistently disabling port <Port that is being disabled>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that there are no areas available to assign to the port during port creation.

Recommended Action Move some ports out of the default switch to make areas available.

FABR-1048

Message `Detected Fabric ID (FID <InheritedFID> inherited) conflict with switch <Switchname> (domain <Domain ID>, FID <Fabric ID>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates that a switch in the fabric has a Fabric ID (FID) conflict with the inherited FID of the local switch.

Recommended Action Make sure that all the switches in the fabric have the same FID or upgrade the switch firmware to a VF-capable firmware.

FABR-1049

Message `Detected Fabric ID (FID <InheritedFID> inherited) conflict with neighbor switch <Switchname> (domain <Domain ID>, FID <Fabric ID>). E_Ports (<Number of E_Ports disabled>) connected to the switch are disabled.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the neighbor switch has a Fabric ID (FID) conflict with the inherited FID of the local switch. All E_Ports directly connected to the conflicting switch are disabled.

Recommended Action Make sure that all the switches in the fabric have the same FID or upgrade the switch firmware to a VF-capable firmware.

FABR-1050

Message `<License> license not present. F_Port trunking cannot be enabled on port(<Port>).`

Message Type LOG

Severity INFO

Probable Cause Indicates that the trunking or Server Application Optimization (SAO) license is not installed.

Recommended Action Install the license required.

FABR-1051

Message `D-Port <Testname> test failed for slot <Slot> and port <Port>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the D_Port test failed for the given slot and port due to one of the following reasons:

- The small form-factor pluggable (SFP) fault detected by electrical loopback test failure.
- The cable fault detected by optical loopback test failure.
- An application-specific integrated circuit (ASIC) issue detected by link traffic test failure.

Recommended Action Replace the faulty SFPs, cables, or blade.

FABR-1052

Message `The configured port speed is invalid. Persistently disabling port <Port that is being disabled>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the configured speed for the specified port is invalid.

Recommended Action Execute the **portCfgSpeed** command to change the port speed.

FABR-1053

Message `The switch is disabled due to an inconsistency found in the interop config parameters.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that the configuration keys have interopmode parameters such as switch.interopMode and switch.mcdtFabricmode set.

Recommended Action Execute the **interopmode** command to reset the parameters.

FABR-1054

Message `Rebooting the standby as it received an update before port [<Port Number>] is expanded.`

Message Type LOG | FFDC

Severity INFO

Probable Cause Indicates that the standby control processor (CP) did not have the port because the port expand operation is still in progress and the standby CP has received a port update. The standby CP reboots automatically to ensure sync and attain the normal state. This is a rare occurrence.

Recommended Action No action is required.

FABR-1055

Message `F_Port trunking cannot be enabled on the slot <Slot Number> port <Port Number> due to inconsistent port configuration.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified F_Port is unable to join its assigned trunk area group because of mismatch in the port configuration with the other trunk area members.

Recommended Action Check the configuration of the port with all other ports intended to be part of the same trunk group. Use the **porttrunkarea --show** to identify the trunk members of the specified F_Port and the **portcfgshow** command to identify the conflicting configuration between the trunk members.

FABS Messages

FABS-1001

Message `<Function name> <Description of memory need>.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the system is low on memory and cannot allocate more memory for new operations. This is usually an internal Fabric OS problem or file corruption. The *Description of memory need* variable specifies the memory size that was being requested. The value can be any whole number.

Recommended Action Reboot or power cycle the switch.

FABS-1002

Message `<Function name> <Description of problem>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that an internal problem has been detected by the software. This is usually an internal Fabric OS problem or file corruption.

Recommended Action Reboot or power cycle the switch.

If the message persists, run the **firmwareDownload** command to update the firmware.

FABS-1004

Message `<Function name and description of problem> process <Process ID number> (<Current command name>) <Pending signal number>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that an operation has been interrupted by a signal. This is usually an internal Fabric OS problem or file corruption.

Recommended Action Reboot or power cycle the switch.

FABS-1005

Message `<Function name and description of problem> (<ID type>= <ID number>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that an unsupported operation has been requested. This is usually an internal Fabric OS problem or file corruption. The following is a possible value for *function name and description of problem* variable:

fabsys_write: Unsupported write operation: process xxx

In this value, xxx is the process ID (PID), which could be any whole number.

Recommended Action Reboot or power cycle the active CP (for modular systems) or the switch (for single-board systems).

If the message persists, run the **firmwareDownload** command to update the firmware.

FABS-1006

Message `<Function name and description of problem>: object <object type id> unit <slot>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that there is no device in the slot with the specified object type ID in the system module record. This could indicate a serious Fabric OS data problem on the switch. The possible values for *function name and description of problem* variable are:

- setSoftState: bad object
- setSoftState: invalid type or unit
- media_sync: Media oid mapping failed
- fabsys_media_i2c_op: Media oid mapping failed
- fabsys_media_i2c_op: obj is not media type
- media_class_hndlr: failed sending media state to blade driver

Recommended Action If the message is isolated, monitor the error messages on the switch. If the error is repetitive or if the fabric failed, failover or reboot the switch.

If the message persists, run the **firmwareDownload** command to update the firmware.

FABS-1007

Message `<Function name>: Media state is invalid - status=<Status value>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Fabric OS has detected an invalid value in an object status field. This is usually an internal Fabric OS problem or file corruption.

Recommended Action Reboot or power cycle the switch.

If the message persists, run the **firmwareDownload** command to update the firmware.

FABS-1008

Message `<Function name>: Media oid mapping failed.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Fabric OS was unable to locate a necessary object handle. This is usually an internal Fabric OS problem or file corruption.

Recommended Action Reboot or power cycle the switch.

FABS-1009

Message `<Function name>: type is not media.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Fabric OS was unable to locate an appropriate object handle. This is usually an internal Fabric OS problem or file corruption.

Recommended Action Reboot or power cycle the switch.

FABS-1010

Message `<Function name>: Wrong media_event <Event number>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Fabric OS detected an unknown event type. This is usually an internal Fabric OS problem or file corruption.

Recommended Action Reboot or power cycle the switch.

If the message persists, run the **firmwareDownload** command to update the firmware.

FABS-1011

Message `<Method name>[<Method tag number>]:Invalid input state 0x<Input state code>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that an unrecognized state code was used in an internal Fabric OS message for a field-replaceable unit (FRU).

Recommended Action Reboot or power cycle the CP or system.

If the message persists, run the **firmwareDownload** command to update the firmware.

FABS-1013

Message `<Method name>[<Method tag number>]:Unknown blade type 0x<Blade type>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates an unrecognized type of blade has been discovered in the system.

This may be caused by an incorrect field-replaceable unit (FRU) header, inability to read the FRU header, or the blade may not be supported by this platform or Fabric OS version.

Recommended Action Verify that the blade is valid for use in this system and this version of Fabric OS.

Reseat the blade.

If this is a valid blade and reseating does not solve the problem, replace the blade.

FABS-1014

Message

```
<Method name>[<Method tag number>]:Unknown FRU type 0x<FRU Object type>.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates an unrecognized type of field-replaceable unit (FRU) has been discovered in the system.

This may be caused by an incorrect FRU header, inability to read the FRU header, or the FRU may not be supported by this platform or Fabric OS version.

Recommended Action

Verify that the FRU is valid for use in this system and this version of Fabric OS.

Reseat the FRU.

If this is a valid FRU and reseating does not solve the problem, replace the FRU

FABS-1015

Message

```
<Method name>[<Method tag number>]:Request to enable FRU type 0x<FRU Object type>,
unit <Unit number> failed. err code <Error code>.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates the specified FRU could not be enabled. This is usually an internal Fabric OS problem.

Recommended Action

Remove and reinsert the FRU.

Reboot or power cycle the CP or system.

If the message persists, run the **firmwareDownload** command to update the firmware.

FBC Messages

FBC-1001

Message `Firmware version on AP blade is incompatible with that on the CP.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the control processor (CP) blade determined that the firmware version running on the application processor (AP) blade is not compatible with that running on CP. The AP and CP blades cannot communicate.

Recommended Action The problem can be corrected by changing the firmware version on either the CP or on the AP blade. You can modify the firmware version on the CP blade by using the **firmwareDownload** command. Refer to the release notes to determine whether a non-disruptive firmware download is supported between the revisions. Because the AP and CP blades cannot communicate, it is not possible to load new firmware on the AP blade. If necessary, send the AP blade back to the factory for a firmware update.

FCMC Messages

FCMC-1001

Message `System is low on memory and has failed to allocate new memory.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the switch is low on memory and failed to allocate new memory for an information unit (IU).

Recommended Action A non-bladed switch will automatically reboot. For a bladed switch, the active CP blade will automatically fail over and the standby CP will become the active CP.

FCOE Messages

FCOE-1001

Message `calloc failed for <object>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a memory failure.

Recommended Action Check the memory usage on the switch using the **memShow** command.

FCOE-1002

Message `Max logingroup limit reached at <limit>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that too many login groups have been added.

Recommended Action Check the maximum login group value displayed in the message.

FCOE-1003

Message `<device>: member in another logingroup <lg> being removed.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the device World Wide Name (WWN) you are trying to add is present in some other login group, and therefore it will be removed from that login group and added to the new login group.

Recommended Action Check the login group changes using the **fcoelogincfg --show** command.

FCOE-1004

Message `<device>: removing member from <lg> failed.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that removing a device from the login group has failed.

Recommended Action Execute the **supportSave** command and restart the system. If the problem persists, contact your switch service provider.

FCOE-1005

Message `<device>: membership check failed in logingroup: <lg>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the membership check for the device has failed.

Recommended Action Check the device for failed membership using the **fcoelogincfg --show** command.

FCOE-1006

Message `file operation failed on <filename> for <operation> operation: errno:<error>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a file operation failure.

Recommended Action Check the error code for the file operation failure and contact your switch service provider for assistance.

FCOE-1007

Message `IfIndex Limit Reached <num_fcoe_entity>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the interface index (IfIndex) limit has reached the maximum.

Recommended Action Check the IfIndex limit displayed in the message.

FCOE-1009

Message `Addition of N_Port mapping failed. Max N_Port mapping limit reached: <max n_port>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the N_Port mapping has reached its maximum limit.

Recommended Action Remove unwanted N_Port mappings using the **fcoelogingroup --remove** command and try adding N_Port mapping using the **fcoelogingroup --add** command.

FCOE-1010

Message `FSS Registration or FCoE Trace initialization failed.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the Fabric OS state synchronization (FSS) registration or initialization of the FCoE trace has failed.

Recommended Action Execute the **supportSave** command and restart the system. If the problem persists, contact your switch service provider.

FCOE-1012

Message `Request to delete port from VLAN <vid> failed.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that a request to delete ports from the specified VLAN has failed.

Recommended Action Execute the **supportSave** command and restart the system. If the problem persists, contact your switch service provider.

FCOE-1014

Message `Request to add ports to VLAN <vid> failed.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that a request to add ports to the specified VLAN has failed.

Recommended Action Execute the **supportSave** command and restart the system. If the problem persists, contact your switch service provider.

FCOE-1015

Message `Request to add MACs to Layer 2 for ifindex 0x<ifindex> failed, rc:<reason code>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that a request to add MAC entries to Layer 2 for the specified slot or port has failed.

Recommended Action Check the reason code for the failure and contact your switch service provider for assistance.

FCOE-1016

Message `Request to delete VLAN <vid> failed.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a request to delete the specified VLAN has failed because the VLAN may be in use.

Recommended Action Disable the active FCoE login session using the **no fcoe** command and try deleting the VLAN again.

FCOE-1017

Message `Request to add FCMAP failed for VLAN <vid>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that a request to add FCMAP has failed. When the VLAN is in use, its FCMAP cannot be modified.

Recommended Action Disable the active FCoE session on VLAN using the **no fcoe** command and try adding the FCMAP again.

FCOE-1019

Message `FLOGI ignored as FCMAP is not configured on FCoE VLAN.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that FCMAP has not been configured on FCoE VLAN.

Recommended Action Configure FCMAP on the FCoE VLAN using the **fcoe --fcmapset** command.

FCOE-1021

Message `Port is already logged in.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the N_Port device has already logged in or is in the process; duplicate FLOGI received.

Recommended Action No action is required.

FCOE-1022

Message `Max FCoE device login limit reached.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the switch has reached its maximum allowed FCoE device limit.

Recommended Action Do not add any more FCoE devices to the switch.

FCOE-1023

Message `<portindex>, Too many logins on FCoE controller, max allowed = <MAX_DEVS_PER_CTLR>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the controller has reached its maximum allowed FCoE login limit.

Recommended Action Log out some of the logged-in devices using the **fcoe --resetlogin** command and then log in a new device. You can view the list of logged-in devices using the **fcoe --loginshow** command.

FCOE-1024

Message `FDISC received from E_node without prior FLOGI.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a FDISC frame is received from the end node that has not logged in. The end node must send a fabric login (FLOGI) before it can send an FDISC.

Recommended Action It is due to a CNA or target driver issue. Contact CNA or target driver support team for assistance.

FCOE-1025

Message `FCoE logout received on FIP VN port.`

Message Type LOG

Severity WARNING

Probable Cause Indicates pre-FIP logout for a device that has logged in using the FCoE Initialization Protocol (FIP).

Recommended Action It is due to a CNA or target driver issue. Contact CNA or target driver support team for assistance.

FCOE-1026

Message `FDISC/FLOGI mismatch. FDISC addressed to different FCF than base FLOGI.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the base port has sent a fabric login (FLOGI) but the subsequent FDISC frames that were received on the switch do not match the original FLOGI.

Recommended Action It is due to a CNA or target driver issue. Contact CNA or target driver support team for assistance.

FCOE-1027

Message `<message> : <mac1>:<mac2>:<mac3>:<mac4>:<mac5>:<mac6>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the Fibre Channel Forwarders (FCF) controller is not found for the DA. The end node may be sending the FLOGI with a wrong DA MAC address.

Recommended Action Some parameters are not exchanged correctly between the switch and the end device. Reconfigure the port.

FCOE-1028

Message `<message> : <wwn1>:<wwn2>:<wwn3>:<wwn4>:<wwn5>:<wwn6>:<wwn7>:<wwn8>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the FCoE device with the specified World Wide Name (WWN) is not a member of the login group.

Recommended Action Change the FCoE login group policy on the switch using the **fcoelogingroup** command so that the device can log in.

FCOE-1029

Message `Version mismatch between FIP FDISC and root VN port.`

Message Type LOG

Severity WARNING

Probable Cause Indicates a version mismatch between the fabric login (FLOGI) and FDISC.

Recommended Action It is due to a CNA or target driver issue. Contact CNA or target driver support team for assistance.

FCOE-1030

Message `Version mismatch between FIP LOGO and root VN port.`

Message Type LOG

Severity WARNING

Probable Cause Indicates a version mismatch between the FCoE initialization protocol (FIP) logout and the base fabric login (FLOGI).

Recommended Action It is due to a CNA or target driver issue. Contact CNA or target driver support team for assistance.

FCOE-1031

Message `FCoE port deleted port <port> slot <slot>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that an FCoE port has been deleted.

Recommended Action No action is required.

FCOE-1032

Message `We are in WARM RECOVERING state...`

Message Type LOG

Severity WARNING

Probable Cause Indicates that high availability (HA) failover or switch reboot may be in progress.

Recommended Action Wait until the chassis has fully recovered before you perform any operations.

FCOE-1033

Message `FIP v1 FLOGI received - VF port in use.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a device is trying to log in to a port that already has a device logged in.

Recommended Action No action is required.

FCOE-1034

Message `Discarded frame received on priority <pkt_ctrlp->pri_in> for which PFC/FCoE is disabled.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a frame is received on the specified priority, for which priority-based flow control (PFC) or FCoE is disabled.

Recommended Action Change the CEE map assigned to the FCoE map to accommodate the PFC for the specified FCoE priority or change the FCoE priority using the **fabric-map default** command under the FCoE configuration mode.

FCOE-1037

Message `Logingroup dropped for switch WWN: <switch WWN>, due to name conflict while merging.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that same login group name exists for two different switches that have different organizationally unique identifiers (OUIs), but the last three bytes are same.

Recommended Action Create the login group for the switch World Wide Name (WWN) with another name that will not lead to a name conflict.

FCOE-1038

Message `logingroup#<logingroup number> (<logingroup name>) created.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified login group is added to the switch login group table.

Recommended Action No action is required.

FCOE-1039

Message `Logingroup <logingroup name> deleted.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified login group is deleted from the switch login group table.

Recommended Action No action is required.

FCOE-1040

Message `Logingroup name changed from <old logingroup name> to <new logingroup name>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the login group has been renamed.

Recommended Action No action is required.

FCOE-1041

Message `Transaction aborted.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the ongoing FCoE login configuration transaction is aborted.

Recommended Action No action is required.

FCOE-1042

Message `FCoE login configuration transaction saved fabric-wide.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the FCoE login configuration transaction is saved fabric-wide.

Recommended Action No action is required.

FCOE-1043

Message `FCoE login configuration management disabled.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the FCoE login configuration management is disabled.

Recommended Action No action is required.

FCOE-1044

Message `FCoE login configuration management enabled.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the FCoE login configuration management is enabled.

Recommended Action No action is required.

FCOE-1045

Message `FCoE port <port number> is configured as VE port.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified FCoE port is configured as a virtual expansion (VE) port.

Recommended Action No action is required.

FCOE-1046

Message `fcoed.conf file is truncated. Please reconfigure FCoE ports.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the magic number in the fcoed.conf file does not match. Therefore, the fcoed.conf file is truncated and updated with a new magic number.

Recommended Action Reconfigure the FCoE ports as all the port configurations will be lost.

FCOE-1047

Message `fcoed.conf file is not present, therefore creating.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the fcoed.conf file is not available and therefore creating a new file.

Recommended Action No action is required.

FCOE-1048

Message `FCoE port <port number> is configured as VF port.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified FCoE port is configured as a virtual fabric (VF) port.

Recommended Action No action is required.

FCPD Messages

FCPD-1001

Message `Probing failed on <error string>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a Fibre Channel Protocol (FCP) switch probed devices on a loop port, and probing failed on the L_Port, arbitrated loop physical address (AL_PA), or the F_Port. For ALPA, the valid range is 0x00 through 0xFF. The *error* variable can be either of the following:

- L_Port *port_number* ALPA *alpa_number*
- F_Port *port_number*

This could happen due to some firmware issue with the device controller on the specified port.

Recommended Action Contact the device vendor for any firmware-related issues. Also, consider upgrading the device firmware.

FCPD-1002

Message `port <port number>, bad R_CTL for fcp probing: 0x<R_CTL value>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the response frame received on the specified port for an inquiry request contains an invalid value in the routing control field. This could happen due to some firmware issue with the device controller on the specified port.

Recommended Action Contact the device vendor for any firmware-related issues. Also, consider upgrading the device firmware.

FCPD-1003

Message `Probing failed on <error string> which is possibly a private device which is not supported in this port type.`

Message Type LOG

Severity INFO

Probable Cause Indicates that device probing has failed because private devices will not respond to the switch port login (PLOGI) during probing.

Recommended Action The Brocade 4100, 4900, 5000, 7500, and AP 7600 do not support private loop devices. Refer to the switch vendor for a list of other port types that support private devices for inclusion into the fabric.

FCPH Messages

FCPH-1001

Message `<function>: <failed function call> failed, out of memory condition.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the switch is low on memory and failed to allocate new memory for a Fibre Channel driver instance.

The *function* value can only be fc_create. This function creates a Fibre Channel driver instance.

The *failed function call* can only be kmalloc_wrapper, which has failed. This function call is for kernel memory allocation.

Recommended Action A non-bladed switch will automatically reboot. For a bladed switch, the active CP blade will automatically fail over and the standby CP will become the active CP.

FCPH-1002

Message `Port <Port Number> has been disabled since switch requires authentication when device authentication policy is set to ON.`

Message Type LOG

Severity WARNING

Probable Cause Indicates a device that does not support authentication has tried to log in to the switch when the device authentication policy is in ON status on the switch.

Recommended Action Enable the authentication on the device or set the device authentication status to PASSIVE/OFF on the switch if it is not mandatory. Use the **authUtil** command to change the device authentication policy.

FCPH-1003

Message `New port <Port Number> has same Port WWN as old port <Port Number> as part of duplicate Port WWN detection policy.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the specified new port has the same Port World Wide Name (PWWN) as the old port.

Recommended Action No action is required.

FCPH-1004

Message

```
NPIV port <Port Number> has same Port WWN as old port <Port Number> with pid
0x<Port PID> as part of duplicate Port WWN detection policy.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the specified N_Port ID virtualization (NPIV) port has the same Port World Wide Name (PWWN) as the old port.

Recommended Action

No action is required.

FCPH-1005

Message

```
FDISC exch=0x<ExchangeId> sid=0x<SourceID> did=0x<DestinationID> on port <Port>
rejected; temporary mem alloc error. Please bounce port of affected device.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that in busy login conditions, the buffer used for quick memory allocations (known as *atomic malloc*) can be quickly depleted and not replenished before the next allocation occurs.

Recommended Action

Reset the specified port using the **portDisable** and **portEnable** commands.

FCR Messages

FCR-1001

Message `FC router proxy device in edge created at port <port number>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a proxy device at a port in the edge fabric has been imported at the specified port.

Recommended Action No action is required.

FCR-1002

Message `FC router proxy device in edge deleted at port <port number>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a proxy device at a port in the edge fabric has been deleted at the specified port.

Recommended Action No action is required.

FCR-1003

Message `FC router physical DEVICES newly exported at port <port number>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that one or more physical devices have been newly exported through the specified port.

Recommended Action No action is required.

FCR-1004

Message `FC router physical devices offline at port <port number>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that one or more physical devices connected to the specified port have gone offline.

Recommended Action Verify that the devices were intended to be taken offline. If not, verify that the devices are functioning properly. Verify that all small form-factor pluggables (SFPs) are seated correctly. Check for faulty cables, deteriorated SFPs, or dirty connections. Replace the cables and the SFPs if necessary.

FCR-1005

Message `FC router LSAN zone device removed at port <port number>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a device is removed from the logical storage area network (LSAN) zone in the edge fabric.

Recommended Action No action is required.

FCR-1006

Message `FC router LSAN zone device added at port <port number>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a device is added to a logical storage area network (LSAN) zone in the edge fabric.

Recommended Action No action is required.

FCR-1007

Message `FC router LSAN zone deleted at port <port number>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a logical storage area network (LSAN) zone attached to the specified port was deleted in the edge fabric.

Recommended Action No action is required.

FCR-1008

Message `FC router LSAN zone created at port <port number>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a logical storage area network (LSAN) zone was created at the specified port in the edge fabric.

Recommended Action No action is required.

FCR-1009

Message `FC router LSAN zone enabled at port <port number>: <enabled name>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a logical storage area network (LSAN) zone was enabled in the edge fabric attached to the specified port. The enabled LSAN zone configuration is listed.

Recommended Action No action is required.

FCR-1010

Message `FC router LSAN zone disabled at port <port number>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a logical storage area network (LSAN) zone is disabled in the edge fabric attached to the specified port.

Recommended Action No action is required.

FCR-1011

Message `Remote LSAN zone updated in domain <domain ID>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a logical storage area network (LSAN) zone update was received from another domain.

Recommended Action No action is required.

FCR-1012

Message `FC Router fabric build completed on port <port number>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Fibre Channel router has completed a fabric build at the specified port.

Recommended Action No action is required.

FCR-1013

Message `Phantom FSPF database exchange completed on port <port number>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified EX_Port has completed the fabric shortest path first (FSFP) database exchange.

Recommended Action No action is required.

FCR-1015

Message `New EX_Port or VEX_Port added on port <port number> in domain <domain ID>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that an EX_Port was created on the specified port in the specified domain.

Recommended Action No action is required.

FCR-1016

Message `FCR fabric no longer reachable at port id <port number> (0x<port number (hex)>) fabric ID <fabric ID>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a fabric is no longer accessible through the backbone fabric. This may be caused by a link or switch failure.

Recommended Action No action is required.

FCR-1018

Message `FC router proxy device entries exhausted on port <port number>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the number of proxy devices is greater than allowed by the port resource.

Recommended Action Remove excess logical storage area network (LSAN) zones or devices until the number of proxy devices exported is within the range allowed by the port resource. Use the **fcrResourceShow** command to view resources including LSAN zone resources, LSAN device resources, and proxy device port resources. Use the **fcrProxyDevshow** command to view how many proxy devices are created in the fabric with the port resource problem. LSAN zones are removed using standard zoning commands such as **zoneShow**, **zoneRemove**, **zoneDelete**, **cfgDelete**, and **cfgDisable** in the edge fabric. Proxy devices can be removed by zoning operations or by bringing physical devices offline (for example, disabling the port that a device is attached to, and then disconnecting the cable or disabling the device.

FCR-1019

Message `EX_Port or VEX_Port entries exhausted at port <port number>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the number of EX_Port or VEX_Port entries being created is greater than allowed by the port resource.

Recommended Action Disable EX_Ports or VEX_Ports until the number of ports is within the range allowed by the port resource. The EX_Port or VEX_Port limit is displayed using the **fcrRouteShow** command. Use the **portDisable** command to disable EX_Ports.

FCR-1020

Message `Local LSAN zone entries for FC router exhausted; max limit: <LSAN zone limit>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the number of LSAN zones created within a MetaSAN exceeds the local LSAN zone database limitations.

Recommended Action Remove excess LSAN zones so that the number of LSAN zones created is within the range of the local database limitations. To do that, perform the following steps:

1. Use the **portDdisable** command to disable all the EX_Ports that received this error message.
2. Use the **portDdisable** command to disable all the other EX_Ports on that FCR connected to the same edge fabrics to which the EX_Ports disabled in step 1 are connected.

3. Use zoning commands on the edge fabrics, to reduce the LSAN zone entries on the edge fabrics.
4. Use the **portEnable** command on each EX_Port, one at a time, and verify that this error is not reported again.

FCR-1021

Message `Local LSAN device entries exhausted while updating LSAN zone <zone name> device entries.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the number of devices created through logical storage area network (LSAN) zones within the MetaSAN exceeds the local LSAN zone database limitations.

Recommended Action Remove excess device entries within LSAN zones so that the number of devices is within the range of the local zone database limitations.

FCR-1022

Message `Local proxy device slot entries exhausted.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that resources to persistently store the proxy device slot to the remote world wide name (WWN) have been consumed.

Recommended Action Remove the proxy device slots by using the **fcrProxyConfig** command or limit proxy devices by removing logical storage area network (LSAN) zone entries.

FCR-1023

Message `Local phantom port WWN entries exhausted.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the number of port World Wide Names (WWNs) detected to be in use exceeds the local port WWN resources.

Recommended Action Limit the number of port WWNs required by limiting the remote edge fabric connectivity (which limits the number of translate domains). You can also limit the number of proxy devices for a translate domain (which limits the number of translate domain ports required) by limiting the devices specified in logical storage area network (LSAN) zones.

FCR-1024

Message `Local LSAN zone <zone name> device entries for edge LSAN exhausted.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the number of devices in a logical storage area network (LSAN) defined in the edge fabric is greater than allowed by the local LSAN zone database limitations.

Recommended Action Remove excess device entries from this LSAN zone until the number of devices is within the range of the local LSAN zone database limitations.

FCR-1025

Message `Local phantom node WWN entries exhausted.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the number of node World Wide Names (WWNs) detected to be in use exceeds the local node WWN resources.

Recommended Action Reduce the number of node WWNs required by limiting the remote edge fabric connectivity (which limits the number of translate domains).

FCR-1026

Message `In slot <slot number>, Node WWN roll over.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the node World Wide Name (WWN) pool has rolled over in the specified slot, and WWN entries not detected to be in use are reused as needed.

Recommended Action It is unlikely that WWN conflicts will occur as a result of pool rollover unless the switch is deployed in a very large MetaSAN environment with a large number of logical storage area network (LSAN) devices and fabrics, or there are highly dynamic changes to EX_Port connectivity. WWN conflicts might cause unpredictable behavior in management applications. To avoid WWN conflicts, all EX_Ports attached to fabrics with highly dynamic changes to EX_Port connectivity should be disabled and then re-enabled.

FCR-1027

Message `In slot <slot number>, Port WWN roll over.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the port World Wide Name (WWN) pool has rolled over in the specified slot, and WWN entries not detected to be in use are reused as needed.

Recommended Action It is unlikely that WWN conflicts will occur as a result of pool rollover unless the switch is deployed in a very large MetaSAN environment with a large number of logical storage area network (LSAN) devices and fabrics, or there are highly dynamic changes to EX_Port connectivity. WWN conflicts might cause unpredictable behavior in management applications. To avoid WWN conflicts, all EX_Ports attached to fabrics with highly dynamic changes to EX_Port or VEX_Port connectivity should be disabled and then re-enabled.

FCR-1028

Message `In slot <slot number>, node WWN pool 95 percent allocated.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the node World Wide Name (WWN) pool is close to rollover in the specified slot, and that the WWN entries not detected to be in use will be reused as needed.

Recommended Action It is unlikely that WWN conflicts will occur as a result of pool rollover unless the switch is deployed in a very large MetaSAN environment with a large number of logical storage area network (LSAN) devices and fabrics, or there are highly dynamic changes to EX_Port or VEX_Port connectivity. WWN conflicts might cause unpredictable behavior in management applications. To avoid WWN conflicts, all EX_Ports attached to fabrics with highly dynamic changes to EX_Port connectivity should be disabled and then re-enabled.

FCR-1029

Message `In slot <slot number>, Port WWN pool 95 percent allocated.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the port World Wide Name (WWN) pool has rolled over in the specified slot, and WWN entries not detected to be in use are reused as needed.

Recommended Action It is unlikely that WWN conflicts will occur as a result of pool rollover unless the switch is deployed in a very large MetaSAN environment with a large number of logical storage area network (LSAN) devices and fabrics, or there are highly dynamic changes to EX_Port connectivity. WWN conflicts might cause unpredictable behavior in management applications. To avoid WWN conflicts, all EX_Ports attached to fabrics with highly dynamic changes to EX_Port connectivity should be disabled and then re-enabled.

FCR-1030

Message `Physical device <device WWN> came online at fabric <fabric ID>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the physical device World Wide Name (WWN) came online in the specified fabric.

Recommended Action No action is required.

FCR-1031

Message `Physical device <device WWN> went offline in fabric <fabric ID>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the physical device World Wide Name (WWN) went offline in the specified fabric.

Recommended Action No action is required.

FCR-1032

Message `Edge fabric enabled security on port <port number> in fabric <fabric ID>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that Secure mode was turned on in the edge fabric.

Recommended Action No action is required.

FCR-1033

Message `Edge fabric disabled security on port <port number> in fabric <fabric ID>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that Secure mode was turned off in the edge fabric.

Recommended Action No action is required.

FCR-1034

Message `LSAN zone added in backbone fabric.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a new logical storage area network (LSAN) zone was added to the backbone fabric.

Recommended Action No action is required.

FCR-1035

Message `LSAN zone device <device WWN> added in the backbone fabric.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a new device to a logical storage area network (LSAN) zone was added to the backbone fabric.

Recommended Action No action is required.

FCR-1036

Message `LSAN zone <zone name> enabled in the backbone fabric.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified logical storage area network (LSAN) zone was enabled in the backbone fabric. The enabled LSAN zone configuration is listed.

Recommended Action No action is required.

FCR-1037

Message `LSAN zone disabled in the backbone fabric.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a logical storage area network (LSAN) zone is disabled in the backbone fabric.

Recommended Action No action is required.

FCR-1038

Message `Total zone entries exceeded local fabric limits by <overflow> entries, in zone: <zone name>, zone limit: <LSAN zone limit>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the number of cfg, zone, or alias entries created in a local fabric is greater than the local switch's zone database limitations.

Recommended Action Remove excess cfg, zone, or alias entries so that the number of logical storage area network (LSAN) zones created is within the range of the local database limitations.

FCR-1039

Message `Local LSAN zone <zone name> device entries for backbone LSAN exhausted.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of devices in the specified logical storage area network (LSAN) defined in the backbone fabric is greater than allowed by the local LSAN zone database limitations.

Recommended Action Remove excess device entries from this LSAN zone until the number of devices is within the range of the local LSAN zone database limitations.

FCR-1040

Message `Proxy device deleted in the backbone fabric.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a proxy device created in the backbone fabric was deleted.

Recommended Action No action is required.

FCR-1041

Message `LSAN zone device removed in the backbone fabric.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a logical storage area network (LSAN) zone device within the backbone fabric was removed.

Recommended Action No action is required.

FCR-1042

Message `LSAN zone removed in the backbone fabric.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a logical storage area network (LSAN) zone within the backbone fabric was removed.

Recommended Action No action is required.

FCR-1043

Message `Proxy device created in the backbone fabric.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a proxy device was created in the backbone fabric.

Recommended Action No action is required.

FCR-1048

Message `On EX port (<port number>) setting port <credit type> credits failed.`

Message Type LOG | FFDC

Severity ERROR

Probable Cause Indicates that the indicated credit type was not set. Setting port credits failed.

Recommended Action Send the First Failure Data Capture (FFDC) log to the support.

FCR-1049

Message `EX_Port (<port number>) received an ELP command that is not supported.`

Message Type LOG

Severity ERROR

Probable Cause Indicates an incoming exchange link parameter (ELP) command that is not supported.

Recommended Action Use the **portEnable** and **portDisable** to enable or disable the port.

If the problem persists, contact your switch service provider.

FCR-1053

Message `Port <port number> was disabled, <disable reason>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the specified port was disabled because of a mismatched configuration parameter.

Recommended Action Use the specified disable reason to identify a possible configuration parameter mismatch between the EX_Port and the switch at the other end of the link.

FCR-1054

Message

```
Port <port number> received ILS <command> of incorrect size (<actual payload
size>); valid ILS size is <expected payload size>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that an internal link service (ILS) IU of invalid size was received from the switch on the other end of the link.

Recommended Action

Check the error message log on the other switch using the **errShow** command for additional messages.

Check for a faulty cable or deteriorated small form-factor pluggable (SFP). Replace the cable or the SFP if necessary.

Run the **portLogDumpPort** command on both the receiving and transmitting ports.

Run the **fabStatsShow** command on the transmitting switch.

If the message persists, collect switch information using the **supportSave** command, and contact your switch service provider.

FCR-1055

Message

```
Switch with domain ID <domain ID> does not support backbone to edge imports.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that a switch that does not support backbone-to-edge routing was detected in the backbone. Edge-to-edge routing will work, but backbone-to-edge routing may fail.

Recommended Action

No action is required if backbone-to-edge routing is not required. Otherwise, replace the switch with one that supports backbone-to-edge routing.

FCR-1056

Message

```
Switch <switch WWN> with front domain ID <domain ID> does not support backbone to
edge imports.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that a switch that does not support backbone-to-edge routing is running in the MetaSAN.

Recommended Action

No action is required if backbone-to-edge routing is not needed. Otherwise, replace the switch with one that supports backbone-to-edge routing.

FCR-1057

Message `EX_Port(<port number>) incompatible long distance parameters on link.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the port, which is configured in long distance mode, has incompatible long distance parameters.

Recommended Action Check the port configuration on both sides of the link using the **portCfgShow** command.

Investigate the other switch for more details. Run the **errShow** command on the other switch to view the error log for additional messages.

FCR-1058

Message
```
Port <port number> isolated due to mismatched configuration parameter;
<segmentation reason>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that the specified port was isolated after segmentation caused by mismatched configuration parameters or by a domain ID assigned by the principal switch that did not match the insistent domain ID of this port.

Recommended Action Check the switches on both ends of the link for a possible mismatch in switch or port configuration parameters such as Operating Mode, E_D_TOV, R_A_TOV, Domain ID Offset, and so on.

Run the **portCfgExport** command to modify the appropriate parameters on the local switch.

Run the appropriate configuration command to modify the switch or port parameters on the remote switch.

FCR-1059

Message `EX_Port <port number> was disabled due to an authentication failure.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the authentication, which uses the Diffie Hellman - Challenge Handshake Authentication Protocol (DH-CHAP), failed on the EX_Port.

Recommended Action Verify that the shared secrets on both sides of the link match.

Disable and enable the ports by using the **portDisable** and the **portEnable** commands to restart authentication.

FCR-1060

Message `EX_Port(<port number>) has an incompatible configuration setting.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that virtual channel (VC) Link Init is enabled on the local switch and the remote switch is negotiating in R_RDY mode. The fabric might not form properly.

Recommended Action Check the configuration on the local switch using the **portCfgShow** command to verify that the VC Link Init is disabled, if the remote switch is configured in R_RDY mode or only capable of R_RDY mode.

- VC_RDY mode: Virtual channel flow control mode. This is a proprietary protocol.
- R_RDY mode: Receiver-ready flow control mode. This is the Fibre Channel standard protocol, that uses R_RDY primitive for flow control.

FCR-1061

Message `Backbone fabric created on port <port number>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a backbone fabric was built on the specified port.

Recommended Action No action is required.

FCR-1062

Message `Port <port number> disabled, system only supports <maximum ports> EX/VEX_ports.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the maximum number of supported EX_Ports or VEX_Ports was exceeded. To enable the specified port, disable any other operational port and then re-enable the port.

Recommended Action No action is required.

FCR-1063

Message `Fabric <fabric ID> for switch with domain ID: <domain ID> mismatch with local fabric ID <local fabric ID>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the fabric ID of the switch does not match the local switch.

Recommended Action Run the **switchShow** command to display the fabric ID. Change the fabric ID to match on both ends by modifying either the local or remote host using the **fcrConfigure** command.

FCR-1064

Message `Fabric ID of backbone FC-Routers mismatch or overlap.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that either a backbone fabric split and both are connected to a common edge fabric, or the fabric ID of two backbone fabrics connected to an edge fabric are the same.

Recommended Action If the backbone fabric split, merge the fabrics.

If two (or more) backbone fabrics have the same IDs, make the fabric IDs unique using the **fcrConfigure** command.

FCR-1065

Message `Fabric on port <port number> was assigned two different fabric IDs.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that another port on the switch is connected to the same edge fabric with a different fabric ID assignment.

Recommended Action Change the port fabric ID to the same value as the other ports connected to the edge fabric using the **portCfgExport** or **portCfgVexport** commands.

FCR-1066

Message

```
Fabric on port <port number> has the same fabric ID as in another fabric switch
<Conflict switch wwn>.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that either the fabric split, or there is another fabric (possibly the backbone) that has the same fabric ID as the fabric connected to the specified port.

Recommended Action

If the fabric split, merge the fabrics and manually re-enable the port.

If there is another fabric with the same ID, change the fabric ID for the port using the **portCfgExport** or **portcfgVExport** commands.

FCR-1067

Message

```
Zone configurations, total LSAN zones and aliases, exceeded on port <port number>
by <overflow> entries; max entries: <LSAN zone limit>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the total number of zone configurations created in connected fabric exceeds the maximum number supported by the Fibre Channel.

The limit includes both active and configured information that is part of be zoning database in the edge fabric. Non-LSAN zones are not counted in the limit.

Recommended Action

Limit the logical storage area network (LSAN) zoning-related zone configuration in the edge fabric connected to this port.

FCR-1068

Message

```
The FC Routing service is disabled.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the FC Routing service is disabled. This is caused by issuing the **fosConfig –-disable fcr**, **configDefault**, or the **configDownload** command with the **fcrState** set to 2 (disabled). Note that the FC Routing service is disabled by the factory.

Recommended Action

No action is required.

FCR-1069

Message `The FC Routing service is enabled.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the FC Routing service is enabled. This is caused by the **fosConfig –-enable fcr** or the **configDownload** command with the **fcrState** set to 1 (enabled). Note that the FC Routing service is disabled by the factory.

Recommended Action No action is required.

FCR-1070

Message `The FC Routing configuration is set to default.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the FC Routing configuration is set to the default by the user. This removes all prior FC Routing configurations.

Recommended Action No action is required.

FCR-1071

Message `Port <port number> is changed from non FCR port to FCR port.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the port became an EX_Port or VEX_Port.

Recommended Action No action is required.

FCR-1072

Message `Port <port number> is changed from FCR port to non FCR port.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the port is no longer an EX_Port or VEX_Port.

Recommended Action No action is required.

FCR-1073

Message `Switch with domain ID <domain ID> in fabric <fabric ID> has lower limit of LSAN Zones supported.`

Message Type LOG

Severity INFO

Probable Cause Indicates that an older version switch in the backbone or edge that supports a different limit of logical storage area network (LSAN) zones was detected.

Recommended Action Use the **fcrResourceShow** command on all Fibre Channel Routers in the Meta-SAN to find lowest supported LSAN zone limits. Ensure the total number of LSAN zones in the Meta-SAN are within the lowest supported limit of LSAN zones.

FCR-1074

Message `HA sync lost as remote CP supports only <LSAN Count> LSAN Zones.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the remote control processor (CP) has older firmware, which supports a lower number of logical storage area network (LSAN) zones. This is causing the loss of high availability (HA) sync.

Recommended Action Keep the number of LSAN zones to the lower limit of the two CPs or upgrade the remote CP.

FCR-1075

Message `Zone Name configuration is larger than <Zone Name Limit> characters in the edge fabric connected to port <port number>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the zone name configuration size created in the connected fabric exceeds the maximum supported by the FC Router. This size is equal to the total number of characters used by all the zone names in the edge fabric zoning database.

The limit includes both LSAN and non-LSAN zone names defined in the zoning name database of the edge fabric.

Recommended Action Limit the zone configuration size in the edge fabric connected to this port by either reducing the number of zones or changing the zone names to smaller names.

FCR-1076

Message `Port <port number> disabled, system only supports <maximum fds> front domains.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the maximum number of supported front domains was exceeded. To enable the specified port, disable any other operational front domain and then re-enable the port.

Recommended Action Make sure to remain within the maximum number of supported front domains.

FCR-1077

Message `Port <port number> rejected fabric binding request/check from the M-Model switch; <Fabric ID>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that an M-Model edge switch attempted to either activate or check the fabric binding. This port will be disabled if this event occurred during a check of fabric binding and not during failure to activate fabric binding. The error is caused when the binding list details configured on the M-Model switch do not match with the currently configured front port domain ID and WWN of the EX_Port on which this operation was attempted.

Recommended Action Ensure that the M-Model switch has the same currently configured details such as the front port domain ID and WWN of the EX_Port on which this operation was attempted.

FCR-1078

Message `LSAN name <LSAN name> is too long. It is dropped.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the length of the logical storage area network (LSAN) name exceeds the limit of 64 characters.

Recommended Action Change the name and reactivate the zone database.

FCR-1079

Message `Domain <Domain> has conflict matrix database with local domain.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the specified domain has a different matrix database from the local domain.

Recommended Action Change the matrix database.

FCR-1080

Message `The pause response timer for domain <Domain> expired.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that during the Coordinated HotCode protocol, a switch in the fabric has not responded to the pause message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been the result of the rejected pause message.

Recommended Action No action is required.

FCR-1081

Message `The pause message is rejected by the domain <Domain>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that during the Coordinated HotCode protocol, a switch in the fabric has rejected the pause message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been the result of the rejected pause message.

Recommended Action No action is required.

FCR-1082

Message `The pause retry count is exhausted for the domain <Domain>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that during the Coordinated HotCode protocol, a switch in the fabric did not accept the pause message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been the result of this issue.

Recommended Action No action is required.

FCR-1083

Message `The resume message is rejected by the domain <Domain>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that during the Coordinated HotCode protocol, a switch in the fabric has rejected the pause message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been the result of the rejected resume message.

Recommended Action No action is required.

FCR-1084

Message `The resume retry count is exhausted for the domain <Domain>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that during the Coordinated HotCode protocol, a switch in the fabric did not accept the resume message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been the result of this issue.

Recommended Action No action is required.

FCR-1085

Message `HA sync lost as remote CP does not support FCR based matrix.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the remote control processor (CP) has older firmware, which does not support the FCR-based matrix while the local CP has the feature enabled. This is causing the loss of the high availability (HA) synchronization.

Recommended Action Disable the FCR-based matrix or upgrade the remote CP.

FCR-1086

Message `HA sync lost as remote CP does not support 8 Gbps-capable FC based EX_Ports.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the remote control processor (CP) has older firmware, which does not support 8 Gbps-capable FC based EX_Port. This is causing the loss of the high availability (HA) synchronization.

Recommended Action Disable 8 Gbps-capable FC based EX_Ports or upgrade the remote CP.

FCR-1087

Message `ExPort <ExPort > connects to fabric <fabric > with capability to use XISL domain <Domain >.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the EX_Port connects to the logical fabric containing a domain that has the capability to use extended ISL (XISL).

Recommended Action Disable "Allow to use XISL" mode of the domain by using the **configure** command.

FCR-1088

Message `LSAN <Enforce/Speed> tag <Tag Name> added.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the user has added a LSAN tag.

Recommended Action No action is required.

FCR-1089

Message `LSAN <Enforce/Speed> tag <Tag Name> removed.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the user has removed a LSAN tag.

Recommended Action No action is required.

FCR-1091

Message `Backbone Fabric ID changed to <Tag>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the backbone fabric ID has been changed.

Recommended Action No action is required.

FCR-1092

Message `FCR ELS trap entries exhausted.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the FCR ELS trap entries are exhausted.

Recommended Action Execute the **supportSave** command and contact your switch service provider.

FCR-1093

Message `Slave EX-Port <Slave> interopmode conflicts with trunk master <Master>. Disabling the port.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the slave EX_Port is disabled due to interop conflict with trunk master

Recommended Action Configure the slave EX_Port with the trunk master interop mode.

FCR-1094

Message

```
No Integrated Routing license present. EX-Port <ExPort> will not perform device
sharing with other Brocade Native mode fabric(s).
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that an EX_Port has been configured in Brocade Native mode. Device sharing will not occur with other Brocade Native mode fabrics because the Integrated Routing license is not installed.

Recommended Action

Install Integrated Routing license if device sharing is needed with other Brocade Native mode fabrics.

FCR-1095

Message

```
The EX-Port <ExPort> is configured in 'McData/Open' Mode which is no longer
supported, hence will be disabled next time port is offline and online.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that an EX_Port has been configured in 'McData/Open' mode. Initially after HA failover, the EX_Port will come up in McDATA mode. Further toggling will disable the port.

Recommended Action

Remove the 'McData/Open' interop modes in all EX_Ports

FCR-1096

Message

```
Failed to allocate <data type> for <operation phase>: port <port number>.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that the authentication process failed because the system is low on memory.

Data type is the payload or structure that failed to get memory.

Operation phase specifies which operation of a particular authentication phase failed.

Recommended Action

Usually this problem is transient. The authentication may fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

FCR-1097

Message

```
Failed to get <data type> for <message phase> message: port <port number>, retval
<error code>.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that the authentication process failed to get a particular authentication value at certain phase.

Data type is the payload or structure that failed to get memory.

Recommended Action

Usually this problem is transient. The authentication may fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

FCR-1098

Message

```
Invalid message code for <message phase> message: port <port number>.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates the receiving payload does not have valid message code for a particular authentication phase.

Recommended Action

Usually this problem is transient. The authentication may fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

FCR-1099

Message

```
HA sync lost as remote CP does not support Inter Chassis Link EX_Ports.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that the remote control processor (CP) has older firmware that does not support inter-chassis link (ICL) EX_Ports. This is causing loss of the high availability (HA) synchronization.

Recommended Action

Disable EX_Ports on ICL links or upgrade the firmware on remote CP to v7.2.0 or later.

FCR-1100

Message `16G EX_Port ICL topology for fabric <Fabric ID> is unbalanced.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the current configuration of the EX_Port inter-chassis link (ICL) paths are unbalanced.

Recommended Action Investigate the current EX_Port ICL configuration to ensure that all recommendations for cabling are satisfied. Once cabling recommendations are satisfied, FCR-1101 message will be generated confirming ICL paths are balanced.

FCR-1101

Message `16G EX_Port ICL topology for fabric <Fabric ID> is balanced.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the existing EX_Port inter-chassis link (ICL) configuration that was resulting in an unbalanced topology for the corresponding fabric has been corrected.

Recommended Action No action is required.

FCR-1102

Message `ICL EX_Port <Port Numbers> need to be present in base switch to make a recommended topology.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that some of the ICL ports in a quad small form-factor pluggable (QSFP) are not present in the base switch. Ideally, all ports in the QSFP group should be present in the base switch.

Recommended Action Move the specified ICL EX_Ports of the QSFP group into the base switch using the **lscfg --config** command.

FCR-1103

Message `EX_Port <Port Number> ELS PLOGI from did <DID> to sid <SID> wwn <device wwn> NOT ZONED`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that FCR has received an ELS request for unzoned devices

Recommended Action Send the First Failure Data Capture (FFDC) log to the support.

FCR-1104

Message `In Edge fabric <Fabric-id> EX-Port <EX-Port>, domain-id <old_did> changes to <new_did>`

Message Type LOG

Severity INFO

Probable Cause Indicates that Phantom domain-id got changed in edge fabric

Recommended Action No action is required.

FCR-1105

Message `FIPS mode is enabled. SHA-1 hash type is not recommended in edge fabric <edge_fabric> connected to EX-port <port number>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the received authentication payload from edge fabric contains SHA-1 hash type.

Recommended Action SHA-1 is not a recommended setting when FIPS is enabled in edge fabric.

FICN Messages

FICN-1003

Message `FICON Tape Emulation License Key is not installed.`

Message Type LOG

Severity WARNING

Probable Cause Indicates FICON Tape Emulation requires a License Key.

Recommended Action Use the appropriate License Key.

FICN-1004

Message `FICON XRC Emulation License Key is not installed.`

Message Type LOG

Severity WARNING

Probable Cause Indicates FICON eXtended Remote Copy (XRC) Emulation requires a License Key.

Recommended Action Use the appropriate License Key.

FICN-1005

Message `FICON GEPort <GE port number> TID <Tunnel number> Feature Change verified Xrc <1 or 0 - XRC Emulation Enabled or Disabled> TapeWrt <1 or 0 - Tape Write Emulation Enabled or Disabled> TapeRd <1 or 0 - FICON Tape Read Emulation Enabled or Disabled> TinTir <1 or 0 - FICON TIN/TIR Emulation Enabled or Disabled> DvcAck <1 or 0 - FICON Device Level Ack Emulation Enabled or Disabled> RdBlkId <1 or 0 - FICON Write Emulation Read Block ID Emulation Enabled or Disabled>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the configuration was changed manually.

Recommended Action No action is required.

FICN-1006

Message

```
FICON GEPort <GE port number> TID <Tunnel number> Feature Change failed Xrc <1 or
0 - XRC Emulation Enabled or Disabled> TapeWrt <1 or 0 - Tape Write Emulation
Enabled or Disabled> TapeRd <1 or 0 - FICON Tape Read Emulation Enabled or
Disabled> TinTir <1 or 0 - FICON TIN/TIR Emulation Enabled or Disabled> DvcAck <1
or 0 - FICON Device Level Ack Emulation Enabled or Disabled> RdBlkId <1 or 0 -
FICON Write Emulation Read Block ID Emulation Enabled or Disabled>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that the feature change has failed because the FCIP tunnel ID associated with the FICON tunnel is still active.

Recommended Action Disable the applicable FCIP tunnel to make the feature change effective.

FICN-1007

Message

```
DevDiskEgr:FICON Selective Reset:Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> State=0x<Current Emulation
State> stat_array=0x<the Last 4 Status values that were received from the device>.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates a Selective Reset from the channel was received as either a normal part of path recovery or the starting sequence in an error case.

Recommended Action If there was a job failure associated with this event, contact your vendor's customer support.

FICN-1008

Message

```
DevDiskEgr:FICON Purge Path received Path=0x<VEPortNumber HostDomain HostPort
DeviceDomcontactain><DevicePort LPAR CUADDR DeviceAddr>.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates a FICON Purge Path was received from the channel as a part of path recovery.

Recommended Action If there was a job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1009

Message

```
DevIng:CmdReject Sense Data rcvd:Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> LastCmds=0x<the Last 4 commands
issued to the device> Sense Data:Bytes0-0xB=0x<bytes 0-3 of sense data from the
device><bytes 4-7 of sense data from the device><bytes 8-0x0b of sense data from
the device>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates a Unit Check status was received from a device and a sense command was issued to read the sense data.

Recommended Action If there was a job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1010

Message

```
DevDiskEgr:Device level exception flag found for Path=0x<VEPortNumber HostDomain
HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>: Oxid=0x<The OXID that
was reported in the Device Level Exception Frame>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates a Device Level Exception frame was received from the FICON channel.

Recommended Action If there was a job or I/O failure associated with this event, contact your vendor's customer support for assistance.

FICN-1011

Message

```
DevDiskIng:XRC Incorrect RRS SeqNum Rcvd Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> Expected=0x<The RRS Sequence
number that was expected from the device> Received=0x<The RRS Sequence number that
was actually received from the device> Oxid=0x<The data frame's OXID>.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates the Control unit or device presented a Read Record Set Sequence number different from the SDM's expected sequence number.

Recommended Action If there was an XRC volume or session suspended associated with this event, contact your vendor's customer support for assistance.

FICN-1012

Message

```
DevDiskIng:Device level exception found for Path=0x<VEPortNumber HostDomain
HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>: Oxid=0x<The OXID that
was reported in the Device Level Exception Frame>.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates a Device Level Exception frame received from the FICON direct attached storage device (DASD) Control Unit.

Recommended Action If there was a job or I/O failure associated with this event, contact your vendor's customer support for assistance.

FICN-1013

Message

```
DevDiskIng:Status=0x<Status that was received from the DASD device in an odd
state> received in odd state=0x<The current emulation state> from
Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR
DeviceAddr> sent LBY.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that when the device sent the status in an incorrect state, the emulation processing rejected the status with an LBY frame.

Recommended Action If there was a job or I/O failure associated with this event, contact your vendor's customer support for assistance.

FICN-1014

Message

```
DevEgr:Device level exception flag found for Path=0x<VEPortNumber HostDomain
HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>: Oxid=0x<The OXID used
to deliver the non-AS Device Level Exception>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates a frame was received that indicated a device level exception.

Recommended Action If there was an I/O failure associated with this event, contact your vendor's customer support for assistance.

FICN-1015

Message

```
DevEgr:cuPath=0x<VEPortNumber HostDomain HostPort DeviceDomain>******:Discarding
Invalid LRCd SOF=0x<The invalid Frame's SOF value (SOFiX or SOFnx)> count=<The
total number of frames that have been received from the peer with incorrect FICON
LRC values>.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates a frame was received from the peer emulation processing with an invalid Longitudinal Redundancy Checking (LRC) values. This indicates data corruption between the emulation processing components.

Recommended Action Contact your vendor's customer support for assistance.

FICN-1016

Message

```
DevIng:Received Logical Path Removed response:Path=0x<VEPortNumber HostDomain
HostPort DeviceDomain><DevicePort LPAR><CUADDR>**.
```

Message Type LOG

Severity INFO

Probable Cause Indicates the FICON Control Unit sent a Logical Path Removed (LPR) frame to the FICON channel.

Recommended Action No action is required.

FICN-1017

Message

```
DevIng:Received Logical Path Established response:Path=0x<VEPortNumber HostDomain
HostPort DeviceDomain><DevicePort LPAR><CUADDR>**.
```

Message Type LOG

Severity INFO

Probable Cause Indicates the FICON Control Unit sent an Logical Path Established (LPE) frame to the FICON channel.

Recommended Action No action is required.

FICN-1018

Message

```
DevIng:FCUB Lookup failed for Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR>******.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates the FICON Control Unit sent a frame that cannot be associated with a FICON Control Unit number (CUADDR).

Recommended Action Contact your vendor's customer support for assistance.

FICN-1019

Message

```
DevTapeEgr:AS Link Level Reject (LRJ) from Chan on Path=0x<VEPortNumber HostDomain
HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> LastCmd=0x<the Last 4
commands issued to the device> LastStatus=0x<the Last 4 status values received
from the device>.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates the FICON channel indicated in the path issued a Link Level Reject (LRJ) frame for a sequence from the device.

Recommended Action If there was a job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1020

Message

```
DevTapeEgr:FICON Cancel received Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> state=0x<the current emulation
state for the device> tflags=0x<the current emulation tape control flags for the
device> sflags=0x<the current emulation status control flags for the device>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates the FICON channel issued a Cancel sequence for a device in emulation.

Recommended Action If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1021

Message

```
DevTapeEgr:FICON Tape Cancel:Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> Elapsed Time=<the current SIO
time in seconds for the device>.<the current SIO time in milliseconds for the
device> seconds.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates the FICON channel issued a Cancel sequence for a device in emulation.

Recommended Action

If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1022

Message

```
DevTapeEgr:FICON Selective Reset:Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> State=0x<the current state of
the device that received the selective reset> statArray=0x<the last 4 status
values received from the device> cmdArray=0x<the last 4 commands that were issued
to the device> tflags=0x<the current emulation tape control flags for the device>
sflags=0x<the current emulation status control flags for the device>.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates the FICON channel issued a Selective Reset for a device that was active in emulation.

Recommended Action

If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1023

Message

```
DevTapeEgr:FICON Selective Reset:Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> Elapsed Time=<the current SIO
time in seconds for the device>.<the current SIO time in milliseconds for the
device> seconds.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates the FICON channel issued a Selective Reset sequence for a device.

Recommended Action

If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1024

Message `DevTapeEgr:FICON Purge received Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the FICON channel issued a Purge Path command sequence for a device.

Recommended Action If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1025

Message `DevTapeIng:Auto Sense Data received on Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> Bytes0-0xB=0x<bytes 0-3 of sense data from the device><bytes 4-7 of sense data from the device><bytes 8-0x0b of sense data from the device>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the FICON Tape Write Pipelining processed sense data from a FICON device.

Recommended Action If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1026

Message `DevTapeIng:UnusualStatus:WriteCancelSelr:Generating Final Ending Status Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the FICON Tape Write Pipelining is completing an emulated Selective Reset sequence.

Recommended Action If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1027

Message

```
DevTapeIng:Device level exception found for Path=0x<VEPortNumber HostDomain
HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>: Oxid=0x<The OXID of
the frame that included the Device Level Exception>.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates an active emulation device delivered a Device Level Exception frame to the emulation processing.

Recommended Action If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1028

Message

```
HostDiskIng:FICON Cancel received Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> state=0x<The current emulation
state of the device>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates an active emulation device received a cancel operation from the FICON channel.

Recommended Action If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1029

Message

```
HostDiskIng:FICON Selective Reset:Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> state=0x<The current emulation
state of the device> LastCmds=0x<The last 4 commands received from the channel for
this device> LastStatus=0x<The last 4 status values presented to the channel for
this device>.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates an active disk emulation device received a Selective Reset from the FICON channel.

Recommended Action If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1030

Message `HostDiskIng:FICON Purge received:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates an active disk emulation device received a FICON Purge Path from the channel.

Recommended Action If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1031

Message `HostDiskIng:FICON System Reset received on Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR><CUADDR>**.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the FICON channel sent a System Reset to the disk control unit.

Recommended Action No action is required. The MVS system was either set to initial program load (IPL) or performing error recovery.

FICN-1032

Message `HostDiskIng:XRC Read Channel Extender Capabilities detected on Path: 0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the eXtended Remote Copy (XRC) System Data mover was restarted to discover the capabilities of the channel extension equipment.

Recommended Action No action is required. This is a part of the XRC initialization.

FICN-1033

Message `HostEgr:Logical Path Established on Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR><CUADDR>**.`

Message Type LOG

Severity INFO

Probable Cause Indicates the peer-side FICON Control Unit has accepted a logical path establishment command sequence with the FICON channel.

Recommended Action No action is required. This is a part of the FICON path initialization.

FICN-1034

Message `HostEgr:Discarding Invalid LRCd Frame on Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort>****** count=<The total number of frames that have been received with an invalid LRC.>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the channel emulation processing received a frame with an invalid FICON LRC from the peer. This indicates that the channel side noted corruption from the Control Unit- or device-side processing.

Recommended Action Contact your vendor's customer support for assistance.

FICN-1035

Message `HostIng:FICON System Reset received on Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort><LPAR><CUADDR>**.`

Message Type LOG

Severity WARNING

Probable Cause Indicates a locally connected FICON channel issued a System Reset to the specified FICON Control Unit.

Recommended Action No action is required. This is a part of the FICON path initialization.

FICN-1036

Message `HostIng:FICON RLP Request on Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort><LPAR><CUADDR>**.`

Message Type LOG

Severity INFO

Probable Cause Indicates a locally connected FICON channel issued a Remove Logical Path sequence to the specified FICON Control Unit.

Recommended Action No action is required. This is a part of the FICON path deactivation.

FICN-1037

Message `HostIng:FICON ELP Request on Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort><LPAR><CUADDR>**.`

Message Type LOG

Severity INFO

Probable Cause Indicates a locally connected FICON channel issued an Establish Logical Path sequence to the specified FICON Control Unit.

Recommended Action No action is required. This is a part of the FICON path activation.

FICN-1038

Message `fcFicIngHost:FDCB Lookup failed for Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort>******.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a locally connected FICON channel sent a frame that could not be associated with a FICON device.

Recommended Action Contact your vendor's customer support for assistance.

FICN-1039

Message `HostIng:FCUB Lookup failed for Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR>********.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a locally connected FICON channel sent a frame that could not be associated with a FICON Control Unit.

Recommended Action Contact your vendor's customer support for assistance.

FICN-1040

Message `HostTapeEgr:Tape:CmdReject Sense Data Rcvd:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> LastCmds=0x<Last 4 commands received from the channel for this device> SenseData:Bytes0-0xB=0x<Bytes 0-3 of sense data from the device><Bytes 4-7 of sense data from the device><Bytes 8-0x0b of sense data from the device>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates an active disk emulation device received a FICON Purge Path from the channel.

Recommended Action If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1041

Message `HostTapeEgr:AS Link Level Reject (LRJ) from CU Rx Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> LastCmd=0x<Last 4 commands issued to this device from the channel> LastStatus=0x<Last 4 status values sent to the channel from this device>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that a Link Level Reject (LRJ) received from a device indicates that the Control Unit has lost the logical path to the Logical Partition (LPAR).

Recommended Action If this was an unexpected event, contact your vendor's customer support for assistance.

FICN-1042

Message

```
HostTapeIng:FICON Cancel received Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> state=0x<the current emulation
state for this device>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates a job was canceled during a Tape Write Pipelining.

Recommended Action If this was an unexpected event (cancel is normally an operator event), contact your vendor's customer support for assistance.

FICN-1043

Message

```
HostTapeIng::FICON Selective Reset:Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> state=0x<the current emulation
state for this device> LastCmds=0x<the last 4 commands received from the channel
for this device> LastStatus=0x<the last 4 status values presented to the channel
for this device>.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates that protocol errors in emulation in the Control Unit or network errors can cause a Selective Reset.

Recommended Action If this was an unexpected event, contact your vendor's customer support for assistance.

FICN-1044

Message

```
HostTapeIng:FICON Selective Reset:Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> Elapsed Time=<the number of
seconds since the last IO started for this device>.<the number of milliseconds
since the last IO started for this device> seconds.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates that protocol errors in emulation in the Control Unit or network errors can cause a Selective Reset.

Recommended Action If this was an unexpected event, contact your vendor's customer support for assistance.

FICN-1045

Message

```
HostTapeIng:FICON Purge received:Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates a Purge Path was received from the locally connected FICON channel. This is performed during the path recovery.

Recommended Action If this was an unexpected event, contact your vendor's customer support for assistance.

FICN-1046

Message

```
HostTapeIng:LRJ received on Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> lastCmds=0x<Last 4 commands
received from the channel for this device> lastStatus=0x<Last 4 status values
presented to the channel for this device> treating as system reset event.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that a Link Level Reject (LRJ) from a FICON channel indicates that the channel no longer has a path established to the Control Unit.

Recommended Action This is normally an unexpected event; contact your vendor's customer support for assistance.

FICN-1047

Message

```
fcFicSetEmulation:Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> FDCB Not Idle state=0x<Current
emulation state of the FICON device> prevState=0x<Previous emulation state of the
FICON device> set to state=0x<The new state to which the device is transitioning>.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates there is an internal emulation error. This message should not be encountered.

Recommended Action This is an unexpected event; contact your vendor's customer support for assistance.

FICN-1048

Message

```
DevDiskEgr:FICON Cancel received Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> state=0x<Current emulation state
of the FICON device> sflags=0x<The current emulation status flags>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates the operator has canceled a read or write job.

Recommended Action This is an unexpected event; contact your vendor's customer support for assistance.

FICN-1049

Message

```
ProcessIngTirData:Lost Logical Path for Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr><CUADDR>** Index=<Current
processing index in the TIR data from the locally connected channel or control
unit>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates a TIR received from a FICON endpoint indicates that it no longer has an established path to its peer.

Recommended Action This is an unexpected event; contact your vendor's customer support for assistance.

FICN-1050

Message

```
ProcessEgrTirData:Lost Logical Path for Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr><CUADDR>** Index=<Current
processing index in the TIR data from the remotely connected channel or control
unit>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates a TIR received from a far-side FICON endpoint indicates that it no longer has an established path to its peer.

Recommended Action This is an unexpected event; contact your vendor's customer support for assistance.

FICN-1051

Message `XRC Session Established: SessID=<SDM Assigned Session ID>, Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>`

Message Type LOG

Severity INFO

Probable Cause Indicates a PSF command has been received to initiate an eXtended Remote Copy (XRC) session with the extended direct attached storage device (DASD) device.

Recommended Action No action is required. This is a part of the XRC session establishment.

FICN-1052

Message `XRC Session Terminated: SessID=<SDM Assigned Session ID>, Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.`

Message Type LOG

Severity INFO

Probable Cause Indicates a PSF command has been received to break an eXtended Remote Copy (XRC) session with the extended direct attached storage device (DASD) device.

Recommended Action If this was an unexpected event, contact your vendor's customer support for assistance.

FICN-1053

Message `XRC Withdraw From Session: SessID=<SDM Assigned Session ID>, Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.`

Message Type LOG

Severity INFO

Probable Cause Indicates a PSF command has been received to withdraw from the eXtended Remote Copy (XRC) session with the extended direct attached storage device (DASD) device.

Recommended Action If this was an unexpected event, contact your vendor's customer support for assistance.

FICN-1054

Message

```
XRC Device Suspended: SessID=<SDM Assigned Session ID>, Path=0x<VEPortNumber
HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates a PSF command has been received to suspend an eXtended Remote Copy (XRC) session with the extended direct attached storage device (DASD) device.

Recommended Action If this was an unexpected event, contact your vendor's customer support for assistance.

FICN-1055

Message

```
XRC All Devices Suspended: SessID=<SDM Assigned Session ID>, Path=0x<VEPortNumber
HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates a PSF command has been received to suspend all extended direct attached storage device (DASD) devices from the eXtended Remote Copy (XRC) session.

Recommended Action If this was an unexpected event, contact your vendor's customer support for assistance.

FICN-1056

Message

```
FICON Emulation Error Error Code=<The internal emulation error code value>,
Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR
DeviceAddr> LastStates=0x<The 4 oldest emulation states for this device><The prior
emulation state for this device><The current emulation state for this device>.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates an internal coding error within emulation processing.

Recommended Action This is an unexpected event; contact your vendor's customer support for assistance.

FICN-1057

Message `Error return from frame generation processing for a FICON device: Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates an internal resource shortage caused an error so that an emulation frame could not be created and sent to a device.

Recommended Action This is an unexpected event; contact your vendor's customer support for assistance.

FICN-1058

Message `Error return from frame generation processing for a FICON control unit: Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort><LPAR><CUADDR>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates an internal resource shortage caused an error so that an emulation frame could not be created and sent to a Control Unit.

Recommended Action This is an unexpected event; contact your vendor's customer support for assistance.

FICN-1059

Message `Error return from frame generation for a FICON Image: Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort><LPAR>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates an internal resource shortage caused an error so that an emulation frame could not be created and sent to an Logical Partition (LPAR).

Recommended Action This is an unexpected event; contact your vendor's customer support for assistance.

FICN-1060

Message `Error return from fcFwdPrcEgressFrame: Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates an internal resource shortage caused an error so that an emulation frame could not be created and sent to a device.

Recommended Action This is an unexpected event; contact your vendor's customer support for assistance.

FICN-1061

Message `Error return from fcFwdRemoveEmulHashEntry: Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates an internal issue has been encountered in the removal of an existing fast path hash table entry.

Recommended Action This is an unexpected event; contact your vendor's customer support for assistance.

FICN-1062

Message `Ingress Abort:Oxid=0x<the OXID of the aborted exchange>:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>:LastStates=0x<prior emulation state array><previous emulation state><current emulation state>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates an abort operation has been received from the local FC interface for an active emulation exchange.

Recommended Action This is an unexpected event; contact your vendor's customer support for assistance.

FICN-1063

Message

```
Egress Abort:Oxid=0x<the OXID of the aborted exchange>:Path=0x<VEPortNumber
HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR
DeviceAddr>:LastStates=0x<prior emulation state array><previous emulation
state><current emulation state>.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates an abort operation has been received from a peer FC interface for an active emulation exchange.

Recommended Action

This is an unexpected event; contact your vendor's customer support for assistance.

FICN-1064

Message

```
Ingress Abort:Oxid=0x<the OXID of the aborted exchange>:Unknown Path on
GEPort=<GEPortNumber> VEPort=<VEPortNumber> from SID=0x<Source Domain><Source
Port> to DID=0x<Destination Domain><Destination Port>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates an abort operation has been received from a local FC interface for an exchange.

Recommended Action

If there were associated I/O errors at the same time as this event, contact your vendor's customer support for assistance.

FICN-1065

Message

```
Egress Abort:Oxid=0x<the OXID of the aborted exchange>:Unknown Path on
GEPort=<GEPortNumber> VEPort=<VEPortNumber> from SID=0x<Source Domain ><Source
Port> to DID=0x<Destination Domain><Destination Port>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates an abort operation has been received from a peer FC interface for an exchange.

Recommended Action

If there were associated I/O errors at the same time as this event, contact your vendor's customer support for assistance.

FICN-1066

Message
```
MemAllocFailed for GEPort=<VEPortNumber> VEport=<GE0 or GE1 number> could not
create required structure.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates an internal resource limit has been encountered so that additional control block memory could not be allocated.

Recommended Action This is an unexpected event; either the maximum number of emulation devices are already in use or there is an internal memory leak. Contact your vendor's customer support for assistance.

FICN-1067

Message
```
Ingress Abort:Oxid=0x<the OXID of the aborted exchange>:Abort for
CH=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR>****.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates an abort operation has been received from a local FC interface for an emulation CH exchange.

Recommended Action If there were associated I/O errors at the same time as this event, contact your vendor's customer support for assistance.

FICN-1068

Message
```
Ingress Abort:Oxid=0x<the OXID of the aborted exchange>:Abort for
CU=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR><CUADDR>**.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates an abort operation has been received from a local FC interface for an emulation Control Unit exchange.

Recommended Action If there were associated I/O errors at the same time as this event, contact your vendor's customer support for assistance.

FICN-1069

Message `Emulation Configuration Error on TunnelId <Tunnel ID>:.`

Message Type LOG

Severity ERROR

Probable Cause Indicates an error has been noted in the FICON configuration. Refer to the string for the nature of the configuration issue.

Recommended Action If resolution of the configuration issue cannot be completed, contact your vendor's customer support for assistance.

FICN-1070

Message

```
DevTapeIngr:Exceptional Status rcvd on Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> state=0x<current emulation
state> status=0x<the exceptional status value>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates the normal end of tape status (0x0D or 0x05) is received from the device or error status (including Unit Check 0x02) is received from an active emulation device.

Recommended Action The end of tape is a normal event during pipelining and not the unit check. If there are associated I/O error messages with this event, contact your vendor's customer support for assistance.

FICN-1071

Message

```
HostTapeIngr:Tape Loaded on Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates the tape I/Os are processed from a locally connected Logical Partition (LPAR), which indicates that a tape is loaded on a device.

Recommended Action No action is required.

FICN-1072

Message

```
DevTapeEgr:Tape Loaded on Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates the tape I/Os are processed from a locally connected Logical Partition (LPAR), which indicates that a tape is loaded on a device.

Recommended Action No action is required.

FICN-1073

Message

```
HostTapeIngr:Unloaded:Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>:states=0x<4 prior emulation
states><previous emulation state><current emulation state>:cmds=0x<last 4
commands received from the channel for this device>:status=0x<last 4 status values
sent to the channel for this device>:flags=0x<tape report bit flags (0x80-Tape
Loaded,0x40-WriteEmul,0x20-RdBlkEmul,0x10-RdCpEmul)>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates a Rewind and Unload I/O has been processed from a locally connected Logical Partition (LPAR), which indicates that a tape should be unloaded on a device.

Recommended Action No action is required.

FICN-1074

Message

```
HostTapeIngr:WriteReport:Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>:Emuls=0x<the number of idle
state to non-idle state transitions while this tape was loaded>:Cmds=0x<the number
of emulated host write commands processed while this tape was
loaded>:Chains=0x<the number of emulated host chains processed while this tape was
loaded>:MBytes=<the number of emulated write Kilobytes processed while this tape
was loaded>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates a Rewind and Unload I/O has been processed from a locally connected Logical Partition (LPAR) and Tape Write Pipelining was performed on the currently loaded tape.

Recommended Action No action is required.

FICN-1075

Message

```
HostTapeIngr:ReadBlkReport:Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>:Emuls=0x<the number of idle
state to non-idle state transitions while this tape was loaded>:Cmds=0x<the number
of emulated host read commands processed while this tape was loaded>:Chains=0x<the
number of emulated host chains processed while this tape was loaded>:MBytes=<the
number of emulated read Kilobytes processed while this tape was loaded>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates a Rewind and Unload I/O has been processed from a locally connected Logical Partition (LPAR) and Read Block pipelining was performed on the currently loaded tape.

Recommended Action No action is required.

FICN-1076

Message

```
HostTapeIngr:ReadCpReport:Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>:Emuls=0x<the number of idle
state to non-idle state transitions while this tape was loaded>:Cmds=0x<the number
of emulated host read commands processed while this tape was loaded>:Chains=0x<the
number of emulated host chains processed while this tape was loaded>:MBytes=<the
number of emulated read Kilobytes processed while this tape was loaded>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates a Rewind and Unload I/O has been processed from a locally connected Logical Partition (LPAR) and Read Channel Program pipelining was performed on the currently loaded tape.

Recommended Action No action is required.

FICN-1077

Message

```
DevTapeEgr:Unloaded:Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>:states=0x<4 prior emulation
states><previous emulation state><current emulation state>:cmds=0x<last 4
commands received from the channel for this device>:status=0x<last 4 status values
received from the channel for this device>:flags=0x<tape report bit flags
(0x80-Tape Loaded,0x40-WriteEmul,0x20-RdBlkEmul,0x10-RdCpEmul)>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates a Rewind and Unload I/O has been processed from a remotely connected Logical Partition (LPAR), which indicates that a tape should be unloaded on a device.

Recommended Action No action is required.

FICN-1078

Message

```
DevTapeEgr:WriteReport:Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>:Emuls=0x<the number of idle
state to non-idle state transitions while this tape was loaded>:Cmds=0x<the number
of emulated host write commands processed while this tape was
loaded>:Chains=0x<the number of emulated host chains processed while this tape was
loaded>:MBytes=<the number of emulated write Kilobytes processed while this tape
was loaded>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates a Rewind and Unload I/O has been processed from a remotely connected Logical Partition (LPAR) and Write Tape Pipelining was performed on the currently loaded tape.

Recommended Action No action is required.

FICN-1079

Message

```
DevTapeEgr:ReadBlkReport:Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>:Emuls=0x<the number of idle
state to non-idle state transitions while this tape was loaded>:Cmds=0x<the number
of emulated host read commands processed while this tape was loaded>:Chains=0x<the
number of emulated host chains processed while this tape was loaded>:MBytes=<the
number of emulated read Kilobytes processed while this tape was loaded>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates a Rewind and Unload I/O has been processed from a remotely connected Logical Partition (LPAR) and Read Block pipelining was performed on the currently loaded tape.

Recommended Action No action is required.

FICN-1080

Message

```
DevTapeEgr:ReadCpReport:Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>:Emuls=0x<the number of idle
state to non-idle state transitions while this tape was loaded>:Cmds=0x<the number
of emulated host read commands processed while this tape was loaded>:Chains=0x<the
number of emulated host chains processed while this tape was loaded>:MBytes=<the
number of emulated read Kilobytes processed while this tape was loaded>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates a Rewind and Unload I/O has been processed from a remotely connected Logical Partition (LPAR) and Read Channel Program pipelining was performed on the currently loaded tape.

Recommended Action No action is required.

FICN-1081

Message

```
DevTapeIng:LRJ received on Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> lastCmds=0x<Last 4 commands
received from the channel for this device> lastStatus=0x<Last 4 status values
presented to the channel for this device> treating as system reset event.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates a Link Level Reject (LRJ) from a FICON channel indicates that the channel does not have a path established to the Control Unit.

Recommended Action This is normally an unexpected event; contact your vendor's customer support for assistance.

FICN-1082

Message

```
EmulEls:CSWR_RSCN received on GEPort=<GEPortNumber> VEPort=<VEPortNumber>
Domain=0x<Domain> Port=0x<Port Host/Device Side>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates an attached port which had a FICON emulated path established has logged out from the switch.

Recommended Action This may be an unexpected event; contact your vendor's customer support for assistance.

FICN-1083

Message

```
EmulEls:SW_RSCN received on GEPort=<GEPortNumber> VEPort=<VEPortNumber>
Domain=0x<Domain> Port=0x<Port Host/Device Side>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates an attached port with the established FICON emulated path has logged out from the switch.

Recommended Action This may be an unexpected event; contact your vendor's customer support for assistance.

FICN-1084

Message

```
fcFicInit: No DRAM2 memory available, FICON emulation is disabled.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates a faulty DRAM2 was detected and access to its address range is prohibited.

Recommended Action This is an unexpected event; contact your vendor's customer support for assistance.

FICN-1085

Message `FICON FCIP Tunnel is Up on GE<Either ge0 or ge1>,tunnel Id=<The configured tunnel ID (0-7)>.`

Message Type LOG

Severity INFO

Probable Cause Indicates a FICON FCIP tunnel has been established successfully to the peer switch.

Recommended Action No action is required.

FICN-1086

Message `FICON FCIP Tunnel is Down on GE<Either ge0 or ge1>,tunnel Id=<The configured tunnel ID (0-7)>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a FICON FCIP tunnel to the peer switch has been terminated.

Recommended Action This is an unexpected event; contact your vendor's customer support for assistance.

FICN-1087

Message `DevTeraEgr:AS Link Level Reject (LRJ) from Chan on Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> LastCmd=0x<the Last 4 commands issued to the device> LastStatus=0x<the Last 4 status values received from the device>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the FICON channel indicated in the path issued an Link Level Reject (LRJ) frame for a sequence from the device.

Recommended Action If there was a job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1088

Message

```
DevTeraEgr:FICON Cancel received Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> state=0x<the current emulation
state for the device> tflags=0x<the current emulation tera control flags for the
device> sflags=0x<the current emulation status control flags for the device>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates the FICON channel issued a Cancel sequence for a device in emulation.

Recommended Action If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1089

Message

```
DevTeraEgr:FICON Tera Cancel:Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> Elapsed Time=<the current SIO
time in seconds for the device>.<the current SIO time in milliseconds for the
device> seconds.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates the FICON channel issued a Cancel sequence for a device in emulation.

Recommended Action If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1090

Message

```
DevTeraEgr:FICON Selective Reset:Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> State=0x<the current state of
the device that received the selective reset> statArray=0x<the last 4 status
values received from the device> cmdArray=0x<the last 4 commands that were issued
to the device> tflags=0x<the current emulation tera control flags for the device>
sflags=0x<the current emulation status control flags for the device>.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates the FICON channel issued a Selective Reset for a device that was active in emulation.

Recommended Action If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1091

Message

```
DevTeraEgr:FICON Selective Reset:Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> Elapsed Time=<the current SIO
time in seconds for the device>.<the current SIO time in milliseconds for the
device> seconds.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates the FICON channel issued a Selective Reset sequence for a device.

Recommended Action If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1092

Message

```
DevTeraEgr:FICON Purge received Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates the FICON channel issued a Purge Path command sequence for a device.

Recommended Action If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1093

Message

```
DevTeraIng:Auto Sense Data received on Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> Bytes0-0xB=0x<bytes 0-3 of sense
data from the device><bytes 4-7 of sense data from the device><bytes 8-0x0b of
sense data from the device>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates the FICON tera write pipelining processed sense data from a FICON device.

Recommended Action If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1094

Message

```
DevTeraIng:UnusualStatus:WriteCancelSelr:Generating Final Ending Status
Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR
DeviceAddr>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates the FICON tera write pipeline is completing an emulated Selective Reset sequence.

Recommended Action If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1095

Message

```
DevTeraIng:Device level exception found for Path=0x<VEPortNumber HostDomain
HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>: Oxid=0x<The OXID of
the frame that included the Device Level Exception>.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates an active emulation device delivered a Device Level Exception frame to the emulation processing.

Recommended Action If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1096

Message

```
HostTeraEgr:CmdReject Sense Data Rcvd:Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> LastCmds=0x<Last 4 commands
received from the channel for this device> SenseData:Bytes0-0xB=0x<Bytes 0-3 of
sense data from the device><Bytes 4-7 of sense data from the device><Bytes 8-0x0b
of sense data from the device>.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates an active Teradata emulation sequence received a Command Reject Sense from the device.

Recommended Action If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1097

Message

```
HostTeraEgr:AS Link Level Reject (LRJ) from CU Rx Path=0x<VEPortNumber HostDomain
HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> LastCmd=0x<Last 4
commands issued to this device from the channel> LastStatus=0x<Last 4 status
values sent to the channel from this device>.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates a Link Level Reject (LRJ) received from a device indicates that the Control Unit has lost the logical path to the Logical Partition (LPAR).

Recommended Action

If this was an unexpected event; contact your vendor's customer support for assistance.

FICN-1098

Message

```
HostTeraIng:FICON Cancel received Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> state=0x<the current emulation
state for this device>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates a job was canceled during a Write Tape Pipelining.

Recommended Action

If this was an unexpected event (cancel is normally an operator event), contact your vendor's customer support for assistance.

FICN-1099

Message

```
HostTeraIng::FICON Selective Reset:Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> state=0x<the current emulation
state for this device> LastCmds=0x<the last 4 commands received from the channel
for this device> LastStatus=0x<the last 4 status values presented to the channel
for this device>.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that the channel recognized a timeout condition and issued a Selective Reset.

Recommended Action

If this was an unexpected event, contact your vendor's customer support for assistance.

FICN-1100

Message

```
HostTeraIng:FICON Selective Reset:Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> Elapsed Time=<the number of
seconds since the last IO started for this device>.<the number of milliseconds
since the last IO started for this device> seconds.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates that protocol errors in emulation in the Control Unit or network errors can cause Selective Reset.

Recommended Action If this was an unexpected event, contact your vendor's customer support for assistance.

FICN-1101

Message

```
HostTeraIng:FICON Purge received:Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates a Purge Path was received from the locally connected FICON channel. This is performed during the path recovery.

Recommended Action If this was an unexpected event, contact your vendor's customer support for assistance.

FICN-1102

Message

```
HostTeraIng:LRJ received on Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> lastCmds=0x<Last 4 commands
received from the channel for this device> lastStatus=0x<Last 4 status values
presented to the channel for this device> treating as system reset event.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates a Link Level Reject (LRJ) from a FICON channel indicates that the channel believes that it no longer has a path established to the Control Unit.

Recommended Action This is normally an unexpected event; contact your vendor's customer support for assistance.

FICN-1103

Message

```
DevTeraIngr:Exceptional Status rcvd on Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> state=0x<current emulation
state> status=0x<the exceptional status value>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the status (0x0D or 0x05) indicating the device is going down was received from the device or error status (including Unit Check 0x02) is received from an active emulation device.

Recommended Action The device doing down is a normal event during pipelining and not the unit check. If there are associated I/O error messages with this event, contact your vendor's customer support for assistance.

FICN-1104

Message

```
DevTeraEgr:Device Ready on Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates the Teradata device has been initialized and is ready for emulation operations.

Recommended Action No action is required.

FICN-1105

Message

```
DevTeraIng:LRJ received on Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> lastCmds=0x<Last 4 commands
received from the channel for this device> lastStatus=0x<Last 4 status values
presented to the channel for this device> treating as system reset event.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates a Link Level Reject (LRJ) from a FICON channel indicates that the channel does not have a path established to the Control Unit.

Recommended Action This is normally an unexpected event; contact your vendor's customer support for assistance.

FICN-1106

Message

```
DevPrintEgr:AS Link Level Reject (LRJ) from Chan on Path=0x<VEPortNumber
HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>
LastCmd=0x<the Last 4 commands issued to the device> LastStatus=0x<the Last 4
status values received from the device>.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates the FICON channel indicated in the path issued a Link Level Reject (LRJ) frame for a sequence from the device.

Recommended Action

If there was a job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1107

Message

```
DevPrintEgr:FICON Cancel received Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> state=0x<the current emulation
state for the device> tflags=0x<the current emulation tera control flags for the
device> sflags=0x<the current emulation status control flags for the device>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates the FICON channel issued a Cancel sequence for a device in emulation.

Recommended Action

If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1108

Message

```
DevPrintEgr:FICON Tera Cancel:Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> Elapsed Time=<the current SIO
time in seconds for the device>.<the current SIO time in milliseconds for the
device> seconds.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates the FICON channel issued a Cancel sequence for a device in emulation.

Recommended Action

If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1109

Message

```
DevPrintEgr:FICON Selective Reset:Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> State=0x<the current state of
the device that received the selective reset> statArray=0x<the last 4 status
values received from the device> cmdArray=0x<the last 4 commands that were issued
to the device> tflags=0x<the current emulation tera control flags for the device>
sflags=0x<the current emulation status control flags for the device>.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates the FICON channel issued a Selective Reset for a device that was active in emulation.

Recommended Action If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1110

Message

```
DevPrintEgr:FICON Selective Reset:Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> Elapsed Time=<the current SIO
time in seconds for the device>.<the current SIO time in milliseconds for the
device> seconds.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates the FICON channel issued a Selective Reset sequence for a device.

Recommended Action If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

FICN-1111

Message

```
DevPrintEgr:FICON Purge received Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates the FICON channel issued a Purge Path command sequence for a device.

Recommended Action If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1112

Message

```
DevPrintIng:Auto Sense Data received on Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> Bytes0-0xB=0x<bytes 0-3 of sense
data from the device><bytes 4-7 of sense data from the device><bytes 8-0x0b of
sense data from the device>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates the FICON Printer write pipelining processed sense data from a FICON device.

Recommended Action If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1113

Message

```
DevPrintIng:LRJ received on Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> lastCmds=0x<Last 4 commands
received from the channel for this device> lastStatus=0x<Last 4 status values
presented to the channel for this device> treating as system reset event.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates a Link Level Reject (LRJ) from a FICON channel indicates that the channel does not have a path established to the Control Unit.

Recommended Action This is normally an unexpected event; contact your vendor's customer support for assistance.

FICN-1114

Message

```
DevPrintIng:Device level exception found for Path=0x<VEPortNumber HostDomain
HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>: Oxid=0x<The OXID of
the frame that included the Device Level Exception>.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates an active emulation device delivered a Device Level Exception frame to the emulation processing.

Recommended Action If there was an unexpected job failure or I/O Error associated with this event, contact your vendor's customer support for assistance.

FICN-1115

Message `HostPrintEgr:CmdReject Sense Data Rcvd:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> LastCmds=0x<Last 4 commands received from the channel for this device> SenseData:Bytes0-0xB=0x<Bytes 0-3 of sense data from the device><Bytes 4-7 of sense data from the device><Bytes 8-0x0b of sense data from the device>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates an active Print emulation sequence received Command Reject Sense data from the device.

Recommended Action If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-1116

Message `HostPrintEgr:AS Link Level Reject (LRJ) from CU Rx Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> LastCmd=0x<Last 4 commands issued to this device from the channel> LastStatus=0x<Last 4 status values sent to the channel from this device>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that a Link Level Reject (LRJ) was received from a device indicating that the Control Unit has lost the logical path to the Logical Partition (LPAR).

Recommended Action If this was an unexpected event; contact your vendor's customer support for assistance.

FICN-1117

Message `HostPrintIng:FICON Cancel received Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> state=0x<the current emulation state for this device>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates a job was canceled during Print write pipelining.

Recommended Action If this was an unexpected event (cancel is normally an operator event), contact your vendor's customer support for assistance.

FICN-1118

Message

```
HostPrintIng::FICON Selective Reset:Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> state=0x<the current emulation
state for this device> LastCmds=0x<the last 4 commands received from the channel
for this device> LastStatus=0x<the last 4 status values presented to the channel
for this device>.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates that the channel recognized a timeout condition and issued a Selective Reset.

Recommended Action If this was an unexpected event, contact your vendor's customer support for assistance.

FICN-1119

Message

```
HostPrintIng:FICON Selective Reset:Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> Elapsed Time=<the number of
seconds since the last IO started for this device>.<the number of milliseconds
since the last IO started for this device> seconds.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates that the channel recognized a timeout condition and issued a Selective Reset.

Recommended Action If this was an unexpected event, contact your vendor's customer support for assistance.

FICN-1120

Message

```
HostPrintIng:FICON Purge received:Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates a Purge Path was received from the locally connected FICON channel. This is performed during FICON path recovery.

Recommended Action If this was an unexpected event, contact your vendor's customer support for assistance.

FICN-1121

Message

```
HostPrintIng:LRJ received on Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain><DevicePort LPAR CUADDR DeviceAddr> lastCmds=0x<Last 4 commands
received from the channel for this device> lastStatus=0x<Last 4 status values
presented to the channel for this device> treating as system reset event.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates than a Link Level Reject (LRJ) received from a FICON channel indicates that the channel no longer has a path established to the Control Unit.

Recommended Action This is normally an unexpected event; contact your vendor's customer support for assistance.

FICN-1122

Message

```
DevPrintIng:UnusualStatus:WriteCancelSelr:Generating Final Ending Status
Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR
DeviceAddr>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates the FICON Print write pipeline sequence has received unit check status.

Recommended Action If there was an unexpected job failure or I/O error associated with this event, contact your vendor's customer support for assistance.

FICN-2005

Message

```
FICON VEPort <VE port number> Feature Change verified Xrc <1 or 0 - XRC Emulation
Enabled or Disabled> TapeWrt <1 or 0 - Tape Write Emulation Enabled or Disabled>
TapeRd <1 or 0 - FICON Tape Read Emulation Enabled or Disabled> TinTir <1 or 0 -
FICON TIN/TIR Emulation Enabled or Disabled> DvcAck <1 or 0 - FICON Device Level
Ack Emulation Enabled or Disabled> RdBlkId <1 or 0 - FICON Write Emulation Read
Block ID Emulation Enabled or Disabled>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates the configuration was changed manually.

Recommended Action No action is required.

FICN-2006

Message

```
FICON VEPort <VE port number> Feature Change failed Xrc <1 or 0 - XRC Emulation
Enabled or Disabled> TapeWrt <1 or 0 - Tape Write Emulation Enabled or Disabled>
TapeRd <1 or 0 - FICON Tape Read Emulation Enabled or Disabled> TinTir <1 or 0 -
FICON TIN/TIR Emulation Enabled or Disabled> DvcAck <1 or 0 - FICON Device Level
Ack Emulation Enabled or Disabled> RdBlkId <1 or 0 - FICON Write Emulation Read
Block ID Emulation Enabled or Disabled>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates the FCIP Tunnel ID associated with the FICON tunnel must be down or disabled for a feature change to become effective.

Recommended Action Disable the applicable FCIP tunnel to make the feature change effective.

FICN-2064

Message

```
Ingress Abort:Oxid=0x<the OXID of the aborted exchange>:Unknown Path on
VEPort=<VEPortNumber> from SID=0x<Source Domain><Source Port> to
DID=0x<Destination Domain><Destination Port>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates an abort operation has been received from a local FC interface for an exchange.

Recommended Action If there were associated I/O errors at the same time as this event, contact your vendor's customer support for assistance.

FICN-2065

Message

```
Egress Abort:Oxid=0x<the OXID of the aborted exchange>:Unknown Path on
VEPort=<VEPortNumber> from SID=0x<Source Domain ><Source Port> to
DID=0x<Destination Domain><Destination Port>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates an abort operation has been received from a peer FC interface for an exchange.

Recommended Action If there were associated I/O errors at the same time as this event, contact your vendor's customer support for assistance.

FICN-2066

Message `MemAllocFailed for VEport=<VEPortNumber> could not create required structure.`

Message Type LOG

Severity WARNING

Probable Cause Indicates an internal resource limit has been encountered so that additional control block memory could not be allocated.

Recommended Action This is an unexpected event; either the maximum number of emulation devices are already in use or there is an internal memory leak. Contact your vendor's customer support for assistance.

FICN-2082

Message `EmulEls:CSWR_RSCN received on VEPort=<VEPortNumber> Domain=0x<Host/Device Side Domain> Port=0x<Host/Device Side Port>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates an attached port which had a FICON emulated path established has logged out from the switch.

Recommended Action This may be an unexpected event; contact your vendor's customer support for assistance.

FICN-2083

Message `EmulEls:SW_RSCN received on VEPort=<VEPortNumber> Domain=0x<Host/Device Side Domain> Port=0x<Host/Device Side Port>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates an attached port with the established FICON emulated path has logged out from the switch.

Recommended Action This may be an unexpected event; contact your vendor's customer support for assistance.

FICN-2085

Message `FICON or FCP Emulation Enabled FCIP Tunnel is Up on VEPort=<VEPortNumber>.`

Message Type LOG

Severity INFO

Probable Cause Indicates a FICON or Fibre Channel Protocol (FCP) emulation-enabled FCIP tunnel has been established successfully to the peer switch.

Recommended Action No action is required.

FICN-2086

Message `FICON or FCP Emulation Enabled FCIP Tunnel is Down on VEport=<VEPortNumber>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a FICON or Fibre Channel Protocol (FCP) emulation-enabled FCIP tunnel to the peer switch has been terminated.

Recommended Action This is an unexpected event; contact your vendor's customer support for assistance.

FICN-2087

Message `FICON connected 3900 printer discovered Path=0x<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>-invalid compression mode.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that FICON Printer emulation is enabled, but cannot be performed for this device because the compression mode on the tunnel is not set to None or Aggressive.

Recommended Action If you desire FICON Printer emulation for this device, modify the tunnel compression mode to None (mode 0) or Aggressive (mode 3).

FICU Messages

FICU-1001

Message `<error message>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that one of the configuration management functions have failed. The *key* variable is a component of the Fabric OS configuration database and is for support use only. The *error* variable is an internal error number.

Recommended Action Execute the **haFailover** command on the switch if it has redundant control processors (CPs) or reboot the switch. Execute the **switchStatusShow** command to check if the flash memory is full. If the flash memory is full, execute the **supportSave** command to clear the core files.

FICU-1002

Message
```
<function name>: Failed to get RNID from Management Server Domain=<domain>
rc=<error>.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates that the fibre connectivity control unit port (FICON-CUP) daemon failed to get the switch request node ID (RNID) from the management server because of a Fabric OS problem. The *domain* variable displays the domain ID of the target switch for this RNID. The *error* variable is an internal error number.

Recommended Action If this is a bladed switch, execute the **haFailover** command. If the problem persists, or if this is a non-bladed switch, download a new firmware version using the **firmwareDownload** command.

FICU-1003

Message `<function name>: <message> FICON-CUP License Not Installed: (<error>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the fibre connectivity control unit port (FICON-CUP) license is not installed on the switch.

Recommended Action Execute the **licenseShow** command to check the installed licenses on the switch. The switch cannot be managed using FICON-CUP commands until the FICON-CUP license is installed. Contact your switch supplier for a FICON-CUP license. Execute the **licenseAdd** command to add the license to your switch.

FICU-1004

Message `<function name>: Failed to set FICON Management Server (FMS) mode: conflicting PID Format:<pid_format>, FMS Mode:<mode>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a process ID (PID) format conflict was encountered. The core PID format is required for fibre connectivity control unit port (FICON-CUP).

The *pid_format* variable displays the PID format currently running on the fabric, and is one of the following:

- 0 - VC-encoded PID format
- 1 - Core PID format
- 2 - Extended-edge PID format

The *mode* variable displays whether FICON Management Server (FMS) mode is enabled, and is one of the following: 0 means FMS mode is enabled and 1 means FMS mode is disabled.

Recommended Action To enable FMS mode, the core PID format must be used in the fabric. Change the PID format to core PID using the **configure** command and re-enable FMS Mode using the **ficonCupSet** command. Refer to the *Fabric OS Administrator's Guide* for information on core PID mode.

FICU-1005

Message `Failed to initialize <module>, rc = <error>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that initialization of a module within the fibre connectivity control unit port (FICON-CUP) daemon failed.

Recommended Action Download a new firmware version using the **firmwareDownload** command.

FICU-1006

Message `Control Device Allegiance Reset: (Logical Path: 0x<PID>:0x<channel image ID>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the path with the specified process ID (PID) and channel image ID lost allegiance to a fibre connectivity control unit port (FICON-CUP) device.

Recommended Action Check if the FICON channel corresponding to the PID in the message is functioning correctly.

FICU-1007

Message `<function name>: Failed to allocate memory while performing <message>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that memory resources are low. This may be a transient problem.

Recommended Action Check the memory usage on the switch using the **memShow** command.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

FICU-1008

Message `FMS mode has been enabled. Port(s):<port number(s)> have been disabled due to port address conflict.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified ports were disabled when the FICON Management Server (FMS) mode was enabled. This is due to a port address conflict or the port address being reserved for the CUP management port.

Recommended Action No action is required.

FICU-1009

Message `FMS Mode enable failed due to insufficient frame filtering resources on some ports.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the frame filtering resources required to enable FICON Management Server mode (fmsMode) were not available on some of the ports.

Recommended Action Execute the **haFailover** command on the switch if it has redundant control processors (CPs) or reboot the switch.

FICU-1010

Message `FMS mode enable failed due to port(s) with areas 0xFE or 0xFF is(are) connected to device(s).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the FICON Management Server (FMS) mode was not enabled because ports with areas 0xFE or 0xFF are connected to devices.

Recommended Action Disable ports with areas 0xFE or 0xFF using the **portDisable** command.

FICU-1011

Message `FMS mode has been enabled.`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates that the FICON Management Server mode (fmsMode) has been enabled.

Recommended Action No action is required.

FICU-1012

Message `FMS mode has been disabled.`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates that the FICON Management Server mode (fmsMode) has been disabled.

Recommended Action No action is required.

FICU-1013

Message `Host data file cannot be reset to proper size.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the file system is too full to create the host data file at the proper size.

Recommended Action Execute the **switchStatusShow** command to check if the flash memory is full. If the flash memory is full, execute the **supportSave** command to clear the core files.

FICU-1017

Message `FMSMODE enable failed because reserved area is bound to a device.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that one or both of the reserved areas 0xFE and 0xFF is bound to a device.

Recommended Action Execute the **wwnaddress --show** command to display all devices currently bound to areas. Execute the **wwnaddress --unbind** command to release the reserved area from the device.

FICU-1018

Message `FMSMODE enable noticed swapped ports.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that some ports are swapped at the time FICON Management Server mode (fmsMode) is enabled.

Recommended Action Verify the expected FICON port address and port number relationship. For more information, refer to the "FICON and FICON CUP in Virtual Fabrics" section of the *FICON Administrator's Guide*.

FICU-1019

Message `Switch has been set offline by LP(<LP ID>).`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates that the FICON Management Server (FMS) has disabled the switch.

Recommended Action No action is required.

FICU-1020

Message `Port Addrs (<port mask>) have been Blocked by <source>.`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates that the FICON Management Server (FMS) has blocked ports.

Recommended Action No action is required.

FICU-1021

Message `Port Addrs (<port mask>) have been Unblocked by <source>.`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates the FICON Management Server (FMS) has unblocked ports.

Recommended Action No action is required.

FICU-1022

Message `Detected FC8-48 and/or FC8-64 that are not manageable when FMS mode is enabled.`

Message Type LOG

Severity INFO

Probable Cause Indicates the presence of unmanageable ports such as 48-port blade ports in the virtual fabric-disabled chassis.

Recommended Action No action is required. For more information on the FICON CUP restrictions, refer to the *FICON Administrator's Guide*.

FICU-1023

Message `Detected 48 port blade when FMS mode is enabled.`

Message Type LOG

Severity INFO

Probable Cause Indicates presence of 48-port blade ports in the switch.

Recommended Action No action is required. For more information on the FICON CUP restrictions, refer to the *FICON Administrator's Guide*.

FICU-1024

Message `Detected 64 port blade when FMS mode is enabled.`

Message Type LOG

Severity INFO

Probable Cause Indicates presence of 64-port blade ports in the switch.

Recommended Action No action is required. For more information on the FICON CUP restrictions, refer to the *FICON Administrator's Guide*.

FKLB Messages

FKLB-1001

Message `exchange <xid> overlapped, pid=<pid>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the FC kernel driver has timed out the exchange while the application is still active. When the FC kernel driver reuses the exchange, the application will overlap. This happens on a timed-out exchange; it automatically recovers after the application times out the exchange.

Recommended Action No action is required.

FLOD Messages

FLOD-1001

Message `Unknown LSR type: port <port number>, type <LSR header type>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the link state record (LSR) type is unknown. The following two LSR header types are the only known types:

- 1 - Unicast
- 3 - Multicast

Recommended Action No action is required; the record is discarded.

FLOD-1003

Message `Link count exceeded in received LSR, value = <link count number>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the acceptable link count received was exceeded in the link state record (LSR).

Recommended Action No action is required; the record is discarded.

FLOD-1004

Message `Excessive LSU length = <LSU length>.`

Message Type LOG | FFDC

Severity ERROR

Probable Cause Indicates that the link state update (LSU) size exceeds the value the system can support.

Recommended Action Reduce the number of switches in the fabric or reduce the number of redundant inter-switch links (ISLs) between two switches.

FLOD-1005

Message `Invalid received domain ID: <domain number>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the received link state record (LSR) contained an invalid domain number.

Recommended Action No action is required; the LSR is discarded.

FLOD-1006

Message `Transmitting invalid domain ID: <domain number>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the transmitted link state record (LSR) contained an invalid domain number.

Recommended Action No action is required; the LSR is discarded.

FSPF Messages

FSPF-1001

Message `Input Port <port number> out of range.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified input port number is out of range because it does not exist on the switch.

Recommended Action No action is required. This is a temporary kernel error that does not affect your system. If the problem persists, execute the **supportSave** command and contact your service provider.

FSPF-1002

Message `Wrong neighbor ID (<domain ID>) in Hello message from port <port number>, expected ID = <domain ID>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the switch has received a wrong domain ID from its neighbor switch in the HELLO message from a specified port. This may happen when a domain ID for a switch has been changed.

Recommended Action No action is required.

FSPF-1003

Message `Remote Domain ID <domain number> out of range, input port = <port number>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified remote domain ID is out of range.

Recommended Action No action is required. The frame is discarded.

FSPF-1005

Message `Wrong Section Id <section number>, should be <section number>, input port = <port number>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that an incorrect section ID was reported from the specified input port. The section ID is part of the fabric shortest path first (FSPF) protocol and is used to identify a set of switches that share an identical topology database.

Recommended Action This switch does not support a non-zero section ID. Any connected switch from another manufacturer with a section ID other than 0 is incompatible in a fabric of Brocade switches. Disconnect the incompatible switch.

FSPF-1006

Message `FSPF Version <FSFP version> not supported, input port = <port number>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the fabric shortest path first (FSPF) version is not supported on the specified input port.

Recommended Action Update the FSPF version by running the **firmwareDownload** command. All current versions of the Fabric OS support FSPF version 2.

FSPF-1007

Message `ICL triangular topology is broken between the neighboring domains: <domain number> and <domain number>. Please fix it ASAP.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the inter-chassis link (ICL) triangular topology is broken and becomes linear. It may cause frame drop or performance slowdown.

Recommended Action Connect the two domains using ICL or regular inter-switch link (ISL) to form a triangular topology.

FSPF-1008

Message `ICL triangular topology is formed among the domains: <domain number> (self), <domain number>, and <domain number>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the inter-chassis link (ICL) triangular topology is formed.

Recommended Action No action is required.

FSPF-1009

Message `16G ICL topology is not recommended on local domain <domain number>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the current 16 Gbps inter-chassis link (ICL) topology is not recommended.

Recommended Action Use the **switchShow**, **islShow**, and **lsdbShow** commands to identify the neighbor domains that violate the ICL connectivity requirement.

FSPF-1010

Message `ICL Topology is valid on local domain <domain number>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the current inter-chassis link (ICL) topology is valid for routing from the local switch.

Recommended Action No action is required.

FSPF-1011

Message `16G ICL topology is unbalanced.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the current configuration of inter-chassis link (ICL) paths are unbalanced.

Recommended Action Investigate current ICL configuration to ensure that all recommendations for cabling are satisfied.

FSPF-1012

Message `All existing ICL topology imbalances have been corrected.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the existing inter-chassis link (ICL) configuration that was resulting in an unbalanced topology has been corrected.

Recommended Action No action is required.

FSPF-1013

Message `Exceeded maximum number of supported paths (16) to one or more remote domains.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that there are more than 16 (maximum number of paths supported) available shortest cost paths to reach one or more remote domains. Traffic may be impacted or follow unexpected traffic patterns.

Recommended Action Use the **fabricShow -paths**, **topologyShow**, and **lsDbShow** commands to get additional details about which remote domains are violating the maximum paths limit. Refer to the *Fabric OS Administrator's Guide* for information on the causes and potential impacts.

FSPF-1014

Message `All previously reported maximum path violations have been corrected.`

Message Type LOG

Severity INFO

Probable Cause Indicates that all existing violations of the maximum paths limit have been corrected.

Recommended Action No action is required.

FSS Messages

FSS-1001

Message `Component (<component name>) dropping HA data update (<update ID>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that an application has dropped a high availability (HA) data update.

Recommended Action For a dual control processor (CP) system, enable the HA state synchronization using the **haSyncStart** command. For non-bladed systems, restart the switch using the **reboot** command.

If the problem persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

FSS-1002

Message `Component (<component name>) sending too many concurrent HA data update transactions (<dropped update transaction ID>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that an application has sent too many concurrent high availability (HA) data updates.

Recommended Action For a dual CP system, enable the HA state synchronization using the **haSyncStart** command. For non-bladed systems, restart the switch using the **reboot** command.

If the problem persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

FSS-1003

Message `Component (<component name>) misused the update transaction (<transaction ID>) without marking the transaction begining.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Fabric OS state synchronization (FSS) service has dropped the update because an application did not set the transaction flag correctly.

Recommended Action For a dual CP system, enable the high availability (HA) state synchronization using the **haSyncStart** command. For non-bladed systems, restart the switch using the **reboot** command.

If the problem persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

FSS-1004

Message `Memory shortage.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the system ran out of memory.

Recommended Action Execute the **memShow** command to view memory usage in the switch.

For a dual CP system, enable the high availability (HA) state synchronization using the **haSyncStart** command. For non-bladed systems, restart the switch using the **reboot** command.

If the problem persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

FSS-1005

Message `FSS read failure.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the read system call to the Fabric OS state synchronization (FSS) device has failed.

Recommended Action If the problem persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

FSS-1006

Message `No FSS message available.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that data is not available on the Fabric OS state synchronization (FSS) device.

Recommended Action If the problem persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

FSS-1007

Message `<component name>: Faulty Ethernet connection.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that the Ethernet connection between the active control processor (CP) and the standby CP is not healthy. This error occurs when the standby CP does not respond to a request from the active CP within five seconds. This usually indicates a problem with the internal Ethernet connection and the disruption of the synchronization process.

Recommended Action Execute the **supportShow** or **supportSave** command to validate the network configuration and then execute the **haSyncStart** command to restore the high availability (HA) synchronization. If the problem persists, contact your switch service provider.

FSS-1008

Message `FSS Error: <Error Message>.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that a Fabric OS state synchronization (FSS) error has occurred.

Recommended Action Execute the **supportSave** command and contact your switch service provider.

FSS-1009

Message `FSS Error: <Error Message>.`

Message Type LOG | FFDC

Severity ERROR

Probable Cause Indicates that a Fabric OS state synchronization (FSS) error has occurred for the specified component. The error code is displayed in the message.

Recommended Action Execute the **supportSave** command and contact your switch service provider.

FSS-1010

Message `FSS Warning: <Warning Message>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a Fabric OS state synchronization (FSS) error may have occurred.

Recommended Action Execute the **supportSave** command and contact your switch service provider.

FSS-1011

Message `FSS Info: <Info Message>.`

Message Type LOG

Severity INFO

Probable Cause Indicates a Fabric OS state synchronization (FSS) related informational message.

Recommended Action No action is required.

FSSM Messages

FSSM-1002

Message `HA State is in sync.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the high availability (HA) state of the active control processor (CP) is in synchronization with the HA state of the standby CP. If the standby CP is healthy, the failover will be nondisruptive.

Recommended Action No action is required.

FSSM-1003

Message `HA State out of sync.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the high availability (HA) state of the active control processor (CP) is out of synchronization with the HA state of the standby CP. If the active CP failover occurs when the HA state is out of synchronization, the failover is disruptive.

Recommended Action If this message was logged as a result of a user-initiated action (such as running the **reboot** command), no action is required.

Otherwise, execute the **haSyncStart** command on the active CP to resynchronize the HA state.

If the HA state does not synchronize, execute the **haDump** command to diagnose the problem.

If the problem persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

FSSM-1004

Message `Incompatible software version in HA synchronization.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that the active control processor (CP) and the standby CP in a dual CP system are running firmware that is incompatible with each other. If the active CP fails, the failover will be disruptive.

In a switch system, this message is logged when a firmware upgrade or downgrade was invoked. The new firmware version is not compatible with the current running version. This causes a disruptive firmware upgrade or downgrade.

Recommended Action For a dual CP system, execute the **firmwareDownload** command to load compatible firmware on the standby CP.

FV Messages

FV-1001

Message `Flow Vision daemon initialized.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Flow Vision daemon has successfully initilized.

Recommended Action No action is required.

FV-1002

Message `Flow Vision Config Replay Completed Successfully.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Flow Vision config replay has successfully completed.

Recommended Action No action is required.

FV-3000

Message `Flow <flow_name> is created with features <feature_list>.`

Message Type AUDIT

Class CFG

Severity INFO

Probable Cause Indicates that the specified flow has been created.

Recommended Action No action is required.

FV-3001

Message `Flow <flow_name> is deleted.`

Message Type AUDIT

Class CFG

Severity INFO

Probable Cause Indicates that the specified flow has been deleted.

Recommended Action No action is required.

FV-3002

Message `Flow <flow_name> is activated for the feature(s) <feature_list>.`

Message Type AUDIT

Class CFG

Severity INFO

Probable Cause Indicates that the specified flow has been activated.

Recommended Action No action is required.

FV-3003

Message `Flow <flow_name> is deactivated for the feature(s) <feature_list>.`

Message Type AUDIT

Class CFG

Severity INFO

Probable Cause Indicates that the specified flow has been deactivated.

Recommended Action No action is required.

FV-3004

Message `Configuration of Flow <flow_name> is changed for the feature(s) <feature_list>.`

Message Type AUDIT

Class CFG

Severity INFO

Probable Cause Indicates that configuration of the specified flow has been changed.

Recommended Action No action is required.

FV-3005

Message `Flow <flow_name> is reset for the feature(s) <feature_list>.`

Message Type AUDIT

Class CFG

Severity INFO

Probable Cause Indicates that the specified flow is being reset.

Recommended Action No action is required.

FV-3006

Message `Port(s) <port_number_or_range> is(are) being configured as SIM Port. Some of the ports may not be eligible to become SIM Port.`

Message Type AUDIT

Class CFG

Severity INFO

Probable Cause Indicates that the specified ports are configured as SIM ports.

Recommended Action No action is required.

FV-3007

Message `Port(s) <port_number_or_range> being deconfigured as SIM Port. Some of the ports may be already deconfigured as SIM Port.`

Message Type AUDIT

Class CFG

Severity INFO

Probable Cause Indicates that the specified ports are deconfigured as SIM ports.

Recommended Action No action is required.

FV-3008

Message `All ports are being configured as SIM Port. Some of the ports may not be eligible to become SIM Port.`

Message Type AUDIT

Class CFG

Severity INFO

Probable Cause Indicates that all ports are configured as SIM ports.

Recommended Action No action is required.

FV-3009

Message `All ports being deconfigured as SIM Port. Some of the ports may be already deconfigured as SIM Port.`

Message Type AUDIT

Class CFG

Severity INFO

Probable Cause Indicates that all ports are deconfigured as SIM ports.

Recommended Action No action is required.

FV-3010

Message `Control configuration for flows has been changed.`

Message Type AUDIT

Class CFG

Severity INFO

Probable Cause Indicates that control configuration has been changed.

Recommended Action No action is required.

FV-3011

Message `Control configuration has been changed for all applicable flows.`

Message Type AUDIT

Class CFG

Severity INFO

Probable Cause Indicates that control configuration has been changed for all applicable flows.

Recommended Action No action is required.

FV-3012

Message `All flows are deactivated for the feature(s) <feature_list>.`

Message Type AUDIT

Class CFG

Severity INFO

Probable Cause Indicates that all flows are deactivated.

Recommended Action No action is required.

FV-3013

Message `All user created flows are deleted.`

Message Type AUDIT

Class CFG

Severity INFO

Probable Cause Indicates that all user created flows are deleted.

Recommended Action No action is required.

FV-3014

Message `All flows are reset for the feature(s) <feature_list>.`

Message Type AUDIT

Class CFG

Severity INFO

Probable Cause Indicates that all user created flows are deleted.

Recommended Action No action is required.

FW Messages

FW-1001

Message
```
<label>, value has changed(High=<High value>, Low=<Low value>). Current value is
<Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the internal temperature of the switch has changed.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. To prevent recurring messages, disable the changed alarm for this threshold. If you receive a temperature-related message, check for an accompanying fan-related message and check fan performance. If all fans are functioning normally, check the climate control in your lab.

FW-1002

Message
```
<Label>, is below low boundary (High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that the internal temperature of the switch has fallen below the low boundary.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Typically, low temperatures mean that the fans and airflow of a switch are functioning normally.

Verify that the location temperature is within the operational range of the switch. Refer to the hardware reference manual for the environmental temperature range of your switch.

FW-1003

Message
```
<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that the internal temperature of the switch has risen above the high boundary to a value that might damage the switch.

Recommended Action This message generally appears when a fan fails. If so, a fan-failure message accompanies this message. Replace the fan.

FW-1004

Message `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the internal temperature of the switch has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. If you receive a temperature-related message, check for an accompanying fan-related message and check fan performance. If all fans are functioning normally, check the climate control in your lab.

FW-1005

Message `<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the speed of the fan has changed. Fan problems typically contribute to temperature problems.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Consistently abnormal fan speeds generally indicate that the fan is malfunctioning.

FW-1006

Message `<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the speed of the fan has fallen below the low boundary. Fan problems typically contribute to temperature problems.

Recommended Action Consistently abnormal fan speeds generally indicate that the fan is failing. Replace the fan field-replaceable unit (FRU).

FW-1007

Message `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the speed of the fan has risen above the high boundary. Fan problems typically contribute to temperature problems.

Recommended Action Consistently abnormal fan speeds generally indicate that the fan is failing. Replace the fan field-replaceable unit (FRU).

FW-1008

Message `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the speed of the fan has changed from a value outside of the acceptable range to a value within the acceptable range. Fan problems typically contribute to temperature problems.

Recommended Action No action is required. Consistently abnormal fan speeds generally indicate that the fan is failing. If this message occurs repeatedly, replace the fan field-replaceable unit (FRU).

FW-1009

Message `<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the state of the power supply has changed from faulty to functional or from functional to faulty.

Recommended Action If the power supply is functioning correctly, no action is required.

If the power supply is functioning below the acceptable boundary, verify that it is seated correctly in the chassis. Run the **psShow** command to view the status of the power supply. If the power supply continues to be a problem, replace the faulty power supply.

FW-1010

Message `<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the power supply is faulty. The power supply is not producing enough power.

Recommended Action Verify that you have installed the power supply correctly and that it is correctly seated in the chassis. If the problem persists, replace the faulty power supply.

FW-1011

Message `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the power supply is functioning properly.

Recommended Action Set the high boundary above the normal operation range.

FW-1012

Message `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the power supply counter changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1033

Message `<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the temperature of the small form-factor pluggable (SFP) has changed. Frequent fluctuations in SFP temperature may indicate a deteriorating SFP.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1034

Message `<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the temperature of the small form-factor pluggable (SFP) has fallen below the low boundary.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1035

Message `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the temperature of the small form-factor pluggable (SFP) has risen above the high boundary. Frequent fluctuations in temperature may indicate a deteriorating SFP.

Recommended Action Replace the SFP.

FW-1036

Message

```
<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the temperature of the small form-factor pluggable (SFP) has changed from a value outside of the acceptable range to a value within the acceptable range. Frequent fluctuations in temperature may indicate a deteriorating SFP.

Recommended Action

No action is required.

FW-1037

Message

```
<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is
<Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the receive power value of the small form-factor pluggable (SFP) has changed. The receive performance area measures the amount of incoming laser to help you determine whether the SFP is in good working condition. If the counter often exceeds the threshold, the SFP is deteriorating.

Recommended Action

Incoming laser fluctuations usually indicate a deteriorating SFP. If the message persists, replace the SFP.

FW-1038

Message

```
<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the receive power value of the small form-factor pluggable (SFP) has fallen below the low boundary. The receive performance area measures the amount of incoming laser to help you determine whether the SFP is in good working condition. If the counter often exceeds the threshold, the SFP is deteriorating.

Recommended Action

Verify that your optical components are clean and function properly. Replace deteriorating cables or SFPs. Check for damage from heat or age.

FW-1039

Message `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the receive power value of the small form-factor pluggable (SFP) has risen above the high boundary. The receive performance area measures the amount of incoming laser to help you determine whether the SFP is in good working condition. If the counter often exceeds the threshold, the SFP is deteriorating.

Recommended Action Replace the SFP before it deteriorates.

FW-1040

Message `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the receive power value of the small form-factor pluggable (SFP) has changed from a value outside of the acceptable range to a value within the acceptable range. The receive performance area measures the amount of incoming laser to help you determine whether the SFP is in good working condition. If the counter often exceeds the threshold, the SFP is deteriorating.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1041

Message `<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the transmit power value of the small form-factor pluggable (SFP) has changed. The transmit performance area measures the amount of outgoing laser to help you determine whether the SFP is in good working condition. If the counter often exceeds the threshold, the SFP is deteriorating.

Recommended Action Transmitting laser fluctuations usually indicates a deteriorating SFP. If the message persists, replace the SFP.

FW-1042

Message

```
<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the transmit power value of the small form-factor pluggable (SFP) has fallen below the low boundary. The transmit performance area measures the amount of outgoing laser to help you determine whether the SFP is in good working condition. If the counter often exceeds the threshold, the SFP is deteriorating.

Recommended Action

Verify that your optical components are clean and function properly. Replace deteriorating cables or SFPs. Check for damage from heat or age.

FW-1043

Message

```
<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the transmit power value of the small form-factor pluggable (SFP) has risen above the high boundary. The transmit performance area measures the amount of outgoing laser to help you determine whether the SFP is in good working condition. If the counter often exceeds the threshold, the SFP is deteriorating.

Recommended Action

Replace the SFP.

FW-1044

Message

```
<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the transmit power value of the small form-factor pluggable (SFP) has changed from a value outside of the acceptable range to a value within the acceptable range. The transmit performance area measures the amount of outgoing laser to help you determine whether the SFP is in good working condition. If the counter often exceeds the threshold, the SFP is deteriorating.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1045

Message `<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the value of the small form-factor pluggable (SFP) voltage has changed. If the supplied voltage of the SFP transceiver is outside of the normal range, this may indicate a hardware failure.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. If the message persists, replace the SFP.

FW-1046

Message `<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the value of the small form-factor pluggable (SFP) voltage has fallen below the low boundary.

Recommended Action Verify that your optical components are clean and function properly. Replace deteriorating cables or SFPs. Check for damage from heat or age.

FW-1047

Message `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the value of the small form-factor pluggable (SFP) voltage has risen above the high boundary.

Recommended Action The supplied current of the SFP transceiver is outside of the normal range, indicating possible hardware failure. If the current rises above the high boundary, you must replace the SFP.

FW-1048

Message `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the value of the small form-factor pluggable (SFP) voltage has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1049

Message `<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the value of the small form-factor pluggable (SFP) voltage has changed. Frequent voltage fluctuations indicate that the SFP is deteriorating.

Recommended Action Replace the SFP.

FW-1050

Message `<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the value of the small form-factor pluggable (SFP) voltage has fallen below the low boundary.

Recommended Action Configure the low threshold to 1 so that the threshold triggers an alarm when the value falls to 0 (Out_of_Range). If continuous or repeated alarms occur, replace the SFP before it deteriorates.

FW-1051

Message `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the value of the small form-factor pluggable (SFP) voltage has risen above the high boundary. High voltages indicate possible hardware failures.

Recommended Action Frequent voltage fluctuations indicate that the SFP is deteriorating. Replace the SFP.

FW-1052

Message `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the value of the small form-factor pluggable (SFP) voltage has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1053

Message `<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the value of the small form-factor pluggable (SFP) Power on Hours has fallen below the low boundary.

Recommended Action Configure the low threshold to 1 so that the threshold triggers an alarm when the value falls to 0 (Out_of_Range). If continuous or repeated alarms occur, replace the SFP before it deteriorates.

FW-1054

Message `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the value of the small form-factor pluggable (SFP) Power on Hours has risen above the high boundary. The high value indicates the maximum lifetime use of the SFP.

Recommended Action Replace the SFP.

FW-1113

Message `<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of times E_Ports have gone down has changed. E_Ports go down each time you remove a cable or small form-factor pluggable (SFP). SFP failures also cause E_Ports to go down. Down E_Port may be caused by transient errors.

Recommended Action Check both ends of the physical connection and verify that the SFPs and cables are functioning properly.

FW-1114

Message `<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of times E_Ports have gone down has fallen below the low boundary. E_Ports go down each time you remove a cable or small form-factor pluggable (SFP). SFP failures also cause E_Ports to go down. Down E_Port may be caused by transient errors.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of E_Port failures means that the switch is functioning normally.

FW-1115

Message `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of times E_Ports have gone down has risen above the high boundary. E_Ports go down each time you remove a cable or small form-factor pluggable (SFP). SFP failures also cause E_Ports to go down. Down E_Port may be caused by transient errors.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Check both ends of the physical connection and verify that the SFP functions properly.

FW-1116

Message `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of times E_Ports have gone down has changed from a value outside of the acceptable range to a value within the acceptable range. E_Ports go down each time you remove a cable or small form-factor pluggable (SFP). SFP failures also cause E_Ports to go down. Down E_Port may be caused by transient errors.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1117

Message `<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of fabric reconfigurations has changed. The following occurrences can cause a fabric reconfiguration:

- Two switches with the same domain ID have connected to one another.
- Two fabrics have joined.
- An E_Port has gone offline.
- A principal link has segmented from the fabric.

Recommended Action Verify that the cable is properly connected at both ends. Verify that the small form-factor pluggables (SFPs) have not become faulty. An inexplicable fabric reconfiguration might be a transient error and might not require troubleshooting.

FW-1118

Message

```
<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of fabric reconfigurations has fallen below the low boundary. The following occurrences can cause a fabric reconfiguration:

- Two switches with the same domain ID have connected to one another.
- Two fabrics have joined.
- An E_Port has gone offline.
- A principal link has segmented from the fabric.

A low number of fabric reconfigurations means that the fabric is functioning normally.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1119

Message

```
<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of fabric reconfigurations has risen above the high boundary. The following occurrences can cause a fabric reconfiguration:

- Two switches with the same domain ID have connected to one another.
- Two fabrics have joined.
- An E_Port has gone offline.
- A principal link has segmented from the fabric.

Recommended Action Verify that all inter-switch link (ISL) cables are properly connected at both ends. Verify that the small form-factor pluggable (SFP) has not become faulty. An inexplicable fabric reconfiguration might be a transient error and might not require troubleshooting.

FW-1120

Message

```
<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of fabric reconfigurations has changed from a value outside of the acceptable range to a value within the acceptable range. The following occurrences can cause a fabric reconfiguration:

- Two switches with the same domain ID have connected to one another.
- Two fabrics have joined.
- An E_Port has gone offline.
- A principal link has segmented from the fabric.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1121

Message

```
<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is
<Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of domain ID changes has changed. Domain ID changes occur when there is a conflict of domain IDs in a single fabric and the principal switch must assign another domain ID to the switch.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1122

Message

```
<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of domain ID changes has fallen below the low boundary. Domain ID changes occur when there is a conflict of domain IDs in a single fabric and the principal switch has to assign another domain ID to the switch. A low number of domain ID changes means that the fabric is functioning normally.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1123

Message

```
<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of domain ID changes has risen above the high boundary. Domain ID changes occur when there is a conflict of domain IDs in a single fabric and the principal switch has to assign another domain ID to the switch.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1124

Message

```
<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of domain ID changes has changed from a value outside of the acceptable range to a value within the acceptable range. Domain ID changes occur when there is a conflict of domain IDs in a single fabric and the principal switch has to assign another domain ID to the switch.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1125

Message

```
<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is
<Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of segmentations has changed. Segmentation changes might occur due to the following reasons:

- Zone conflicts.
- Domain conflicts.
- Segmentation of the principal link between two switches.

- Incompatible link parameters. During E_Port initialization, ports exchange link parameters. Rarely, incompatible parameters result in segmentation.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1126

Message

```
<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of segmentations has fallen below the low boundary. Segmentation changes might occur due to the following reasons:

- Zone conflicts.
- Domain conflicts.
- Segmentation of the principal link between two switches.
- Incompatible link parameters. During E_Port initialization, ports exchange link parameters. Rarely, incompatible parameters result in segmentation.

A low number of segmentation errors means that the fabric is functioning normally.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1127

Message

```
<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of segmentations has risen above the high boundary. Segmentation changes might occur due to the following reasons:

- Zone conflicts.
- Domain conflicts.
- Segmentation of the principal link between two switches.
- Incompatible link parameters. During E_Port initialization, ports exchange link parameters. Rarely, incompatible parameters result in segmentation.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1128

Message

```
<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of segmentations has changed from a value outside of the acceptable range to a value within the acceptable range. Segmentation changes might occur due to the following reasons:

- Zone conflicts.
- Domain conflicts.
- Segmentation of the principal link between two switches.
- Incompatible link parameters. During E_Port initialization, ports exchange link parameters. Rarely, incompatible parameters result in segmentation.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1129

Message

```
<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is
<Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of zone changes has changed. Zone changes occur when there is a change to the effective zone configuration.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1130

Message

```
<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of zone changes has fallen below the low boundary. Zone changes occur when there is a change to the effective zone configuration. A low number of zone configuration changes means that the fabric is functioning normally.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1131

Message

```
<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of zone changes has risen above the high boundary. Zone changes occur when there is a change to the effective zone configuration.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1132

Message

```
<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of zone changes has changed from a value outside of the acceptable range to a value within the acceptable range. Zone changes occur when there is a change to the effective zone configuration.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1133

Message

```
<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is
<Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of fabric logins has changed. Fabric logins occur when a port or device initializes with the fabric. The event is called fabric login (FLOGI).

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1134

Message

```
<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of fabric logins has fallen below the low boundary. Fabric logins occur when a port or device initializes with the fabric. The event is called fabric login (FLOGI). A low number of fabric logins means that the fabric is functioning normally.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1135

Message

```
<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of fabric logins has risen above the high boundary. Fabric logins occur when a port or device initializes with the fabric. The event is called fabric login (FLOGI).

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1136

Message

```
<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of fabric logins has changed from a value outside of the acceptable range to a value within the acceptable range. Fabric logins occur when a port or device initializes with the fabric. The event is called fabric login (FLOGI).

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1137

Message `<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of small form-factor pluggable (SFP) state changes has changed. SFP state changes occur when the SFP is inserted or removed.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1138

Message `<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of small form-factor pluggable (SFP) state changes has fallen below the low boundary. SFP state changes occur when the SFP is inserted or removed. A low number of SFP state changes means that the switch is functioning normally.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1139

Message `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of small form-factor pluggable (SFP) state changes has risen above the high boundary. SFP state changes occur when the SFP is inserted or removed.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1140

Message

```
<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of small form-factor pluggable (SFP) state changes has changed from a value outside of the acceptable range to a value within the acceptable range. SFP state changes occur when the SFP is inserted or removed.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1160

Message

```
<Port Name> <Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of link failures that the port experiences has changed. Link loss errors occur when a link experiences a loss of signal and fails. Both physical and hardware problems can cause link loss errors. Link loss errors frequently occur due to a loss of synchronization.

Recommended Action

Check both ends of your cable connection. Verify that the cable and small form-factor pluggables (SFPs) are not faulty.

Losses of synchronization commonly causes link failures. If you receive concurrent loss of synchronization errors, troubleshoot the loss of synchronization.

FW-1161

Message

```
<Port Name> <Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of link failures that the port experiences has fallen below the low boundary. Link loss errors occur when a link experiences a loss of signal and fails. Both physical and hardware problems can cause link loss errors. Link loss errors frequently occur due to a loss of synchronization. Check for concurrent loss of synchronization errors and, if applicable, troubleshoot them. A low number of link loss errors means that the switch is functioning normally.

Recommended Action

Check for concurrent loss of synchronization errors and, if applicable, troubleshoot them. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1162

Message

```
<Port Name> <Label>, is above high boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the number of link failures that the port experiences has risen above the high boundary. Link loss errors occur when a link experiences a loss of signal and fails. Both physical and hardware problems can cause link loss errors. Link loss errors frequently occur due to a loss of synchronization.

Recommended Action

Check both ends of your cable connection. Verify that the cable and small form-factor pluggables (SFPs) are not faulty.

Losses of synchronization commonly cause link failures. If you receive concurrent loss of synchronization errors, troubleshoot the loss of synchronization.

FW-1163

Message

```
<Port Name> <Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of link failures that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range. Link loss errors occur when a link experiences a loss of signal and fails. Both physical and hardware problems can cause link loss errors. Link loss errors frequently occur due to a loss of synchronization. Check for concurrent loss of synchronization errors and, if applicable, troubleshoot them.

Recommended Action

Check for concurrent loss of synchronization errors and, if applicable, troubleshoot them. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1164

Message

```
<Port Name> <Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of synchronization losses that the port experiences has changed. Loss of synchronization errors frequently occur due to a faulty small form-factor pluggable (SFP) or cable. Signal losses often create synchronization losses.

Recommended Action Check both ends of your cable connection. Verify that the cable and SFPs are not faulty.

If you continue to experience synchronization loss errors, troubleshoot your host bus adapter (HBA) and contact your switch service provider.

FW-1165

Message

```
<Port Name> <Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of synchronization losses that the port experiences has fallen below the low boundary. Loss of synchronization errors frequently occur due to a faulty small form-factor pluggable (SFP) or cable. Signal losses often create synchronization losses. A low number of synchronization losses means that the switch is functioning normally.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1166

Message

```
<Port Name> <Label>, is above high boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that the number of synchronization losses that the port experiences has risen above the high boundary. Loss of synchronization errors frequently occur due to a faulty small form-factor pluggable (SFP) or cable. Signal losses often create synchronization losses.

Recommended Action Check both ends of your cable connection. Verify that the cable and SFPs are not faulty.

If you continue to experience loss of synchronization errors, troubleshoot your host bus adapter (HBA) and contact your switch service provider.

FW-1167

Message

```
<Port Name> <Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of synchronization losses that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range. Loss of synchronization errors frequently occur due to a faulty small form-factor pluggable (SFP) or cable. Signal losses often create synchronization losses.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1168

Message

```
<Port Name> <Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of signal losses that the port experiences has changed. Loss of signal generally indicates a physical problem.

Recommended Action

Check both ends of your cable connection. Verify that the cable and small form-factor pluggables (SFPs) are not faulty.

FW-1169

Message

```
<Port Name> <Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of signal losses that the port experiences has fallen below the low boundary. Loss of signal generally indicates a physical problem. A low number of signal loss errors means that the switch is functioning normally.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1170

Message

```
<Port Name> <Label>, is above high boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the number of signal losses that the port experiences has risen above the high boundary. Loss of signal generally indicates a physical problem.

Recommended Action

Check both ends of your cable connection. Verify that the cable is not faulty.

FW-1171

Message

```
<Port Name> <Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of signal losses that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range. Frequent loss of signal generally indicates a physical problem.

Recommended Action

Check both ends of your cable connection. Verify that the cable and small form-factor pluggables (SFPs) are not faulty.

FW-1172

Message

```
<Port Name> <Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of protocol errors that the port experiences has changed. Occasional protocol errors occur due to software glitches. Persistent protocol errors occur due to hardware problems.

Recommended Action

Check both ends of your cable connection. Verify that the cable and small form-factor pluggables (SFPs) are not faulty.

FW-1173

Message

```
<Port Name> <Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of protocol errors that the port experiences has fallen below the low boundary. Occasional protocol errors occur due to software glitches. Persistent protocol errors occur due to hardware problems. A low number of protocol errors means that the switch is functioning normally.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1174

Message

```
<Port Name> <Label>, is above high boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the number of protocol errors that the port experiences has risen above the high boundary. Occasional protocol errors occur due to software glitches. Persistent protocol errors occur due to hardware problems.

Recommended Action

Check both ends of your connection. Verify that your cable and small form-factor pluggables (SFPs) are not faulty.

FW-1175

Message

```
<Port Name> <Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of protocol errors that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range. Occasional protocol errors occur due to software glitches. Persistent protocol errors occur due to hardware problems.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1176

Message

```
<Port Name> <Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of invalid words that the port experiences has changed. Invalid words usually indicate a hardware problem with a small form-factor pluggable (SFP) or cable.

Recommended Action Verify that both ends of the connections, the SFP, and the cable are not faulty.

FW-1177

Message

```
<Port Name> <Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of invalid words that the port experiences has fallen below the low boundary. Invalid words usually indicate a hardware problem with a small form-factor pluggable (SFP) or cable. A low number of invalid words means that the switch is functioning normally.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1178

Message

```
<Port Name> <Label>, is above high boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that the number of invalid words that the port experiences has risen above the high boundary. Invalid words usually indicate a hardware problem with a small form-factor pluggable (SFP) or cable.

Recommended Action Verify that both ends of the connections, the SFP, and the cable are not faulty.

FW-1179

Message

```
<Port Name> <Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of invalid words that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range. Invalid words usually indicate a hardware problem with a small form-factor pluggable (SFP) or cable.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1180

Message

```
<Port Name> <Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of invalid cyclic redundancy checks (CRCs) that the port experiences has changed. Frequent fluctuations in CRC errors generally indicate an aging fabric.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Check your small form-factor pluggables (SFPs), cables, and connections for faulty hardware. Verify that all optical hardware is clean.

FW-1181

Message

```
<Port Name> <Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of invalid cyclic redundancy checks (CRCs) that the port experiences has fallen below the low boundary. A low number of invalid CRCs means that the switch is functioning normally.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1182

Message

```
<Port Name> <Label>, is above high boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the number of invalid cyclic redundancy checks (CRCs) that the port experiences has risen above the high boundary. This error generally indicates a deteriorating fabric hardware.

Recommended Action

Check your small form-factor pluggables (SFPs), cables, and connections for faulty hardware. Verify that all optical hardware is clean.

FW-1183

Message

```
<Port Name> <Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of invalid cyclic redundancy checks (CRCs) that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range. Frequent fluctuations in CRC errors generally indicate an aging fabric.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Check your small form-factor pluggables (SFPs), cables, and connections for faulty hardware. Verify that all optical hardware is clean.

FW-1184

Message

```
<Port Name> <Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the percentage of incoming traffic that the port experiences has changed.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1185

Message
```
<Port Name> <Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the percentage of incoming traffic that the port experiences has fallen below the low boundary.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1186

Message
```
<Port Name> <Label>, is above high boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that the percentage of incoming traffic that the port experiences has risen above the high boundary.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1187

Message
```
<Port Name> <Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the percentage of incoming traffic that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1188

Message

```
<Port Name> <Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the percentage of outgoing traffic that the port experiences has changed.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1189

Message

```
<Port Name> <Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the percentage of outgoing traffic that the port experiences has fallen below the low boundary.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1190

Message

```
<Port Name> <Label>, is above high boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the packet loss and utilization areas for VE_Port has risen above the high boundary.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1191

Message `<Port Name> <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the percentage of outgoing traffic that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1192

Message `<Port Name> <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of state changes that the port experiences has changed. The state of the port has changed for one of the following reasons: the port has gone offline, has come online, is testing, is faulty, has become an E_Port, has become an F_Port, has segmented, or has become a trunk port.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1193

Message `<Port Name> <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of state changes that the port experiences has fallen below the low boundary. The state of the port has changed for one of the following reasons: the port has gone offline, has come online, is testing, is faulty, has become an E_Port, has become an F_Port, has segmented, or has become a trunk port.

A low number of port state changes means that the switch is functioning normally.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1194

Message

```
<Port Name> <Label>, is above high boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the number of state changes that the port experiences has risen above the high boundary. The state of the port has changed for one of the following reasons: the port has gone offline, has come online, is testing, is faulty, has become an E_Port, has become an F_Port, has segmented, or has become a trunk port.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1195

Message

```
<Port Name> <Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of state changes that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range. The state of the port has changed for one of the following reasons: the port has gone offline, has come online, is testing, is faulty, has become an E_Port, has become an F_Port, has segmented, or has become a trunk port.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1196

Message

```
<Port Name> <Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of link resets that the port experiences has changed. Link resets occur due to link timeout errors that indicate no frame activity.

Recommended Action

Check both ends of your cable connection. Verify if the cable and small form-factor pluggables (SFPs) are faulty.

FW-1197

Message

```
<Port Name> <Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of link resets that the port experiences has fallen below the low boundary level. Link resets occur due to link timeout errors that indicate no frame activity. A low number of link resets means that the switch is functioning normally.

Recommended Action

Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1198

Message

```
<Port Name> <Label>, is above high boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the number of link resets that the port experiences has increased above the high boundary level. Link resets occur due to link timeout errors that indicate no frame activity. Both physical and hardware problems can cause link resets to increase.

Recommended Action

Check both ends of your cable connection. Verify if the cable and small form-factor pluggables (SFPs) are faulty.

FW-1199

Message

```
<Port Name> <Label>, is between high and low boundaries(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of link resets that the port experiences has changed from a value beyond the acceptable range to a value within the acceptable range. Link resets occur due to link timeout errors that indicate no frame activity. Both physical and hardware problems can cause link resets to increase.

Recommended Action

Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1200

Message

```
<Port Name> <Label>, value has changed(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of C3 transmit timeout frames has changed.

Recommended Action Check the target device; it could be slow.

FW-1201

Message

```
<Port Name> <Label>, is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of C3 transmit timeout frames is below the low threshold. A low number of C3 transmit timeout means that the switch is functioning normally.

Recommended Action Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1202

Message

```
<Port Name> <Label>, is above high boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type AUDIT | LOG

Class FW

Severity ERROR

Probable Cause Indicates that the number of C3 transmit timeout frames is above the high threshold.

Recommended Action Check the target device; it could be slow.

FW-1203

Message `<Port Name> <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of C3 transmit timeout frames is between the high and low thresholds.

Recommended Action Check the target device; it could be slow.

FW-1204

Message `<Port Name> <Label> value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the trunk utilization has changed.

Recommended Action No action is required.

FW-1205

Message `<Port Name> <Label> is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the trunk utilization has reduced below the low boundary threshold.

Recommended Action No action is required.

FW-1206

Message

```
<Port Name> <Label> is above high boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that the trunk utilization is above its threshold level.

Recommended Action Increase the bandwidth by adding more links to the trunk.

FW-1207

Message

```
<Port Name> <Label> is between high and low boundaries(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the trunk utilization is between the low and high thresholds.

Recommended Action No action is required.

FW-1216

Message

```
<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is
<Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of Arbitrated Loop Physical Address (ALPA) cyclic redundancy check (CRC) errors has changed. This indicates that errors have been detected in the FC frame. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S_ID) and destination ID (D_ID) pairs change. These messages might also be caused by dirty equipment, temperature fluctuations, and aging equipment. You should set your high boundaries to five- or six-digit figures, because only large numbers of messages indicate a problem in this area.

Recommended Action Verify that your optical components are clean and function properly. Replace deteriorating cables or small form-factor pluggables (SFPs). Check for damage from heat or age.

FW-1217

Message

```
<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of Arbitrated Loop Physical Address (ALPA) cyclic redundancy check (CRC) errors has fallen below the low boundary. This indicates that errors have been detected in the FC frame. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S_ID) and destination ID (D_ID) pairs change. These messages might also be caused by dirty equipment, temperature fluctuations, and aging equipment. You should set your high boundaries to five- or six-digit figures, because only large numbers of messages indicate a problem in this area.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low level of invalid CRC errors means that the switch is functioning normally.

FW-1218

Message

```
<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the number of cyclic redundancy check (CRC) errors has risen above the high boundary. This indicates that errors have been detected in the FC frame. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S_ID) and destination ID (D_ID) pairs change. These messages might also be caused by dirty equipment, temperature fluctuations, and aging equipment. You should set your high boundaries to five- or six-digit figures, because only large numbers of messages indicate a problem in this area.

Recommended Action

You should configure a five- or six-figure high boundary for this area. Only five-figure (or higher) values for CRC errors indicate problems. Check for a faulty cable or deteriorated small form-factor pluggable (SFP). Replace the cable or the SFP if necessary. Clean the connectors. Check for damage from heat or deterioration from age.

FW-1219

Message

```
<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of cyclic redundancy check (CRC) errors has changed from a value outside of the acceptable range to a value within the acceptable range. This indicates that errors have been detected in the FC frame. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S_ID) and destination ID (D_ID) pairs change. These messages might also be caused by dirty equipment, temperature fluctuations, and aging equipment. You should set your high boundaries to five- or six-digit figures, because only large numbers of messages indicate a problem in this area.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1240

Message

```
<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is
<Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of end-to-end cyclic redundancy check (CRC) errors has changed. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S_ID) and destination ID (D_ID) pairs change. These messages might also be caused by dirty equipment, temperature fluctuations, and aging equipment.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1241

Message

```
<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of end-to-end cyclic redundancy check (CRC) errors has fallen below the low boundary. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S_ID) and destination ID (D_ID) pairs change. These messages might also be caused by dirty equipment, temperature fluctuations, and aging equipment.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of CRC errors means that the fabric is functioning normally. The CRC error area of the end-to-end performance monitor class helps you tune the fabric. To reduce CRC messages, experiment with alternative topologies and cabling schemes.

FW-1242

Message

```
<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that the number of end-to-end cyclic redundancy check (CRC) errors has risen above the high boundary. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S_ID) and destination ID (D_ID) pairs change. These messages might also be caused by dirty equipment, temperature fluctuations, and aging equipment.

Recommended Action The CRC error area of the end-to-end performance monitor class helps you tune the fabric. To reduce CRC errors, experiment with alternative topologies and cabling schemes. Clean equipment, check temperatures, and replace old hardware.

FW-1243

Message

```
<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of end-to-end cyclic redundancy check (CRC) errors has changed from a value outside of the acceptable range to a value within the acceptable range. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S_ID) and destination ID (D_ID) pairs change. These messages might also be caused by dirty equipment, temperature fluctuations, and aging equipment.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1244

Message `<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of end-to-end word frames that the switch receives has changed. Receive performance messages appear due to the number of word frames that travel from the configured S_ID to the D_ID pair.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1245

Message `<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of end-to-end word frames that the switch receives has fallen below the low boundary. Receive performance messages appear due to the number of word frames that travel from the configured S_ID to the D_ID pair.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1246

Message `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of end-to-end word frames that the switch receives has risen above the high boundary. Receive performance messages appear due to the number of word frames that travel from the configured S_ID to the D_ID pair.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1247

Message `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of end-to-end word frames that the switch receives has changed from a value outside of the acceptable range to a value within the acceptable range. Receive performance messages appear due to the number of word frames that travel from the configured S_ID to the D_ID pair.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1248

Message `<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of end-to-end word frames that the switch transmits has changed. Transmit performance messages appear due to the number of word frames that travel from the configured S_ID to the D_ID pair.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1249

Message `<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of end-to-end word frames that the switch transmits has fallen below the low boundary. Transmit performance messages appear due to the number of word frames that travel from the configured S_ID to the D_ID pair.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1250

Message `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of end-to-end word frames that the switch transmits has risen above the high boundary. Transmit performance messages appear due to the number of word frames that travel from the configured S_ID to the D_ID pair.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1251

Message `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of end-to-end word frames that the switch transmits has changed from a value outside of the acceptable range to a value within the acceptable range. Transmit performance messages appear due to the number of word frames that travel from the configured S_ID to the D_ID pair.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1272

Message `<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of frame types or commands that the port receives has changed. The port has received Small Computer System Interface (SCSI) Read, SCSI Write, SCSI Read and Write, SCSI Traffic, or IP commands in a frame.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1273

Message `<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of frame types or commands that the port receives has fallen below the low boundary. The port has received a Small Computer System Interface (SCSI) Read, SCSI Write, SCSI Read and Write, SCSI Traffic, or IP commands in a frame.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1274

Message `<Label>, is above high boundary(High=<Filter Counter>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type AUDIT | LOG

Class FW

Severity INFO

Probable Cause Indicates that the number of frame types or commands that the port receives has risen above the high boundary. The port has received a Small Computer System Interface (SCSI) Read, SCSI Write, SCSI Read and Write, SCSI Traffic, or IP commands in a frame.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1275

Message `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of frame types or commands that the port receives has changed from a value outside of the acceptable range to a value within the acceptable range. The port has received a Small Computer System Interface (SCSI) Read, SCSI Write, SCSI Read and Write, SCSI Traffic, or IP commands in a frame.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1296

Message

```
<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is
<Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of Telnet violations has changed. Telnet violations indicate that a Telnet connection request has been received from an unauthorized IP address. The TELNET_POLICY contains a list of IP addresses that are authorized to establish Telnet connections to switches in the fabric.

Recommended Action

Execute the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1297

Message

```
<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of Telnet violations has fallen below the low boundary. Telnet violations indicate that a Telnet connection request has been received from an unauthorized IP address. The TELNET_POLICY contains a list of IP addresses that are authorized to establish Telnet connections to switches in the fabric.

Recommended Action

No action is required.

FW-1298

Message

```
<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the number of Telnet violations has risen above the high boundary. Telnet violations indicate that a Telnet connection request has been received from an unauthorized IP address. The TELNET_POLICY contains a list of IP addresses that are authorized to establish Telnet connections to switches in the fabric.

Recommended Action

Execute the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1299

Message `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of Telnet violations has changed from a value outside of the acceptable range to a value within the acceptable range. Telnet violations indicate that a Telnet connection request has been received from an unauthorized IP address. The TELNET_POLICY contains a list of IP addresses that are authorized to establish Telnet connections to switches in the fabric.

Recommended Action No action is required.

FW-1300

Message `<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of Hypertext Transfer Protocol (HTTP) violations has changed. HTTP violations indicate that a browser connection request has been received from an unauthorized IP address. The HTTP_POLICY contains a list of IP addresses that are authorized to establish browser connections to the switches in the fabric.

Recommended Action Execute the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1301

Message `<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of Hypertext Transfer Protocol (HTTP) violations has fallen below the low boundary. HTTP violations indicate that a browser connection request has been received from an unauthorized IP address. The HTTP_POLICY contains a list of IP addresses that are authorized to establish browser connections to the switches in the fabric.

Recommended Action No action is required.

FW-1302

Message

```
<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the number of Hypertext Transfer Protocol (HTTP) violations has risen above the high boundary. HTTP violations indicate that a browser connection request has been received from an unauthorized IP address. The HTTP_POLICY contains a list of IP addresses that are authorized to establish browser connections to the switches in the fabric.

Recommended Action

Execute the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1303

Message

```
<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of Hypertext Transfer Protocol (HTTP) violations has changed from a value outside of the acceptable range to a value within the acceptable range. HTTP violations indicate that a browser connection request has been received from an unauthorized IP address. The HTTP_POLICY contains a list of IP addresses that are authorized to establish browser connections to the switches in the fabric.

Recommended Action

No action is required.

FW-1304

Message

```
<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is
<Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of application programming interface (API) violations has changed. API violations indicate that an API connection request has been received from an unauthorized IP address. The Simple Network Management Protocol policy (SNMP_POLICY) contains a list of IP addresses that are authorized to establish API connections to switches in the fabric.

Recommended Action Execute the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1305

Message

```
<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of application programming interface (API) violations has fallen below the low boundary. API violations indicate that an API connection request has been received from an unauthorized IP address. The Simple Network Management Protocol policy (SNMP_POLICY) contains a list of IP addresses that are authorized to establish API connections to switches in the fabric.

Recommended Action No action is required.

FW-1306

Message

```
<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that the number of application programming interface (API) violations has risen above the high boundary. API violations indicate that an API connection request has been received from an unauthorized IP address. The Simple Network Management Protocol policy (SNMP_POLICY) contains a list of IP addresses that are authorized to establish API connections to switches in the fabric.

Recommended Action Execute the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1307

Message

```
<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of application programming interface (API) violations has changed from a value outside of the acceptable range to a value within the acceptable range. API violations indicate that an API connection request has been received from an unauthorized IP address. The Simple Network Management Protocol policy (SNMP_POLICY) contains a list of IP addresses that are authorized to establish API connections to switches in the fabric.

Recommended Action

No action is required.

FW-1308

Message

```
<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is
<Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of read SNMP (RSNMP) violations has changed. RSNMP violations indicate that an SNMP "get" operation request has been received from an unauthorized IP address.

Recommended Action

Execute the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1309

Message

```
<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of read SNMP (RSNMP) violations has fallen below the low boundary. RSNMP violations indicate that an SNMP "get" operation request has been received from an unauthorized IP address.

Recommended Action

No action is required.

FW-1310

Message `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the number of read SNMP (RSNMP) violations has risen above the high boundary. RSNMP violations indicate that an SNMP "get" operation request has been received from an unauthorized IP address.

Recommended Action Execute the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1311

Message `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of read SNMP (RSNMP) violations has changed from a value outside of the acceptable range to a value within the acceptable range. RSNMP violations indicate that an SNMP "get" operation request has been received from an unauthorized IP address.

Recommended Action No action is required.

FW-1312

Message `<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of write SNMP (WSNMP) violations has changed. WSNMP violations indicate that an SNMP "get/set" operation request has been received from an unauthorized IP address.

Recommended Action Execute the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1313

Message

```
<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of write SNMP (WSNMP) violations has fallen below the low boundary. WSNMP violations indicate that an SNMP "get/set" operation request has been received from an unauthorized IP address.

Recommended Action

No action is required.

FW-1314

Message

```
<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the number of write SNMP (WSNMP) violations has risen above the high boundary. WSNMP violations indicate that an SNMP "get/set" operation request has been received from an unauthorized IP address.

Recommended Action

Execute the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1315

Message

```
<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of write SNMP (WSNMP) violations has changed from a value outside of the acceptable range to a value within the acceptable range. WSNMP violations indicate that an SNMP "get/set" operation request has been received from an unauthorized IP address.

Recommended Action

No action is required.

FW-1316

Message `<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of SCSI Enclosure Services (SES) violations has changed. SES violations indicate that a Small Computer System Interface (SCSI) Enclosure Services request has been received from an unauthorized World Wide Name (WWN). The SES_POLICY contains a list of WWNs of device ports that are allowed to access the SES Server functionality.

Recommended Action Execute the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1317

Message `<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of SCSI Enclosure Services (SES) violations has fallen below the low boundary. SES violations indicate that a Small Computer System Interface (SCSI) Enclosure Services request has been received from an unauthorized World Wide Name (WWN). The SES_POLICY contains a list of WWNs of device ports that are allowed to access the SES Server functionality.

Recommended Action No action is required.

FW-1318

Message `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the number of SCSI Enclosure Services (SES) violations has risen above the high boundary. SES violations indicate that a Small Computer System Interface (SCSI) Enclosure Services request has been received from an unauthorized World Wide Name (WWN). The SES_POLICY contains a list of WWNs of device ports that are allowed to access the SES Server functionality.

Recommended Action Execute the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1319

Message

```
<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of SCSI Enclosure Services (SES) violations has changed from a value outside of the acceptable range to a value within the acceptable range. SES violations indicate that a Small Computer System Interface (SCSI) Enclosure Services (SES) request has been received from an unauthorized World Wide Name (WWN). The SES_POLICY contains a list of WWNs of device ports that are allowed to access the SES Server functionality.

Recommended Action

No action is required.

FW-1320

Message

```
<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is
<Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of Management Server (MS) violations has changed. MS violations indicate that an MS access request has been received from an unauthorized World Wide Name (WWN). The MS_POLICY contains a list of WWNs of device ports that are allowed to access the Management Server functionality.

Recommended Action

Execute the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1321

Message

```
<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of Management Server (MS) violations has fallen below the low boundary. MS violations indicate that an MS access request has been received from an unauthorized World Wide Name (WWN). The MS_POLICY contains a list of WWNs of device ports that are allowed to access the Management Server functionality.

Recommended Action

No action is required.

FW-1322

Message `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the number of Management Server (MS) violations has risen above the high boundary. MS violations indicate that an MS access request has been received from an unauthorized World Wide Name (WWN). The MS_POLICY contains a list of WWNs of device ports that are allowed to access the Management Server functionality.

Recommended Action Execute the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1323

Message `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of Management Server (MS) violations has changed from a value outside of the acceptable range to a value within the acceptable range. MS violations indicate that an MS access request has been received from an unauthorized World Wide Name (WWN). The MS_POLICY contains a list of WWNs of device ports that are allowed to access the Management Server functionality.

Recommended Action No action is required.

FW-1324

Message `<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of serial violations has changed. Serial violations indicate that an unauthorized serial port request has been received. The SERIAL_POLICY contains a list of switch World Wide Names (WWNs) for which serial port access is enabled.

Recommended Action Execute the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1325

Message `<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of serial violations has fallen below the low boundary. Serial violations indicate that an unauthorized serial port request has been received. The SERIAL_POLICY contains a list of switch World Wide Names (WWNs) for which serial port access is enabled.

Recommended Action No action is required.

FW-1326

Message `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the number of serial violations has risen above the high boundary. Serial violations indicate that an unauthorized serial port request has been received. The SERIAL_POLICY contains a list of switch World Wide Names (WWNs) for which serial port access is enabled.

Recommended Action Run the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1327

Message `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of serial violations has changed from a value outside of the acceptable range to a value within the acceptable range. Serial violations indicate that an unauthorized serial port request has been received. The SERIAL_POLICY contains a list of switch World Wide Names (WWNs) for which serial port access is enabled.

Recommended Action No action is required.

FW-1328

Message `<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of front panel violations has changed. Front panel violations indicate that an unauthorized front panel request has been received. The FRONTPANEL_POLICY contains a list of switch World Wide Names (WWNs) for which front panel access is enabled.

Recommended Action Execute the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1329

Message `<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of front panel violations has fallen below the low boundary. Front panel violations indicate that an unauthorized front panel request has been received. The FRONTPANEL_POLICY contains a list of switch World Wide Names (WWNs) for which front panel access is enabled.

Recommended Action No action is required.

FW-1330

Message `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the number of front panel violations has risen above the high boundary. Front panel violations indicate that an unauthorized front panel request has been received. The FRONTPANEL_POLICY contains a list of switch World Wide Names (WWNs) for which front panel access is enabled.

Recommended Action Execute the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1331

Message `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of front panel violations has changed from a value outside of the acceptable range to a value within the acceptable range. Front panel violations indicate that an unauthorized front panel request has been received. The FRONTPANEL_POLICY contains a list of switch World Wide Names (WWNs) for which front panel access is enabled.

Recommended Action No action is required.

FW-1332

Message `<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of Switch Connection Control (SCC) policy violations has changed. SCC violations indicate that an unauthorized switch tried to join the fabric. The SCC_POLICY contains a list of switches by World Wide Name (WWN) that are allowed to be members of a fabric.

Recommended Action Execute the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1333

Message `<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of Switch Connection Control (SCC) policy violations has fallen below the low boundary. SCC violations indicate that an unauthorized switch tried to join the fabric. The SCC_POLICY contains a list of switches by World Wide Name (WWN) that are allowed to be members of a fabric.

Recommended Action No action is required.

FW-1334

Message `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the number of Switch Connection Control (SCC) policy violations has risen above the high boundary. SCC violations indicate that an unauthorized switch tried to join the fabric. The SCC_POLICY contains a list of switches by World Wide Name (WWN) that are allowed to be members of a fabric.

Recommended Action Execute the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1335

Message `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of Switch Connection Control (SCC) policy violations has changed from a value outside of the acceptable range to a value within the acceptable range. SCC violations indicate that an unauthorized switch tried to join the fabric. The SCC_POLICY contains a list of switches by World Wide Name (WWN) that are allowed to be members of a fabric.

Recommended Action No action is required.

FW-1336

Message `<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of Device Connection Control (DCC) violations has changed. DCC violations indicate that an unauthorized device tried to join the fabric. The DCC_POLICY allows for the specification of rules for binding device ports (typically HBA ports) to specific switch ports. DCC policies ensure that whenever a device performs a fabric login (FLOGI) request, the World Wide Name (WWN) specified in the FLOGI is validated to be connected to the authorized port. Enforcement for private loop devices not performing FLOGI is done through the name server.

Recommended Action Execute the **errShow** command to determine the device WWN, switch WWN, and switch port. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1337

Message

```
<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of Device Connection Control (DCC) violations has fallen below the low boundary. DCC violations indicate that an unauthorized device tried to join the fabric. The DCC_POLICY allows for the specification of rules for binding device ports (typically HBA ports) to specific switch ports. DCC policies ensure that whenever a device performs a fabric login (FLOGI) request, the World Wide Name (WWN) specified in the FLOGI is validated to be connected to the authorized port. Enforcement for private loop devices not performing FLOGI is done through the name server.

Recommended Action No action is required.

FW-1338

Message

```
<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that the number of Device Connection Control (DCC) violations has risen above the high boundary. DCC violations indicate that an unauthorized device tried to join the fabric. The DCC_POLICY allows for the specification of rules for binding device ports (typically HBA ports) to specific switch ports. DCC policies ensure that whenever a device performs a fabric login (FLOGI) request, the World Wide Name (WWN) specified in the FLOGI is validated to be connected to the authorized port. Enforcement for private loop devices not performing FLOGI is done through the name server.

Recommended Action Execute the **errShow** command to determine the device WWN, switch WWN, and switch port. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1339

Message `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of Device Connection Control (DCC) violations has changed from a value outside of the acceptable range to a value within the acceptable range. DCC violations indicate that an unauthorized device tried to join the fabric. The DCC_POLICY allows for the specification of rules for binding device ports (typically HBA ports) to specific switch ports. DCC policies ensure that whenever a device performs a fabric login (FLOGI) request, the World Wide Name (WWN) specified in the FLOGI is validated to be connected to the authorized port. Enforcement for private loop devices not performing FLOGI is done through the name server.

Recommended Action No action is required.

FW-1340

Message `<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of login violations has changed. Login violations indicate that a login failure has been detected.

Recommended Action Execute the **errShow** command to determine the IP location of the login attempt. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1341

Message `<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of login violations has fallen below the low boundary. Login violations indicate that a login failure has been detected.

Recommended Action No action is required.

FW-1342

Message `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the number of login violations has risen above the high boundary. Login violations indicate that a login failure has been detected.

Recommended Action Execute the **errShow** command to determine the IP location of the login attempt. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1343

Message `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of login violations has changed from a value outside of the acceptable range to a value within the acceptable range. Login violations indicate that a login failure has been detected.

Recommended Action No action is required.

FW-1344

Message `<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of invalid timestamps has changed. Invalid timestamp violations indicate that a packet with an invalid timestamp has been received from the primary fabric configuration server (FCS). When the primary FCS downloads a new configuration to other switches in the fabric, the packet is tagged with a timestamp. The receiving switch compares this timestamp to its current time. If the difference is too great, it rejects the packet. This counter keeps track of packets rejected due to invalid timestamps.

Recommended Action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1345

Message

```
<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of invalid timestamps has fallen below the low boundary. Invalid timestamp violations indicate a packet with an invalid timestamp has been received from the primary fabric configuration server (FCS). When the primary FCS downloads a new configuration to other switches in the fabric, the packet is tagged with a timestamp. The receiving switch compares this timestamp to its current time. If the difference is too great, it rejects the packet. This counter keeps track of packets rejected due to invalid timestamps.

Recommended Action

No action is required.

FW-1346

Message

```
<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the number of invalid timestamps has risen above the high boundary. Invalid timestamp violations indicate a packet with an invalid timestamp has been received from the primary fabric configuration server (FCS). When the primary FCS downloads a new configuration to other switches in the fabric, the packet is tagged with a timestamp. The receiving switch compares this timestamp to its current time. If the difference is too great, it rejects the packet. This counter keeps track of packets rejected due to invalid timestamps.

Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1347

Message

```
<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of invalid timestamps has changed from a value outside of the acceptable range to a value within the acceptable range. Invalid timestamp violations indicate a packet with an invalid timestamp has been received from the primary fabric configuration server (FCS). When the primary FCS downloads a new configuration to other switches in the fabric, the packet is tagged with a timestamp. The receiving switch compares this timestamp to its current time. If the difference is too great, it rejects the packet. This counter keeps track of packets rejected due to invalid timestamps.

Recommended Action

No action is required.

FW-1348

Message

```
<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is
<Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of invalid signatures has changed. Invalid signature violations indicate that a packet with an invalid signature has been received from the primary fabric configuration server (FCS). When the primary FCS downloads a new configuration to the other switches in the fabric, the packet is signed using the private key of the primary FCS. The receiving switch must verify this signature with the public key of the primary FCS switch. If verification fails, it rejects the packet. This counter keeps track of the number of packets received with invalid signatures.

Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1349

Message

```
<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of invalid signatures has fallen below the low boundary. Invalid signature violations indicate that a packet with an invalid signature has been received from the primary fabric configuration server (FCS). When the primary FCS downloads a new configuration to the other switches in the fabric, the packet is signed using the private key of the primary FCS. The receiving switch must verify this signature with the public key of the primary FCS switch. If verification fails, it rejects the packet. This counter keeps track of the number of packets received with invalid signatures.

Recommended Action

No action is required.

FW-1350

Message

```
<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the number of invalid signatures has risen above the high boundary. Invalid signature violations indicate that a packet with an invalid signature has been received from the primary fabric configuration server (FCS). When the primary FCS downloads a new configuration to the other switches in the fabric, the packet is signed using the private key of the primary FCS. The receiving switch must verify this signature with the public key of the primary FCS switch. If verification fails, it rejects the packet. This counter keeps track of the number of packets received with invalid signatures.

Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1351

Message

```
<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of invalid signatures has changed from a value outside of the acceptable range to a value within the acceptable range. Invalid signature violations indicate that a packet with an invalid signature has been received from the primary fabric configuration server (FCS). When the primary FCS downloads a new configuration to the other switches in the fabric, the packet is signed using the private key of the primary FCS. The receiving switch must verify this signature with the public key of the primary FCS switch. If verification fails, it rejects the packet. This counter keeps track of the number of packets received with invalid signatures.

Recommended Action

No action is required.

FW-1352

Message

```
<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is
<Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of invalid certificates has changed. This violation indicates that a packet with an invalid certificate has been received from the primary fabric configuration server (FCS). Before a new primary FCS switch sends any configuration data to any switch in the fabric, it first sends its certificate to all the switches in the fabric. The receiving switch must verify that the sender is the primary FCS switch and its certificate is signed by the Root CA recognized by the receiving switch. This counter keeps track of the number of packets received with invalid certificates.

Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1353

Message

```
<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of invalid certificates has fallen below the low boundary. This violation indicates that a packet with an invalid certificate has been received from the primary fabric configuration server (FCS). Before a new primary FCS switch sends any configuration data to any switch in the fabric, it first sends its certificate to all the switches in the fabric. The receiving switch must verify that the sender is the primary FCS switch and its certificate is signed by the Root CA recognized by the receiving switch. This counter keeps track of the number of packets received with invalid certificates.

Recommended Action

No action is required.

FW-1354

Message

```
<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the number of invalid certificates has risen above the high boundary. This violation indicates that a packet with an invalid certificate has been received from the primary fabric configuration server (FCS). Before a new primary FCS switch sends any configuration data to any switch in the fabric, it first sends its certificate to all the switches in the fabric. The receiving switch must verify that the sender is the primary FCS switch and its certificate is signed by the Root CA recognized by the receiving switch. This counter keeps track of the number of packets received with invalid certificates.

Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1355

Message

```
<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of invalid certificates has changed from a value outside of the acceptable range to a value within the acceptable range. This violation indicates that a packet with an invalid certificate has been received from the primary fabric configuration server (FCS). Before a new primary FCS switch sends any configuration data to any switch in the fabric, it first sends its certificate to all the switches in the fabric. The receiving switch has to verify that the sender is the primary FCS switch and its certificate is signed by the Root CA recognized by the receiving switch. This counter keeps track of the number of packets received with invalid certificates.

Recommended Action

No action is required.

FW-1356

Message

```
<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is
<Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of authentication failures has changed. Authentication failures can occur for many reasons. The switch on the other side may not support the protocol, have an invalid certificate, not be signed properly, or send unexpected packets. The port where authentication fails is segmented. This counter keeps track of the number of authentication failures.

Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1357

Message

```
<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of authentication failures has fallen below the low boundary. Authentication failures can occur for many reasons. The switch on the other side may not support the protocol, have an invalid certificate, not be signed properly, or send unexpected packets. The port where authentication fails is segmented. This counter keeps track of the number of authentication failures.

Recommended Action No action is required.

FW-1358

Message

```
<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that the number of authentication failures has risen above the high boundary. Authentication failures can occur for many reasons. The switch on the other side may not support the protocol, have an invalid certificate, not be signed properly, or send unexpected packets. The port where authentication fails is segmented. This counter keeps track of the number of authentication failures.

Recommended Action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1359

Message

```
<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of authentication failures has changed from a value outside of the acceptable range to a value within the acceptable range. Authentication failures can occur for many reasons. The switch on the other side might not support the protocol, have an invalid certificate, not be signed properly, or send unexpected packets. The port where authentication fails is segmented. This counter keeps track of the number of authentication failures.

Recommended Action No action is required.

FW-1360

Message

```
<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is
<Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of Switch Link Authentication Protocol (SLAP) faulty packets has changed. This counter keeps track of the number of unexpected SLAP packets and SLAP packets with faulty transmission IDs.

Recommended Action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1361

Message

```
<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of switch link authentication protocol (SLAP) faulty packets has fallen below the low boundary. This counter keeps track of the number of unexpected SLAP packets and SLAP packets with faulty transmission IDs.

Recommended Action No action is required.

FW-1362

Message

```
<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that the number of Switch Link Authentication Protocol (SLAP) faulty packets has risen above the high boundary. This counter keeps track of the number of unexpected SLAP packets and SLAP packets with faulty transmission IDs.

Recommended Action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1363

Message

```
<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of Switch Link Authentication Protocol (SLAP) faulty packets has changed from a value outside of the acceptable range to a value within the acceptable range. This counter keeps track of the number of unexpected SLAP packets and SLAP packets with faulty transmission IDs.

Recommended Action No action is required.

FW-1364

Message `<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of time service (TS) out-of-sync violations has changed.

Recommended Action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1365

Message `<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of time service (TS) out-of-sync violations has fallen below the low boundary.

Recommended Action No action is required.

FW-1366

Message `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the number of time service (TS) out-of-sync violations has risen above the high boundary.

Recommended Action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1367

Message

```
<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of time service (TS) out-of-sync violations has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action No action is required.

FW-1368

Message

```
<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is
<Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of no-FCS violations has changed. This counter records how often the switch loses contact with the primary fabric configuration server (FCS) switch. When the primary FCS switch in the fabric sends its certificate to a switch, the receiving switch saves the World Wide Name (WWN) of that primary FCS switch. If a secure switch finds that there are no FCSs in the fabric, but it still has the WWN of the last primary FCS switch, it increments this counter and resets the WWN of the primary FCS to all zeroes.

Recommended Action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1369

Message

```
<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of no-FCS violations has fallen below the low boundary. This counter records how often the switch loses contact with the primary fabric configuration server (FCS) switch. When the primary FCS switch in the fabric sends its certificate to a switch, the receiving switch saves the World Wide Name (WWN) of that primary FCS switch. If a secure switch finds that there are no FCSs in the fabric, but it still has the WWN of the last primary FCS switch, it increments this counter and resets the WWN of the primary FCS to all zeroes.

Recommended Action No action is required.

FW-1370

Message

```
<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that the number of no-FCS violations has risen above the high boundary. This counter records how often the switch loses contact with the primary fabric configuration server (FCS) switch. When the primary FCS switch in the fabric sends its certificate to a switch, the receiving switch saves the World Wide Name (WWN) of that primary FCS switch. If a secure switch finds that there are no FCSs in the fabric, but it still has the WWN of the last primary FCS switch, it increments this counter and resets the WWN of the primary FCS to all zeroes.

Recommended Action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1371

Message

```
<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of no-FCS violations has changed from a value outside of the acceptable range to a value within the acceptable range. This counter records how often the switch loses contact with the primary fabric configuration server (FCS) switch. When the primary FCS switch in the fabric sends its certificate to a switch, the receiving switch saves the World Wide Name (WWN) of that primary FCS switch. If a secure switch finds that there are no FCSs in the fabric, but it still has the WWN of the last primary FCS switch, it increments this counter and resets the WWN of the primary FCS to all zeroes.

Recommended Action No action is required.

FW-1372

Message

```
<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is
<Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of incompatible security database violations has changed. This violation indicates the number of secure switches with different version stamps have been detected. When a switch is in secure mode, it connects only to another switch that is in secure mode and has a compatible security database. A compatible security database means that the version stamp and fabric configuration server (FCS) policy matches exactly.

Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1373

Message

```
<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of incompatible security database violations has fallen below the low boundary. This violation indicates the number of secure switches with different version stamps have been detected. When a switch is in secure mode, it connects only to another switch that is in secure mode and has a compatible security database. A compatible security database means that the version stamp and fabric configuration server (FCS) policy matches exactly.

Recommended Action

No action is required.

FW-1374

Message

```
<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the number of incompatible security database violations has risen above the high boundary. This violation indicates the number of secure switches with different version stamps have been detected. When a switch is in secure mode, it connects only to another switch that is in secure mode and has a compatible security database. A compatible security database means that the version stamp and fabric configuration server (FCS) policy matches exactly.

Recommended Action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1375

Message

```
<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of incompatible security database violations has changed from a value outside of the acceptable range to a value within the acceptable range. This violation indicates the number of secure switches with different version stamps that have been detected. When a switch is in secure mode, it connects only to another switch that is in secure mode and has a compatible security database. A compatible security database means that the version stamp and fabric configuration server (FCS) policy matches exactly.

Recommended Action No action is required.

FW-1376

Message

```
<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is
<Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of illegal commands has changed. This counter tracks how many times commands allowed only on the primary fabric configuration server (FCS) switch have been executed on a non-primary FCS switch. There are many commands that can be executed only on the primary FCS switch, as well as one security command that can be executed only on a backup FCS switch. The counter increments every time someone issues one of these commands on a switch where it is not allowed.

Recommended Action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1377

Message

```
<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of illegal commands has fallen below the low boundary. This counter tracks how many times commands allowed only on the primary fabric configuration server (FCS) switch have been executed on a non-primary FCS switch. There are many commands that can be executed only on the primary FCS switch, as well as one security command that can be executed only on a backup FCS switch. The counter increments every time someone issues one of these commands on a switch where it is not allowed.

Recommended Action

No action is required.

FW-1378

Message

```
<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the number of illegal commands has risen above the high boundary. This counter tracks how many times commands allowed only on the primary fabric configuration server (FCS) switch have been executed on a non-primary FCS switch. There are many commands that can be executed only on the primary FCS switch, as well as one security command that can be executed only on a backup FCS switch. The counter increments every time someone issues one of these commands on a switch where it is not allowed.

Recommended Action

Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

FW-1379

Message

```
<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of illegal commands has changed from a value outside of the acceptable range to a value within the acceptable range. This counter tracks how many times commands allowed only on the primary fabric configuration server (FCS) switch have been executed on a non-primary FCS switch. There are many commands that can be executed only on the primary FCS switch, as well as one security command that can be executed only on a backup FCS switch. The counter increments every time someone issues one of these commands on a switch where it is not allowed.

Recommended Action

No action is required.

FW-1400

Message

```
<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is
<Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the flash memory usage percentage has changed. Flash memory increases and decreases slightly with normal operation of the switch.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1401

Message

```
<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the flash memory usage percentage has fallen below the low boundary. Flash memory increases and decreases slightly with normal operation of the switch.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1402

Message `<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type AUDIT | LOG

Class FW

Severity WARNING

Probable Cause Indicates that the flash memory usage percentage has risen above the high boundary. Flash memory increases and decreases slightly with normal operation of the switch.

Recommended Action Remove some unwanted files to create some flash space. Execute the **supportSave** command to remove files from the kernel space.

FW-1403

Message `<Label>,is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the CPU or memory usage is between the boundary limits.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1404

Message `<Label>,is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type AUDIT | LOG

Class FW

Severity WARNING

Probable Cause Indicates that the CPU or memory usage is above its threshold. If this RASLOG pertains to memory usage, then the usage is above the middle memory threshold.

Recommended Action No action is required.

FW-1405

Message `<Label>,is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type AUDIT | LOG

Class FW

Severity INFO

Probable Cause Indicates that the memory usage is below the low memory threshold.

Recommended Action No action is required.

FW-1406

Message `<Label>,is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type AUDIT | LOG

Class FW

Severity CRITICAL

Probable Cause Indicates that the memory usage is above the high memory threshold.

Recommended Action No action is required.

FW-1407

Message `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the memory usage is between the high and middle memory thresholds.

Recommended Action No action is required.

FW-1408

Message `<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the memory usage is between the low and high or middle memory thresholds.

Recommended Action No action is required.

FW-1424

Message `Switch status changed from <Previous state> to <Current state>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the switch is not in a healthy state. This occurred because of a policy violation.

Recommended Action Execute the **switchStatusShow** command to determine the policy violation.

FW-1425

Message `Switch status changed from <Bad state> to HEALTHY.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the switch status has changed to a healthy state. This occurred because a policy is no longer violated.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1426

Message `Switch status change contributing factor Power supply: <Number Bad> bad, <Number Missing> absent.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the switch is not in a healthy state. This occurred because the number of faulty or missing power supplies is greater than or equal to the policy set by the **switchStatusPolicySet** command.

Recommended Action Replace the faulty or missing power supply.

FW-1427

Message `Switch status change contributing factor Power supply: <Number Bad> bad.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the switch is not in a healthy state. This occurred because the number of faulty power supplies is greater than or equal to the policy set by the **switchStatusPolicySet** command.

Recommended Action Replace the faulty power supply.

FW-1428

Message `Switch status change contributing factor Power supply: <Number Missing> absent.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the switch is not in a healthy state. This occurred because the number of missing power supplies is greater than or equal to the policy set by the **switchStatusPolicySet** command.

Recommended Action Replace the missing power supply.

FW-1429

Message `Switch status change contributing factor: Power supplies are not redundant.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the switch is not in a healthy state. This occurred because the power supplies are not in the correct slots for redundancy.

Recommended Action Rearrange the power supplies so that one is in an odd slot and another in an even slot to make them redundant.

FW-1430

Message `Switch status change contributing factor <string>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the switch is not in a healthy state. This occurred because the number of faulty temperature sensors is greater than or equal to the policy set by the **switchStatusPolicySet** command. A temperature sensor is faulty when the sensor value is not in the acceptable range or is faulty.

Recommended Action Replace the field-replaceable unit (FRU) with the faulty temperature sensor.

FW-1431

Message `Switch status change contributing factor Fan: <Number Bad> bad.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the switch is not in a healthy state. This occurred because the number of faulty fans is greater than or equal to the policy set by the **switchStatusPolicySet** command. A fan is faulty when the value is not in the acceptable range or is faulty.

Recommended Action Replace the faulty or deteriorating fan field-replaceable units (FRUs).

FW-1432

Message `Switch status change contributing factor WWN: <Number Bad> bad.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the switch is not in a healthy state. This occurred because the number of faulty World Wide Name (WWN) cards is greater than or equal to the policy set by the **switchStatusPolicySet** command.

Recommended Action Replace the faulty WWN card.

FW-1433

Message `Switch status change contributing factor CP: CP non-redundant (<CP Number>) faulty.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the switch is not in a healthy state. This occurred because the number of faulty CPs is greater than or equal to the policy set by the **switchStatusPolicySet** command. The CPs are not redundant.

If you power cycle a chassis in dual-domain configuration, and then reset the micro-switch of the active CP before the heartbeat is up, this will cause both CPs to come up in a non-redundant state.

Recommended Action Execute the **firmwareShow** command to verify if both the CPs have compatible firmware levels. Execute the **firmwareDownload** command to install the same level of firmware to both CPs. Replace any faulty CPs.

If you reset the micro-switch (the latch on the CP blade) on the active CP before the heartbeat was up on a power cycle, and the CPs came up non-redundant, then you should reboot the CPs again to clear the problem.

FW-1434

Message `Switch status change contributing factor Blade: <Number Bad> blade failures (<Blade Numbers>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the switch is not in a healthy state. This occurred because the number of blade failures is greater than or equal to the policy set by the **switchStatusPolicySet** command.

Recommended Action Replace the faulty blade.

FW-1435

Message `Switch status change contributing factor Flash: usage out of range.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the switch is not in a healthy state. This occurred because the flash memory usage is out of range. The policy was set using the **switchStatusPolicySet** command.

Recommended Action Execute the **supportSave** command to clear out the kernel flash.

FW-1436

Message `Switch status change contributing factor Marginal ports: <Number of marginal ports> marginal out of <Total number of ports> ports:config(<Percentage configured> percent,<Actual threshold limit>). (Port(s) <port list>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the switch is not in a healthy state. This occurred because the number of marginal ports is greater than or equal to the policy set using the **switchStatusPolicySet** command. A port is faulty when the port value is Link Loss, Synchronization Loss, Signal Loss, Invalid word, Protocol error, CRC error, Port state change, or Buffer Limited Port is above the high boundary.

Recommended Action Replace the faulty or deteriorating small form-factor pluggable (SFP). Execute the **fwportdetailshow** command to know the reason for marginal ports.

FW-1437

Message `Switch status change contributing factor Faulty ports: <Number of faulty ports> faulty out of <Total number of ports> ports:config(<Percentage configured> percent,<Actual threshold limit>). (Port(s) <port list>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the switch is not in a healthy state. This occurred because the number of faulty ports is greater than or equal to the policy set by the **switchStatusPolicySet** command. A port is considered faulty due to hardware failure such as a faulty small form-factor pluggable (SFP) or port.

Recommended Action Replace any faulty or deteriorating SFPs.

FW-1438

Message `Switch status change contributing factor Missing SFPs: <Number of missing SFPs> missing SFPs out of <Total number of SFPs> SFPs:config(<Percentage configured> percent,<Actual threshold limit>). (Port(s) <port list>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the switch is not in a healthy state. This occurred because the number of missing small form-factor pluggable (SFPs) is greater than or equal to the policy set by the **switchStatusPolicySet** command.

Recommended Action Execute the **switchStatusPolicySet** command to modify the SFP policy or to add SFPs to the empty ports.

FW-1439

Message `Switch status change contributing factor Switch offline.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the switch is not in a healthy state. This occurred because the switch is offline.

Recommended Action Execute the **switchEnable** command.

FW-1440

Message `<FRU label> state has changed to <FRU state>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the state of the specified field-replaceable unit (FRU) has changed to absent.

Recommended Action Verify that the event was planned.

FW-1441

Message `<FRU label> state has changed to <FRU state>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the state of the specified field-replaceable unit (FRU) has changed to inserted. This means that a FRU is inserted but not powered on.

Recommended Action Verify that the event was planned.

FW-1442

Message `<FRU label> state has changed to <FRU state>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the state of the specified field-replaceable unit (FRU) has changed to on.

Recommended Action Verify that the event was planned.

FW-1443

Message `<FRU label> state has changed to <FRU state>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the state of the specified field-replaceable unit (FRU) has changed to off.

Recommended Action Verify that the event was planned.

FW-1444

Message `<FRU label> state has changed to <FRU state>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the state of the specified field-replaceable unit (FRU) has changed to faulty.

Recommended Action Replace the FRU.

FW-1445

Message `Four power supplies are now required for 2X redundancy, Switch Status Policy values changed.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the switch requires four power supplies and the prior Switch Status Policy parameters will be overwritten to reflect this. The presence of an AP blade means that more than one power supply may be required to provide adequate power. So (even if the AP blade is powered down or removed) the Switch Status Policy values will now reflect the need for four power supplies to maintain full (2X) redundancy.

Recommended Action No action required unless there are fewer than four power supplies active in the chassis. If there are fewer than four, insert additional power supplies so that there are four active power supplies.

FW-1446

Message `Four power supplies now required for 2X redundancy, not enforced by Fabric Watch due to Switch Status Policy overridden by User.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the switch now requires four power supplies for full (2X) redundancy, but the user has previously overridden the Switch Status Policy values pertaining to the number of power supplies. So those values will not be automatically changed.

With no AP blades, the default value is 3 (out of service), indicating switch status is down or 0 indicating no checking for switch status marginal.

When an AP blade is or has been present, the default value is 2 (out of service) indicating switch status is down or 1 (out of service) indicating switch status is marginal.

Recommended Action To maintain full (2X) redundancy and proper monitoring by Fabric Watch, supply four active power supplies and enter the default values associated with the presence of an AP blade using the **switchStatusPolicySet** command.

FW-1447

Message `Switch status change contributing factor Core Blade: <Number Bad> Core blade failures (<Switch State>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the switch is not in a healthy state. This occurred because the number of core blade failures is greater than or equal to the policy set by the **switchStatusPolicySet** command.

Recommended Action Replace the faulty core blade.

FW-1448

Message `Switch status change contributing factor Error ports: <Number of Error ports> Error out of <Total number of ports> ports:config(<Percentage configured> percent,<Actual threshold limit>). (Port(s) <port list>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the switch is not in a healthy state. This occurred because the number of faulty ports is greater than or equal to the policy set by the **switchStatusPolicySet** command. A port is faulted because of port segmentation or port disable.

Recommended Action Execute the **switchShow** command to know the reason for port segmentation and port disable. Take the necessary action to bring the port up.

FW-1500

Message `Mail overflow - Alerts being discarded.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the mail alert overflow condition has occurred.

Recommended Action Resolve or disable the mail alert using the **fwMailCfg** command.

FW-1501

Message `Mail overflow cleared - <Mails discarded> alerts discarded.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the mail overflow condition has cleared.

Recommended Action No action is required.

FW-1502

Message `Invalid Email address <Invalid address> is configured from pre-7.0.0 config file.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the configuration file has invalid e-mail addresses.

Recommended Action Reconfigure a valid e-mail address.

FW-1510

Message
```
<Area string> threshold exceeded(High=<Threshold high>). Current value is
<Current value>: Port <Port number> disabled.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified port is now disabled because the link on this port had multiple link failures that exceeded the Fabric Watch threshold on the port. Both physical and hardware problems can cause link failures. Link failures frequently occur due to a loss of synchronization. Link failures also occur due to hardware failures, a defective small form-factor pluggable (SFP), or a faulty cable.

Protocol errors indicates CRC sum disparity. Occasionally, these errors occur due to software glitches. Persistent errors occur due to hardware problems.

Recommended Action Check for concurrent loss of synchronization errors. Check the SFP and the cable. Then, enable the port using the **portEnable** command.

FW-1511

Message

```
<Port Name> <Label>, has crossed lower threshold boundary to in between(High=<High
value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of link failures that the port experiences has changed and crossed the lower threshold boundary to a value within the acceptable range. Link loss errors occur when a link experiences a loss of signal and fails. Both physical and hardware problems can cause link loss errors. Link loss errors frequently occur due to a loss of synchronization. Check for concurrent loss of synchronization errors and, if applicable, troubleshoot them.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1512

Message

```
<Port Name> <Label>, has dropped below upper threshold boundary to in
between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of link failures that the port experiences has changed and dropped below the upper threshold boundary to a value within the acceptable range. Link loss errors occur when a link experiences a loss of signal and fails. Both physical and hardware problems can cause link loss errors. Link loss errors frequently occur due to a loss of synchronization. Check for concurrent loss of synchronization errors and, if applicable, troubleshoot them.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1513

Message

```
<Port Name> <Label>, has crossed lower threshold boundary to in between(High=<High
value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of synchronization losses that the port experiences has changed and crossed the lower threshold boundary to a value within the acceptable range. Loss of synchronization errors frequently occur due to a faulty small form-factor pluggable (SFP) or cable. Signal losses often create synchronization losses.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1514

Message

```
<Port Name> <Label>, has dropped below upper threshold boundary to in
between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of synchronization losses that the port experiences has changed and dropped below the upper threshold boundary to a value within the acceptable range. Loss of synchronization errors frequently occur due to a faulty small form-factor pluggable (SFP) or cable. Signal losses often create synchronization losses.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1515

Message

```
<Port Name> <Label>, has crossed lower threshold boundary to in between(High=<High
value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of signal losses that the port experiences has changed and crossed the lower threshold boundary to a value within the acceptable range. Loss of signal generally indicates a physical problem.

Recommended Action Frequent loss of signal generally indicates a physical problem. Check both ends of your cable connection. Verify that the cable and small form-factor pluggables (SFPs) are not faulty.

FW-1516

Message

```
<Port Name> <Label>, has dropped below upper threshold boundary to in
between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of signal losses that the port experiences has changed and dropped below the upper threshold boundary to a value within the acceptable range. Loss of signal generally indicates a physical problem.

Recommended Action Frequent loss of signal generally indicates a physical problem. Check both ends of your cable connection. Verify that the cable and small form-factor pluggables (SFPs) are not faulty.

FW-1517

Message

```
<Port Name> <Label>, has crossed lower threshold boundary to in between(High=<High
value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of protocol errors that the port experiences has changed and crossed the lower threshold boundary to a value within the acceptable range. Occasional protocol errors occur due to software glitches. Persistent protocol errors occur due to hardware problems.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1518

Message

```
<Port Name> <Label>, has dropped below upper threshold boundary to in
between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of protocol errors that the port experiences has changed and dropped below the upper threshold boundary to a value within the acceptable range. Occasional protocol errors occur due to software glitches. Persistent protocol errors occur due to hardware problems.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1519

Message

```
<Port Name> <Label>, has crossed lower threshold boundary to in between(High=<High
value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of invalid words that the port experiences has changed and crossed the lower threshold boundary to a value within the acceptable range. Invalid words usually indicate a hardware problem with a small form-factor pluggable (SFP) or cable.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1520

Message `<Port Name> <Label>, has dropped below upper threshold boundary to in between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of invalid words that the port experiences has changed and dropped the below upper threshold boundary to a value within the acceptable range. Invalid words usually indicate a hardware problem with a small form-factor pluggable (SFP) or cable.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1521

Message `<Port Name> <Label>, has crossed lower threshold boundary to in between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of invalid cyclic redundancy checks (CRCs) that the port experiences crossed the lower threshold boundary to a value within the acceptable range.

Recommended Action Frequent fluctuations in CRC errors generally indicate an aging fabric. Check your small form-factor pluggables (SFPs), cables, and connections for faulty hardware. Verify that all optical hardware is clean.

FW-1522

Message `<Port Name> <Label>, has dropped below upper threshold boundary to in between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of invalid cyclic redundancy checks (CRCs) that the port experiences has dropped below the upper threshold boundary to a value within the acceptable range.

Recommended Action Frequent fluctuations in CRC errors generally indicate an aging fabric. Check your small form-factor pluggables (SFPs), cables, and connections for faulty hardware. Verify that all optical hardware is clean.

FW-1523

Message `<Port Name> <Label>, has crossed lower threshold boundary to in between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the percentage of incoming traffic that the port experiences has changed and crossed the lower threshold boundary to a value within the acceptable range.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1524

Message `<Port Name> <Label>, has dropped below upper threshold boundary to in between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the percentage of incoming traffic that the port experiences has changed and dropped below the upper threshold boundary to a value within the acceptable range.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1525

Message `<Port Name> <Label>, has crossed lower threshold boundary to in between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the percentage of outgoing traffic that the port experiences has changed and crossed the lower threshold boundary to a value within the acceptable range.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1526

Message `<Port Name> <Label>, has dropped below upper threshold boundary to in between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the percentage of outgoing traffic that the port experiences has changed and dropped below the upper threshold boundary to a value within the acceptable range.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1527

Message `<Port Name> <Label>, has crossed lower threshold boundary to in between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of state changes that the port experiences has changed and crossed the lower threshold boundary to a value within the acceptable range. The state of the port has changed for one of the following reasons: the port has gone offline, has come online, is testing, is faulty, has become an E_Port, has become an F_Port, has segmented, or has become a trunk port.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1528

Message `<Port Name> <Label>, has dropped below upper threshold boundary to in between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of state changes that the port experiences has changed and dropped below the upper boundary to a value within the acceptable range. The state of the port has changed for one of the following reasons: the port has gone offline, has come online, is testing, is faulty, has become an E_Port, has become an F_Port, has segmented, or has become a trunk port.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1529

Message

```
<Port Name> <Label>, has crossed lower threshold boundary to in between(High=<High
value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of link resets that the port experiences has changed and crossed the lower threshold boundary to a value within the acceptable range. Link resets occur due to link timeout errors that indicate no frame activity at all. Both physical and hardware problems can cause link resets to increase.

Recommended Action

Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1530

Message

```
<Port Name> <Label>, has dropped below upper threshold boundary to in
between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of link resets that the port experiences has changed and dropped below the upper threshold boundary to a value within the acceptable range. Link resets occur due to link timeout errors that indicate no frame activity. Both physical and hardware problems can cause link resets to increase.

Recommended Action

Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-1531

Message

```
<Port Name> <Label>, has crossed lower threshold boundary to in between(High=<High
value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the number of C3 transmit timeout frames has crossed the lower threshold boundary and is in between the low and high thresholds.

Recommended Action

Check the target device; it could be slow.

FW-1532

Message
```
<Port Name> <Label>, has dropped below upper threshold boundary to in
between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of C3 transmit timeout frames has dropped below the upper threshold boundary and is in between the low and high thresholds.

Recommended Action Check the target device; it could be slow.

FW-1533

Message
```
<Port Name> <Label> has crossed lower threshold boundary to in between(High=<High
value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the trunk utilization crossed the lower threshold boundary to in between the low and high thresholds.

Recommended Action No action is required.

FW-1534

Message
```
<Port Name> <Label> has dropped below threshold upper boundary to in
between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the trunk utilization has dropped below the upper threshold boundary to in between the low and high thresholds.

Recommended Action No action is required.

FW-1535

Message `Fabric Watch has stopped portfencing feature for <Area String> loss area in <Port Name> class since FOS6.3. Disabling port fencing feature for this.`

Message Type LOG

Severity INFO

Probable Cause Indicates that Port Fencing is configured for link loss and synchronization loss in previous versions, but upgrading to a new version resets the bit because Port Fencing is not supported.

Recommended Action No action is required. You are informed that the Port Fencing bit is reset.

FW-2000

Message `FW Monitoring is disabled since MAPS is enabled.`

Message Type LOG

Severity INFO

Probable Cause Indicates that Fabric Watch is not monitoring the switch because MAPS is enabled.

Recommended Action Verify that the event was planned.

FW-3001

Message `Event: <Event Name>, Status: success, Info:<Event Related Info>.`

Message Type AUDIT

Class CFG

Severity INFO

Probable Cause Indicates that Port Fencing was enabled or disabled successfully.

Recommended Action No action is required.

FW-3010

Message `<Port Name> <Label> value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the circuit utilization has changed.

Recommended Action Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-3011

Message `<Port Name> <Label> is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the circuit utilization is below the low boundary threshold.

Recommended Action No action is required.

FW-3012

Message `<Port Name> <Label> is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the circuit utilization is above the high boundary threshold.

Recommended Action No action is required.

FW-3013

Message `<Port Name> <Label> is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the circuit utilization is between the high and low boundary thresholds.

Recommended Action No action is required.

FW-3014

Message `<Port Name> <Label> value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the packet loss that the circuit experiences has changed.

Recommended Action Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-3015

Message `<Port Name> <Label> is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the packet loss that the circuit experiences is below the low boundary threshold.

Recommended Action No action is required.

FW-3016

Message `<Port Name> <Label> is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the packet loss that the circuit experiences is above the high boundary threshold.

Recommended Action No action is required.

FW-3017

Message `<Port Name> <Label> is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the packet loss that the circuit experiences is between the low and high boundary thresholds.

Recommended Action No action is required.

FW-3018

Message `<Port Name> <Label> value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the number of state changes that the circuit experiences has changed. The state of the circuit has changed because the circuit has gone offline or the circuit has come online.

Recommended Action Respond to this message as is appropriate to the particular policy of the end-user installation.

FW-3019

Message

```
<Port Name> <Label> is below low boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates the number of state changes that the circuit experiences is below the low boundary level. The state of the circuit has changed because the circuit has gone offline or the circuit has come online.

Recommended Action

No action is required.

FW-3020

Message

```
<Port Name> <Label> is above high boundary(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates the number of state changes that the circuit experiences has increased above the high boundary threshold. The state of the circuit has changed because the circuit has gone offline, the circuit has come online, or the circuit is testing.

Recommended Action

No action is required.

FW-3021

Message

```
<Port Name> <Label> is between high and low boundaries(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates the number of state changes that the circuit experiences has increased above the high boundary threshold. The state of the circuit has changed because the circuit has gone offline, the circuit has come online, or the circuit is testing.

Recommended Action

No action is required.

FW-3022

Message `Timebase for <Key> is changed to Minute as Seconds is not supported.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the timebase for the class is changed implicitly to minutes because a seconds timebase is not supported.

Recommended Action No action is required.

HAM Messages

HAM-1001

Message `Standby CP is not healthy, device <device name> status BAD, Severity = <severity level>.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that a standby control processor (CP) device error is reported by the high availability manager (HAM) health monitor, with the specified device and severity level. The severity level can be critical, major, or minor.

The active CP will continue to function normally. Because the standby CP is not healthy, non-disruptive failover is not possible.

Recommended Action Restart the standby CP blade by ejecting the card and reseating it. If the problem persists, replace the standby CP.

HAM-1002

Message `Standby CP is healthy.`

Message Type LOG

Severity INFO

Probable Cause Indicates that all standby control processor (CP) devices monitored by the high availability manager (HAM) health monitor reported no error.

Recommended Action No action is required.

HAM-1004

Message `Processor rebooted - <Reboot Reason>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the switch has been restarted because of a user action or an error. The switch restart can be initiated by the **firmwareDownload**, **fastBoot**, **haFailover**, and **reboot** commands. Some examples of errors that may initiate this message are hardware errors, software errors, compact flash errors, or memory errors. The *Reboot Reason* variable can be one of the following:

- Hafailover
- Reset

- Fastboot
- Giveup Master:SYSM
- CP Faulty:SYSM
- FirmwareDownload
- ConfigDownload:MS
- ChangeWWN:EM
- Reboot:WebTool
- Fastboot:WebTool
- Software Fault:Software Watchdog
- Software Fault:Kernel Panic
- Software Fault:ASSERT
- Reboot:SNMP
- Fastboot:SNMP
- Reboot
- Chassis Config
- Reboot:API
- Reboot:HAM
- EMFault:EM

Recommended Action Execute the **errShow** command on both control processors (CPs) to view the error log for additional messages that may indicate reason for the switch restart.

HAM-1005

Message `HeartBeat Miss reached threshold.`

Message Type LOG

Severity INFO

Probable Cause Indicates that either the active CP Ethernet Media Access Controller (EMAC) or the standby CP is down. The active CP will run a diagnostic test on EMAC and will wait for the standby CP to reset it if it is down.

Recommended Action No action is required.

HAM-1006

Message `EMAC controller for Active CP is BAD.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the local Ethernet Media Access Controller (EMAC) on the active CP has been marked BAD as determined by the diagnostic test run by the high availability manager (HAM) module.

Recommended Action The standby CP will take over and reset the active CP. The system will be non-redundant because the standby CP becomes the active CP.

HAM-1007

Message `Need to reboot the system for recovery, reason: <reason name>.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the switch in current condition needs to be restarted to achieve a reliable recovery. The reasons can be one of the following:

- The standby CP was not ready when failover occurred.
- The failover occurred when the last logical switch (LS) transaction was incomplete.
- The switch failed when timeout occurred at certain stage.
- The cold or warm recovery has failed.

Recommended Action If auto-reboot is enabled, the switch will automatically restart. Otherwise, execute the **reboot** command to manually restart the switch.

HAM-1008

Message `Rebooting the system for recovery - auto-reboot is enabled.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the recovery by auto-reboot is enabled, and therefore the switch automatically restarts. This message is displayed if the event logged in HAM-1007 has occurred and auto-reboot is enabled.

Recommended Action Wait until the switch is up to perform any operations.

HAM-1009

Message `Need to MANUALLY REBOOT the system for recovery - auto-reboot is disabled.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the recovery by auto-restart is disabled, therefore the switch needs to be manually restarted for recovery. This message is displayed if the event logged in HAM-1007 has occurred and auto-reboot is disabled.

Recommended Action Execute the **reboot** command to restart the switch manually.

HAM-1010

Message `Maunually trigger haReboot/reboot for recovery from OOM when appropriate.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that out of memory (OOM) condition has been detected when the switch was not ready for warm recovery.

Recommended Action Manually trigger the switch restart for cold recovery, if needed; or wait until switch is ready for warm recovery and execute the **haReboot** or **haFailover** command.

HAM-1011

Message `haReboot is automatically triggered for warm recovery from OOM.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that out of memory (OOM) condition has been detected when switch was ready for warm recovery. The **haReboot** is automatically triggered.

Recommended Action No action is required. The **haReboot** is automatically triggered to recover from the OOM condition.

HAM-1013

Message `<error message>.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that the software watchdog has detected termination of a restartable daemon, but could not restart the daemon.

Recommended Action Manually initiate a restart or failover, if needed.

HAM-1014

Message `<error message>.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that the software watchdog has detected termination of a restartable daemon and needs to restart or initiate a failover.

Recommended Action Execute the **reboot** command to restart the system or initiate a failover by using the **haFailover** command.

HAM-1015

Message `<info message>.`

Message Type AUDIT

Class RAS

Severity INFO

Probable Cause Indicates that a terminated software component has been restarted.

Recommended Action No action is required.

HAMK Messages

HAMK-1001

Message `Warm Recovery Failed.`

Message Type LOG | FFDC

Severity CRITICAL

Probable Cause Indicates that the switch failed during the warm recovery.

Recommended Action This event triggers the switch restart automatically and attempts a cold recovery.

Execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

HAMK-1002

Message `Heartbeat down.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the active control processor (CP) blade determined that the standby CP blade is down. This can be a result of a user-initiated action such as firmware download, the standby CP blade being reset or removed, or an error in the standby CP blade.

Recommended Action Monitor the standby CP blade for a few minutes. If this message is due to a standby CP restart, the HAMK-1003 message will display after the standby CP is restarted.

If the standby CP does not connect to the active CP after 10 minutes, restart the standby CP blade by ejecting the blade and reseating it.

HAMK-1003

Message `Heartbeat up.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the active control processor (CP) blade detected the standby CP blade. This means that the standby CP blade is available to take over in case a failure happens in the active CP blade. Typically, this message is displayed when the standby CP blade restarts.

Recommended Action No action is required.

HAMK-1004

Message `Resetting standby CP (double reset may occur).`

Message Type LOG

Severity INFO

Probable Cause Indicates that the standby control processor (CP) is being reset due to a loss of heartbeat. Typically, this message is displayed when the standby CP has been restarted. Note that in certain circumstances, a CP may experience a double reset and restart twice. A CP can recover automatically even if it has restarted twice.

Recommended Action No action is required.

HIL Messages

HIL-1101

Message `Slot <slot number> faulted, <nominal voltage> (<measured voltage>) is above threshold.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the blade voltage is above threshold.

Recommended Action Replace the faulty blade or switch (for non-bladed switches).

HIL-1102

Message `Slot <slot number> faulted, <nominal voltage> (<measured voltage>) is below threshold.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the blade voltage is below threshold.

Recommended Action Replace the faulty blade or switch (for non-bladed switches).

HIL-1103

Message `Blower <blower number> faulted, <nominal voltage> (<measured voltage>) is above threshold.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the fan voltage is above threshold.

Recommended Action Run the **psShow** command to verify the power supply status.

Try to reseat the faulty fan field-replaceable units (FRUs) and power supply FRU to verify that they are seated properly.

If the problem persists, replace the fan FRU or the power supply FRU as necessary.

HIL-1104

Message

```
Blower <blower number> faulted, <nominal voltage> (<measured voltage>) is below
threshold.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that the fan voltage is below threshold.

Recommended Action

Run the **psShow** command to verify the power supply status.

Try to reseat the faulty fan field-replaceable units (FRUs) and power supply FRU to verify that they are seated properly.

If the problem persists, replace the fan FRU or the power supply FRU as necessary.

HIL-1105

Message

```
Switch error, <nominal voltage> (<measured voltage>) above threshold.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that the switch voltage is above threshold. This message is specific to non-bladed switches.

Recommended Action

For switches that do not have field-replaceable units (FRUs), replace the entire switch.

If the 12 volt level is faulty, replace one or both power supplies; if any other voltage is faulty, replace the entire switch.

HIL-1106

Message

```
Switch error, <nominal voltage> (<measured voltage>) below threshold.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that the switch voltage is below threshold. This message is specific to non-bladed switches.

Recommended Action

For switches that do not have field-replaceable units (FRUs), replace the entire switch.

If the 12 volt level is faulty, replace one or both power supplies; if any other voltage is faulty, replace the entire switch.

HIL-1107

Message `Switch faulted, <nominal voltage> (<measured voltage>) above threshold. System preparing for reset.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the switch voltage is above threshold. This message is specific to non-bladed switches.

Recommended Action For switches that do not have field-replaceable units (FRUs), replace the entire switch.

If the 12 volt level is faulty, replace one or both power supplies; if any other voltage is faulty, replace the entire switch.

HIL-1108

Message `Switch faulted, <nominal voltage> (<measured voltage>) below threshold. System preparing for reset.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the switch voltage is below threshold. This message is specific to non-bladed switches.

Recommended Action For switches that do not have field-replaceable units (FRUs), replace the entire switch.

If the 12 volt level is faulty, replace one or both power supplies; if any other voltage is faulty, replace the entire switch.

HIL-1201

Message `Blower <blower number>, speed (<measured speed> RPM) above threshold.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the fan speed (in RPM) has risen above the maximum threshold. A high speed does not necessarily mean that the fan is faulty.

Recommended Action Run the **tempShow** command to verify that the switch temperatures are within operational ranges. Refer to the hardware reference manual for the temperature range of your switch.

Make sure that the area is well-ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Run the **fanShow** command to monitor the speed of the fan generating this error.

If the fan continues to generate this message, replace the fan FRU.

HIL-1202

Message `Blower <blower number> faulted, speed (<measured speed> RPM) below threshold.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified fan speed (in RPM) has fallen below the minimum threshold.

Recommended Action Replace the fan FRU.

HIL-1203

Message `Fan <fan number> faulted, speed (<measured speed> RPM) above threshold.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified fan speed (in RPM) has risen above the maximum threshold. A high speed does not necessarily mean that the fan is faulty.

Recommended Action Run the **tempShow** command to verify that the switch temperatures are within operational ranges. Refer to the hardware reference manual for the temperature range of your switch.

Make sure that the area is well-ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Run the **fanShow** command to monitor the speed of the fan generating this error.

If the fan continues to generate this message, replace the fan FRU.

HIL-1204

Message `Fan <fan number> faulted, speed (<measured speed> RPM) below threshold.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified fan speed (in RPM) has fallen below the minimum threshold. This message is specific to non-bladed switches.

Recommended Action Replace the fan field-replaceable unit (FRU).

For switches that do not have FRUs, replace the entire switch.

HIL-1206

Message `Fan <fan number> sensor <sensor number> , speed (<measured speed> RPM) below threshold.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified fan speed (in RPM) has fallen below the minimum threshold. This problem can quickly cause the switch to overheat. This message is specific to non-bladed switches.

Recommended Action Replace the fan field-replaceable unit (FRU).

HIL-1207

Message `Fan <fan number> is faulty.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the fan is faulty.

Recommended Action Use the **tempShow** command to verify that the switch temperatures are within operational ranges. Refer to the hardware reference manual for the temperature range of your switch.

Make sure that the area is well-ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Use the **fanShow** command to monitor the status of the fan generating this error.

If the fan continues to generate this message, replace the switch because the fan is not field-replaceable.

HIL-1208

Message `Fan <fan number> is not faulty.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the fan is not faulty.

Recommended Action This can only occur on switches with non-removable fans. It follows a previous indication of faultiness.

If the fan continues to generate this message, it indicates oscillation between faulty and non-faulty behavior. Replace the switch because the fan is not field-replaceable.

HIL-1301

Message `1 blower failed or missing. Replace failed or missing blower assembly immediately.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a fan field-replaceable unit (FRU) has failed or has been removed. This message is often preceded by a low speed error message. This problem can cause the switch to overheat.

Recommended Action Replace the affected fan FRU immediately.

HIL-1302

Message `<count> blowers failed or missing. Replace failed or missing blower assemblies immediately.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that multiple fan field-replaceable units (FRUs) have failed or are missing on a switch. This message is often preceded by a low fan speed message.

Recommended Action Replace the affected fan FRUs immediately.

HIL-1303

Message `One fan failed. Replace failed fan FRU immediately.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that a fan field-replaceable unit (FRU) has failed. This message is often preceded by a low fan speed message.

Recommended Action Replace the faulty fan FRU immediately.

HIL-1304

Message `Two fans failed. Replace failed fan FRUs immediately.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that multiple fan field-replaceable units (FRUs) have failed. This message is often preceded by a low fan speed message.

Recommended Action Replace the faulty fan FRUs immediately.

HIL-1305

Message `One or two fans failed. Replace failed fan FRUs immediately.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that multiple fan field-replaceable units (FRUs) have failed. This message is often preceded by a low fan speed message.

Recommended Action Replace the faulty fan FRUs immediately.

HIL-1306

Message `Three fans failed. Replace failed fan FRUs immediately.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that three fan field-replaceable units (FRUs) have failed. This message is often preceded by a low fan speed message.

Recommended Action Replace the faulty fan FRUs immediately.

HIL-1307

Message `Four or five fans failed. Replace failed fan FRUs immediately.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that multiple fan field-replaceable units (FRUs) have failed. This message is often preceded by a low fan speed message.

Recommended Action Replace the faulty fan FRUs immediately.

HIL-1308

Message `All fans failed. Replace failed fan FRUs immediately.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that all fans have failed. This message is often preceded by a low fan speed message.

Recommended Action Replace the faulty fan field-replaceable units (FRUs) immediately.

HIL-1309

Message `<count> fan FRUs failed. Replace failed fan FRUs immediately.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that multiple fans have failed. This message is often preceded by a low fan speed message.

Recommended Action Replace the faulty fan field-replaceable units (FRUs) immediately.

HIL-1310

Message `<count> fan(s) faulty.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that multiple fans have failed. This message is often preceded by a low fan speed message.

Recommended Action Because the fans are not field-replaceable, replace the switch if the temperature is high.

HIL-1311

Message `No fans are faulty.`

Message Type LOG

Severity INFO

Probable Cause Indicates recovery from an earlier condition of one or more fans having failed.

Recommended Action This can only occur on switches with non-removable fans. It follows a previous indication of faultiness.

If the fan continues to generate this message, it indicates oscillation between faulty and non-faulty behavior. Replace the switch because the fan is not field-replaceable.

HIL-1401

Message `One fan FRU missing. Install fan FRU immediately.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a fan field-replaceable unit (FRU) has been removed.

Recommended Action Install the missing fan FRU.

HIL-1402

Message `Two fan FRUs missing. Install fan FRUs immediately.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that two fan field-replaceable units (FRUs) have been removed.

Recommended Action Install the missing fan FRUs immediately.

HIL-1403

Message `All fan FRUs missing. Install fan FRUs immediately.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that all fan field-replaceable units (FRUs) have been removed.

Recommended Action Install the missing fan FRUs immediately.

HIL-1404

Message `<count> fan FRUs missing. Install fan FRUs immediately.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that one or more fan field-replaceable units (FRUs) have been removed.

Recommended Action Install the missing fan FRUs immediately.

HIL-1501

Message `Slot <slot number>, high temperature (<measured temperature>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the temperature of this blade has risen above the warning threshold.

Recommended Action Run the **fanShow** command to verify all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

HIL-1502

Message `Slot <slot number>, high temperature (<measured temperature>). Unit will be shut down in 2 minutes if temperature remains high.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the temperature of this blade has risen above the critical threshold. This usually follows a high-temperature message.

Recommended Action Run the **fanShow** command to verify all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

If the message persists, replace the blade.

HIL-1503

Message `Slot <slot number>, unit shutting down.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the temperature of this blade has been above the maximum threshold for at least two minutes. The blade is shut down to prevent damage. This usually follows a high-temperature warning message.

Recommended Action Run the **fanShow** command to verify all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

If the message persists, replace the faulty blade.

HIL-1504

Message `System within normal temperature specifications (<measured temperature> C).`

Message Type LOG

Severity INFO

Probable Cause Indicates that temperatures in the system have returned to normal.

Recommended Action No action is required.

HIL-1505

Message

```
High temperature (<measured temperature> C), fan speed increasing per
environmental specifications.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that temperatures in the system have risen above the warning threshold and that the fan speed is being increased.

Recommended Action

Run the **fanShow** command to verify all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

HIL-1506

Message

```
High temperature (<measured temperature> C) exceeds system temperature limit.
System will shut down within 2 minutes.
```

Message Type

FFDC | LOG

Severity

CRITICAL

Probable Cause

Indicates that temperatures in the system have risen above the critical threshold.

Recommended Action

Run the **fanShow** command to verify that all fans are working properly. Replace any deteriorating fan field-replaceable units (FRUs).

Make sure that the area is well-ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

HIL-1507

Message

```
High temperature warning time expired. System preparing for shutdown.
```

Message Type

FFDC | LOG

Severity

CRITICAL

Probable Cause

Indicates that temperatures in the system have risen above the critical threshold.

Recommended Action

To avoid causing damage to the switch, the system shuts down automatically. To help prevent future problems, make sure that all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

HIL-1508

Message `Fan faulty warning time expired. System preparing for shutdown.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that temperatures in the system have remained above the critical threshold too long.

Recommended Action To avoid causing damage to the switch, the system shuts down automatically. To help prevent future problems, make sure that all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

HIL-1509

Message `High temperature (<measured temperature> C). Warning time expired. System preparing for shutdown.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that temperatures in the system have risen above the critical threshold.

Recommended Action To avoid causing damage to the switch, the system shuts down automatically. To help prevent future problems, make sure that all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

HIL-1510

Message `Current temperature (<measured temperature> C) is below shutdown threshold. System shutdown canceled.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that temperatures in the system have dropped below the critical threshold; the system can continue operation.

Recommended Action To help prevent future problems, make sure that all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

HIL-1511

Message `Fan speed increasing per environmental specifications.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that temperatures in the system have risen above the warning threshold and that the fan speed is being increased.

Recommended Action Run the **fanShow** command to verify all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

HIL-1512

Message `High temperature (<measured temperature> C), Exceeds environmental specifications.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that temperatures in the system have risen above the warning threshold.

Recommended Action Run the **fanShow** command to verify all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within the operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

HIL-1601

Message `Using backup temperature sensor. Attention needed.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that temperature readings from the primary sensor are out of range.

Recommended Action Run the **fanShow** command to verify that all fans are operating correctly. Replace any deteriorating fan field-replaceable units (FRUs).

Run the **tempShow** command to verify temperature values. If any sensor is too high, monitor the switch. Try rebooting or power cycling the switch.

HIL-1602

Message `Multiple temperature sensors failed. Service immediately.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that temperature readings from multiple sensors are out of range.

Recommended Action Run the **fanShow** command to verify that all fans are operating correctly. Replace any deteriorating fan field-replaceable units (FRUs).

Run the **tempShow** command to verify temperature values. If any sensor is too high, monitor the switch. Try rebooting or power cycling the switch.

HIL-1603

Message `<failure count> fans out of service. System is shutting down immediately.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the total fan failure count is greater than or equal to two.

Recommended Action To avoid causing damage to the switch, the system shuts down automatically. To help prevent future problems, make sure that all the fans are working properly.

HIL-1605

Message `High temperature (<measured temperature> C), fan speed increasing per environmental specifications.`

Message Type LOG

Severity INFO

Probable Cause Indicates that temperatures in the system have risen above the threshold and that the fan speed is being increased.

Recommended Action No action is required.

HIL-1610

Message `Fan/PS unit <Combo fan/power supply unit number> not supplying power, fan speeds may not be available. Please ensure that the unit has power and the switch is on.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the power supply is not connected to a power source, is not switched on, or the unit is faulty. This message is applicable only to the Brocade 5100, 6505, 6510, 6520, and VA-40FC.

Recommended Action Ensure the power cord is connected to the unit with a valid power source and then switch on the unit (if applicable). If the problem persists, try reseating the unit. If the problem still persists, replace the FRU.

HIL-1611

Message `MISMATCH in PSU-FAN Air Flow direction. Replace PSU with fan air flows in same direction. System will be shut down in 2 minutes.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the airflows of the power supply and fan assemblies are moving in the reverse or opposite direction, which could overheat the system. The airflow of the power supply and fan assemblies must move in the same direction or the system will shut down in two minutes. This message is applicable only to the Brocade 6510.

Recommended Action Use the **chassisShow** command to check the airflow directions of the power supply and fan assemblies. Ensure that the airflows run in the same direction.

HIL-1612

Message `MISMATCH in PSU-FAN Air Flow direction. System shut down.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that the airflows of the power supply and fan assemblies are moving in the reverse or opposite direction. The system will shut down immediately. This message is applicable only to the Brocade 6510.

Recommended Action Ensure that the airflows of the power supply and fan assemblies run in the same direction.

HIL-1613

Message `PSU-FAN FRUS Air Flow matched. System shutdown canceled.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the airflows of the power supply and fan assemblies have changed to move in the same direction. The system continues to operate. This message is applicable only to the Brocade 6510.

Recommended Action Ensure that the airflows of the power supply and fan assemblies run in the same direction.

HIL-1614

Message `MISMATCH in Fan airflow direction. Replace FRU with fan airflow in same direction.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the airflow of the fan is in the reverse direction. This may heat up the system.

Recommended Action Replace the fan field-replaceable units (FRUs) in such a manner that the air flows in the same direction as the remaining fans. Refer to the *Hardware Reference Manual* of your switch for instructions to replace the fan FRUs.

HIL-1615

Message `MISMATCH in PSU-Fan FRUs airflow direction. Replace PSU with fan airflow in same direction.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the airflow of the power supply unit (PSU) fan is in the reverse direction. This may heat up the system.

Recommended Action Replace the PSU fan field-replaceable unit (FRU) in such a manner that the air flows in the same direction as the remaining fans. Refer to the *Hardware Reference Manual* of your switch for instructions to replace the PSU fan FRU.

HIL-1650

Message `Unable to detect both WWN cards in chassis. Access to WWN halted.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that one or both of the World Wide Name (WWN) cards is missing. Both WWN cards must be present for normal operation.

Recommended Action Make sure both WWN cards are inserted.

HIL-1651

Message `On switch/slot <Slot Id>. WWN is corrupted on both cards.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that World Wide Name (WWN) is corrupted in one or both of the WWN cards. At least one WWN card must have a valid WWN for normal operation.

Recommended Action Contact your switch service provider for assistance.

HLO Messages

HLO-1001

Message `Incompatible Inactivity timeout <dead timeout> from port <port number>, correct value <value>.`

Message Type LOG | FFDC

Severity ERROR

Probable Cause Indicates that the hello (HLO) message was incompatible with the value specified in the fabric shortest path first (FSPF) protocol. The Brocade switch will not accept FSPF frames from the remote switch.

In Fabric OS, the HLO dead timeout value is not configurable, so this error can only occur when the Brocade switch is connected to a switch from another manufacturer.

Recommended Action The dead timeout value of the remote switch must be compatible with the value specified in the FSPF protocol. Refer to the documentation for the other manufacturer's switch to change this value.

HLO-1002

Message `Incompatible Hello timeout <HLO timeout> from port <port number>, correct value <correct value>.`

Message Type LOG | FFDC

Severity ERROR

Probable Cause Indicates that the hello (HLO) message was incompatible with the value specified in the fabric shortest path first (FSPF) protocol. The Brocade switch will not accept FSPF frames from the remote switch.

In Fabric OS, the HLO timeout value is not configurable, so this error can only occur when the Brocade switch is connected to a switch from another manufacturer.

Recommended Action The HLO timeout value of the remote switch must be compatible with the value specified in the FSPF protocol. Refer to the documentation for the other manufacturer's switch to change this value.

HLO-1003

Message

```
Invalid Hello received from port <port number>, Domain = <domain ID>, Remote Port
= <remote port ID>.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that the hello (HLO) message received was invalid and the frame was dropped. The Brocade switch will not accept fabric shortest path first (FSPF) frames from the remote switch.

The switch has received an invalid HLO because either the domain or port number in the HLO message has an invalid value. This error can only occur when the Brocade switch is connected to a switch from another manufacturer.

Recommended Action

The HLO message of the remote switch must be compatible with the value specified in the FSPF protocol. Refer to the documentation for the other manufacturer's switch to change this value.

HMON Messages

HMON-1001

Message `<Failure description>.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that there was a problem reading an essential file containing configuration information from the nonvolatile storage device. This could be the result of a missing file or a corrupt file system.

Recommended Action Execute the **firmwareDownload** command to reinstall the firmware to your switch.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

HSL Messages

HSL-1000

Message `HSL initialization failed.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates a hardware subsystem layer (HSL) initialization failure. This error is caused by other system errors.

Recommended Action Execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

HSL-1001

Message `Failed to acquire system MAC address pool.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates failure to acquire the system address. This error is caused by other system errors.

Recommended Action Execute the **errShow** command to view the error log for other system errors, and take appropriate corrective actions.

HSL-1002

Message `SFP for interface <InterfaceName> is inserted.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a small form-factor pluggable (SFP) transceiver has been inserted in the specified interface.

Recommended Action No action is required.

HSL-1003

Message `SFP for interface <InterfaceName> is removed.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a small form-factor pluggable (SFP) transceiver has been removed from the specified interface.

Recommended Action No action is required.

HSL-1004

Message `Incompatible SFP for interface <InterfaceName> is detected.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that an incompatible small form-factor pluggable (SFP) transceiver for the interface has been inserted.

Recommended Action Disable the interface using the **shutdown** command and insert an SFP transceiver that is supported on the interface. After the SFP transceiver is inserted, re-enable the interface using the **no shutdown** command.

HSL-1005

Message `Failed to initialize with FSS.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates a failure to initialize the Fabric OS State Synchronization (FSS) service. This error is caused by other system errors.

Recommended Action Execute the **errShow** command to view the error log for other system errors, and take appropriate corrective actions.

HSL-1006

Message `Failed to get kernel page size <PageSize> bytes for mmap.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that there is not enough contiguous kernel memory.

Recommended Action Execute the **errShow** command to view the error log for other system errors, and take appropriate corrective actions.

HSL-1007

Message `Failed to read SFP for interface <InterfaceName>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates failure to read the small form-factor pluggable (SFP) transceiver on the specified interface.

Recommended Action Disable the interface using the **shutdown** command and re-insert the SFP transceiver. After the SFP transceiver is inserted, re-enable the interface using the **no shutdown** command. If the problem persists, contact your switch service provider.

HTTP Messages

HTTP-1001

Message `Switch PID format has changed to <current PID format>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the port ID (PID) format was changed.

Recommended Action No action is required. For more information on PID format, refer to the *Fabric OS Administrator's Guide*.

HTTP-1002

Message `Zoning transaction initiated by User: <User Name>, Role: <User Role> completed successfully.`

Message Type AUDIT | LOG

Class ZONE

Severity INFO

Probable Cause Indicates that the zoning database has been changed.

Recommended Action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

HTTP-1003

Message `Zoning transaction initiated by User: <User Name>, Role: <User Role> could not be completed successfully - <Reason Message>.`

Message Type AUDIT | LOG

Class ZONE

Severity INFO

Probable Cause Indicates an error in completing the zoning transaction because of the specified reason.

Recommended Action Check the ZONE events in the error message log by using the **errShow** command, and take appropriate corrective actions.

IBD Messages

IBD-1000

Message

```
Slot <slot number> Port GE<port number>: Maximum attempts to restart failed.
Disabling port.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that the specified port has crashed unexpectedly and restarting attempts have failed.

Recommended Action

Power cycle the blade using the **slotPowerOff** and **slotPowerOn** commands.

IPAD Messages

IPAD-1000

Message
```
<Type of managed entity>/<Instance number of managed entity> <Type of network
interface>/<Instance number of network interface> <Protocol address family>
<Source of address change> <Value of address and prefix> DHCP <DHCP enabled or
not>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the local IP address has been changed manually or it was reconfigured automatically by the Dynamic Host Configuration Protocol (DHCP) server.

Recommended Action No action is required.

IPAD-1001

Message
```
<Type of managed entity>/<Instance number of managed entity> <Protocol address
family> <Source of address change> <Value of address> DHCP <DHCP enabled or not>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the gateway IP address has been changed manually or it was reconfigured automatically by the Dynamic Host Configuration Protocol (DHCP) server.

Recommended Action No action is required.

IPAD-1002

Message
```
Switch name has been successfully changed to <Switch name>.
```

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates that the switch name has been changed.

Recommended Action No action is required.

IPAD-1003

Message `DNS parameters saved successfully.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Domain Name System (DNS) parameters are saved successfully.

Recommended Action No action is required.

IPAD-1004

Message `DNS parameters removed successfully.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Domain Name System (DNS) parameters are removed successfully.

Recommended Action No action is required.

IPS Messages

IPS-1001

Message `<message> FTR_AFA/FTR_AE License Not Installed (<error>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that either Advanced FICON Acceleration (FTR_AFA) or Advanced Extension (FTR_AE) license is not installed or assigned to the slot.

Recommended Action Run the **licenseShow** command to verify the slot-based licenses are installed on the switch. Contact your switch supplier for an appropriate slot-based license. Run the **licenseAdd** and **licenseSlotCfg** commands to add the license to your switch and activate it.

IPS-1002

Message `Failed to initialize <module> rc = <error>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the initialization of a module within the IPS daemon failed.

Recommended Action Download a new firmware version using the **firmwareDownload** command.

IPS-1003

Message `<function name>: Failed to allocate memory while performing <message>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that memory resources are low. This may be a transient problem.

Recommended Action Check the memory usage on the switch using the **memShow** command.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

IPS-1004

Message `Port Config Mode Mismatch slot (<slot>) port(ge<port>): current mode is (<current mode>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that configured port mode is different from the intended use.

Recommended Action Change the port configuration (by deleting configured FCIP tunnels or iSCSI sessions) to return the port mode to neutral before attempting to configure the port for a different mode or use.

IPS-1005

Message `Tunnel Authorization Failure for slot (<slot>) port(ge<port>) tunnel ID(<tunnel number>) reason (<reason>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that tunnel setup failed because of an authorization failure from the remote side. A reason for such a failure could be a WWN mismatch.

Recommended Action Change the tunnel configuration on one side of the tunnel to authorize the remote side to set up the tunnel.

IPS-1006

Message `Tunnel Configuration Mismatch for slot (<slot>) port(<port>) tunnel ID(<tunnel number>) reason (<reason>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that tunnel setup failed because of a configuration mismatch between the two ends. The *reason* field indicates the cause for configuration mismatch.

Recommended Action Change the tunnel configuration on one side of the tunnel to match that of the other side to set up the tunnel.

IPS-1007

Message `FX8-24 blade (<slot>) is not at the correct revision. Unable to use IPSec on FCIP Tunnel (<port>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the tunnel configuration failed because the FX8-24 blade is not at the correct revision to support IPSec enabled tunnels on VEs 22-31.

Recommended Action Contact your switch vendor to acquire the correct hardware revision blade.

ISNS Messages

ISNS-1001

Message `Configuration peering with external iSNS server <New config iSNS server IP address> slot/port <New config Slot number>/ge<New config port number> (current <Current iSNS server IP address> <Current slot number>/ge<Current port number>).`

Message Type LOG

Severity INFO

Probable Cause Indicates that a user has issued the **isnscCfg** command.

Recommended Action No action is required.

ISNS-1002

Message `Start peering with external iSNS server <iSNS server IP address> slot/port <Slot number>/ge<Port number>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that peering has started with the specified external Internet Storage Name Service (iSNS) server.

Recommended Action No action is required.

ISNS-1003

Message `Peering with external iSNS server is disabled.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the IP address of the Internet Storage Name Service (iSNS) server is zero. Therefore, peering is disabled.

Recommended Action If you wish to enable the iSNS server, use the **isnscCfg** command to show or set the server IP address; otherwise, no action is required.

ISNS-1004

Message `Timeout refreshing iSNS database with iSNS server <iSNS server IP address> slot/port <Slot number>/ge<Port number> Reg-Period <Registration-Period in seconds>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Internet Storage Name Service (iSNS) client fails to receive a successful response for a DevAttrQry within the specified registration period.

Recommended Action Verify the connection of the iSNS server to the slot and port.

ISNS-1005

Message `User request re-register with external iSNS server <iSNS server IP address> slot/port <Slot number>/ge<Port number>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a user has requested to re-register with the specified external Internet Storage Name Service (iSNS) server.

Recommended Action No action is required.

ISNS-1006

Message `Start re-register with external iSNS server <iSNS server IP address> slot/port <Slot number>/ge<Port number>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the re-register with the specified external Internet Storage Name Service (iSNS) server has started.

Recommended Action No action is required.

ISNS-1008

Message `Peering with external iSNS server <iSNS server IP address> not started because configuration unchanged.`

Message Type LOG

Severity INFO

Probable Cause Indicates that peering with the external Internet Storage Name Service (iSNS) server was already started with the same configuration.

Recommended Action No action is required. You may change the configuration and retry the peering with the external iSNS server.

ISNS-1009

Message `Peering with external iSNS server <iSNS server IP address> not started because no virtual targets found.`

Message Type LOG

Severity INFO

Probable Cause Indicates that no virtual targets were found, and therefore peering was not started.

Recommended Action No action is required. Peering will resume automatically when virtual targets are detected.

ISNS-1010

Message `Slot/port <Slot>/ge<Port> is out of range.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the slot or port is out of range.

Recommended Action Retry with a valid slot and port. Refer to the appropriate hardware reference manual for valid slot and port ranges.

ISNS-1011

Message `iSNS Client Service is <iSNS client State (enabled/disabled)>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the current state of the Internet Storage Name Service (iSNS) client is enabled or disabled.

Recommended Action No action is required. Use the **fosConfig** command to display, enable, or disable the iSNS client service.

ISNS-1013

Message `iSNS server connection failure.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Internet Storage Name Service (iSNS) client failed to establish a connection with the iSNS server.

Recommended Action Verify the connection of the iSNS server to the slot and port.

Use the **isnscCfg** command to display or correct the server IP address.

ISNS-1014

Message `Start peering with external iSNS server <iSNS server IP address> on management port.`

Message Type LOG

Severity INFO

Probable Cause Indicates that peering has started with the specified external Internet Storage Name Service (iSNS) on the management port.

Recommended Action No action is required.

KAC Messages

KAC-1002

Message `KAC(<Key Vault Type>) communication Error: Error connecting to <Backup or Primary>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the Key Archive Client (KAC) is unable to communicate with the primary or backup key vault.

Recommended Action Determine whether the configured key vault is operational; if not, change the switch key vault settings or resolve the operational problem at the key vault.

KAC-1004

Message `KAC <Operation Description> to Key Vault failed.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the Key Archive Client (KAC) is unable to do the specified operation to the primary or backup key vault.

Recommended Action Determine whether the configured key vault is operational; if not, change the switch key vault settings or resolve the operational problem at the key vault.

KAC-1006

Message `Switch to Key Vault trustee link was not established.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the trustee link was not established between the switch and the key vault.

Recommended Action Establish a trustee link between the switch and the key vault. Refer to the *Fabric OS Encryption Administrator's Guide* for instructions to establish a trusted link.

KAC-1007

Message `KAC key archival operation to Key Vault failed, LUN=<LUN Number>, keyID=<Key ID Value>, errno=<Error Number>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Key Archive Client (KAC) is unable to archive the key to primary or backup key vault.

Recommended Action Determine whether the configured key vault is operational; if not, change the switch key vault settings or resolve the operational problem at the key vault.

KAC-1008

Message `Putting of TEP failed. Check if there is already an unapproved TEP, then delete it. Error code=<Error code from LKM>, string=<Error string>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that there was already a pending unapproved Trusted link Establishment Package (TEP) at the Lifetime Key Manager (LKM).

Recommended Action Log in to LKM and delete the unapproved TEP.

KAC-1009

Message `Primary(<Primary Keyvault IP Address>) and Backup(<Backup Keyvault IP Address>) Key Vaults are not in sync. Detected key mismatch with KeyID = <KeyID>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the primary and backup key vault contents are not in sync.

Recommended Action Synchronize the contents of the primary and backup key vaults using instructions provided by the key vault provider.

KAC-1010

Message `Archival for KeyID <KeyID> failed to <Keyvault IP Address>. Error code=<Error code>, string=<Error string>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that archiving of Data Encryption Key (DEK) to the key vault failed.

Recommended Action No action is required.

KAC-1011

Message `Archival of Dummy DEK to the KV <Keyvault IP Address> failed. Dummy DEK: <Dummy Key Id>, KeyCount: <Key Count>. Error code=<Error code>, string=<Error string>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that archiving of dummy Data Encryption Key (DEK) to the key vault failed.

Recommended Action No action is required.

KAC-1012

Message `Retrieval of Dummy DEK from the KV <Keyvault IP Address> failed. Dummy DEK: <Dummy Key Id>, KeyCount: <Key Count>. Error code=<Error code>, string=<Error string>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that retrieving of dummy Data Encryption Key (DEK) from the key vault failed.

Recommended Action No action is required.

KAC-1013

Message `Archival of the Actual DEK to the KV <Keyvault IP Address> failed. Actual Key: <Actual Key Id>. Error code=<Error code>, string=<Error string>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that archiving of actual Data Encryption Key (DEK) to the key vault failed.

Recommended Action No action is required.

KAC-1014

Message `Retrieval of Actual DEK from the KV <Keyvault IP Address> failed. Actual Key: <Actual Key Id>. Error code=<Error code>, string=<Error string>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that retrieving of actual Data Encryption Key (DEK) from the key vault failed.

Recommended Action No action is required.

KAC-1015

Message `KAC(<Key Vault Type>) communication Error: Error connecting to <Key Vault IP>. Error code=<Error code>, string=<Error string>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the Key Archive Client (KAC) is unable to communicate with the primary or backup key vault.

Recommended Action Change the switch key vault settings and make sure the configured key vault is operational.

KAC-1016

Message

```
Error: Key ID mismatched in request/response. Requested key ID <Key ID in
response> and key in response <Requested Key Id>. Error code=<Error code>,
string=<Error string>.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates a mismatch between the requested key ID and the key in the response from the key vault.

Recommended Action Determine whether the configured key vault is operational; if not, change the switch key vault settings or resolve the operational problem at the key vault.

KAC-1017

Message

```
Error: KV parameter [<param name>] configured on BES is not supported by the Key
Vault. Please fix the configuration of the parameter to ensure key operations
function as expected.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates a mismatch between the configured key vault parameters on the Brocade Encryption Switch (BES) and the functionality supported by the key vault.

Recommended Action De-register the key vaults, set the correct value for key vault parameter, and re-register the key vaults.

KAC-1018

Message

```
KAC(<Key Vault Type>) communication to <Backup or Primary> restored.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that Key Archival Client communication with the *primary* or *backup* key vault is restored.

Recommended Action None

KSWD Messages

KSWD-1001

Message `<Software component>:<Software component Process ID> failed to refresh (<Current time>:<Refresh time>).`

Message Type FFDC | LOG

Severity WARNING

Probable Cause Indicates that one of the critical daemons is found to be unresponsive. An abort signal is sent.

Recommended Action Copy the warning message along with any core file information and contact your switch service provider.

KSWD-1002

Message `Detected termination of process <Software component>:<Software component Process ID>.`

Message Type FFDC | LOG

Severity WARNING

Probable Cause Indicates that a process on the switch has ended unexpectedly.

Recommended Action Copy the warning message along with any core file information and contact your switch service provider.

KTRC Messages

KTRC-1001

Message `Dump memory size exceeds dump file size.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the dump memory size has exceeded the dump file size.

Recommended Action Execute the **supportSave** command and reload the switch. If the problem persists, contact your switch service provider.

KTRC-1002

Message `Concurrent trace dumping.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the initial background dump has not completed.

Recommended Action No action is required.

KTRC-1003

Message `Cannot open ATA dump device.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the advanced technology attachment (ATA) dump driver is not initialized properly.

Recommended Action Execute the **supportSave** command and reload the switch. If the problem persists, contact your switch service provider.

KTRC-1004

Message `Cannot write to ATA dump device.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the write boundary in the advanced technology attachment (ATA) dump device has been exceeded.

Recommended Action Execute the **supportSave** command and reload the switch. If the problem persists, contact your switch service provider.

KTRC-1005

Message `Trace initialization failed. <Reason initialization failed>. <Internal error code>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that trace was unable to initialize.

Recommended Action Execute the **supportSave** command and reload the switch. If the problem persists, contact your switch service provider.

L2SS Messages

L2SS-1001

Message `Linux socket error - error reason: <reason>, socket name: <socketname>, error name: <errorname>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that an error has occurred in the Linux socket.

Recommended Action Reboot or power cycle the switch.

L2SS-1002

Message `Initialization error: <reason>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the Layer 2 system (L2SYS) encountered an error during initialization.

Recommended Action Reboot or power cycle the switch.

L2SS-1003

Message `Message Queue Error: Message queue create failed.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the Layer 2 system (L2SYS) encountered system service manager (SSM) message queue errors.

Recommended Action Reboot or power cycle the switch.

L2SS-1004

Message `FDB error: Error in creating AVL tree.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the Layer 2 system (L2SYS) has encountered an error while initializing the AVL tree.

Recommended Action Reboot or power cycle the switch.

L2SS-1005

Message `MAC-address-table hash failed even after two attempts for slot <slot> chip <chip>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the media access control (MAC) address table hash failed even after two hash changes on the specified chip.

Recommended Action Reboot or power cycle the switch.

L2SS-1006

Message `MAC-address-table table on slot <Slot_id> chip <Chip_id> is 95 percent full.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the media access control (MAC) address table on the chip is 95 percent full.

Recommended Action Clear some of the entries using the **no mac-address-table static** command or wait until the old entries age out.

L2SS-1007

Message `MAC-address-table on slot <Slot_id> chip <Chip_id> is less than 90 percent full.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the media access control (MAC) address table on the specified chip is less than 90 percent full.

Recommended Action No action is required. The Layer 2 system (L2SYS) starts learning the entries.

L2SS-1008

Message `Hardware GID limit reached on chip <Chip_id>, GID limit at <Max_gid>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that all dynamic group IDs (GIDs) are allocated.

Recommended Action Clear some of the ACL entries using the **clear counters access-list mac** command.

L3SS Messages

L3SS-1004

Message

```
<Function Name>, <Line No>: HW/Driver Error (possibly the CAM is full): <HW Error
Message>, rc=<Error Code>.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates an error in the hardware or the driver of the Layer 3 subsystem (L3SS). L3SS may have passed invalid parameters or the hardware Content Addressable Memory (CAM) may be full.

Recommended Action

Retry or clear the CAM.

LACP Messages

LACP-1001

Message `<module> Error opening socket (<error>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates that initialization of the specified module within the Link Aggregation Control Protocol (LACP) daemon has failed.

Recommended Action Download a new firmware using the **firmwareDownload** command.

LACP-1002

Message `<msg>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that some of the fields received in the Link Aggregation Control Protocol Data Unit (LACPDU) are invalid.

Recommended Action No action is required.

LANCE Messages

LANCE-1000

Message

```
Slot <slot number> Port GE<port number>: Maximum attempts to restart failed.
Disabling port.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that the specified port has crashed unexpectedly and restarting attempts have failed.

Recommended Action

Power cycle the blade using the **slotPowerOff** and **slotPowerOn** commands.

LFM Messages

LFM-1001

Message `The Logical Fabric Manager service is disabled.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Logical Fabric Manager service is disabled. Note that the Logical Fabric Manager service is enabled by the factory setting and it is not user-configurable.

Recommended Action No action is required.

LFM-1002

Message `The Logical Fabric Manager service is enabled.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Logical Fabric Manager service is enabled. Note that the Logical Fabric Manager service is enabled by the factory setting and it is not user-configurable.

Recommended Action No action is required.

LFM-1003

Message `The Logical Fabric Manager configuration is set to default.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Logical Fabric Manager configuration is set to default. This will remove all prior Logical Fabric Manager configurations. This operation is not supported currently.

Recommended Action No action is required.

LFM-1004

Message `HA is out of sync for opcode <HA OPCODE>, error value <error value>.`

Message Type LOG | FFDC

Severity CRITICAL

Probable Cause Indicates loss of high availability (HA) sync with remote control processor (CP).

Recommended Action Collect the supportsave information using the **supportsave** command and contact the Brocade technical support.

LFM-1005

Message `Logical port <portnum> disabled with reason <reason code>(<reason string>)`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the specified logical port is disabled for an internal logging purpose. This could be due to port segmentation.

Recommended Action Check the reason for port disable using the **switchShow** command, and take appropriate corrective action.

LFM-1006

Message `The switch with domain <domain> with firmware version <version> has joined the FID <FID> fabric and may not be compatible with XISL use.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the firmware version on the specified switch is not compatible with XISL.

Recommended Action Check the release notes to verify if this firmware is compatible with XISL. If it is not, remove the switch from the fabric.

LOG Messages

LOG-1000

Message `Previous message repeated <repeat count> time(s).`

Message Type LOG

Severity INFO

Probable Cause Indicates that the previous message was repeated the specified number of times.

Recommended Action No action is required.

LOG-1001

Message `A log message was dropped.`

Message Type LOG | FFDC

Severity WARNING

Probable Cause Indicates that a log message was dropped. A trace dump file has been created.

Recommended Action Execute the **reboot** command for non-bladed switches or the **haFailover** command on bladed switches.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

LOG-1002

Message `A log message was dropped.`

Message Type FFDC | LOG

Severity WARNING

Probable Cause Indicates that a message was not recorded by the error logging system. A trace dump file has been created. The message may still be visible through Simple Network Management Protocol (SNMP) or other management tools.

Recommended Action Execute the **reboot** command for non-bladed switches or the **haFailover** command on bladed switches.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

LOG-1003

Message `The log has been cleared.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the persistent error log has been cleared.

Recommended Action No action is required.

LOG-1004

Message `Log message <Log message that has been blocked> flooding detected and blocked.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a message has been flooding and was blocked.

Recommended Action Execute the **reboot** command.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

LOG-1005

Message `Log message <Log message that has been disabled> has been disabled.`

Message Type AUDIT | LOG

Class RAS

Severity INFO

Probable Cause Indicates that the specified message has been disabled from logging.

Recommended Action No action is required.

LOG-1006

Message `Log message <Log message that has been enabled> has been enabled.`

Message Type AUDIT | LOG

Class RAS

Severity INFO

Probable Cause Indicates that the specified message has been enabled for logging.

Recommended Action No action is required.

LOG-1007

Message `Log Module <Log Module that has been disabled> has been disabled.`

Message Type AUDIT | LOG

Class RAS

Severity INFO

Probable Cause Indicates that the specified module has been disabled from logging.

Recommended Action No action is required.

LOG-1008

Message `Log Module <Log Module that has been enabled> has been enabled.`

Message Type AUDIT | LOG

Class RAS

Severity INFO

Probable Cause Indicates that the specified module has been enabled for logging.

Recommended Action No action is required.

LOG-1009

Message `Internal Log message <Log message that has been enabled to be sent to syslog server> has been enabled for syslog logging.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified internal message has been enabled for syslog logging.

Recommended Action No action is required.

LOG-1010

Message `Internal Log message <Log message that has been disabled from being sent to syslog server> has been disabled from syslog logging.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified internal message has been disabled from syslog logging.

Recommended Action No action is required.

LOG-1011

Message `Log Message <Log Message Id> severity has been changed to <Severity>.`

Message Type AUDIT | LOG

Class RAS

Severity INFO

Probable Cause Indicates that the severity level of the specified log message has been changed.

Recommended Action No action is required.

LSDB Messages

LSDB-1001

Message `Link State ID <link state ID> out of range.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified link state ID is out of the acceptable range. The valid link state ID is the same as the valid domain ID, with a range from 1 through 239. The switch will discard the record because it is not supported.

Recommended Action No action is required.

LSDB-1002

Message `Local Link State Record reached max incarnation.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the local link state record (LSR) reached the maximum number of incarnations.

An "incarnation" is a progressive number that identifies the most recent version of the link state record (LSR). The switch generates its local LSR when first enabled. The incarnation number will begin again at 0x80000001 after reaching 0x7FFFFFFF.

Recommended Action No action is required.

LSDB-1003

Message `No database entry for local Link State Record, domain <local domain>.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that there is no local link state record (LSR) entry in the link state database (LSDB). The switch should always generate its own local entry when starting up.

An "incarnation" is a progressive number that identifies the most recent version of the LSR. The switch generates its local LSR when first enabled. By disabling and enabling the switch, a new local LSR is generated.

Recommended Action Run the **switchDisable** and **switchEnable** commands. A new local LSR is generated during the switch enable.

LSDB-1004

Message `No Link State Record for domain <local domain>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that there is no link state record (LSR) for the specified local domain.

Recommended Action No action is required. The other switch will pass the LSR after the fabric is stable.

MAPS Messages

MAPS-1001

Message
```
<object>, Condition=<condition>, Current Value:<ms, values, units>,
RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.
```

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

MAPS-1002

Message
```
<object>, Condition=<condition>, Current Value:<ms, values, units>,
RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

MAPS-1003

Message
```
<object>, Condition=<condition>, Current Value:<ms, values, units>,
RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

MAPS-1004

Message `<object>, Condition=<condition>, Current Value:<ms, values, units>, RuleName=<Rule name>, Dashboard Category=<Dashboard Category>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified rule has been triggered because the errors are above the configured threshold.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

MAPS-1010

Message `Port(s) fenced due to RuleName=<Rule name>, Condition=<condition>, Obj:<object> <ms, values, units>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified rule has been triggered because the errors are above the configured threshold, and therefore the specified ports are fenced.

Recommended Action Respond to this message as is appropriate to the particular policy of the end-user installation.

MAPS-1011

Message `Port(s) decommissioned due to RuleName=<Rule name>, Condition=<condition>, Obj:<object> <ms, values, units>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified rule has been triggered because the errors are above the configured threshold, and therefore the specified ports are fenced.

Recommended Action Respond to this message as is appropriate to the particular policy of the end-user installation.

MAPS-1012

Message `Port decommission action failed on port <object>, with reason string, <reason>`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the port decommission has failed on an object.

Recommended Action Respond to this message as is appropriate to the particular policy of the end-user installation.

MAPS-1020

Message `Switch wide status has changed from <Previous state> to <Current state>.`

Message Type LOG | AUDIT

Class MAPS

Severity WARNING

Probable Cause Indicates that the switch is not in a healthy state. This occurred because of a rule violation.

Recommended Action Check the accompanying RASLog messages to determine the cause of the state change.

MAPS-1021

Message `RuleName=<Rule name>, Condition=<condition>, Obj:<object, units> <Old state> has contributed to switch status <New state>.`

Message Type LOG | AUDIT

Class MAPS

Severity WARNING

Probable Cause Indicates that the switch status has changed to a healthy state. This occurred because none of the factors are violated.

Recommended Action No action is required.

MAPS-1100

Message `Rule <Rule name> is created.`

Message Type LOG | AUDIT

Class MAPS

Severity INFO

Probable Cause Indicates that the specified rule was created in the system.

Recommended Action Make sure the configuration change is expected.

MAPS-1101

Message `Rule <Rule name> is deleted.`

Message Type LOG | AUDIT

Class MAPS

Severity INFO

Probable Cause Indicates that the specified rule was deleted from the system.

Recommended Action Make sure the configuration change is expected.

MAPS-1102

Message `Rule <Rule name> is modified.`

Message Type LOG | AUDIT

Class MAPS

Severity INFO

Probable Cause Indicates that the specified rule was modified in the system.

Recommended Action Make sure the configuration change is expected.

MAPS-1110

Message `Policy <Policy name> is created.`

Message Type LOG | AUDIT

Class MAPS

Severity INFO

Probable Cause Indicates that the specified policy was created in the system.

Recommended Action Make sure the configuration change is expected.

MAPS-1111

Message `Policy <Policy name> is deleted.`

Message Type LOG | AUDIT

Class MAPS

Severity INFO

Probable Cause Indicates that the specified policy was deleted from the system.

Recommended Action Make sure the configuration change is expected.

MAPS-1112

Message `Policy <Source Policy name> cloned to <Target Policy name>.`

Message Type LOG | AUDIT

Class MAPS

Severity INFO

Probable Cause Indicates that the specified policy was cloned in the system.

Recommended Action Make sure the configuration change is expected.

MAPS-1113

Message `Policy <Policy name> activated.`

Message Type LOG | AUDIT

Class MAPS

Severity INFO

Probable Cause Indicates that the specified policy was activated in the system.

Recommended Action Make sure the configuration change is expected.

MAPS-1114

Message `Rule <Rule name> added to Policy <Policy name>.`

Message Type LOG | AUDIT

Class MAPS

Severity INFO

Probable Cause Indicates that the specified rule was added to the specified policy.

Recommended Action Make sure the configuration change is expected.

MAPS-1115

Message `Rule <Rule name> deleted from Policy <Policy name>.`

Message Type LOG | AUDIT

Class MAPS

Severity INFO

Probable Cause Indicates that the specified rule was deleted from the specified policy.

Recommended Action Make sure the configuration change is expected.

MAPS-1116

Message `Policy <Policy name> updated.`

Message Type LOG | AUDIT

Class MAPS

Severity INFO

Probable Cause Indicates that the specified policy was updated.

Recommended Action Make sure the configuration change is expected.

MAPS-1120

Message `Group <Group name> created.`

Message Type LOG | AUDIT

Class MAPS

Severity INFO

Probable Cause Indicates that the specified group was created.

Recommended Action Make sure the configuration change is expected.

MAPS-1121

Message `Group <Group name> deleted.`

Message Type LOG | AUDIT

Class MAPS

Severity INFO

Probable Cause Indicates that the specified group was deleted.

Recommended Action Make sure the configuration change is expected.

MAPS-1122

Message `Group <Source group name> cloned to <Target group name>.`

Message Type LOG | AUDIT

Class MAPS

Severity INFO

Probable Cause Indicates that the specified group was cloned.

Recommended Action Make sure the configuration change is expected.

MAPS-1123

Message `Group <Group name> modified.`

Message Type LOG | AUDIT

Class MAPS

Severity INFO

Probable Cause Indicates that the specified group was modified.

Recommended Action Make sure the configuration change is expected.

MAPS-1124

Message `Flow <Flow name> imported.`

Message Type LOG | AUDIT

Class MAPS

Severity INFO

Probable Cause Indicates that the specified flow from Flow Vision is imported into MAPS.

Recommended Action Make sure the configuration change is expected.

MAPS-1125

Message `Flow <Flow name> deimported.`

Message Type LOG | AUDIT

Class MAPS

Severity INFO

Probable Cause Indicates that the specified flow was removed from MAPS.

Recommended Action Make sure the configuration change is expected.

MAPS-1126

Message `Imported flow <Flow name> is a stale flow or currently does not exist in flow vision.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified flow does not exist in Flow Vision.

Recommended Action Make sure the configuration change is expected.

MAPS-1127

Message `Imported flow <Flow name> is initialized as stale flow because it is <Flow description>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that MAPS has imported the specified flow present in the configuration and initialized it as stale flow due to the mentioned reason.

Recommended Action Make sure the configuration change is expected.

MAPS-1130

Message `Actions <List of actions configured> configured.`

Message Type LOG | AUDIT

Class MAPS

Severity INFO

Probable Cause Indicates that the specified list of actions are configured.

Recommended Action Make sure the configuration change is expected.

MAPS-1131

Message `Monitoring on members <List of members/objects > of type <Type of members/objects> is paused.`

Message Type LOG | AUDIT

Class MAPS

Severity INFO

Probable Cause Indicates that monitoring on the specified list of members is paused.

Recommended Action Make sure the configuration change is expected.

MAPS-1132

Message `Monitoring on members <List of members/objects > of type <Type of members/objects> has resumed.`

Message Type LOG | AUDIT

Class MAPS

Severity INFO

Probable Cause Indicates that monitoring on the specified list of members has resumed.

Recommended Action Make sure the configuration change is expected.

MAPS-1200

Message `Fabric Watch Thresholds are converted to MAPS policies.`

Message Type LOG | AUDIT

Class MAPS

Severity INFO

Probable Cause Indicates that the current Fabric Watch configuration has converted to corresponding MAPS policies.

Recommended Action Verify the MAPS policies and make sure the rules are valid before enabling MAPS.

MAPS-1201

Message `MAPS has started monitoring with <Policy name> policy and Fabric Watch is disabled from monitoring.`

Message Type LOG | AUDIT

Class MAPS

Severity INFO

Probable Cause Indicates that MAPS has started monitoring the system and therefore Fabric Watch monitoring has been disabled.

Recommended Action Make sure the configuration change is expected.

MAPS-1202

Message `MAPS Disabled.`

Message Type LOG | AUDIT

Class MAPS

Severity INFO

Probable Cause Indicates that MAPS has been disabled. MAPS will continue to monitor the system until reboot or High Availability (HA) failover.

Recommended Action Make sure the configuration change is expected. To activate Fabric Watch monitoring and disable MAPS, reboot or fail over the system.

MAPS-1203

Message `dashboard <data type> data has been cleared.`

Message Type LOG | AUDIT

Class MAPS

Severity WARNING

Probable Cause Indicates that the dashboard has been cleared.

Recommended Action No action is required.

MCAST_SS Messages

MCAST_SS-1001

Message `Socket Error: <op> (<reason>) for socket <sockname> the error code <errorname>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that an error has occurred in the Linux socket.

Recommended Action Restart the multicast subsystem (MCAST_SS) daemon.

MCAST_SS-1002

Message `Socket Error: <op> sock name <sock> Error <error> type <type> seq <seq> pid <pid>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the error has occurred while processing the hardware abstraction layer (HAL) message.

Recommended Action Restart the multicast subsystem (MCAST_SS) daemon.

MCAST_SS-1003

Message `Learning error: <op> (<reason>) - VLAN <vid> MAC/group <address>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the multicast subsystem (MCAST_SS) has encountered an error while learning the media access control (MAC) addresses.

Recommended Action Restart the MCAST_SS daemon.

MCAST_SS-1004

Message `NSM error: <op> (<reason>) for VLAN <vid> port <port>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the multicast subsystem (MCAST_SS) has encountered an error during a network service module (NSM) event.

Recommended Action Restart the MCAST_SS daemon.

MCAST_SS-1005

Message `Message error: Invalid message type <type> expecting <value1> or <value2> or <value3>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the type of the message received from the driver is invalid.

Recommended Action Restart the MCAST_SS daemon.

MCAST_SS-1006

Message `Message error: <op> (<reason>) Invalid message length <length> expecting <length1>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that length of the message received from the driver is invalid.

Recommended Action Restart the MCAST_SS daemon.

MCAST_SS-1007

Message `Initialization error: <op> (<reason>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the multicast subsystem (MCAST_SS) has encountered an error during initialization.

Recommended Action Restart the MCAST_SS daemon.

MCAST_SS-1008

Message `HAL error: <op> (<reason>) - VLAN <vid> MAC/group <address>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the multicast subsystem (MCAST_SS) has encountered the hardware abstraction layer (HAL) errors.

Recommended Action Restart the MCAST_SS daemon.

MCAST_SS-1009

Message `L2SS error : <op> (<reason>) VLAN <vid> MAC <mac address>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the multicast subsystem (MCAST_SS) has encountered the Layer 2 subsystem (L2SS) related errors.

Recommended Action Restart the MCAST_SS daemon.

MCAST_SS-1010

Message `Message Queue error: <op> (<reason>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the multicast subsystem (MCAST_SS) has encountered the message queue errors.

Recommended Action Restart the MCAST_SS daemon.

MCAST_SS-1011

Message `IDB error: <op> (<reason>) port id <portid> not found.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified port ID is invalid.

Recommended Action Restart the MCAST_SS daemon.

MCAST_SS-1012

Message `IDB error: <op> (<reason>) VLAN VID <vid> not found.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified VLAN ID (VID) is invalid.

Recommended Action Restart the MCAST_SS daemon.

MCAST_SS-1013

Message `Snooping DB error: <op> (<reason>) Group Not found - VLAN <vid> group <group address>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the group address lookup for the specified VLAN has failed.

Recommended Action Restart the MCAST_SS daemon.

MCAST_SS-1014

Message `Snooping DB error: <op> (<reason>) MAC Not found - VLAN <vid> MAC-addr <mac address>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the media access control (MAC) address lookup for the specified VLAN has failed.

Recommended Action Restart the MCAST_SS daemon.

MCAST_SS-1015

Message `HSL error: <op> (<reason>) failed for message <message> VLAN <vid> MAC <mac address> mgid <mgid> CPU <cpu>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified hardware subsystem layer (HSL) related operation has failed.

Recommended Action Restart the MCAST_SS daemon.

MCAST_SS-1016

Message `Message error: <op> (<reason>) <length>(<length1>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the length of the message received from the driver is invalid.

Recommended Action Restart the MCAST_SS daemon.

MCAST_SS-1017

Message `Learning error: <op> (<reason>) Invalid number <port> for ifindex <ifindex>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the multicast subsystem (MCAST_SS) has encountered an error while learning the media access control (MAC) addresses.

Recommended Action Restart the MCAST_SS daemon.

MCAST_SS-1018

Message `Memory Alloc Error: <op> (<reason>) type <memtype>/<memsize>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the multicast subsystem (MCAST_SS) has encountered an error during the memory allocation.

Recommended Action Restart the MCAST_SS daemon.

MCAST_SS-1019

Message `Ptree Error: <op> (<reason>) VLAN <vid> MAC/group <address>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the multicast subsystem (MCAST_SS) has encountered an error during the Ptree operation.

Recommended Action Restart the MCAST_SS daemon.

MCAST_SS-1020

Message `List Error: <op> (<reason>) VLAN <vid> MAC <mac address> group <group address>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the multicast subsystem (MCAST_SS) has encountered an error during the List operation.

Recommended Action Restart the MCAST_SS daemon.

MFIC Messages

MFIC-1001

Message `failure at sysmod_scn registry rc= <failure reason>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the system is temporarily out of resources.

Recommended Action No action is required; this message is often transitory.

If the message persists, run the **reboot** or the **haFailover** command (if applicable).

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

MFIC-1002

Message `Chassis FRU header not programmed for switch NID, using defaults (applies only to FICON environments).`

Message Type LOG

Severity INFO

Probable Cause Indicates that custom switch node descriptor (NID) fields have not been programmed in nonvolatile storage. The default values are used. The Switch NID is used only in the following SB ELS frames: Request Node Identification Data (RNID) and Registered Link Incident Record (RLIR). The use of SB-3 link incident registration and reporting is typically limited to FICON environments.

Recommended Action No action is required if SB-3 link incident registration and reporting is not used by the host or if default values are desired for the switch node descriptor fields.

MFIC-1003

Message `Effective Insistent domain ID for the fabric changed from <state> to <state>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that one or more switches joined the fabric with an insistent domain ID (IDID) mode setting that is different from the current effective IDID mode for the fabric. This message also occurs when the IDID for the fabric has been turned on or off. The possible values for the state are "On" and "Off".

Recommended Action IDID mode is a fabric-wide mode; make sure that any switches added to the fabric are configured with the same IDID mode as the fabric. If you are enabling or disabling IDID mode, this message is for information purposes only, and no action is required. IDID mode can be set using the **configure** command in the CLI or checking the Advanced Web Tools **Switch Admin > Configure > Fabric > Insistent Domain ID Mode** check box. The switch must be disabled to change the IDID mode.

MM Messages

MM-1001

Message `VPD block 0 CRC is bad.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that CRC in the VPD block 0 is bad. This could indicate corruption or tampering.

This message occurs only on the Brocade 6547 switch.

Recommended Action Execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

MPTH Messages

MPTH-1001

Message `Null parent, lsId = <number>.`

Message Type LOG | FFDC

Severity ERROR

Probable Cause Indicates that a null parent was reported. The minimum cost path (MPATH) uses a tree structure in which the parent is used to connect to the root of the tree.

Recommended Action No action is required.

MPTH-1002

Message `Null lsrP, lsId = <ls ID number>.`

Message Type LOG | FFDC

Severity ERROR

Probable Cause Indicates that a link state record (LSR) is null.

Recommended Action No action is required.

MPTH-1003

Message `No minimum cost path in candidate list.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the fabric shortest path first (FSPF) module has determined that there is no minimum cost path (MPATH) available in the candidate list.

Recommended Action No action is required.

MQ Messages

MQ-1004

Message `mqRead, queue = <queue name>, queue ID = <queue ID>, type = <message type>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates an unexpected message has been received in the specified message queue. The *queue name* value is always fspf_q. The *queue ID* and *message type* values can be any of the following:

- 2 - MSG_TX
- 3 - MSG_INTR
- 4 - MSG_STR
- 6 - MSG_ASYNC_IU
- 7 - MSG_LINIT_IU
- 8 - MSG_RSCN
- 9 - MSG_IOCTL
- 10 - MSG_ACCEPT
- 11 - MSG_IU_FREE
- 12 - MSG_US
- 13 - MSG_EXT_RSCN
- 14 - MSG_RDTS_START
- 15 - MSG_RDTS_SENDEFP
- 16 - MSG_RDTS_RESET

Recommended Action No action is required.

MQ-1005

Message `queue <queue name>: queue full (miss=<miss count>).`

Message Type LOG | FFDC

Severity WARNING

Probable Cause Indicates that the specified message queue is full.

Recommended Action No action is required.

MQ-1006

Message `queue <queue name>: msg too long (<number of bytes>:<message queue size>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates the incoming message size is larger than the message queue size.

Recommended Action No action is required.

MS Messages

MS-1001

Message

```
MS Platform Segmented port=<port number> (0x<port number (hex)>) (<reason for
segmentation> <domain> (0x<domain (hex)>)).
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the Management Server (MS) has segmented from another switch domain at the specified port because of errors or inconsistencies defined in the MS platform service.

Recommended Action

Reboot or power cycle the switch.

MS-1002

Message

```
MS Platform Service Unstable(<message string><domain number>).
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the Management Server (MS) platform service is unstable.

The *message string* value can be one of the following:

- No Resp for GCAP from: The switch did not respond to a request for a GCAP (MS Get Capabilities) command.
- GCAP sup but not PL by: GCAP is supported but the flag for MS platform service is not set.
- GCAP Rejected (reason =BUSY) by: GCAP is not supported by another switch.
- Reject EXGPLDB from: The request to the exchange platform database was rejected. The remote switch may be busy.

The *domain number* is the target domain that caused the error.

Recommended Action

The recommended actions are as follows:

- No Resp for GCAP from: No action is required.
- GCAP sup but not PL by: Set the flag for the MS platform service.
- GCAP Rejected (reason =BUSY) by: Execute the **firmwareDownload** command to upgrade the firmware level on the switch to a level that supports reliable commit service (RCS). RCS is supported in Fabric OS v2.6, v3.1 and later, and v4.1 and later.
- Reject EXGPLDB from: Wait a few minutes and try the command again.

MS-1003

Message `MS detected Unstable Fabric(<message string><domain number>).`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Management Server (MS) detected an unstable fabric; the command or operation may not be successfully completed. This message is often transitory.

The *message string* value can be one of the following:

- DOMAIN_INVALID for a req from: The domain is invalid for a request.
- No WWN for: Unable to acquire the World Wide Name (WWN) for the corresponding domain.

The *domain number* is the target domain that caused error.

Recommended Action The fabric may be reconfiguring, forming, or merging. Wait a few minutes and try the operation again.

Execute the **fabricShow** command or the **secFabricShow** command to verify that the number of domains matches the Management Server known domains.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

MS-1004

Message `MS detected ONLY 1 Domain(d=<domain in local resource>).`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Management Server (MS) detected an unstable count of domains in its own local resource. This message is often transitory.

Recommended Action The fabric may be reconfiguring, forming, or merging. Wait a few minutes and try the operation again.

Execute the **fabricShow** command or the **secFabricShow** command to verify that the number of domains matches the Management Server known domains.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

MS-1005

Message `MS Invalid CT Response from d=<domain>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the Management Server (MS) received an invalid common transport (CT) response from the switch domain. MS expects either a CT accept IU or a reject IU; the MS received neither response, which violates the Fibre Channel - Generic Services (FS-GS) specification.

Recommended Action Check the integrity of the FC switch at the specified domain. It is not sending correct MS information as defined by the Fibre Channel - Framing and Signaling (FC-FS) standard.

MS-1006

Message `MS Unexpected iu_data_sz=<number of bytes>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the Management Server (MS) received an information unit (IU) data of unexpected size. The IU payload and the IU size may be inconsistent with each other or with the command that is currently being processed.

Recommended Action Wait a few minutes and try the operation again.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

MS-1008

Message `MS Failure while initializing <action>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the Management Server (MS) failed while initializing the specified action. This message is often transitory.

The *action* can be one of the following:

- while writing to ms_els_q: MS is unable to write a message to the MS Extended Link Service Queue.
- while inserting timer to timer list: MS is unable to add a timer to a resource.

Recommended Action If the error persists, check the available memory on the switch using the **memShow** command.

MS-1009

Message

```
RLIR event. Slot/Port <slot number>/<port number> (0x<PID (hex)>). Device Port Tag
is 0x<port tag>. <message text>.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates a registered link incident record (RLIR) has been generated for one of the actions indicated by the *message* value.

The *message* value can be one of the following:

- Exceeded bit error rate threshold
- Loss of signal or synchronization
- Not operational seq recognized
- Primitive sequence timeout
- Unrecognized link incident

Recommended Action

Persistent RLIR incidents are likely the result of SAN hardware problems such as bad cables or small form-factor pluggable (SFP) transceivers. If the message persists, replace hardware.

MS-1021

Message

```
MS WARMBOOT failure(FSS_MS_WARMINIT failed. Reason=<failure reason>).
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that the Fabric OS state synchronization (FSS) warm recovery failed during the WARM INIT phase of a reboot.

Recommended Action

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

MS-1022

Message

```
Management Server Platform Service <Activated or Deactivated>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the Management Server (MS) platform service is being activated or deactivated.

Recommended Action

No action is required.

MS-1023

Message `Management Server Topology Discovery Service <Enabled or Disabled>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Management Server (MS) topology discovery service is being enabled or disabled.

Recommended Action No action is required.

MS-1024

Message `Management Server Access Control List is Updated.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Management Server (MS) Access Control List (ACL) is saved to nonvolatile storage.

Recommended Action No action is required.

MS-1025

Message `Possible Failover could have occurred while enabling MS Platform Service.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a failover occurred when Management Server (MS) platform service was being enabled. This can leave the fabric in an inconsistent state.

Recommended Action If any inconsistency in MS platform service exists within the fabric, enable MS platform service.

MS-1026

Message `MS Platform disabled port <port number> domain <domain> to block enabling Platform service through merge operation.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Management Server (MS) has disabled the specified E_Port connected to the specified domain because an implicit enable operation of the MS platform service has been blocked.

Recommended Action Enable MS platform service on the switch and re-enable the port to join the fabric.

MS-1027

Message `Fabric Name - <fabric_name> configured.`

Message Type AUDIT | LOG

Class FABRIC

Severity INFO

Probable Cause Indicates that the specified fabric name is configured or renamed.

Recommended Action No action is required.

MS-1028

Message `Fabric Name - <fabric_name> Cleared.`

Message Type AUDIT | LOG

Class FABRIC

Severity INFO

Probable Cause Indicates that the specified fabric name is cleared.

Recommended Action No action is required.

MS-1029

Message `Duplicate Fabric Name - <fabric_name> matching with FID <Fabric ID>.`

Message Type AUDIT | LOG

Class FABRIC

Severity ERROR

Probable Cause Indicates that the configured fabric name is already used for another partition.

Recommended Action Select a different fabric name and reconfigure.

MS-1030

Message `Fabric Name - <fabric_name> <cmd> Failed for domain <domain>.`

Message Type AUDIT | LOG

Class FABRIC

Severity ERROR

Probable Cause Indicates that fabric name configure or clear operation failed in Fibre Channel Router (FCR).

Recommended Action Wait for fabric to stabilize and retry the operation.

MSTP Messages

MSTP-1001

Message `<message>: <message>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the system has failed to allocate memory.

Recommended Action Check the memory usage on the switch using the **memShow** command.

Restart or power cycle the switch.

MSTP-1002

Message `<message>: <message>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the system has failed to initialize.

Recommended Action Restart or power cycle the switch.

MSTP-1003

Message `<message>: <message>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a connection, transfer, or receiving error in the socket.

Recommended Action If this is a bladed switch, execute the **haFailover** command. If the problem persists or if this is a non-bladed switch, download a new firmware version using the **firmwareDownload** command.

MSTP-2001

Message `<message>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the multiple spanning tree protocol (MSTP) bridge mode has changed.

Recommended Action No action is required.

MSTP-2002

Message `<Bridge mode information>. My Bridge ID: <Bridge ID> Old Root: <Old Root ID> New Root: <New Root ID>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the multiple spanning tree protocol (MSTP) bridge or bridge instance root has been changed.

Recommended Action No action is required.

MSTP-2003

Message `MSTP instance <instance> is created.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified multiple spanning tree protocol (MSTP) instance has been created.

Recommended Action No action is required.

MSTP-2004

Message `MSTP instance <instance> is deleted.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified multiple spanning tree protocol (MSTP) instance has been deleted.

Recommended Action No action is required.

MSTP-2005

Message `VLAN <vlan_ids> is <action> on MSTP instance <instance>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified multiple spanning tree protocol (MSTP) instance has been modified.

Recommended Action No action is required.

MSTP-2006

Message `MSTP instance <instance> brigde priority is changed from <priority_old> to <priority_new>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified multiple spanning tree protocol (MSTP) instance priority has been modified.

Recommended Action No action is required.

NBFS Messages

NBFS-1001

Message

```
Duplicate E_Port SCN from port <portnumber> in state <state change name> (<state
change number>).
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates a duplicate E_Port state change notification (SCN) was reported. The neighbor finite state machine (NBFSM) states are as follows:

- 0 - Down
- 1 - Init
- 2 - Database Exchange
- 3 - Database Acknowledge Wait
- 4 - Database Wait
- 5 - Full

Recommended Action

No action is required.

NBFS-1002

Message

```
Wrong input: <state name> to neighbor FSM, state <current state name>, port
<portnumber>.
```

Message Type

FFDC | LOG

Severity

ERROR

Probable Cause

Indicates the wrong input was sent to the neighbor finite state machine (NBFSM). NBFSM states are as follows:

- 0 - Down
- 1 - Init
- 2 - Database Exchange
- 3 - Database Acknowledge Wait
- 4 - Database Wait
- 5 - Full

If this error occurs repeatedly, then there is a problem in the protocol implementation between two switches.

Recommended Action

Run the **nbrStateShow** command to check the neighbor state of the port listed in the message. If it is Full, then this message can safely be ignored. Otherwise, run the **portDisable** and **portEnable** commands to refresh the port.

NBFS-1003

Message

```
DB_XMIT_SET flag not set in state <current state name>, input <state name>, port
<portnumber>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates the database transmit set flag was not set for the specified input state on the specified port. Neighbor finite state machine (NBFSM) states are as follows:

- 0 - Down
- 1 - Init
- 2 - Database Exchange
- 3 - Database Acknowledge Wait
- 4 - Database Wait
- 5 - Full

Recommended Action

No action is required. The Fabric OS automatically recovers from this problem.

NBFS-1004

Message

```
Wrong input: <state name> to neighbor FSM, state <current state name>, port
<portnumber>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates the wrong input was sent to the neighbor finite state machine (NBFSM). NBFSM states are as follows:

- 0 - Down
- 1 - Init
- 2 - Database Exchange
- 3 - Database Acknowledge Wait
- 4 - Database Wait
- 5 - Full

If this error occurs repeatedly, then there is a problem in the protocol implementation between two switches.

Recommended Action

Run the **nbrStateShow** command to check the neighbor state of the port listed in the message. If it is Full, then this message can safely be ignored. Otherwise, run the **portDisable** and **portEnable** commands to refresh the port.

NBFS-1005

Message

```
FSPF experiencing link issues on port <port string> in state <current state name>
(<state change number>).
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that FSPF is experiencing issues with frames on the link leading to unexpected inputs being sent to the neighbor finite state machine (NBFSM). NBFSM states are as follows:

- 0 - Down
- 1 - Init
- 2 - Database Exchange
- 3 - Database Acknowledge Wait
- 4 - Database Wait
- 5 - Full

If this error occurs repeatedly, then there is a problem running the FSPF exchange and synchronization protocol between two switches across the identified link.

Recommended Action

Run the **nbrStateShow** command to check the neighbor state of the port listed in the message. If it is Full, then this message can safely be ignored. Otherwise, please check the **portStatsShow** command to see if there are errors on the link. If there are errors, consider running the D-Port Diagnostics tests on the link and/or consider replacing and faulty or bad equipment such as cables or optics.

NS Messages

NS-1001

Message

```
The response for request 0x<CT command code> from remote switch 0x<Domain Id> is
larger than the max frame size the remote switch can support.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the response payload exceeds the maximum frame size the remote switch can handle.

Recommended Action

Execute the **firmwareDownload** command to upgrade the remote switch with Fabric OS v4.3 or later, or Fabric OS v3.2 or later, as appropriate for the switch type, so that it can support GMI to handle frame fragmentation and reassembly.

You can also reduce the number of devices connected to the local switch.

NS-1002

Message

```
Remote switch 0x<Domain Id> has firmware revision lower than 2.2: <Firmware
Revision 1st character><Firmware Revision 2nd character><Firmware Revision 3rd
character><Firmware Revision 4th character> which is not supported.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the local switch cannot interact with the remote switch because of incompatible or obsolete firmware.

Recommended Action

Execute the **firmwareDownload** command to upgrade the remote switch to the latest level of firmware.

NS-1003

Message

```
Number of local devices <Current local device count>, exceeds the standby can
support <Local device count that standby can support>, can't send update.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the Name Server on the standby control processor (CP) has a lower supported capability than the active CP because of different firmware versions running on the active and standby CPs. This means that the active and standby CPs are out of sync. Any execution of the **haFailover** or **firmwareDownload** commands will be disruptive.

Recommended Action To avoid disruption of traffic in the event of an unplanned failover, schedule a firmware download so that the active and standby CPs have the same firmware version.

Reduce the local device count to follow the capability of the earliest version of firmware.

NS-1004

Message

```
Number of local devices <Current local device count>, exceeds the standby can
support <Local device count that standby can support>, can't sync.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the Name Server on the standby control processor (CP) has a lower supported capability than the active CP because of different firmware versions running on the active and standby CPs. This means that the active and standby CPs are out of sync. Any execution of the **haFailover** or **firmwareDownload** commands will be disruptive.

Recommended Action To avoid disruption of traffic in the event of an unplanned failover, schedule a firmware download so that the active and standby CPs have the same firmware version.

Reduce the local device count to follow the capability of the earliest version of firmware.

NS-1005

Message

```
Zone size of <Effective Zone Size> has over the supporting limit of <Support Zone
Size> for the remote switch domain ID <Remote Switch Domain ID>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates the effective zone size has exceeded the limit that a remote switch can support. The oversized portion will be truncated.

Recommended Action Reduce the zone size to 1024 or smaller, or upgrade the software of the remote switch to support 2048 zones.

NS-1006

Message

```
Duplicate WWN was detected with PID 0x<existing device PID> and 0x<new device
PID>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that an existing device has the same World Wide Name (WWN) as that of a new device that has come online.

Recommended Action The switch will process the new process ID (PID) and leave the existing PID intact. Subsequent switch operations will clean up the obsolete PID. However, it is recommended that administrators remove devices with a duplicate WWN.

NS-1007

Message `NS has detected a logical ISL port <LISL port number> in TI zone <TI zone name> in fabric <Fabric ID>. Routing may not be setup correctly.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a logical inter-switch link (LISL) is detected in a traffic isolation (TI) zone.

Recommended Action Remove the LISL port from the TI zone because the routing may not be set up correctly.

NS-1008

Message `Open FR license not installed.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that Open FR license is not installed and therefore local devices involved in Open FR will not function.

Recommended Action Install the Open FR license or relocate Open FR devices to a licensed switch.

NS-1009

Message `NS has detected a device with Node WWN as zero, pid 0x<device PID>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a device has logged in with node World Wide Node Name (WWNN) as zero. Brocade Network Advisor (BNA) will not show the port connectivity.

Recommended Action Check the device that logged in. The device could be faulty.

NS-1010

Message `CSCTL mode enabled on port <csctlport> QoS zoning will be ignored for devices on this port.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that class-specific control (CS_CTL) mode has been enabled on the specified port that has devices as members of a quality of service (QoS) zone.

Recommended Action Remove the CS_CTL configured devices from the QoS zone.

NS-1011

Message `NS has detected a failover flag disabled TI zone in a base switch <Domain Id> in fabric ID <Fabric ID>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a failover-disabled traffic isolation (TI) zone has been detected in a base switch fabric.

Recommended Action Enable the failover flag or remove the TI zone with the disabled failover flag because the routing may not be set up correctly.

NS-1012

Message `Detected duplicate WWPN [<WWPN>] - devices removed with PID 0x<existing device PID> and 0x<new device PID>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the devices with the same World Wide Port Name (WWPN) have been removed from the Name Server database.

Recommended Action Verify the device reported with duplicate WWPN.

NS-1013

Message `SIM_PORT with WWPN[<WWPN>] creating duplicate condition with PID 0x<duplicate device PID>. Removed PID 0x<disabled device PID> and disabled port <disabled Port>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the SIM port that is causing the duplicate condition has been removed from the Name Server database and the port is disabled.

Recommended Action Verify the device reported with duplicate World Wide Port Name (WWPN) and re-enable the port if necessary.

NS-1014

Message `Domain Capability is not available for domain <Domain>. Rejoin this domain to the fabric. Reason Code <Reason Code>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that domain capability is unavailable for the specified domain.

Recommended Action Remove and rejoin the specified domain to the fabric.

NS-1015

Message `Failed to update client capability to ESS (Exchange Switch Support) after maximum number of retries - return code <Failed return code>. Failing sync dump to standby CP.`

Message Type LOG

Severity INFO

Probable Cause Indicates that Exchange Switch Support (ESS) is unable to update its capability. Failed to send the sync dump to standby control processor (CP).

Recommended Action Verify that HA synchronization has failed using the **haShow** command. If HA synchronization has failed, execute the **haSyncStart** command on active CP to resynchronize the HA state.

NSM Messages

NSM-1001

Message `Interface <InterfaceName> is online.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified interface has come online after the protocol dependencies are resolved.

Recommended Action No action is required.

NSM-1002

Message `Interface <InterfaceName> is protocol down.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified interface has gone offline because one of the protocol dependencies is unresolved.

Recommended Action Check for the reason codes using the **show interface** command and resolve the protocol dependencies.

The following are the possible reason codes:

- Admin down
- Link protocol down
- DOT1x authenticating
- Minimum member links not UP (applicable only for port-channel interfaces)
- DOT1x authentication failed
- BRCD remote link negotiation failed/LLDP disabled
- LAG negotiating/failed
- LAG admin state is down
- UNKNOWN

NSM-1003

Message `Interface <InterfaceName> is link down.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified interface has gone offline because the link is down.

Recommended Action Check whether the connectivity between the peer ports is proper, and the remote link is up using the **show interface** command.

NSM-1004

Message `Interface <InterfaceName> is created.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified logical interface has been created.

Recommended Action No action is required.

NSM-1005

Message `The FCoE VLAN: <VlanName> is in use. Therefore, cannot disable the FCoE VLAN.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified Fibre Channel over Ethernet (FCoE) VLAN is used in the FCoE daemon (fcoed) and therefore cannot be disabled.

Recommended Action Remove all the FCoE sessions from the FCoE VLAN member ports and then disable the FCoE VLAN.

NSM-1006

Message `FCoE on VLAN: <VlanName> has been disabled successfully.`

Message Type LOG

Severity INFO

Probable Cause Indicates that FCoE has been disabled on the specified VLAN.

Recommended Action No action is required.

NSM-1007

Message `Chassis is <status>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the chassis has been enabled or disabled.

Recommended Action No action is required.

NSM-1008

Message `Blade (<slot number>) is <status>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified blade has been enabled or disabled.

Recommended Action No action is required.

NSM-1009

Message `Interface <InterfaceName> is deleted.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified logical interface has been deleted.

Recommended Action No action is required.

NSM-1010

Message `InterfaceMode changed from <Mode_old> to <Mode_new> for interface <InterfaceName>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the interface mode has been changed.

Recommended Action No action is required.

NSM-1011

Message `OperationalEndpointMode changed from <Mode_old> to <Mode_new> for interface <InterfaceName>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the interface operational endpoint mode has been changed.

Recommended Action No action is required.

NSM-1012

Message `VLAN classifier group <group_id> is created.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified VLAN classifier group has been created.

Recommended Action No action is required.

NSM-1013

Message `VLAN classifier group <group_id> is deleted.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified VLAN classifier group has been deleted.

Recommended Action No action is required.

NSM-1014

Message `VLAN classifier rule <rule_id> is created.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified VLAN classifier rule has been created.

Recommended Action No action is required.

NSM-1015

Message `VLAN classifier rule <rule_id> is deleted.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified VLAN classifier rule has been deleted.

Recommended Action No action is required.

NSM-1016

Message `VLAN classifier rule <rule_id> is <action> on VLAN classifier group <group_id>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified VLAN classifier group has been modified.

Recommended Action No action is required.

NSM-1017

Message `Interface <InterfaceName> is <action> on interface <Logical_InterfaceName>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the logical interface member list has been changed.

Recommended Action No action is required.

NSM-1018

Message `<count> VLANs <except> will be allowed on interface <Logical_InterfaceName>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the VLAN membership has been changed for the specified interface.

Recommended Action No action is required.

NSM-1019

Message `Interface <InterfaceName> is administratively up.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the administrative status of the specified interface has changed to up.

Recommended Action No action is required.

NSM-1020

Message `Interface <InterfaceName> is administratively down.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the administrative status of the specified interface has changed to down.

Recommended Action No action is required.

ONMD Messages

ONMD-1000

Message `LLDP is enabled.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the link layer discovery protocol (LLDP) is enabled globally.

Recommended Action No action is required.

ONMD-1001

Message `LLDP is disabled.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the link layer discovery protocol (LLDP) is disabled globally.

Recommended Action No action is required.

ONMD-1002

Message `LLDP global configuration is changed.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the link layer discovery protocol (LLDP) global configuration has been changed.

Recommended Action No action is required.

ONMD-1003

Message `LLDP is enabled on interface <InterfaceName>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the link layer discovery protocol (LLDP) is enabled on the specified interface.

Recommended Action No action is required.

ONMD-1004

Message `LLDP is disabled on interface <InterfaceName>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the link layer discovery protocol (LLDP) is disabled on the specified interface.

Recommended Action No action is required.

ONMD-1005

Message `Using auto-sense on interface <InterfaceName> to update DCBX version.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the auto-sense feature is used to detect the Data Center Bridging eXchange (DCBX) version on the specified interface. The DCBX version field will be automatically updated between the Converged Enhanced Ethernet (CEE) version and the pre-CEE version depending on the link neighbor.

Recommended Action No action is required.

PDM Messages

PDM-1001

Message `Failed to parse the pdm config.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Parity Data Manager (PDM) process could not parse the configuration file. This may be caused by a missing configuration file during the installation.

Recommended Action Execute the **firmwareDownload** command to reinstall the firmware.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

PDM-1002

Message `ipcInit failed.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Parity Data Manager (PDM) process could not initialize the inter-process communication (IPC) mechanism.

Recommended Action If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

PDM-1003

Message `pdm [-d] -S <service> -s <instance>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a syntax error occurred when trying to launch the Parity Data Manager (PDM) process.

Recommended Action Execute the **firmwareDownload** command to reinstall the firmware.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

PDM-1004

Message `PDM memory shortage.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Parity Data Manager (PDM) process ran out of memory.

Recommended Action Reboot or power cycle the switch.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

PDM-1005

Message `FSS register failed.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Parity Data Manager (PDM) failed to register with the Fabric OS synchronization service (FSS).

Recommended Action Execute the **firmwareDownload** command to reinstall the firmware.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

PDM-1006

Message `Too many files in sync.conf.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the sync.conf configuration file contains too many entries.

Recommended Action Execute the **firmwareDownload** command to reinstall the firmware.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

PDM-1007

Message `File not created: <file name>. errno=<errno>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Parity Data Manager (PDM) process failed to create the specified file.

Recommended Action Execute the **firmwareDownload** command to reinstall the firmware.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

PDM-1008

Message `Failed to get the number of U_Ports.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Parity Data Manager (PDM) system call to getCfg failed.

Recommended Action Execute the **firmwareDownload** command to reinstall the firmware.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

PDM-1009

Message `Can't update Port Config Data.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Parity Data Manager (PDM) system call to setCfg failed.

Recommended Action Execute the **firmwareDownload** command to reinstall the firmware.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

PDM-1010

Message `File open failed: <file name>, errno=<errno>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Parity Data Manager (PDM) process could not open the specified file.

Recommended Action Execute the **firmwareDownload** command to reinstall the firmware.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

PDM-1011

Message
```
File read failed: <file name>, Length(read=<Number of character read>,
expected=<Number of characters expected>), errno=<errno returned by read>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Parity Data Manager (PDM) process could not read data from the specified file.

Recommended Action Execute the **firmwareDownload** command to reinstall the firmware.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

PDM-1012

Message
```
File write failed: <file name>. Length(read=<Number of character read>,
write=<Number of characters written>), errno=<errno returned by write>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Parity Data Manager (PDM) process could not write data to the specified file.

Recommended Action Execute the **firmwareDownload** command to reinstall the firmware.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

PDM-1013

Message `File empty: <File Name>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the switch configuration file */etc/fabos/fabos.[0|1].conf* is empty.

Recommended Action Execute the **firmwareDownload** command to reinstall the firmware.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

PDM-1014

Message `Access sysmod failed.`

Message Type LOG

Severity WARNING

Probable Cause Indicates a system call to sysMod failed.

Recommended Action Execute the **firmwareDownload** command to reinstall the firmware.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

PDM-1017

Message `System (<Error Code>): <Command>.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the specified system call failed.

Recommended Action Execute the **firmwareDownload** command to reinstall the firmware.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

PDM-1019

Message `File path or trigger too long.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that one line of the pdm.conf file is too long.

Recommended Action Execute the **firmwareDownload** command to reinstall the firmware.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

PDM-1020

Message `Long path name (<Path>/<File Name>), Skip.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the specified file path name is too long. The maximum character limit is 49 characters.

Recommended Action Use path names not exceeding 49 characters in length for the files to be replicated.

PDM-1021

Message `Failed to download area port map.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a system call failed.

Recommended Action Execute the **firmwareDownload** command to reinstall the firmware.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

PDM-1022

Message `The switch is configured only with IPv6 addresses.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Parity Data Manager (PDM) cannot synchronize with its peer because the firmware does not support IPv6.

Recommended Action Configure the local switch with IPv4 addresses.

PDM-1023

Message `RADIUS is configured with IPv6 addresses.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Parity Data Manager (PDM) cannot synchronize with its peer because the remote access dial-in user server (RADIUS) is configured with IPv6 addresses. IPv6 is not supported by older firmware.

Recommended Action Configure RADIUS with IPv4 addresses.

PDM-1024

Message `DNS is configured with IPv6 addresses.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Parity Data Manager (PDM) cannot synchronize with its peer because the Domain Name Service (DNS) is configured with IPv6 addresses. IPv6 is not supported by older firmware.

Recommended Action Configure DNS with IPv4 addresses.

PDM-1025

Message `LDAP is configured with IPv6 addresses.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Parity Data Manager (PDM) cannot synchronize with its peer because the Lightweight Directory Access Protocol (LDAP) server is configured with IPv6 addresses. IPv6 is not supported by older firmware.

Recommended Action Configure the LDAP server with IPv4 addresses.

PDM-1026

Message `User defined roles configured.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Parity Data Manager (PDM) cannot synchronize with its peer because the user-defined roles are configured. User-defined roles are not supported by older firmware.

Recommended Action Remove user-defined roles configuration.

PDTR Messages

PDTR-1001

Message `<informational message>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that information has been written to the panic dump files. The watchdog register codes are as follows:

- 0x10000000 - The watchdog timer (WDT) forced a core reset.
- 0x20000000 - The WDT forced a chip reset.
- All other code values are reserved.

Recommended Action Run the **pdShow** command to view the panic dump and core dump files.

PDTR-1002

Message `<informational message>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that information has been written to the panic dump and core dump files and a trap has been generated. The watchdog register codes are as follows:

- 0x10000000 - The watchdog timer (WDT) forced a core reset.
- 0x20000000 - The WDT forced a chip reset.
- All other code values are reserved.

Recommended Action Run the **pdShow** command to view the panic dump and core dump files.

PLAT Messages

PLAT-1000

Message `<Function name> <Error string>.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that nonrecoverable peripheral component interconnect (PCI) errors have been detected.

Recommended Action The system will be faulted and may automatically reboot.

If the system does not reboot automatically, reboot the system manually using the **reboot** command.

Execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

PLAT-1001

Message `CP<Identifies which CP (0 or 1) is doing the reset> resetting other CP (double reset may occur).`

Message Type LOG

Severity INFO

Probable Cause Indicates the other control processor (CP) is being reset. This message is typically generated by a CP that is in the process of becoming the active CP. Note that in certain circumstances a CP may experience a double reset and reboot twice. A CP can recover automatically even if it has rebooted twice.

Recommended Action No action is required.

PLAT-1002

Message `CP<Identifies which CP (0 or 1) is generating the message>: <Error message> CP Fence 0x<CP Fence register. Contents (2 bytes) are platform-specific> 0x<CP Error register. Contents are platform-specific> CP Error 0x<Write control flag. Contents are platform-specific>.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that the control processor (CP) cannot access the inter-integrated circuit (I2C) subsystem because of an error condition or because of being fenced or isolated from the I2C bus.

Recommended Action Reboot the CP if it does not reboot automatically. Reseat the CP if rebooting does not solve the problem. If the problem persists, replace the CP.

PLAT-1003

Message
```
<Info message> Slot <Blade Slot number> C/BE: 0x<Captured Command/Byte-Enables
data> ADBUS: 0x<Captured AD bus data> misc_intr 0x<Bridge reset interrupts>.
```

Message Type LOG | FFDC

Severity CRITICAL

Probable Cause Indicates that peripheral component interconnect (PCI) bus hang was detected.

Recommended Action Replace the field-replaceable unit (FRU).

PLAT-1004

Message
```
Switch has older FPGA rev 0x<FPGA version already installed in HW>. Upgrade to
newer rev 0x<FPGA version which Fabric OS carries> using the fpga_update command.
```

Message Type LOG | FFDC

Severity CRITICAL

Probable Cause Indicates that Fabric OS has older field-programmable gate array (FPGA) version. This message is applicable only to Brocade 5470.

Recommended Action Upgrade FPGA to new version.

PLAT-1005

Message
```
Incompatible midplane detected. All internal ports will be disabled.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates that the chassis has the revision 1.0 midplane.

This message occurs only on the Brocade M6505.

Recommended Action Replace the midplane with a revision 1.1 midplane.

PLAT-1006

Message `Unknown midplane revision.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the chassis has a midplane whose revision is unknown.

This message occurs only on the Brocade M6505.

Recommended Action Install newer firmware in the Chassis Management Controller (CMC).

PLAT-1007

Message `BladeSystem Chassis type is unknown, setting maximum internal port speed to 8Gbps.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Onboard Administrator (OA) could be running an old version of firmware.

If OA firmware is new enough to support Enclosure Information, then OA failed to send the Enclosure Information soon enough to allow the internal ports to run at 16 GFC.

This message occurs only on the Brocade 6548.

Recommended Action No action is required.

PLAT-1008

Message `BladeSystem Enclosure Information arrived late from OA.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Onboard Administrator (OA) failed to send the Enclosure Information soon enough to allow the internal ports to run at 16 GFC.

This message occurs only on the Brocade 6548.

Recommended Action Execute the **hareboot** command, followed by the **portdisable** and **portenable** commands to allow internal ports to run at 16 GFC.

PLAT-1009

Message `BladeSystem Chassis type requires setting maximum internal port speed to 8Gbps.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the chassis has an older midplane that cannot support 16 GFC internal ports.

This message occurs only on the Brocade 6548.

Recommended Action Install the switch in a newer chassis.

PLAT-1072

Message `The chassis is disabled because no Core Blades are available. Insert/replace one or both Core Blades and run chassisenable.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the chassis has been disabled because of the unavailability of the core blades. There must be at least one core blade in enabled state for the chassis to be considered ready. All core blades are either missing, faulted, or powered off. This results in all logical switches (and ports) being disabled.

Recommended Action Make sure that all core blade slots have core blades inserted and their ejector switches are closed. Power on core blades that are powered off, and power cycle or replace the core blades that are faulted.

Run the **chassisenable** command to re-enable the ports.

Running the **fastboot** or **reboot** command will also result in enabling the logical switches and ports.

PMGR Messages

PMGR-1001

Message `Attempt to create switch <FID> succeeded.`

Message Type LOG | AUDIT

Class LS

Severity INFO

Probable Cause Indicates that the switch with the specified fabric ID (FID) was successfully created.

Recommended Action No action is required.

PMGR-1002

Message `Attempt to create switch <FID> failed. Error message: <Error Message>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the switch with the specified fabric ID (FID) was not created.

Recommended Action Refer to the *Error Message* string displayed in the message for possible action.

PMGR-1003

Message `Attempt to delete switch <FID> succeeded.`

Message Type LOG | AUDIT

Class LS

Severity INFO

Probable Cause Indicates that the switch with the specified fabric ID (FID) was successfully deleted.

Recommended Action No action is required.

PMGR-1004

Message `Attempt to delete switch <FID> failed. Error message: <Error Message>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the switch with the specified fabric ID (FID) was not deleted.

Recommended Action Refer to the *Error Message* string displayed in the message for possible action.

PMGR-1005

Message `Attempt to move port(s) to switch <FID> succeeded.`

Message Type LOG

Severity INFO

Probable Cause Indicates a successful attempt to move the ports to the specified switch.

Recommended Action No action is required.

PMGR-1006

Message `Attempt to move port(s) <Ports> on slot <Slot> to switch <FID> failed. Error message: <Error Message>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates an unsuccessful attempt to move the ports to the specified switch.

Recommended Action Refer to the *Error Message* string displayed in the message for possible action.

PMGR-1007

Message `Attempt to change switch <FID> to switch <New FID> succeeded.`

Message Type LOG

Severity INFO

Probable Cause Indicates successful change of the switch fabric ID (FID).

Recommended Action No action is required.

PMGR-1008

Message `Attempt to change switch <FID> to switch <New FID> failed. Error message: <Error Message>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates a failed attempt to change the switch fabric ID (FID).

Recommended Action Refer to the *Error Message* string displayed in the message for possible action.

PMGR-1009

Message `Attempt to change the base switch to switch <FID> succeeded.`

Message Type LOG

Severity INFO

Probable Cause Indicates successful change of the base switch.

Recommended Action No action is required.

PMGR-1010

Message `Attempt to change the base switch to switch <FID> failed. Error message: <Error Message>`

Message Type LOG

Severity WARNING

Probable Cause Indicates a failed attempt to change the base switch.

Recommended Action Refer to the *Error Message* string displayed in the message for possible action.

PMGR-1011

Message `Attempt to move port(s) to switch <FID> succeeded.`

Message Type LOG

Severity INFO

Probable Cause Indicates a successful attempt to move the ports to the specified switch.

Recommended Action No action is required.

PORT Messages

PORT-1003

Message `Port <port number> Faulted because of many Link Failures.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the specified port is now disabled because the link on this port had multiple failures that exceeded an internally set threshold on the port. This problem is typically related to hardware.

Recommended Action Check and replace (if necessary) the hardware attached to both ends of the specified port number, including:

- The media (SFPs)
- The cable (fiber optic or copper inter-switch link (ISL))
- The attached devices

After checking the hardware, execute the **portEnable** command to re-enable the port.

PORT-1004

Message `Port <port number> (0x<port number (hex)>) could not be enabled because it is disabled due to long distance.`

Message Type LOG

Severity INFO

Probable Cause Indicates the specified port is not enabled because other ports in the same group have used the buffers for this port group. This happens when other ports were configured to be long distance.

Recommended Action To enable this port, perform one of the following actions:

- Reconfigure the other E_Ports so they are not long distance.
- Change the other E_Ports so they are not E_Ports.

This will free some buffers and allow this port to be enabled.

PORT-1005

Message `Slot <slot number> port <port on slot> does not support configured L_Port. Issue portCfgLport to clear configuration.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the specified port is configured to be an L_Port, but the port does not support L_Port. If an L_Port is connected, then the port will be disabled because the port does not support L_Port. If an E_Port or F_Port is connected, then the port will not come up because it is configured to be an L_Port.

Recommended Action Execute the **portCfgLport** command to clear the L_Port configuration.

PORT-1006

Message `Configuration changed for port (ID: <port number>) in No_Module or No_Light state.`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates the configuration changes were made to an offline port in the No_Module or No_Light state.

Recommended Action No action is required.

PORT-1007

Message `Port (ID: <port number>) has been renamed to (<port name>).`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates a port has been reconfigured with a different name.

Recommended Action No action is required.

PORT-1008

Message `GigE Port (ID: <port number>) has been enabled.`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates a Gigabit Ethernet port has been enabled.

Recommended Action No action is required.

PORT-1009

Message `GigE Port (ID: <port number>) has been disabled.`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates a Gigabit Ethernet port has been disabled.

Recommended Action No action is required.

PORT-1010

Message `Port (ID: <port number>) QoS is disabled.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the port quality of service (QoS) is disabled due to the best effort setting on the 4 Gbps or 8 Gbps long distance platform.

Recommended Action No action is required.

PORT-1011

Message `Please swap to the previous port blade, disable all F-Port trunk ports on this slot (<slot number>), and then swap back to current blade.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that port in the previous blade had F-port trunking enabled. The current port does not support F-Port trunking.

Recommended Action Perform blade swap to the previous port blade, disable all F-Port trunk ports on this blade.

PS Messages

PS-1000

Message `Failed to initialize Advanced Performance Monitoring.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that an unexpected software error has occurred in Advanced Performance Monitoring. The Performance Monitor has failed to initialize.

Recommended Action The control processor (CP) will reboot or failover automatically. If it does not, reboot or power cycle the switch to reinitiate the firmware.

PS-1001

Message `Advanced Performance Monitoring configuration updated due to change in PID format.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the port ID (PID) format was changed.

Recommended Action No action is required. Refer to the *Fabric OS Administrator's Guide* for more information about the PID format.

PS-1002

Message `Failed to initialize the tracing system for Advanced Performance Monitoring.`

Message Type LOG

Severity INFO

Probable Cause Indicates that an unexpected software error has occurred in Advanced Performance Monitoring. The Performance Monitor tracing system has failed to initialize.

Recommended Action Tracing will not be available for Advanced Performance Monitoring, but other functions will function normally. To activate tracing, reboot or failover the control processor (CP).

PS-1003

Message `Failed to set end-to-end monitoring mask on ISL ports.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the restoring configuration has attempted to set the end-to-end monitoring mask on at least one inter-switch link (ISL) port.

Recommended Action No action is required. End-to-end monitoring is not supported on ISL ports when ISL monitoring is enabled. ISL monitoring can only be disabled through the Fabric Access API.

PS-1004

Message `Failed to add end-to-end monitors on port <port> which is an ISL port.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the restoring configuration has attempted to add end-to-end monitors on at least one inter-switch link (ISL) port.

Recommended Action No action is required. End-to-end monitoring is not supported on ISL ports when ISL monitoring is enabled. ISL monitoring can only be disabled through the Fabric Access API.

PS-1005

Message `ISL monitor on port <port> stopped counting because no hardware resources are available.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that inter-switch link (ISL) and end-to-end monitors have used up all the hardware resources.

Recommended Action To resume counting, delete some end-to-end monitors sharing the same hardware resource pool by using the **perfDelEEMonitor** command.

PS-1006

Message `Failed to add fabricmode toptalker monitors on domain=<domain id>, because end-to-end monitors are configured on this switch.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that end-to-end monitors are configured on the switch.

Recommended Action Delete end-to-end monitors on the switch and re-install the fabric mode Top Talker monitor. End-to-end monitors and fabric mode Top Talker monitors are mutually exclusive.

PS-1007

Message `Failed to add Fabricmode Top Talker on domain=<domain id>. <function name>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that FC Routing (FCR) is enabled on the specified fabric.

Recommended Action Top Talker cannot be installed on a fabric with FCR service enabled. In case Top Talker must be installed on a fabric, disable FCR using the **fosconfig --disable fcr** command.

PS-1008

Message `Failed to delete fabricmode Top Talker monitor on domain <domain id>, Failure reason: <error code>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the fabric is not stable, the domain is not reachable, or the resource is not available.

Recommended Action Wait for the fabric to become stable and then execute the **perfttmon --delete fabricmode** command.

PS-1009

Message `Failed to add the device updates in condb database.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the fabric has more than the allowed number of devices.

Recommended Action Reduce the number of devices configured in the fabric to be within the allowed limit. The maximum number of devices that can be configured in a fabric is 940.

PS-1010

Message `Removed <Toptaker mode> Top Talker on port <Port no>. Reason: <Reason>.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that Top Talker on the specified port has been removed due to memory allocation failure.

Recommended Action Install Top Talker again on the specified port using the **perfttmon --add** command.

PSWP Messages

PSWP-1001

Message

```
PID for port <wwn name corresponding to source port> and port <wwn name
corresponding to destination port> are swapped. New PID for port <wwn name
corresponding to source port> is 0x<wwn name corresponding to destination port>
and port <new area corresponding to source wwn> is 0x<new area corresponding to
destination wwn>.
```

Message Type LOG

Severity INFO

Probable Cause Indicates the **portSwap** command has been issued.

Recommended Action No action is required.

PSWP-1002

Message

```
Port Swap feature enabled.
```

Message Type LOG

Severity INFO

Probable Cause Indicates the port swap feature has been enabled in the switch.

Recommended Action No action is required.

PSWP-1003

Message

```
Port Swap feature disabled.
```

Message Type LOG

Severity INFO

Probable Cause Indicates the port swap feature has been disabled in the switch.

Recommended Action No action is required.

PSWP-1004

Message `Blade Swap complete for slots <slot number corresponding to the source blade> and <slot number corresponding to the destination blade>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the **bladeSwap** command has been issued.

Recommended Action No action is required.

PSWP-1005

Message `Blade Swap undo failed with error code <error code from undoBladeSwap>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the **bladeSwap** command has not been undone.

Recommended Action Use the **portSwapShow** command to display a list of currently swapped ports; then use the **portSwap** command to achieve the desired result.

PSWP-1006

Message `Blade Swap failed on configInit with error code <error code from configInit> in switch number <current switch number>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the **bladeSwap** command failed on access to configuration data.

Recommended Action Retry the command. If the failure persists, contact your switch service provider.

PSWP-1007

Message `Blade Swap failed on fabosInit with error code <error code from fabosInit> in switch number <current switch number>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the **bladeSwap** command failed on access to switch context.

Recommended Action Retry the command. If the failure persists, contact your switch service provider.

RAS Messages

RAS-1001

Message `First failure data capture (FFDC) event occurred.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a first failure data capture (FFDC) event occurred and the failure data has been captured.

Recommended Action Execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

RAS-1002

Message `First failure data capture (FFDC) reached maximum storage size (<log size limit> MB).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the storage size for first failure data capture (FFDC) has reached the maximum.

Recommended Action Execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

RAS-1004

Message `Software 'verify' error detected.`

Message Type LOG | FFDC

Severity WARNING

Probable Cause Indicates an internal software error.

Recommended Action Execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

RAS-1005

Message `Software 'assert' error detected.`

Message Type LOG | FFDC

Severity WARNING

Probable Cause Indicates an internal software error.

Recommended Action Execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

RAS-1006

Message `Support data file (<Uploaded file name>) automatically transferred to remote address ' <Remote target designated by user> '.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the support data was automatically transferred from the switch to the configured remote server.

Recommended Action No action is required.

RAS-1007

Message `System is about to reload.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the system reload was initiated.

Recommended Action No action is required.

RAS-1008

Message `supportftp parameters are not configured. One of the required parameter is missing.`

Message Type LOG

Severity INFO

Probable Cause Indicates that one or more support FTP parameters were not specified with the **supportFtp** command in non-interactive mode.

Recommended Action Specify all support FTP parameters.

RAS-2001

Message `Audit message log is enabled.`

Message Type LOG | AUDIT

Class RAS

Severity INFO

Probable Cause Indicates that the audit message log has been enabled.

Recommended Action No action is required.

RAS-2002

Message `Audit message log is disabled.`

Message Type LOG | AUDIT

Class RAS

Severity INFO

Probable Cause Indicates that the audit message log has been disabled.

Recommended Action No action is required.

RAS-2003

Message `Audit message class configuration has been changed to <New audit class configuration>.`

Message Type LOG | AUDIT

Class RAS

Severity INFO

Probable Cause Indicates that the audit event class configuration has been changed.

Recommended Action No action is required.

RAS-2004

Message `prom access is enabled.`

Message Type LOG | AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the PROM access has been enabled.

Recommended Action No action is required.

RAS-2005

Message `prom access is disabled.`

Message Type LOG | AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the PROM access has been disabled.

Recommended Action No action is required.

RAS-3001

Message `USB storage device plug-in detected.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the USB storage device plug-in has been detected.

Recommended Action No action is required.

RAS-3002

Message `USB storage device enabled.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the USB storage device has been enabled.

Recommended Action No action is required.

RAS-3003

Message `USB storage device was unplugged before it was disabled.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the USB storage device was unplugged before it was disabled.

Recommended Action No action is required. It is recommended to disable the USB storage device using the **usbstorage -d** command before unplugged it from the system.

RAS-3004

Message `USB storage device disabled.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the USB storage device has been disabled.

Recommended Action No action is required.

RAS-3005

Message `CLI: <CLI command>.`

Message Type AUDIT

Class CLI

Severity INFO

Probable Cause Indicates that the specified command was executed on console.

Recommended Action No action is required.

RCS Messages

RCS-1001

Message `RCS has been disabled. Some switches in the fabric do not support this feature.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the reliable commit service (RCS) feature has been disabled on the local switch because not all switches in the fabric support RCS or the switch is in non-native mode.

Recommended Action Run the **rcsInfoShow** command to view RCS capability on the fabric. RCS is supported in Fabric OS v2.6, v3.1 and later, and v4.1 and later.

Run the **firmwareDownload** command to upgrade the firmware for any switches that do not support RCS.

RCS-1002

Message `RCS has been enabled.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the reliable commit service (RCS) feature has been enabled. RCS must be capable on all switches in the fabric to be enabled. If all switches are capable, it is automatically enabled.

Recommended Action No action is required.

RCS-1003

Message `Failed to allocate memory: (<function name>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified reliable commit service (RCS) function has failed to allocate memory.

Recommended Action This message is usually transitory. Wait for few minutes and retry the command.

Check memory usage on the switch using the **memShow** command.

Reboot or power cycle the switch.

RCS-1004

Message `Application(<application name>) not registered.(<error string>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified application did not register with reliable commit service (RCS).

Recommended Action

Run the **haShow** command to view the HA state.

Run the **haDisable** and **haEnable** commands.

Run the **rcsInfoShow** command to view RCS capability on the fabric. RCS is supported in Fabric OS v2.6, v3.1 and later, and v4.1 and later.

Run the **firmwareDownload** command to upgrade the firmware for any switches that do not support RCS.

RCS-1005

Message `Phase <RCS phase>, <Application Name> Application returned <Reject reason>, 0x<Reject code>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a receiving switch is rejecting the specified reliable commit service (RCS) phase.

Recommended Action

If the reject is in the acquire change authorization (ACA) phase, wait for several minutes and then retry the operation from the sender switch.

If the reject is in the stage fabric configuration (SFC) phase, check if the application license exists for the local domain and if the application data is compatible.

RCS-1006

Message `State <RCS phase>, Application <Application Name> AD<Administrative Domain>, RCS CM. Domain <Domain ID that sent the reject> returned 0x<Reject code>. App Response Code <Application Response Code>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified domain rejected a reliable commit service (RCS) phase initiated by an application on the local switch.

- If the reject phase is acquire change authorization (ACA), the remote domain may be busy and could not process the new request.
- If the reject phase is stage fabric configuration (SFC), the data sent by the application may not be compatible or the domain does not have the license to support that application.

Recommended Action If the reject is in the ACA phase, wait for several minutes and then retry the operation.

If the reject is in the SFC phase, check if the application license exists for the remote domain and if the application data is compatible.

RCS-1007

Message

```
Zone DB size and propagation overhead exceeds domain <domain number>'s maximum
supported Zone DB size <max zone db size>. Retry after reducing Zone DB size.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified domain cannot handle the zone database being committed.

Recommended Action Reduce the zone database size.

RCS-1008

Message

```
Domain <domain number> Lowest Max Zone DB size.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates the specified domain has the lowest memory available for the zone database in the fabric. The zone database must be smaller than the memory available on this domain.

Recommended Action Reduce the zone database size.

RCS-1009

Message

```
Request remote domain <domain number> offline because it does not support RCS.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified remote domain is requested to go offline to take it out of the fabric because it does not support reliable commit service (RCS).

Recommended Action Run the **fabricShow** command to verify that the remote domain is out of the fabric.

RCS-1010

Message

```
Domain <domain number> is RCS-incapable. Disabled <Number of E_ports disabled>
E_Port(s) connected to this domain.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that the specified remote domain is RCS-incapable, or the RCS-capable information could not be retrieved for the specified remote domain due to some potential routing issues.

Recommended Action

Run the **rcsInfoShow** command to view RCS capability of the switch.

Investigate for routing issue or check the cabling, and re-enable the disabled E_Ports to attempt another exchange of RCS-capable information.

RCS-1011

Message

```
Remote domain <domain number> is RCS-incapable. Configure this domain as
RCS-capable.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that the specified remote domain is RCS-incapable, or the RCS-capable information could not be retrieved for the specified remote domain due to some potential routing issues.

Recommended Action

Run the **rcsInfoShow** command to view RCS capability of the switch.

Investigate for routing issue or check the cabling, and re-enable the disabled E_Ports to attempt another exchange of RCS-capable information.

RCS-1012

Message

```
Local domain is RCS incapable (ForceDisabled is <Flag which denotes whether switch
is RCS capable or not>), hence reject the RCS_INFO request from domain <domain
number>.
```

Message Type

LOG | FFDC

Severity

WARNING

Probable Cause

Indicates that the specified domain is RCS-incapable.

Recommended Action

Execute the **supportSave** command and contact your switch service provider.

RCS-1013

Message `Remote domain <domain number> is RCS incapable.`

Message Type LOG | FFDC

Severity WARNING

Probable Cause Indicates that the specified remote domain is RCS-incapable.

Recommended Action Execute the **supportSave** command and contact your switch service provider.

RKD Messages

RKD-1001

Message `<Re-key type (First time encryption/Rekey/Write Metadata)> operation <Re-key action (started/completed/cancelled)>. Target: <Target physial WWN>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>. SessionId:<Session ID>/<Session MN>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a first-time encryption, re-key, or write metadata operation was started, completed, or canceled.

Recommended Action No action is required.

RKD-1002

Message `Could not start <Re-key type (First time encryption/Rekey/Write Metadata)> operation. <I/T/L String>. No response from cluster member WWN: <EE WWN> Slot: <EE Slot Number>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that a first-time encryption, re-key, or write metadata operation was not started.

Recommended Action Correct the cluster Ethernet link error and try to start the re-key operation again.

RKD-1003

Message `<Re-key type (First time encryption/Rekey/Write Metadata)> encountered a FATAL SCSI error and will be suspended. <I/T/L String>. Command: <Read/Write>; LBA: <LBA String>; Num Blocks: 0x<Num of Blocks>; Error: <Error String>; SK/ASC: <SCSI Sense Key>/<SCSI ASC>.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that a first-time encryption, re-key, or write metadata operation encountered a fatal SCSI error and was suspended.

Recommended Action Correct the error and resume the re-key operation.

RKD-1004

Message `Message: <Generic re-key message>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the generic re-key message.

Recommended Action No action is required.

RKD-1005

Message `LUN with LSN: <LUN LSN> does no have metadata. Make note of key ID <Key ID for encrypt/decrypt> that will be used for encryption/decryption of the LUN.`

Message Type LOG

Severity WARNING

Probable Cause Indicates uncompressible data on blocks 1 through 16 of the LUN.

Recommended Action Migrate the data on this LUN to a larger LUN and add it to the container using the **-newLUN** option.

RMON Messages

RMON-1001

Message `RMON rising threshold alarm from SNMP OID <oid>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the threshold level was exceeded for the sample type of the remote monitoring (RMON) alarm.

Recommended Action Check the traffic on the interface using the **show interface** command.

Note that you can use the **show interface** command to check the traffic on the interface, provided the statistics on the interface are not cleared using the **clear counters** command.

RMON-1002

Message `RMON falling threshold alarm from SNMP OID <oid>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the threshold level has come down for the sample type of the remote monitoring (RMON) alarm.

Recommended Action Check the traffic on the interface using the **show interface** command.

Note that you can use the **show interface** command to check the traffic on the interface, provided the statistics on the interface are not cleared using the **clear counters** command.

RPCD Messages

RPCD-1001

Message `Authentication Error: client \"<IP address>\" has bad credentials: <bad user name and password pair>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates an authentication error was reported. The specified client IP address has faulty credentials.

Recommended Action Enter the correct user name and password from the Fabric Access API host.

RPCD-1002

Message `Missing certificate file. Secure RPCd is disabled.`

Message Type LOG

Severity WARNING

Probable Cause Indicates a Secure Sockets Layer (SSL) certificate is missing.

Recommended Action To enable remote procedure call daemon (RPCD) in secure mode, install a valid SSL certificate on the switch.

RPCD-1003

Message `Permission denied accessing certificate file. Secure RPCd is disabled.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the Secure Sockets Layer (SSL) certificate file configured on the switch could not be accessed because root did not have read-level access.

Recommended Action Change the file system access level for the certificate file to have root read-level access.

RPCD-1004

Message `Invalid certificate file. Secure RPCd is disabled.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the Secure Sockets Layer (SSL) certificate file has been corrupted.

Recommended Action To enable remote procedure call daemon (RPCD) in secure mode, install a valid SSL certificate on the switch.

RPCD-1005

Message `Missing private key file. Secure RPCd is disabled.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the private key file is missing.

Recommended Action Run the **secCertUtil** command to install a valid private key file.

RPCD-1006

Message `Permission denied accessing private key file. Secure RPCd is disabled.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the private key file configured on the switch could not be accessed because the root did not have read-level access.

Recommended Action Change the file system access level for the private key file to have root read-level access.

RPCD-1007

Message `Invalid private file. Secure RPCd is disabled.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the private key file has been corrupted.

Recommended Action Run the **secCertUtil** command to install a valid private key file.

RTE Messages

RTE-1001

Message

```
Detected route inconsistency. It may cause connectivity issues. If such issues
arise, bounce all ISLs and ICLs on this chassis.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the constraints that are used to determine the paths for Dynamic Path Selection (DPS) are not synchronized from active control processor (CP) to standby CP during the failover. This event causes route inconsistencies.

Recommended Action

Reset all E_ports on the chassis using the **portDisable** and **portEnable** commands.

RTWR Messages

RTWR-1001

Message

```
RTWR <routine: error message> 0x<detail 1>, 0x<detail 2>, 0x<detail 3>, 0x<detail
4>, 0x<detail 5>.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that an error occurred in Reliable Transport With Response (RTWR) due to one of the following reasons:

- The system ran out of memory.
- The domain may be unreachable
- The frame transmission failed.
- An internal error or failure occurred.

The message contains the name of the routine that has an error and other error-specific information. Refer to values in details 1 through 5 for more information.

Recommended Action

Restart the switch.

RTWR-1002

Message

```
RTWR <error message: maximum retries exhausted> 0x<port>, 0x<domain ID>, 0x<retry
count>, 0x<status>, 0x<process ID>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that Reliable Transport With Response (RTWR) has exhausted the maximum number of retries for sending data to the specified domain.

Recommended Action

Execute the **fabricShow** command to verify that the specified domain ID is online.

If the switch with the specified domain ID is offline, enable the switch using the **switchEnable** command.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

RTWR-1003

Message

```
<module name>: RTWR retry <number of times retried> to domain <domain ID>, iu_data
<first word of iu_data>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates the number of times Reliable Transport With Response (RTWR) has failed to get a response and retried.

Recommended Action

Execute the **fabricShow** command to verify that the specified domain ID is reachable.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

SCN Messages

SCN-1001

Message `SCN queue overflow for process <daemon name>.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that an attempt to write a state change notification (SCN) message to a specific queue has failed because the SCN queue for the specified daemon is full. This may be caused by the daemon hanging or the system being busy.

The following are some valid values for the *daemon name*:

- fabricd
- asd
- evmd
- fcpd
- webd
- msd
- nsd
- psd
- snmpd
- zoned
- fspfd
- tsd

Recommended Action If this message is caused by the system being busy, the condition is temporary.

If this message is caused by a hung daemon, the software watchdog will cause the daemon to dump the core and reboot the switch. In this case, execute the **supportSave** command to send the core files using FTP to a secure server location.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

SCN-1002

Message `SCN queue overflow for process <daemon name>.`

Message Type FFDC | LOG

Severity WARNING

Probable Cause Indicates that an attempt to write a state change notification (SCN) message to a specific queue has failed because the SCN queue for the specified daemon is full. This may be caused by the daemon hanging or the system being busy.

The following are some of the valid values for the *daemon name*:

- fabricd
- asd
- evmd
- fcpd
- webd
- msd
- nsd
- psd
- snmpd
- zoned
- fspfd
- tsd

Recommended Action If this message is caused by the system being busy, the condition is temporary.

If this message is caused by a hung daemon, the software watchdog will cause the daemon to dump the core and reboot the switch. In this case, execute the **supportSave** command to send the core files using FTP to a secure server location.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

SEC Messages

SEC-1001

Message `RCS process fails: <reason code>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the reliable commit service (RCS) process failed to complete. RCS is a mechanism for transferring data from one switch to other switches within the fabric. RCS ensures that either all or none of the switches commit to the database. RCS can fail if one switch in the fabric is busy or in an error state that prevents it from accepting the database.

Recommended Action RCS is evoked when the security database is modified by a security command (for example, **secPolicySave**, **secPolicyActivate**, or **distribute**). If the switch is busy, the command may fail the first time. Retry the command.

Run the **rcsInfoShow** command to view RCS capability on the fabric. RCS must be capable on all switches in the fabric to be enabled. If all switches are capable, it is automatically enabled.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

SEC-1002

Message `Security data fails: <Reason Text>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the receiving switch fails to validate the security database sent from the primary fabric configuration server (FCS) switch. This may be caused by several factors: the data package may be corrupted, the time stamp on the package may be out of range as a result of replay attack or out-of-sync time service, or the signature verification failed. Signature verification failure may result from an internal error, such as losing the primary public key or an invalid database.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that switch. The error may also be a result of an internal corruption or a hacker attack to the secure fabric. If you have reason to believe that the error is the result of a possible security breach, take appropriate action as defined by your enterprise security policy.

SEC-1003

Message `Fail to download security data to domain <Domain number> after <Number of retires> retries.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the specified domain failed to download security data after the specified number of attempts, and that the failed switch encountered an error accepting the database download. The primary switch will segment the failed switch after 30 tries.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

SEC-1005

Message `Primary FCS receives data request from domain <Domain number>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the primary fabric configuration server (FCS) received a data request from the specified domain. For example, if the switch fails to update the database or is attacked (data injection), a message is generated to the primary FCS to try to correct and resynchronize with the rest of the switches in the fabric.

Recommended Action Use the **secFabricShow** command to check whether any of the switches in the fabric encountered an error. If one or more of the switches is not in the ready state, and you have reason to believe that the error is the result of a possible security breach, take appropriate action as defined by your enterprise security policy.

SEC-1006

Message `Security statistics error: Failed to reset due to invalid <data>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that invalid data has been received for any statistic-related command for security (**secStatsShow** or **secStatsReset**). The counter is updated automatically when a security violation occurs. This message may also occur if the updating counter fails.

Recommended Action If the message is the result of a user command, retry the statistic command.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

SEC-1007

Message `Security violation: Unauthorized host with IP address <IP address of the violating host> tries to establish API connection.`

Message Type LOG

Severity INFO

Probable Cause Indicates a security violation was reported. The IP address of the unauthorized host is displayed in the message.

Recommended Action Check for unauthorized access to the switch through the API connection.

SEC-1008

Message `Security violation: Unauthorized host with IP address <IP address of the violating host> tries to establish HTTP connection.`

Message Type LOG

Severity INFO

Probable Cause Indicates a security violation was reported. The IP address of the unauthorized host is displayed in the message.

Recommended Action Check for unauthorized access to the switch through the HTTP connection.

SEC-1009

Message `Security violation: Unauthorized host with IP address <IP address of the violating host> tries to establish TELNET connection.`

Message Type LOG

Severity INFO

Probable Cause Indicates a security violation was reported. The IP address of the unauthorized host is displayed in the message.

Recommended Action Check for unauthorized access to the switch through the Telnet connection.

SEC-1010

Message `RCS rejected: <Reason String>.`

Message Type LOG

Severity ERROR

Probable Cause Trying to distribute the database from a non-primary switch.

Recommended Action Resolve the specified error by executing the command only from the primary FCS.

SEC-1016

Message `Security violation: Unauthorized host with IP address <IP address of the violating host> tries to establish SSH connection.`

Message Type LOG

Severity INFO

Probable Cause Indicates a security violation was reported. The IP address of the unauthorized host is displayed in the message.

Recommended Action Check for unauthorized access to the switch through the SSH connection.

SEC-1022

Message `Failed to <operation> PKI objects.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the fabric failed to generate or validate either the public or private key pair or the certificate signing request (CSR).

Recommended Action Run the **secCertUtil show -fcapall** command and verify that all public key infrastructure (PKI) objects exist on the switch. If the private key does not exist, follow the steps for re-creating PKI objects outlined in the *Fabric OS Administrator's Guide*. If a certificate does not exist or is invalid, install the certificate by following the field upgrade process.

SEC-1024

Message `The <DB name> security database is too large to fit in flash.`

Message Type LOG

Severity INFO

Probable Cause Indicates the size of the security database is too large for the flash memory. The size of the security database increases with the number of entries in each policy.

Recommended Action Reduce the size of the security database by reducing the number of entries within each policy.

SEC-1025

Message `Invalid IP address (<IP address>) detected.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can occur only when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1026

Message `Invalid format or character in switch member <switch member ID>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can occur only when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1028

Message `No name is specified.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can occur only when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1029

Message `Invalid character in <policy name>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can occur only when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1030

Message `The length of the name is invalid.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can occur only when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1031

Message `Current security policy DB cannot be supported by standby. CPs will go out of sync.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the security database size is not supported by the standby control processor (CP).

Recommended Action Reduce the security policy size by deleting entries within a policy or by deleting some policies.

SEC-1032

Message `Empty FCS list is not allowed.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1033

Message `Invalid character used in member parameter to add switch to SCC policy; command terminated.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a member parameter in the **secPolicyAdd** command is invalid (for example, it may include an invalid character, such as an asterisk). A valid switch identifier (a WWN, a domain ID, or a switch name) must be provided as a member parameter in the **secPolicyAdd** command. Only the **secPolicyCreate** command supports use of the asterisk for adding switches to policies.

Recommended Action Run the **secPolicyAdd** command using a valid switch identifier (WWN, domain ID, or switch name) to add specific switches to the Switch Connection Control (SCC) policy.

SEC-1034

Message `Invalid member <policy member>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the input list has an invalid member.

Recommended Action Verify the member names, and input the correct information.

SEC-1035

Message `Invalid device WWN <device WWN>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the specified World Wide Name (WWN) is invalid.

Recommended Action Enter the correct WWN value.

SEC-1036

Message `Device name <device name> is invalid due to a missing colon.`

Message Type LOG

Severity ERROR

Probable Cause Indicates one or more device names mentioned in the **secPolicyCreate** or **secPolicyAdd** commands does not have the colon character (:) as required.

Recommended Action Run the **secPolicyCreate** or **secPolicyAdd** command with a properly formatted device name parameter.

SEC-1037

Message `Invalid WWN format <invalid WWN>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the WWN entered in the policy member list has an invalid format.

Recommended Action Run the command again using the standard WWN format; 16 hexadecimal digits grouped as 8 colon-separated pairs, for example, 50:06:04:81:D6:F3:45:42.

SEC-1038

Message `Invalid domain <domain ID>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates an invalid domain ID was entered.

Recommended Action Verify that the domain ID is correct. If it is not, re-run the command using the correct domain ID.

SEC-1039

Message `<message>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the domain ID entered is out of range.

Recommended Action Verify that the domain ID is correct. If it is not, re-run the command using the correct domain ID.

SEC-1040

Message `Invalid portlist (<port list>). Cannot combine * with port member in the same portlist.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the port list contains the wildcard asterisk (*) character. You cannot use the asterisk in a port list.

Recommended Action Enter the port list values without any wildcard characters.

SEC-1041

Message `Invalid port member <port member> in portlist (<port list>). <Reason>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the port member is invalid for one of the following reasons:

- The value is not a number.
- The value is too long. Valid numbers must be between one and three characters long.
- The value cannot be parsed due to invalid characters.

Recommended Action Use valid syntax when entering port members.

SEC-1042

Message `Invalid index/area member <port member> in portlist (<Port list>). Out of range (<Minimum value> - <Maximum value>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates the specified index or area member is not within the minimum and maximum range.

Recommended Action Use valid syntax when entering index or area numbers.

SEC-1043

Message `Invalid port range <Minimum> - <Maximum>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the specified port is not within the minimum and maximum range.

Recommended Action Use valid syntax when entering port ranges.

SEC-1044

Message `Duplicate member <member ID> in (<List>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates the specified member is a duplicate in the input list. The list can be a policy list or a switch member list.

Recommended Action Do not specify any duplicates.

SEC-1045

Message `Too many port members.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1046

Message `Empty list.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1049

Message `Invalid switch name <switch name>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1050

Message `There are more than one switches with the same name <switch name> in the fabric.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1051

Message `Missing brace for port list <port list>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1052

Message `Invalid input.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1053

Message `Invalid pFCS list <pFCS list>`

Message Type LOG

Severity ERROR

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds these error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1054

Message `Invalid FCS list length <list length>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1055

Message `Invalid FCS list <WWN list>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1056

Message `Invalid position <New position>. Only <Number of members in FCS list> members in list.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1057

Message `No change. Both positions are the same.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1059

Message `Fail to <operation, e.g., save, delete, etc.,> <named item> to flash.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the operation failed when writing to flash memory.

Recommended Action Run the **supportFtp - e** command to FTP files from the switch and remove them from the flash memory.

SEC-1062

Message `Invalid number of Domains in Domain List.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that either no domains or domains more than the maximum number supported are specified.

Recommended Action Enter the correct number of domains.

SEC-1063

Message `Failed to reset statistics.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that either the type or the domains specified are invalid.

Recommended Action Enter valid input.

SEC-1064

Message `Failed to sign message.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the public key infrastructure (PKI) objects on the switch are not in a valid state and the signature operation failed.

Recommended Action Run the **secCertUtil show -fcapall** command to verify that all PKI objects are valid. If PKI objects are not valid, generate the PKI objects and install the certificate by following the field upgrade process.

SEC-1065

Message `Invalid character in list.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the input list has an invalid character.

Recommended Action Enter valid input.

SEC-1069

Message `Security Database is corrupted.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the security database is corrupted for unknown reasons.

Recommended Action Execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

SEC-1071

Message `No new security policy data to apply.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that no changes in the defined security policy database need to be activated at this time.

Recommended Action Verify that the security event was planned. First change some policy definitions, and then run the **secPolicyActivate** command to activate the policies.

SEC-1072

Message `<Policy type> Policy List is Empty.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the specific policy type is empty. The security database is corrupted for unknown reasons.

Recommended Action Execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

SEC-1073

Message `No FCS policy in list.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the specific policy type is empty. The security database is corrupted for unknown reasons.

Recommended Action Execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

SEC-1074

Message `Cannot execute the command on this switch. Please check the secure mode and FCS status.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a security command was run on a switch that is not allowed to run it either because it is in non-secure mode or because it does not have the required fabric configuration server (FCS) privilege.

Recommended Action If a security operation that is not allowed in non-secure mode is attempted, do not perform the operation in non-secure mode. In secure mode, run the command from a switch that has the required privilege; that is, either a backup FCS or primary FCS.

SEC-1075

Message `Fail to <operation> new policy set on all switches.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1076

Message `NoNodeWWNZoning option has been changed.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the NoNodeWWNZoning option has been changed. If the option is turned on, a zone member can be added using node WWNs, but the member will not be able to communicate with others nodes in the zone.

Recommended Action Re-enable the current zone configuration for the change to take effect.

SEC-1077

Message `Failed to activate new policy set on all switches.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the policy could not be activated. Possible reasons that the policy could not be activated include not enough memory or a busy switch.

Recommended Action Run the **secFabricShow** command to verify that all switches in the fabric are in the ready state. Retry the command when all switches are ready.

SEC-1078

Message `No new data to abort.`

Message Type LOG

Severity ERROR

Probable Cause Indicates there are no new changes in the defined security policy database that can be aborted.

Recommended Action Verify the security event was planned. Verify if there were really any changes to the defined policy database that can be aborted.

SEC-1079

Message `The policy name <policy name> is invalid.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the policy name entered in the **secPolicyCreate**, **secPolicyActivate**, **secPolicyAdd**, or **secPolicyDelete** command was invalid.

Recommended Action Run the command again using a valid policy name.

SEC-1080

Message `Operation denied. Please use secPolicyActivate or distribute commands.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **fabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1081

Message `Entered a name for a DCC policy ID that was not unique.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the Device Connection Control (DCC) policy name given in the **secPolicyCreate** command was the same as another DCC policy.

Recommended Action Make sure that the DCC policy name has a unique alphanumeric string, and run the **secPolicyCreate** command again.

SEC-1082

Message `Failed to create <policy name> policy.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the security policy was not created because of faulty input or low resources.

Recommended Action Use proper syntax when creating policies. If the security database is too large, you must delete other members within the database before adding new members to a policy.

SEC-1083

Message `Name already exists.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **fabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1084

Message `Name exists for different type <Policy name>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the specified policy already exists.

Recommended Action No action is required.

SEC-1085

Message `Failed to create <policy name>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the security policy was not created.

Recommended Action Check that the current policy configuration is valid. For example, the RSNMP policy cannot exist without the WSNMP policy.

SEC-1086

Message `The security database is too large to fit in flash.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the security database has more data than the flash memory can accommodate.

Recommended Action Reduce the number of entries in some policies to decrease the security database size.

SEC-1087

Message `The security database is larger than the data distribution limit of fabric <fabric data distribution limit> bytes.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the security database has more data than can be distributed to some of the switches in the fabric.

Recommended Action Reduce the number of entries in the security policies to decrease the security database size.

SEC-1088

Message `Cannot execute the command. Please try later.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **fabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1089

Message `Policy name <policy name> was not found.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the security policy name in the **secPolicyAdd** command does not exist.

Recommended Action Create the appropriate security policy first, and then use its name in the **secPolicyAdd** command to add new members.

SEC-1090

Message `SCC list contains FCS member. Please remove member from the FCS policy first.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **fabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1091

Message `No policy to remove.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the specified policy member does not exist or the policy itself does not exist.

Recommended Action Verify that the security policy name or member ID is correct.

SEC-1092

Message `<Policy name> Name not found.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **fabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1093

Message `New FCS list must have at least one member in common with current FCS list.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the new fabric configuration server (FCS) list does not have a common member with the existing FCS list.

Recommended Action Resubmit the command with at least one member of the new FCS list in common with the current FCS list.

SEC-1094

Message `Policy member not found.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **fabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1095

Message `Deleting FCS policy is not allowed.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **fabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1096

Message `Failed to delete <policy name> because <reason text>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a policy cannot be removed because deleting it would result in an invalid security policy configuration.

Recommended Action Verify the security policy configuration requirements and remove any policies that require the policy you want to be removed first.

SEC-1097

Message `Cannot find <active or defined> policy set.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the specified policy could not be found.

Recommended Action If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

SEC-1098

Message `No <active or defined> FCS list.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the specified policy could not be found.

Recommended Action Execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

SEC-1099

Message `Please enable your switch before running secModeEnable.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **fabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1100

Message `FCS switch present. Command terminated.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **fabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1101

Message `Failed to enable security on all switches. Please retry later.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the security enable failed on the fabric because one or more switches in the fabric are busy.

Recommended Action Verify that the security event was planned. If the security event was planned, run the **secFabricShow** command to verify that all switches in the fabric are in the ready state. When all switches are in the ready state, retry the operation.

SEC-1102

Message `Fail to download <security data>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the switch failed to download a certificate, security database, or policies. This can happen when the switch does not get enough resources to complete the operation, the fabric has not stabilized, or the policy database is an invalid format.

Recommended Action Wait for the fabric to become stable and then retry the operation. If the policy database is in an illegal format (with **configDownload** command), correct the format and retry the operation.

SEC-1104

Message `Fail to get primary <Certificate or public key>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the switch failed to get either the primary certificate or a primary public key.

Recommended Action Verify the primary switch has a valid certificate installed and retry the operation. If a valid certificate is not installed, install a certificate by following the procedure specified in the *Fabric OS Administrator's Guide*.

SEC-1105

Message `Fail to disable secure mode on all switches.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the switch failed to disable security in the fabric. This could happen if the switch cannot get the required resources to complete the command, and sending to a remote domain fails or the remote domain returns an error.

Recommended Action Run the **secFabricShow** to verify that all switches in the fabric are in the ready state. Retry the command when all switches are ready.

SEC-1106

Message `Failed to sign message data.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that some public key infrastructure (PKI) objects on the switch are not in a valid state, and a signature operation failed.

Recommended Action Run the **secCertUtil show -fcapall** command and verify that all PKI objects exist on the switch. If a failure to validate PKI objects occurs, follow the steps for re-creating PKI objects outlined in the *Fabric OS Administrator's Guide*.

SEC-1107

Message `Stamp is 0.`

Message Type LOG

Severity INFO

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1108

Message `Fail to reset stamp on all switches.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that a version reset operation failed either because the switch could not get all the required resources to perform the operation or because it failed to send the message to all switches in the fabric.

Recommended Action Verify that the security event was planned. If the security event was planned, run the **secFabricShow** command to verify that all switches in the fabric are in the ready state. When all switches are in the ready state, retry the operation.

SEC-1110

Message `FCS list must be the first entry in the [Defined Security policies] section. Fail to download defined database.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that a security policy download was attempted with a defined policy that does not have the fabric configuration server (FCS) policy as the first policy. The FCS policy is required to be the first policy in the defined security database.

Recommended Action Download a correct configuration with the fabric configuration server (FCS) policy as the first policy in the defined security database.

SEC-1111

Message `New defined FCS list must have at least one member in common with current active FCS list. Fail to download defined database.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the defined and active fabric configuration server (FCS) policy list failed to have at least one member in common.

Recommended Action A new FCS policy list must have at least one member in common with the previous FCS policy.

SEC-1112

Message `FCS list must be the first entry in the Active Security policies, and the same as the current active FCS list in the switch.`

Message Type LOG

Severity ERROR

Probable Cause Indicates either a security policy download was attempted with an active policy that does not have the fabric configuration server (FCS) policy as the first policy, or the FCS policy is not the same as the current FCS policy on the switch.

Recommended Action Make sure that the new FCS policy is the same as the current FCS policy on the switch.

SEC-1113

Message `<Key> [ <Feature> license ] going to expire in <Expiry_days> day(s).`

Message Type LOG | AUDIT

Class SECURITY

Severity WARNING

Probable Cause Indicates the license period will expire soon.

Recommended Action Get a new license for this feature.

SEC-1114

Message `<Key> [ <Feature> license ] has expired.`

Message Type LOG | AUDIT

Class SECURITY

Severity WARNING

Probable Cause Indicates the license period has expired.

Recommended Action Get a new license for this feature.

SEC-1115

Message `No primary FCS to failover.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that during an attempted **secFcsFailover**, no primary FCS is present in the fabric.

Recommended Action Run the **secFabricShow** command to verify that all switches in the fabric are in the ready state. When all switches are in the ready state, retry the operation.

SEC-1116

Message `Fail to commit failover.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1117

Message `Fail to set <data>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the switch failed to save the data received by the primary fabric configuration server (FCS) switch. This data can be an FCS password, a non-FCS password, SNMP data, or multiple user authentication data.

Recommended Action Run the **fabricShow** command to verify that all switches in the fabric are in the ready state. When all switches are in the ready state, retry the operation.

SEC-1118

Message `Fail to set SNMP string.`

Message Type LOG

Severity INFO

Probable Cause Indicates the SNMP string could not be set. Usually this problem is transient.

Recommended Action Retry the command.

SEC-1119

Message `Secure mode has been enabled.`

Message Type LOG

Severity INFO

Probable Cause Indicates the secure Fabric OS was enabled by the **secModeEnable** command.

Recommended Action Verify the security event was planned. If the security event was planned, there is no action required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1121

Message `Time is out of range when <text>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the time on the switch is not synchronized with the primary fabric configuration server (FCS), the data packet is corrupted, or a replay attack is launched on the switch.

Recommended Action Verify the security event was planned. If the security event was planned, verify that all switches in the fabric are in time synchronization with the primary FCS and that no external entity is trying to access the fabric. When verification is complete, retry the operation.

SEC-1122

Message `Error code: <Domain ID>, <Error message>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that one of the switches in the fabric could not communicate with the primary fabric configuration server (FCS).

Recommended Action Run the **fabricShow** command to verify that all switches in the fabric are in the ready state. When all switches are in the ready state, retry the operation.

SEC-1123

Message `Security database downloaded by Primary FCS.`

Message Type LOG

Severity INFO

Probable Cause Indicates the security database was successfully downloaded from the primary fabric configuration server (FCS).

Recommended Action No action is required.

SEC-1124

Message `Secure Mode is off.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a secure mode disable is attempted in a non-secure fabric.

Recommended Action No action is required.

SEC-1126

Message `Secure mode has been disabled.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a secure mode disable operation completed successfully.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1130

Message `The Primary FCS has failed over to a new switch.`

Message Type LOG

Severity INFO

Probable Cause Indicates a fabric configuration server (FCS) failover operation was completed successfully.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1135

Message `Secure fabric version stamp has been reset.`

Message Type LOG

Severity INFO

Probable Cause Indicates the version stamp of the secure fabric is reset.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1136

Message `Failed to verify signature <data type, MUA, policy, etc.,>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the receiving switch failed to validate the security database sent from the primary fabric configuration server (FCS) switch. This message usually indicates that the data package is corrupted, the time stamp on the package is out of range as a result of a replay attack or out-of-sync time service, or the signature verification failed. Signature verification failure indicates either an internal error (such as losing the primary public key) or an invalid database.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that switch. This message may also be the result of an internal corruption or a hacker attack to the secure fabric.

SEC-1137

Message `No signature in <data type, MUA, policy, etc.,>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the receiving switch failed to validate the security database sent from the primary fabric configuration server (FCS) switch. This message usually indicates that the data package is corrupted, the time stamp on the package is out of range as a result of a replay attack or out-of-sync time service, or the signature verification failed. Signature verification failure indicates either an internal error (such as losing the primary public key) or an invalid database.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that switch. This message may also be the result of an internal corruption or a hacker attack to the secure fabric.

SEC-1138

Message `Security database download received from Primary FCS.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a non-primary fabric configuration server (FCS) switch received a security database download.

Recommended Action Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1139

Message `The RSNMP_POLICY cannot exist without the WSNMP_POLICY.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the receiving switch failed to validate the security database sent from the primary fabric configuration server (FCS) switch. This message usually indicates that the data package is corrupted, the time stamp on the package is out of range as a result of a replay attack or out-of-sync time service, or the signature verification failed. Signature verification failure indicates either an internal error (such as losing the primary public key) or an invalid database.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that switch. This message may also be the result of an internal corruption or a hacker attack to the secure fabric.

SEC-1142

Message `Reject new policies. <reason text>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the new polices are rejected because of the reason specified.

Recommended Action Use proper syntax when entering policy information.

SEC-1145

Message `A security admin event has occurred. This message is for information purpose only. The message for individual event is: <Event specific data>.`

Message Type LOG

Severity INFO

Probable Cause Indicates one of the following has occurred:

- The names for the specified policies have changed.
- The passwords have changed for the specified accounts.
- The SNMP community strings have been changed.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1146

Message `PID changed: <State>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the PID format of the switch was changed either to extended-edge PID or from extended-edge PID. If the Device Connection Control (DCC) polices existed, all index/area ID values either increased or decreased by 16. The values wrap around after 128. If a DCC policy contains an index/area of 127 before changing to extended-edge PID, then the new index/area is 15, because of the wraparound.

Recommended Action No action is required.

SEC-1153

Message `Error in RCA: RCS is not supported.`

Message Type LOG

Severity INFO

Probable Cause Indicates that reliable commit service (RCS) is not supported.

Recommended Action Run the **rcsInfoShow** command to view RCS capability on the fabric. RCS must be capable on all switches in the fabric to be enabled. If all switches are capable, it is automatically enabled.

For any switch that does not support RCS, obtain the latest firmware version from your switch supplier, and run the **firmwareDownload** command to upgrade the firmware.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

SEC-1154

Message `PID change failed: <Reason> <defined status> <active status>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that either the defined or the active policy could not be updated. If the policy database is very large, it might not be able to change the index/area because the new policy database exceeds the maximum size. This message can also be caused when the switch is short of memory. The status values can be either defined, active, or both. A negative value means that a policy set was failed by the daemon.

Recommended Action Reduce the size of the policy database.

SEC-1155

Message `PID change failed: <Reason> <defined status> <active status>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that either the defined or active policy was too large after modifying the index/area ID. The status values can be either defined, active, or both. A negative value means that a policy set was failed by the daemon.

Recommended Action Reduce the size of the specified policy database.

SEC-1156

Message `Change failed: <Reason> <defined status> <active status>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the security daemon is busy. The status values can be defined, active, or both. A negative value means that a policy set was failed by the daemon.

Recommended Action For the first reject, wait a few minutes and then resubmit the transaction. Fabric-wide commands may take a few minutes to propagate throughout the fabric. Make sure to wait a few minutes between executing commands so that your commands do not overlap in the fabric.

SEC-1157

Message `PID Change failed: <Reason> <defined status> <active status>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the provisioning resources for a security policy failed because of low memory or internal error. The status values can be defined, active, or both. A negative value means that a policy set was failed by the daemon.

Recommended Action Retry the failed command.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

SEC-1158

Message `Invalid name <Policy or Switch name>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the specified name is invalid. The name can be a policy name or a switch name.

Recommended Action Enter a valid name.

SEC-1159

Message `Non_Reachable domain <Domain ID>.`

Message Type LOG

Severity INFO

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1160

Message `Duplicate port <port ID> in port list (<port list>).`

Message Type LOG

Severity INFO

Probable Cause Indicates a duplicate port member exists in the specified port list.

Recommended Action Verify that there is no duplicate port member in the port list.

SEC-1163

Message `System is already in secure mode. Lockdown option cannot be applied.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the lockdown option was attempted while the fabric is in secure mode.

Recommended Action Do not use the lockdown option with the **secModeEnable** command when a switch is already in secure mode.

SEC-1164

Message `Lockdown option cannot be applied on a non-FCS switch.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the attempt to enable security is made on a switch that is not present in the fabric configuration server (FCS) list.

Recommended Action Add the switch to the FCS policy list when using the lockdown option to enable security.

SEC-1165

Message `Low memory, failed to enable security on all switches.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the system is low on memory.

Recommended Action Wait a few minutes and try the command again.

SEC-1166

Message `Non FCS tries to commit failover.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1167

Message `Another FCS failover is in process. Command terminated.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that because another failover is already in progress, this failover attempt cannot proceed.

Recommended Action Verify the security event was planned. If the security event was planned, retry fabric configuration server (FCS) failover after the current failover has completed, if this switch should become the primary FCS. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1168

Message `Primary FCS failover is busy. Please retry later.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1170

Message `This command must be executed on the Primary FCS switch, the first reachable switch in the FCS list.`

Message Type LOG

Severity INFO

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1171

Message `Disabled secure mode due to invalid security object.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the switch is segmented, and secure mode is disabled on the switch because there was no license present or no public key infrastructure (PKI) objects.

Recommended Action Run the **secCertUtil show -fcapall** command to determine whether all PKI objects exist. If they do not exist, run the **secCertUtil** command to create them for the switch.

Run the **licenseAdd** command to install the required license key. Contact your switch supplier to obtain a license if you do not have one.

SEC-1172

Message `Failed to identify role.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the switch is unable to determine its role (primary FCS or backup FCS) in the secure fabric.

Recommended Action Verify all switches in the fabric are in time synchronization with the primary FCS and that no external entity is trying to access the fabric. When verification is complete, retry the operation.

SEC-1173

Message `Lost contact with Primary FCS switch.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the switch has lost contact with the primary fabric configuration server (FCS) switch in the secure fabric. This could result from the primary FCS being disabled.

Recommended Action If the primary FCS was disabled intentionally, no action is required; if not, check the primary FCS.

SEC-1174

Message `Failed to set <FCS or non-FCS> password.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the fabric configuration server (FCS) or non-FCS password could not be set.

Recommended Action Verify all switches in the fabric are in time synchronization with the primary FCS and that no external entity is trying to access the fabric. When verification is complete, retry the operation.

SEC-1175

Message `Failed to install zone data.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the zone database could not be installed on the switch.

Recommended Action Verify all switches in the fabric are in time synchronization with the primary FCS and that no external entity is trying to access the fabric. When verification is complete, retry the operation.

SEC-1176

Message `Failed to generate new version stamp.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the primary fabric configuration server (FCS) failed to generate a new version stamp because the fabric was not stable.

Recommended Action Verify all switches in the fabric are in time synchronization with the primary FCS and that no external entity is trying to access the fabric. When verification is complete, retry the operation.

SEC-1180

Message `Added account <user name> with <role name> authorization.`

Message Type LOG

Severity INFO

Probable Cause Indicates the specified new account has been created.

Recommended Action No action is required.

SEC-1181

Message `Deleted account <user name>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the specified account has been deleted.

Recommended Action No action is required.

SEC-1182

Message `Recovered <number of> accounts.`

Message Type LOG

Severity INFO

Probable Cause Indicates the specified number of accounts has been recovered from backup.

Recommended Action No action is required.

SEC-1183

Message `Policy to binary conversion error: Port <port number> is out range.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a security database conversion has failed because of an invalid value.

Recommended Action Retry the command with a valid value.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

SEC-1184

Message `<Security server (RADIUS/LDAP/TACACS+)> configuration change, action <action>, server ID <server name>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the specified action is applied to the specified remote authentication dial-in user service (RADIUS/LDAP/TACACS+) server configuration. The possible actions are ADD, REMOVE, CHANGE, and MOVE.

Recommended Action No action is required.

SEC-1185

Message `<action> switch DB.`

Message Type LOG

Severity INFO

Probable Cause Indicates the switch database was enabled or disabled as the secondary authentication, authorization, and accounting (AAA) mechanism when remote authentication dial-in user service (RADIUS/LDAP/TACACS+) is the primary AAA mechanism.

Recommended Action No action is required.

SEC-1186

Message `<Security server (RADIUS/LDAP/TACACS+)> <action> Configuration.`

Message Type LOG

Severity INFO

Probable Cause Indicates the RADIUS, LDAP, or TACACS+ configuration was enabled or disabled as the primary authentication, authorization, and accounting (AAA) mechanism.

Recommended Action No action is required.

SEC-1187

Message `Security violation: Unauthorized switch <switch WWN> tries to join fabric.`

Message Type LOG

Severity INFO

Probable Cause Indicates a Switch Connection Control (SCC) security violation was reported. The specified unauthorized switch attempts to join the fabric.

Recommended Action Check the SCC policy to verify the switches allowed in the fabric. If the switch should be allowed in the fabric but it is not included in the SCC policy, add the switch to the policy. If the switch is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

SEC-1188

Message `Security violation: Unauthorized device <device node name> tries to FLOGI to index/area <port number> of switch <switch WWN>.`

Message Type LOG

Severity INFO

Probable Cause Indicates a Device Connection Control (DCC) security violation was reported. The specified device attempted to log in using fabric login (FLOGI) to an unauthorized port. The DCC policy correlates specific devices to specific port locations. If the device changes the connected port, the device will not be allowed to log in.

Recommended Action Check the DCC policy and verify the specified device is allowed in the fabric and is included in the DCC policy. If the specified device is not included in the policy, add it to the policy. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

SEC-1189

Message `Security violation: Unauthorized host with IP address <IP address> tries to do SNMP write operation.`

Message Type LOG

Severity INFO

Probable Cause Indicates an SNMP security violation was reported. The specified unauthorized host attempted to perform a write SNMP operation.

Recommended Action Check the WSNMP policy and verify which hosts are allowed access to the fabric through SNMP. If the host is allowed access to the fabric but is not included in the policy, add the host to the policy. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

SEC-1190

Message `Security violation: Unauthorized host with IP address <IP address> tries to do SNMP read operation.`

Message Type LOG

Severity INFO

Probable Cause Indicates an SNMP security violation was reported. The specified unauthorized host attempted to perform a read SNMP (RSNMP) operation.

Recommended Action Check the RSNMP policy to verify the hosts allowed access to the fabric through SNMP read operations are included in the RSNMP policy. If the host is allowed access but is not included in the RSNMP policy, add the host to the policy. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

SEC-1191

Message `Security violation: Unauthorized host with IP address <Ip address> tries to establish HTTP connection.`

Message Type LOG

Severity INFO

Probable Cause Indicates an HTTP security violation was reported. The specified unauthorized host attempted to establish an HTTP connection.

Recommended Action Determine whether the host IP address specified in the message can be used to manage the fabric through an HTTP connection. If so, add the host IP address to the HTTP policy of the fabric. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

SEC-1192

Message `Security violation: Login failure attempt via <connection method>.`

Message Type LOG

Severity INFO

Probable Cause Indicates a serial or modem login security violation was reported. The wrong password was used while trying to log in through a serial or modem connection; the login failed.

Recommended Action Use the correct password.

SEC-1193

Message `Security violation: Login failure attempt via <connection method>. IP Addr: <IP address>.`

Message Type LOG

Severity INFO

Probable Cause Indicates a specified login security violation was reported. The wrong password was used while trying to log in through the specified connection method; the login failed.

Recommended Action The error message lists the violating IP address. Verify that this IP address is being used by a valid switch admin. Use the correct password.

SEC-1194

Message `This switch does not have all the required PKI objects correctly installed.`

Message Type LOG

Severity WARNING

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1195

Message `This switch has no <component> license.`

Message Type LOG

Severity WARNING

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1196

Message `Switch does not have all default account names.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the default switch accounts admin and user do not exist on the switch when enabling security.

Recommended Action Reset the default admin and user account names on the switch that reported the warning and retry enabling security.

SEC-1197

Message `Changed account <user name>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the specified account has changed.

Recommended Action No action is required.

SEC-1198

Message `Security violation: Unauthorized host with IP address <IP address> tries to establish API connection.`

Message Type LOG

Severity INFO

Probable Cause Indicates an API security violation was reported. The specified unauthorized host attempted to establish an API connection.

Recommended Action Check to see if the host IP address specified in the message can be used to manage the fabric through an API connection. If so, add the host IP address to the API policy of the fabric. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

SEC-1199

Message `Security violation: Unauthorized access to serial port of switch <switch instance>.`

Message Type LOG

Severity INFO

Probable Cause Indicates a serial connection policy security violation was reported. An attempt was made to access the serial console on the specified switch instance when it is disabled.

Recommended Action Check to see if an authorized access attempt is being made on the console. If so, add the switch WWN to the serial policy. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

SEC-1200

Message `Security violation: MS command is forwarded from non-primary FCS switch.`

Message Type LOG

Severity INFO

Probable Cause Indicates a management server (MS) forward security violation was reported. A management server command was forwarded from a non-primary fabric configuration server (FCS) switch.

Recommended Action Check the MS policy and verify that the connection is allowed. If the connection is allowed but not specified, enable the connection in the MS policy. If the MS policy does not allow the connection, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

SEC-1201

Message `Security violation: MS device <device WWN> operates on non-primary FCS switch.`

Message Type LOG

Severity INFO

Probable Cause Indicates a management server (MS) operation security violation was reported. An MS device operation occurred on a non-primary fabric configuration server (FCS) switch.

Recommended Action Check the management server policy and verify the connection is allowed. If the connection is allowed but not specified, enable the connection in the MS policy. If the MS policy does not allow the connection, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

SEC-1202

Message `Security violation: Unauthorized access from MS device node name <device node name>, device port name <device port name>.`

Message Type LOG

Severity INFO

Probable Cause Indicates a management server (MS) security violation was reported. The unauthorized device specified in the message attempted to establish a connection.

Recommended Action Check the MS server policy and verify that the connection is allowed. If the connection is allowed but not specified, enable the connection in the MS policy. If the MS policy does not allow the connection, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

SEC-1203

Message `Login information: Login successful via TELNET/SSH/RSH. IP Addr: <IP address>`

Message Type LOG

Severity INFO

Probable Cause Indicates the IP address of the remote station logging in.

Recommended Action No action is required.

SEC-1250

Message `DCC enforcement API failed: <failed action> err=<status>, key=<data>`

Message Type LOG

Severity WARNING

Probable Cause Indicates an internal error caused the Device Connection Control (DCC) policy enforcement to fail.

Recommended Action Retry the failed security command.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

SEC-1251

Message `Policy to binary conversion error: <text message> <value>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the security database conversion failed because of invalid values. The reason is specified in the *text message* variable and the faulty value is printed in the *value* variable.

Recommended Action Retry the failed security command.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

SEC-1253

Message `Bad DCC interface state during <Phase>, state=<state>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates an internal error has caused the Device Connection Control (DCC) policy update to fail in the provision, commit, or cancel phases.

Recommended Action Retry the failed security command.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

SEC-1300

Message `This switch is in VcEncode mode. Security is not supported.`

Message Type LOG

Severity INFO

Probable Cause Indicates the switch is set up with VC-encoded mode.

Recommended Action Turn off VC-encoded mode before enabling security.

SEC-1301

Message `This switch is in interop mode. Security is not supported.`

Message Type LOG

Severity INFO

Probable Cause Indicates the switch is enabled in interop mode.

Recommended Action Disable interop mode using the **interopMode** command before enabling the Secure Fabric OS feature.

SEC-1302

Message `This switch does not have all the required PKI objects correctly installed.`

Message Type LOG

Severity INFO

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1303

Message `This software version does not support security.`

Message Type LOG

Severity INFO

Probable Cause Indicates the currently installed software version does not support the Brocade Secure Fabric OS feature.

Recommended Action Run the **firmwareDownload** command to update the firmware to the latest version for your specific switch. Verify the firmware you are installing supports the Brocade Secure Fabric OS feature.

SEC-1304

Message `This switch has no security license.`

Message Type LOG

Severity INFO

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1305

Message `This switch has no zoning license.`

Message Type LOG

Severity INFO

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, and the local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database may not be correctly updated for that specific switch.

SEC-1306

Message `Failed to verify certificate with root CA.`

Message Type LOG

Severity INFO

Probable Cause Indicates the certificate could not be verified with root certificate authority (CA). This could happen if an unauthorized switch tries to access the fabric that is not certified by a trusted root CA or a root CA certificate does not exist on the switch.

Recommended Action Run the **secCertUtil show -fcapall** command and verify that all public key infrastructure (PKI) objects exist on the switch. If a failure to validate PKI objects occurs, follow the steps for re-creating PKI objects outlined in the *Fabric OS Administrator's Guide*. If PKI objects are valid, verify that an unauthorized switch is not trying to access the fabric.

SEC-1307

Message `<Security server (RADIUS/LDAP/TACACS+)> server <Server name> authenticated user account '<username>'.`

Message Type LOG

Severity INFO

Probable Cause Indicates that after some servers timed out, the specified RADIUS, LDAP, or TACACS+ server responded to a switch request.

Recommended Action If the message appears frequently, move the responding server to the top of the RADIUS/LDAP/TACACS+ server configuration list using the **aaaConfig** command.

SEC-1308

Message `All <Radius/LDAP/TACACS+ server identity> servers failed to authenticate user account '<username>'.`

Message Type LOG

Severity INFO

Probable Cause Indicates that all servers in the RADIUS, LDAP, or TACACS+ configuration have failed to respond to a switch request within the specified timeout.

Recommended Action Verify the switch has proper network connectivity to the specified RADIUS, LDAP, or TACACS+s servers, and the servers are correctly configured.

SEC-1309

Message `Waiting for RCS transaction to complete: <Wait time in seconds> secs`

Message Type LOG

Severity INFO

Probable Cause Indicates that Fabric OS is still waiting for the reliable commit service (RCS) transaction to complete.

Recommended Action Verify if there are any reliable commit service (RCS) or Reliable Transport With Response (RTWR) errors. If not, the transaction is still in progress.

SEC-1310

Message `Unable to determine data distribution limit of fabric. Please retry later.`

Message Type LOG

Severity INFO

Probable Cause Indicates the data distribution limit could not be obtained from all switches in the fabric. This may happen if the fabric is reconfiguring or a new domain joined the fabric.

Recommended Action Retry the command when the fabric is stable.

SEC-1311

Message `Security mode cannot be enabled because one or more of the password policies is not set to default value.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the security enable failed on the fabric because one or more switches in the fabric have password policies that are not set to the default values.

Recommended Action Verify the security event was planned.

If the security event was planned, run the **passwdCfg --setdefault** command on each switch in the fabric to set the password policies to the default values. Then verify with the **passwdCfg --show** command that password policies are set to the default values on all switches and retry the **secModeEnable** command.

SEC-1312

Message `<MESG Message>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the password configuration parameters changed.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1313

Message `The passwdcfg parameters were set to default values.`

Message Type LOG

Severity INFO

Probable Cause Indicates the password configuration parameters were set to default values.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1314

Message `Reading <IP Address Description> IP address from EM failed.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the call to the environment monitor (EM) module to retrieve the IP address failed.

Recommended Action Reboot the system to fix this error. If the problem persists, contact your switch service provider.

SEC-1315

Message `<Name of command> command failed -<List of databases rejecting distribution> db(s) configured for rejection on this switch.`

Message Type LOG

Severity ERROR

Probable Cause Indicates there was an attempt to distribute databases to a switch that was configured not to accept distributions from the fabric.

Recommended Action Verify the accept distribution configuration for the listed databases. Use the **remoteCfg** command to verify and correct the configuration if necessary.

SEC-1316

Message `<Policy Name> policy WWN List is conflicting with domain <Domain Number>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the newly added switches to the fabric, as specified by domain number, have a conflicting policy with the local switch.

Recommended Action Check the conflicting policy and make the new switches and the local switch policies the same.

SEC-1317

Message `Inconsistent fabric, rejecting transaction`

Message Type LOG

Severity INFO

Probable Cause Indicates that either this domain is performing FDD merge or matched domains are not the same as what CM sees.

Recommended Action If a policy conflict exists, resolve it, and then wait for the fabric to become stable. Retry the distribution.

SEC-1318

Message `Transaction rejected due to inconsistent fabric.`

Message Type LOG

Severity INFO

Probable Cause Indicates that some domains detected an inconsistent fabric.

Recommended Action Resolve the policy conflict, if there is one, and then wait for the fabric to stabilize. Retry the distribution.

SEC-1319

Message `<Event name> updated<Datasets updated> dbs(s).`

Message Type LOG

Severity INFO

Probable Cause Indicates the specified event has occurred.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1320

Message `Non-acl domain <Domain Number> tries to join a fabric with strict fabric wide policy.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a domain not supporting an access control list (ACL) policy tried to join a fabric with the strict fabric-wide policy.

Recommended Action No action is required. The domain is denied by disallowing all its E_Ports from connecting to the fabric.

SEC-1321

Message `Failed secure mode enable command. Reason: <Reason>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the security enable failed on the fabric because the switch has a conflicting configuration such as fabric-wide consistency configuration or AD configuration.

Recommended Action Verify the security event was planned. If the security event was planned, run the **fddCfg --fabwideset** command or **ad --clear** command to clear the fabric wide consistency configuration or AD configuration and retry the **secModeEnable** command.

SEC-1322

Message `Some DCC policy is too large, distribution cancelled.`

Message Type LOG

Severity WARNING

Probable Cause Indicates this fabric is not able to support a Device Connection Control (DCC) policy with more than 256 ports.

Recommended Action Reconfigure any policy that includes more than 256 ports in its member list, and then save the policy configuration changes.

SEC-1323

Message `Key(s) \"<Key Name>\" ignored during configdownload.`

Message Type LOG

Severity INFO

Probable Cause Indicates the specified key is ignored during configuration download.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1324

Message `Fabric transaction failure. RCS error: <Error code>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the reliable commit service (RCS) transaction failed with the specified reason code.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1325

Message `Security enforcement: Switch <switch WWN> connecting to port <Port number> is not authorized to stay in fabric.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that because of a Switch Connection Control (SCC) policy violation, the switch is being disabled on the specified port.

Recommended Action No action is required unless the switch must remain in the fabric. If the switch must remain in the fabric, add the switch World Wide Name (WWN) to the SCC policy, and then attempt to join the switch with the fabric.

SEC-1326

Message `Event: fddcfg --fabwideset, Status: success, Info: Fabric wide configuration set to <Fabric-wide configuration set by user>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the specified event has occurred.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1327

Message `Strict <Policy Name> policy WWN List is conflicting with domain <Domain Number>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the policy is conflicting with the domain.

Recommended Action No action is required. The domain is denied by disallowing all its E_Ports connected to the fabric. If the domain should be allowed to merge with the fabric, then resolve the issue by making the conflicting policies the same.

SEC-1328

Message `Attempt to enable secure mode failed. Reason: <Reason>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the **secModeEnable** command failed on the fabric because the Authentication Policy is enabled on the switch.

Recommended Action Verify the security event was planned. If the security event was planned, run the **authUtil --policy passive** command to disable the Authentication Policy and retry the **secModeEnable** command.

SEC-1329

Message `IPFilter enforcement:Failed to enforce ipfilter policy of <Policy Type> type because of <Error code>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the IP filter policy enforcement failed because of an internal system failure.

Recommended Action Execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

SEC-1330

Message `<Name of command> command failed -<List of databases rejecting distribution> db(s) are coming from a non-Primary switch.`

Message Type LOG

Severity ERROR

Probable Cause Indicates an attempt was made to distribute databases either from a backup fabric configuration server (FCS) switch or a non-FCS switch.

Recommended Action Verify the distribution is initiated by the FCS switch. Use the **secPolicyShow** command to verify and correct the configuration if necessary.

SEC-1331

Message `Attempt to enable secure mode failed. Reason: <Reason>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the **secModeEnable** command failed on the fabric because default IP filter policies are not active on the switch, or an active transaction exists on IP filter policies.

Recommended Action Verify the security event was planned.

If the security event was planned, run the **ipfilter --activate default_ipv4** command or the **ipfilter --activate default_ipv6** command to activate default IP filter policies. Use the **ipfilter --save** or **ipfilter --transabort** commands to save or abort the active transaction on IP filter policies. Then retry the **secModeEnable** command.

SEC-1332

Message `Fabric wide policy is conflicting as <Policy Name> is present in the fabric wide policy and 5.3 or 5.2 switches present in the fabric.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the fabric-wide policy is conflicting.

Recommended Action Remove either the FCS from the fabric-wide policy, or remove Fabric OS v5.3 or Fabric OS v5.2 switches from the fabric, or set the fabric-wide mode for FCS as strict.

SEC-1333

Message `<Name of command> command failed. There are VF enabled switch(s) in fabric. <List of databases rejecting distribution> db(s) distribution is blocked.`

Message Type LOG

Severity ERROR

Probable Cause Indicates there was an attempt to distribute PWD or IPFILTER databases from the fabric to a switch that is VF-enabled

Recommended Action Disable VF on all the switches that have VF-enabled if PWD or IPFILTER databases need to be distributed.

SEC-1334

Message `SSH Daemon is restarted.`

Message Type LOG

Severity INFO

Probable Cause Indicates the Secure Shell (SSH) daemon was not running and it was restarted.

Recommended Action No action is required.

SEC-1335

Message `Strict <Policy Name> policy is conflicting with domain <Domain Number>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the policy is conflicting with the domain.

Recommended Action No action is required. The domain is denied by disallowing all its E_Ports connected to the fabric. If the domain should be allowed to merge with the fabric, then resolve the issue by making the conflicting policies the same.

SEC-1336

Message `<Policy Name> policy is conflicting with domain <Domain Number>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the newly added switches to the fabric, as specified by domain number, have a conflicting policy with the local switch.

Recommended Action Check the conflicting policy and make the new switches and the local switch policies the same.

SEC-1337

Message `Plain-text password is sent during console login`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that plain-text password is sent during console login

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1338

Message `<MESG Message>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the password configuration parameters changed.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1339

Message `Distribute command failed. There are Inflight encryption enabled switch(s) in fabric. Auth db(s) distribution is blocked`

Message Type LOG

Severity ERROR

Probable Cause Indicates there was an attempt to distribute AUTH databases with switch policy (Off/Passive) from the fabric to a switch that has Inflight Encryption enabled

Recommended Action Disable or enable Inflight encryption in all the switches in the fabric

SEC-1340

Message `<Message>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the Device Connection Control (DCC) policy member is configured incorrectly.

Recommended Action Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1341

Message `Failed to update client capability to ESS (Exchange Switch Support) after maximum number of retries - return code <Failed return code>. Failing sync dump to standby CP.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that Exchange Switch Support (ESS) is unable to update its capability. Failed to send the sync dump to standby control processor (CP).

Recommended Action Verify that HA synchronization has failed using the **haShow** command. If HA synchronization has failed, execute the **haSyncStart** command on active CP to resynchronize the HA state.

SEC-1342

Message `HIF mode is enabled. <Warning>`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the local switch received a remote distribution for Switch Connection Control (SCC) policy or fabric-wide data distribution configuration. This may modify SCC policy or strict SCC mode configuration in Fabric Data Distribution (FDD). This configuration change may lead to unexpected behavior when High Integrity Fabrics (HIF) is enabled.

Recommended Action Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1343

Message `PWD policy distributed successfully from Switch <Switch WWN>. User configuration and Password configuration is enforced successfully.`

Message Type LOG

Severity INFO

Probable Cause Indicates password database distribute from switch is successful in the Access Gateway (AG) mode.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-1344

Message `Frequency of security violations exceed limit. Counters will be dropped`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that violation counter updates may be dropped. High number of security violations on the switch.

Recommended Action Identify and address the reason for security violations.

SEC-3001

Message `Event: <Event Name>, Status: success, Info: Security mode <State change: Enabled or Disabled> on the fabric.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates the security mode of the fabric was either enabled or disabled.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3002

Message `Event: <Event Name>, Status: success, Info: <Event Related Info>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates the specified security event has occurred. The event can be one of the following:

- There has been a fabric configuration server (FCS) failover.
- A security policy has been activated.
- A security policy has been saved.
- A security policy has been aborted.
- A non-FCS password has changed.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3003

Message `Event: <Event Name>, Status: success, Info: Created <Policy Name> policy, with member(s) <Member List> .`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates a new security policy with entries has been created. When you use a wildcard (for example, an asterisk) in creating a policy, the audit report displays the wildcard in the event information field.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3004

Message `Event: <Event Name>, Status: success, Info: Created <Policy name> policy.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates a new security policy has been created. When you use a wildcard (for example, an asterisk) in creating a member for a policy, the audit report displays the wildcard in the event information field.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3005

Message `Event: <Event Name>, Status: success, Info: Added member(s) <Members added> to policy <Policy name>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates new members have been added to a security policy. If you use a wildcard (for example, an asterisk) in adding members to a policy, the audit report displays the wildcard in the event information field.

Recommended Action Verify the addition of members to the policy was planned. If the addition of members was planned, no action is required. If the addition of members was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3006

Message `Event: <Event Name>, Status: success, Info: Removed member(s) <Members removed> from policy <Policy name>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates a user has removed the specific members from the security policy. When you use a wildcard (for example, an asterisk) in removing members from a policy, the audit report displays the wildcard in the event information field.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3007

Message `Event: <Event Name>, Status: success, Info: Deleted policy <Deleted policy name>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates the specified security policy was deleted.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3008

Message `Event: <Event Name>, Status: success, Info: FCS member moved from position <Old FCS position> to <New FCS position>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates the fabric configuration server (FCS) list has been modified. One of the members of the list has been moved to a new position in the list.

Recommended Action Verify the modification was planned. If the modification was planned, no action is required. If the modification was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3009

Message `Event: <Event Name>, Status: success, Info: Security Transaction aborted.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates the pending security transaction is aborted.

Recommended Action Verify the security transaction was intentionally aborted. If the security transaction was intentionally aborted, no action is required. If the security transaction was not intentionally aborted, take appropriate action as defined by your enterprise security policy.

SEC-3010

Message `Event: <Event Name>, Status: success, Info: Reset [<Name of security stat(s) reset>] security stat(s).`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates a user has reset all the security statistics.

Recommended Action Verify the security statistics were intentionally reset. If the security statistics were intentionally reset, no action is required. If the security statistics were not intentionally reset, take appropriate action as defined by your enterprise security policy.

SEC-3011

Message `Event: <Event Name>, Status: success, Info: Reset [<Stat name>] statistics on domain(s) [<Domain IDs>].`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates a user has reset a security statistic on the specified domains.

Recommended Action Verify the security statistics were intentionally reset. If the security statistics were intentionally reset, no action is required. If the security statistics were not intentionally reset, take appropriate action as defined by your enterprise security policy.

SEC-3012

Message `Event: <Event Name>, Status: success, Info: Temp Passwd <Password Set or Reset> on domain [<Domain ID>] for account [<Account name>].`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates a user has reset the password for the specified user accounts.

Recommended Action Verify the password was intentionally reset. If the password was intentionally reset, no action is required. If the password was not intentionally reset, take appropriate action as defined by your enterprise security policy.

SEC-3013

Message `Event: <Event Name>, Status: success, Info: Security Version stamp is reset.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates a user has reset the security version stamp.

Recommended Action Verify the security version stamp was intentionally reset. If the security event was planned, no action is required. If the security version stamp was not intentionally reset, take appropriate action as defined by your enterprise security policy.

SEC-3014

Message `Event: <Event Name>, Status: success, Info: <Event related info> <Security server> server <Server Name> for AAA services.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates a user has changed the RADIUS, LDAP, or TACACS+ configuration.

Recommended Action Verify the RADIUS configuration was changed intentionally. If the RADIUS configuration was changed intentionally, no action is required. If the RADIUS configuration was not changed intentionally, take appropriate action as defined by your enterprise security policy.

SEC-3015

Message `Event: <Event Name>, Status: success, Info: Moved <Event option> server <Server name> to position <New position>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates a user has changed the position of the RADIUS, LDAP, or TACACS+ server.

Recommended Action Verify the remote server position was intentionally changed. If the remote server position was intentionally changed, no action is required. If the remote server position was not intentionally changed, take appropriate action as defined by your enterprise security policy.

SEC-3016

Message `Event: <Event Name>, Status: success, Info: Attribute [<Attribute Name>] of <Security server> server <server ID> changed <Attribute related info, if any>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates a user has changed the specified attribute of the RADIUS, LDAP, and TACACS+ server.

Recommended Action Verify the RADIUS/LDAP/TACACS+ attribute was intentionally changed. If the RADIUS attribute was intentionally changed, no action is required. If the RADIUS/LDAP/TACACS+ attribute was not intentionally changed, take appropriate action as defined by your enterprise security policy.

SEC-3017

Message `Event: <Event Name>, Status: success, Info: <Event Related Info>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates a user has changed the RADIUS, LDAP, and TACACS+ configuration.

Recommended Action Verify the RADIUS/LDAP/TACACS+ configuration was intentionally changed. If the RADIUS/LDAP/TACACS+ configuration was intentionally changed, no action is required. If the RADIUS/LDAP/TACACS+ configuration was not intentionally changed, take appropriate action as defined by your enterprise security policy.

SEC-3018

Message `Event: <Event Name>, Status: success, Info: Parameter [<Parameter Name>] changed from [<Old Value>] to [<New Value>].`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates the specified password configuration parameter is changed.

Recommended Action Verify the password configuration parameter was intentionally changed. If the password configuration parameter was intentionally changed, no action is required. If the password configuration parameter was not intentionally changed, take appropriate action as defined by your enterprise security policy.

SEC-3019

Message `Event: <Event Name>, Status: success, Info: Passwdcfg parameters set to default values.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates the password configuration parameters are set to default values.

Recommended Action Verify the password configuration parameter was intentionally set to default values. If the password configuration parameter was intentionally set to default values, no action is required. If the password configuration parameter was not intentionally set to default values, take appropriate action as defined by your enterprise security policy.

SEC-3020

Message `Event: <Event Name>, Status: success, Info: Successful login attempt via <connection method and IP Address>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates a successful login occurred. An IP address is displayed when the login occurs over a remote connection.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3021

Message `Event: <Event Name>, Status: failed, Info: Failed login attempt via <connection method and IP Address>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates a failed login attempt occurred.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3022

Message `Event: <Event Name>, Status: success, Info: Successful logout by user [<User>].`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates the specified user has successfully logged out.

Recommended Action No action is required.

SEC-3023

Message `Event: <Event Name>, Status: failed, Info: Account [<User>] locked, failed password attempts exceeded.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that failed password attempts exceeded the allowed limit; the account has been locked.

Recommended Action The account may automatically unlock after the lockout duration has expired or an administrator may manually unlock the account.

SEC-3024

Message `Event: <Event Name>, Status: success, Info: User account [<User Name>], password changed.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates the user's password was changed.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3025

Message `Event: <Event Name>, Status: success, Info: User account [<User Name>] added. Role: [<Role Type>], Password [<Password Expired or not>], Home Context [<Home AD>], AD/VF list [<AD membership List>].`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates a new user account was created.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3026

Message `Event: <Event Name>, Status: success, Info: User account [<User Name>], role changed from [<Old Role Type>] to [<New Role Type>].`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates a user account role was changed.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3027

Message `Event: <Event Name>, Status: success, Info: User account [<User Name>] [<Changed Attributes>].`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates user account properties were changed.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3028

Message `Event: <Event Name>, Status: success, Info: User account [<User Name>] deleted.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates the specified user account was deleted.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3029

Message `Event: <Event Name>, Status: success, Info: Backup user account \"<User Account Name>\" recovered.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that backup user accounts were recovered.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3030

Message `Event: <Event Name>, Status: success, Info: <Event Specific Info>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates the specified **secCertUtil** operation was performed.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3031

Message `Event: <Event Name>, Status: success, Info: Distributed<List of Databases> db(s) to <Number of domains> domain(s), dom-id(s)<List of Domains>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates the specified event has occurred.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3032

Message `Event: <Event Name>, Status: success, Info: Switch is configured to <accept or reject> <Database name> database.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates the specified event has occurred to accept or reject a certain database.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3033

Message `Event: fddcfg --fabwideset, Status: success, Info: Fabric wide configuration set to <Fabric-wide configuration set by user>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates the specified event has occurred.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3034

Message `Event: aaaconfig, Status: success, Info: Authentication configuration changed from <Previous Mode> to <Current Mode> <Exisisting sessions are terminated or not>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates an authentication configuration has changed.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3035

Message `Event: ipfilter, Status: success, Info: <IP Filter Policy> ipfilter policy(ies) saved.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates the specified IP filter policies has been saved.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3036

Message `Event: ipfilter, Status: failed, Info: Failed to save changes for <IP Filter Policy> ipfilter policy(s).`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates the specified IP filter policies have not been saved.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3037

Message `Event: ipfilter, Status: success, Info: <IP Filter Policy> ipfilter policy activated.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates the specified IP filter policy has been activated.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3038

Message `Event: ipfilter, Status: failed, Info: Failed to activate <IP Filter Policy> ipfilter policy.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates the specified IP filter policy failed to activate.

Recommended Action Verify the security event was planned. If the event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3039

Message `Event:Security Violation , Status: failed, Info: Unauthorized host with IP address <IP address of the violating host> tries to establish connection using <Protocol Connection Type>.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates a security violation was reported. The IP address of the unauthorized host is displayed in the message.

Recommended Action Check for unauthorized access to the switch through the specified protocol connection.

SEC-3044

Message `The FIPS mode has been changed to <Fips Mode>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates there was a change in the Federal Information Processing Standards (FIPS) mode.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3045

Message `Zeroization has been executed on the system.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates the system has been zeroized.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3046

Message `The FIPS Self Tests mode has been set to <Self Test Mode>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates there was a change in the Federal Information Processing Standards (FIPS) Self Test mode.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3047

Message `Info: RBAC permission for a CLI command: <Cmd Name> is failed.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates the user does not have permission to execute this command.

Recommended Action Verify the user has the required permission to execute this command.

SEC-3048

Message `FIPS mode has been enabled in the system using force option.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates the system has been forced to Federal Information Processing Standards (FIPS) mode.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy. Look for the status of the prerequisites that did not conform to FIPS mode.

SEC-3049

Message `Status of bootprom access is changed using fipscfg CLI to : <Access Status>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates the status of boot PROM access has changed using the **fipsCfg** command.

Recommended Action No action is required.

SEC-3050

Message `Event: <Event Name>, Status: success, Info: <Event Specific Info>`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates the specified Secure Shell (SSH) utility operation was performed.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

SEC-3051

Message `The license key <Key> is <Action>.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that a license key is added or removed.

Recommended Action No action is required.

SEC-3061

Message `Role '<Role Name>' is created.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the specified role name has been created.

Recommended Action No action is required.

SEC-3062

Message `Role '<Role Name>' is deleted.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the specified role name has been deleted.

Recommended Action No action is required.

SEC-3063

Message `Role '<Role Name>' is copied from '<Source Role>'.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the specified role name has been copied from the source role.

Recommended Action No action is required.

SEC-3064

Message `Permission to the RBAC class(es) '<RBAC Class Names>' is changed for the role '<Role Name>'.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates the permission to the Role-Based Access Control (RBAC) class is changed for the specified role name.

Recommended Action No action is required.

SEC-3065

Message `Configuration of user-defined roles is uploaded.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates the configuration of user-defined roles has been uploaded.

Recommended Action No action is required.

SEC-3066

Message `Configuration of user-defined roles is downloaded.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates the configuration of user-defined roles has been downloaded.

Recommended Action No action is required.

SEC-3067

Message `Invalid Cipher list <Cipher List>.`

Message Type AUDIT | LOG

Class SECURITY

Severity WARNING

Probable Cause Indicates the input cipher list is an invalid string.

Recommended Action Invalid cipher list input, therefore reverted to previous cipher list.

SEC-4001

Message `Client logged in. <IP Address>, <User Account>, <Application>.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates the client has logged in.

Recommended Action No action is required.

SFLO Messages

SFLO-1001

Message `sFlow is <state> globally.`

Message Type LOG

Severity INFO

Probable Cause Indicates that sFlow is globally enabled or disabled.

Recommended Action No action is required.

SFLO-1002

Message `sFlow is <state> for port <name>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that sFlow is enabled or disabled on the specified port.

Recommended Action No action is required.

SFLO-1003

Message `Global sFlow sampling rate is changed to <sample_rate>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the global sFlow sampling rate has been changed to the specified value.

Recommended Action No action is required.

SFLO-1004

Message `Global sFlow polling interval is changed to <polling_intvl>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the global counter sampling interval has been changed to the specified value.

Recommended Action No action is required.

SFLO-1005

Message `sFlow sampling rate on port <name> is changed to <sample_rate>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the sFlow sampling rate has been changed on the specified port.

Recommended Action No action is required.

SFLO-1006

Message `sFlow polling interval on port <name> is changed to <poling_intvl>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the polling interval has been changed on the specified port.

Recommended Action No action is required.

SFLO-1007

Message `<name> is <state> as sFlow collector.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the sFlow collector is configured or not configured.

Recommended Action No action is required.

SFLO-1008

Message `All the sFlow collectors are unconfigured.`

Message Type LOG

Severity INFO

Probable Cause Indicates that none of the sFlow collectors are configured.

Recommended Action No action is required.

SNMP Messages

SNMP-1001

Message `SNMP service is not available <Reason>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the Simple Network Management Protocol (SNMP) service could not be started because of the specified reason. Therefore, you will not be able to query the switch through SNMP.

Recommended Action Verify that the IP address for the Ethernet and Fibre Channel interface is set correctly. If the specified reason is an initialization failure, restart the switch using the **reboot** command.

SNMP-1002

Message `SNMP <Error Details> initialization failed.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the initialization of the SNMP service failed and therefore you will not be able to query the switch through SNMP.

Recommended Action Restart or power cycle the switch. This will automatically initialize SNMP.

SNMP-1003

Message `Distribution of Community Strings to Secure Fabric failed.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the changes in the SNMP community strings could not be propagated to other switches in the secure fabric.

Recommended Action Retry changing the SNMP community strings on the primary switch.

SNMP-1004

Message `Incorrect SNMP configuration.`

Message Type AUDIT | FFDC | LOG

Class CFG

Severity ERROR

Probable Cause Indicates that the SNMP configuration is incorrect and therefore the SNMP service will not work correctly.

Recommended Action Change the SNMP configuration to the default using the **snmpConfig --default** command.

SNMP-1005

Message `SNMP configuration attribute, <Changed attribute>, <String Value>.`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates that the SNMP configuration has changed. The modified parameter and the old and new parameter values are displayed in the message.

Recommended Action Execute the **snmpConfig --show** command to view the new SNMP configuration.

SNMP-1006

Message `<SNMP Configuration group> configuration was reset to default.`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates that the specified SNMP configuration group was reset to the factory default.

Recommended Action Execute the **snmpConfig --show** command for the group to view the new SNMP configuration.

SNMP-1009

Message `Port traps are <blocked state> on port <port>.`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates the blocked or unblocked status of the port traps on the specified port.

Recommended Action Execute the **snmpTraps --show** command to view the current status of the port.

SNMP-1010

Message `Unsupported security protocol settings detected. Setting SNMP usm privacy protocol configuration to default configuration.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the SNMP User-based Security Model (USM) privacy protocol configuration was found to be incorrect after HA synchronization with version Fabric OS v7.1.0.

Recommended Action Execute the **snmpConfig --show** command to view the new SNMP configuration.

SPC Messages

SPC-1001

Message `S<slot number containing Encryption Engine>, Cryptographic operation enabled.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the cryptographic operation is enabled on an encryption engine.

Recommended Action No action is required.

SPC-1002

Message `S<slot number containing Encryption Engine>, Cryptographic operation disabled.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the cryptographic operation is disabled on an encryption engine.

Recommended Action No action is required.

SPC-1003

Message `S<slot number containing Encryption Engine>, Security Processor faulted.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the security processor is faulted because of an internal error. Cryptographic operations are affected.

Recommended Action To recover a bladed system, execute the **slotPowerOff** and **slotPowerOn** commands on the blade. To recover a non-bladed system, execute the **fastboot** command on the switch.

SPC-2001

Message `S<slot number containing Encryption Engine>, <module name>: Crypto error asserted by Vader/OB1 0x<Reason>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that Crypto error is asserted by the Field-Programmable Gate Array (FPGA).

Recommended Action No action is required.

SPC-2002

Message `S<slot number containing Encryption Engine>, <module name>: Tamper Event: Crypto subsystem cover tampered.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that the Crypto subsystem cover is tampered. The encryption engine is zeroized.

Recommended Action Execute the **cryptocfg --initEE** and **cryptocfg --regEE** commands.

SPC-2003

Message `S<slot number containing Encryption Engine>, <module name>: Data Disable status: 0x<DisableStatus>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the data disable signal status.

Recommended Action No action is required.

SPC-2004

Message `S<slot number containing Encryption Engine>, <module name>: FPGA firmware download failed: 0x<Reason>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that FPGA download has failed.

Recommended Action No action is required.

SPC-2005

Message `S<slot number containing Encryption Engine>, <module name>: FPGA firmware download success.`

Message Type LOG

Severity INFO

Probable Cause Indicates that FPGA download was successful.

Recommended Action No action is required.

SPC-2006

Message `S<slot number containing Encryption Engine>, <module name>: Crypto post tests failed: 0x<Reason>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that Crypto Power-On Self-Test (POST) tests have failed.

Recommended Action No action is required.

SPC-2007

Message `S<slot number containing Encryption Engine>, <module name>: Crypto post tests success: 0x<Reason>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that Crypto Power-On Self-Test (POST) has passed successfully.

Recommended Action No action is required.

SPC-2008

Message `S<slot number containing Encryption Engine>, <module name>: Vader/OB1 recovered from error.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Crypto error from FPGA is de-asserted.

Recommended Action No action is required.

SPC-2009

Message `S<slot number containing Encryption Engine>, <module name>: Tamper event: User zeroization.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that the tamper event triggered due to a user zeroize request. The encryption engine is zeroized.

Recommended Action Execute the **cryptocfg --initEE** and **cryptocfg --regEE** commands.

SPC-2010

Message `S<slot number containing Encryption Engine>, <module name>: Crypto subsystem cover is open.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that the Crypto subsystem cover is open.

Recommended Action Close the Crypto subsystem cover properly.

SPC-2011

Message `S<slot number containing Encryption Engine>, <module name>: OB1 crypto BIST success.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the FPGA built-in self-test (BIST) was successful.

Recommended Action No action is required.

SPC-2012

Message `S<slot number containing Encryption Engine>, <module name>: User zeroization command completed successfully. Tamper INT status <Status>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the user zeroization command has completed successfully. The encryption engine is zeroized.

Recommended Action Execute the **cryptocfg --initEE** and **cryptocfg --regEE** commands.

SPC-2013

Message `S<slot number containing Encryption Engine>, <module name>: Oscillator Failure Detected.`

Message Type LOG

Severity WARNING

Probable Cause Indicates hardware failure.

Recommended Action The shelf life of the system may be reduced. Contact the vendor for further instructions.

SPC-2014

Message `S<slot number containing Encryption Engine>, <module name>: Low Battery Level Detected.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the battery is depleted.

Recommended Action System operation will be unaffected while the facility power is present. Schedule battery replacement with the vendor.

SPC-2040

Message `S<slot number containing Encryption Engine>, <module name>: SPD Device minornum <MinorNum> is already open. state <State>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the Security Policy Database (SPD) device has already opened or is busy for sysctrld or keyappd.

Recommended Action No action is required.

SPC-2041

Message `S<slot number containing Encryption Engine>, <module name>: Alloc freemsg block failed.`

Message Type LOG

Severity ERROR

Probable Cause Indicates an allocation failure for the pool of SB message.

Recommended Action No action is required.

SPC-2042

Message `S<slot number containing Encryption Engine>, <module name>: Alloc msg - no free sbmsgs.`

Message Type LOG

Severity WARNING

Probable Cause Indicates no free message buffer in the free pool.

Recommended Action No action is required.

SPC-2043

Message `S<slot number containing Encryption Engine>, <module name>: Destination device read queue overflow <Device minor>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the device read queue has overflowed.

Recommended Action No action is required.

SPC-2044

Message `S<slot number containing Encryption Engine>, <module name>: Read - device not open <Device minor number>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the SPD device is not opened.

Recommended Action No action is required.

SPC-3001

Message `S<slot number containing Encryption Engine>, <module name>: No input KEK for DEK inject, DEK: <DEK octet 1> <DEK octet 2> <DEK octet 3> <DEK octet 4>, KEK: <KEK octet 1> <KEK octet 2> <KEK octet 3> <KEK octet 4>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the wrapping key encryption key (KEK) for the data encryption key (DEK) to be injected does not exist within the encryption engine CryptoModule.

Recommended Action For opaque key vaults such as DPM, recover the missing master key to the current or alternate position.

SPC-3002

Message `S<slot number containing Encryption Engine>, <module name>: No input KEK for DEK rewrap, DEK: <DEK octet 1> <DEK octet 2> <DEK octet 3> <DEK octet 4>, KEK: <KEK octet 1> <KEK octet 2> <KEK octet 3> <KEK octet 4>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the input wrapping key encryption key (KEK) for the data encryption key (DEK) to be rewrapped does not exist within the encryption engine CryptoModule.

Recommended Action For opaque key vaults such as DPM, recover the missing master key to the current or alternate position.

SPC-3003

Message `S<slot number containing Encryption Engine>, <module name>: No output KEK for DEK rewrap, DEK: <DEK octet 1> <DEK octet 2> <DEK octet 3> <DEK octet 4>, KEK: <KEK octet 1> <KEK octet 2> <KEK octet 3> <KEK octet 4>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the output wrapping key encryption key (KEK) for the data encryption key (DEK) to be rewrapped does not exist within the encryption engine CryptoModule.

Recommended Action No action is required. The KEK will be recovered automatically.

SPC-3004

Message `S<slot number containing Encryption Engine>, <module name>: No output KEK for DEK create, KEK: <KEK octet 1> <KEK octet 2> <KEK octet 3> <KEK octet 4>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates the output wrapping key encryption key (KEK) for the data encryption key (DEK) to be created does not exist within the encryption engine CryptoModule.

Recommended Action For opaque key vaults such as DPM, recover the missing master key to the current or alternate position.

SPC-3005

Message `S<slot number containing Encryption Engine>, <module name>: DEK inject error: <SP status code>, DEK: <DEK octet 1 or other info> <DEK octet 2> <DEK octet 3> <DEK octet 4>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates an error in injecting data encryption key (DEK) into encryption engine. The *SP status code* variable specifies the cause of the error:

- 14 - Invalid input DEK format
- 32 - DEK could not be unwrapped
- 33 - FGPA error upon inject
- 73 - Invalid key encryption key (KEK) format

Recommended Action Contact your switch service provider for assistance.

SPC-3006

Message

```
S<slot number containing Encryption Engine>, <module name>: DEK rewrap error: <SP
status code>, DEK: <DEK octet 1 or other info> <DEK octet 2> <DEK octet 3> <DEK
octet 4>.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates data encryption key (DEK) rewrap error. The *SP status code* variable specifies the cause of the error:

- 2 - Invalid input data encryption key (DEK) format
- 14 - Rewrapping not allowed: primary key encryption key (KEK) generation is in progress
- 31 - DEK could not be wrapped
- 32 - DEK could not be unwrapped
- 33 - FGPA error upon inject
- 73 - Invalid KEK format

Recommended Action

For status code 14, complete primary KEK generation; otherwise, contact your switch service provider.

SPC-3007

Message

```
S<slot number containing Encryption Engine>, <module name>: DEK create error: <SP
status code>, info: <other info>.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates an error in creating data encryption key (DEK). The *SP status code* variable specifies the cause of the error:

- 2 - Invalid input data encryption key (DEK) specification
- 14 - Creation not allowed: primary key encryption key (KEK) generation is in progress
- 21 - No primary KEK exists with which to wrap the DEK
- 31 - DEK could not be wrapped
- 73 - Invalid KEK format
- other - Internal error

Recommended Action

For status code 14, complete primary KEK generation; otherwise, contact your switch service provider.

SPC-3008

Message `S<slot number containing Encryption Engine>, <module name>: SP crypto got READY notification.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the key application (KPD) within the CryptoModule of the encryption engine has been started.

Recommended Action No action is required.

SPC-3009

Message `S<slot number containing Encryption Engine>, <module name>: FIPS certificate mismatch, certificate: <FIPS certificate is CO-0 or User-1>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the Federal Information Protection Standard (FIPS) certificate within the CryptoModule does not match that of the node.

Recommended Action Zeroize the encryption engine (after backing up any needed primary or secondary KEK), then execute the **cryptocfg --initEE** and **cryptocfg --regEE** commands.

SPC-3010

Message `S<slot number containing Encryption Engine>, <module name>: SEK integrity failure during initialization.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the CryptoModule internal Secret Encryption Key has been corrupted or has not been initialized.

Recommended Action Execute the **cryptocfg --initEE** and **cryptocfg --regEE** commands.

SPC-3011

Message

```
S<slot number containing Encryption Engine>, <module name>: Persistent data
storage error: <SP status code>, KEK: <KEK octet 1> <KEK octet 2> <KEK octet 3>
<KEK octet 4>.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates that an attempt to store CryptoModule internal data using the Secret Encryption Key failed; most likely, the encryption engine has been zeroized or tampered with.

Recommended Action Execute the **cryptocfg --initEE** and **cryptocfg --regEE** commands, and then recover or restore the needed primary and secondary KEKs.

SPC-3012

Message

```
S<slot number containing Encryption Engine>, <module name>: Persistent data
retrieval error: <SP status code>.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates that an attempt to read CryptoModule internal data using the Secret Encryption Key failed; most likely, the encryption engine has been zeroized or tampered with.

Recommended Action Execute the **cryptocfg --initEE** and **cryptocfg --regEE** commands, and then recover or restore the needed primary and secondary KEKs.

SPC-3013

Message

```
S<slot number containing Encryption Engine>, <module name>: SEK generation
failure: <SP status code>.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates that the CryptoModule internal Secret Encryption Key could not be generated.

Recommended Action Contact your switch service provider for assistance.

SPC-3014

Message `S<slot number containing Encryption Engine>, <module name>: RNG compare failure: successive values match.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the CryptoModule internal random number generator has failed.

Recommended Action Contact your switch service provider for assistance.

SPC-3015

Message `S<slot number containing Encryption Engine>, <module name>: RSA pairwise key generation test failure.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the CryptoModule could not generate its internal key pair.

Recommended Action Contact your switch service provider for assistance.

SPM Messages

SPM-1001

Message `Init fails: <Reason>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the security processor management (SPM) failed to initialize.

Recommended Action Check the system resources and restart the switch.

SPM-1002

Message `Generic SPM Warning: <Reason>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates an security processor management (SPM) warning based on the reason displayed.

Recommended Action Execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

SPM-1003

Message `Set New Group Cfg SC Enable <SC_Enable> KV Type <KV_Type>.`

Message Type LOG

Severity INFO

Probable Cause Indicates a new group has been configured.

Recommended Action No action is required.

SPM-1004

Message `Initialize Node.`

Message Type LOG

Severity INFO

Probable Cause Indicates a node initialization.

Recommended Action No action is required.

SPM-1005

Message `Set EE Control slot <slot> action <action>.`

Message Type LOG

Severity INFO

Probable Cause Indicates specified control action is taken on encryption engine in specified slot.

Recommended Action No action is required.

SPM-1006

Message `Registered Certificate of type <cert_type>.`

Message Type LOG

Severity INFO

Probable Cause Indicates a certificate registration.

Recommended Action No action is required.

SPM-1007

Message `Deregistered Certificate cid [<cert_id>] type <cert_type> idx <qc_idx>.`

Message Type LOG

Severity INFO

Probable Cause Indicates a certificate de-registration.

Recommended Action No action is required.

SPM-1008

Message `Dergistered SP Certificate in slot <slot>.`

Message Type LOG

Severity INFO

Probable Cause Indicates an security processor (SP) certificate de-registration.

Recommended Action No action is required.

SPM-1009

Message `<cert> Certificate is missing.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified certificate is missing.

Recommended Action Execute the **cryptocfg --initnode** command.

SPM-1010

Message `<cert> Key Vault Certificate is missing.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified key vault certificate is missing.

Recommended Action Deregister and register the key vault.

SPM-1011

Message `Group Cfg Changed Quorum Size <qc_size>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a group configuration has changed the quorum size.

Recommended Action No action is required.

SPM-1012

Message `Authentication Context: <established>.`

Message Type LOG

Severity INFO

Probable Cause Indicates an authentication context.

Recommended Action No action is required.

SPM-1013

Message `Security database is out of sync.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a failure to distribute security database.

Recommended Action Execute the **cryptocfg --sync -securitydb** command to manually sync the security database.

SPM-1014

Message `Warning: Configdownload may change key vault configuration and result in EE going to Operational; Need Valid KEK state.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the master keys downloaded will not be effective unless imported because the encryption engine may have different master key configured.

Recommended Action Import required master keys using the **cryptocfg --recovermasterkey** command to bring the encryption engine online.

SPM-1015

Message `Security database may be out of sync.`

Message Type LOG

Severity WARNING

Probable Cause Indicates a failure to distribute the security database.

Recommended Action Use the **cryptocfg --sync -securitydb** command to manually sync security database.

SPM-1016

Message `Security database is out of sync. This warning can be ignored if the nodes in the EG are running different versions of FOS.`

Message Type LOG

Severity WARNING

Probable Cause Indicates a failure to distribute the security database.

Recommended Action Use the **cryptocfg --sync -securitydb** command to manually sync security database.

SPM-3001

Message `Event: cryptocfg Status: success, Info: Node [<wwnstr>] initialized.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates a node was initialized.

Recommended Action No action is required.

SPM-3002

Message `Event: cryptocfg Status: success, Info: EE in slot <slot> initialized.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates an encryption engine was initialized.

Recommended Action No action is required.

SPM-3003

Message `Event: cryptocfg Status: success, Info: EE in slot <slot> registered.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates an encryption engine was registered.

Recommended Action No action is required.

SPM-3004

Message `Event: cryptocfg Status: success, Info: EE in slot <slot> enabled.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates an encryption engine was enabled.

Recommended Action No action is required.

SPM-3005

Message `Event: cryptocfg Status: success, Info: EE in slot <slot> disabled.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates an encryption engine was disabled.

Recommended Action No action is required.

SPM-3006

Message
```
Event: cryptocfg Status: success, Info: <sourceFile> file exported via scp:
<hostUsername>[<hostIP>]:<hostPath>.
```

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates a file was exported through SCP protocol.

Recommended Action No action is required.

SPM-3007

Message `Event: cryptocfg Status: success, Info: File imported via scp: <hostUsername>[<hostIP>]:<hostPath>.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates a file was imported through SCP protocol

Recommended Action No action is required.

SPM-3008

Message `Event: cryptocfg Status: success, Info: DH challenge generated for vault IP <vaultIP>.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates a DH challenge was generated for a key vault.

Recommended Action No action is required.

SPM-3009

Message `Event: cryptocfg Status: success, Info: DH response accepted.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates a DH response was accepted.

Recommended Action No action is required.

SPM-3010

Message `Event: cryptocfg Status: success, Info: EE in slot <slot> zeroized.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates an encryption engine was zeroized.

Recommended Action No action is required.

SPM-3011

Message `Event: cryptocfg Status: success, Info: Local file \"<filename>\" deleted.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates a locally stored file was deleted.

Recommended Action No action is required.

SPM-3012

Message

```
Event: cryptocfg Status: success, Info: <primaryOrSecondary> key vault
registered. Certificate label: \"<certLabel>\" Certificate file:
\"<certFilename>\" IP address: <IPAddress>.
```

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates a key vault was registered.

Recommended Action No action is required.

SPM-3013

Message `Event: cryptocfg Status: success, Info: Key vault with certificate label \"<certLabel>\" deregistered.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates a key vault was deregistered.

Recommended Action No action is required.

SPM-3014

Message `Event: cryptocfg Status: success, Info: Key archive client registered with certificate file \"<certFilename>\".`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates a key archive client (KAC) certificate was registered.

Recommended Action No action is required.

SPM-3015

Message `Event: cryptocfg Status: success, Info: Key vault type set to <keyVaultType>.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates the key vault type was set.

Recommended Action No action is required.

SPM-3016

Message `Event: cryptocfg Status: success, Info: Master key generated.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates a master key was generated

Recommended Action No action is required.

SPM-3017

Message `Event: cryptocfg Status: success, Info: Master key exported.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates a master key was exported.

Recommended Action No action is required.

SPM-3018

Message `Event: cryptocfg Status: success, Info: <currentOrAlternate> master key recovered.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates a master key was recovered.

Recommended Action No action is required.

SPM-3019

Message `Event: cryptocfg Status: success, Info: System card registered. Certificate label: \"<certLabel>\" Certificate file: \"<certFilename>\".`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates a system card was registered.

Recommended Action No action is required.

SPM-3020

Message `Event: cryptocfg Status: success, Info: System card with certificate label \"<certLabel>\" deregistered.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates a system card was deregistered.

Recommended Action No action is required.

SPM-3021

Message `Event: cryptocfg Status: success, Info: Authentication card registered. Certificate label: \"<certLabel>\" Certificate file: \"<certFilename>\".`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates an authentication card was registered.

Recommended Action No action is required.

SPM-3022

Message `Event: cryptocfg Status: success, Info: Authentication card with certificate label \"<certLabel>\" deregistered.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates an authentication card was deregistered.

Recommended Action No action is required.

SPM-3023

Message `Event: cryptocfg Status: success, Info: System card <enabledOrDisabled>.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates use of the system card was enabled or disabled.

Recommended Action No action is required.

SPM-3024

Message `Event: cryptocfg Status: success, Info: Quorum size set to <quorumsize>.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates the quorum size was set.

Recommended Action No action is required.

SPM-3025

Message `Event: cryptocfg Status: success, Info: File imported via USB: Source: <sourcePath> Destination: <destinationFilename>.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates a file was imported through a USB device.

Recommended Action No action is required.

SPM-3026

Message `Event: cryptocfg Status: success, Info: File exported via usb: Source: <sourcePath> Destination: <destinationFilename>.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates a file was exported through a USB device

Recommended Action No action is required.

SPM-3027

Message `Event: cryptocfg Status: success, Info: Recovery card registered. Certificate label: \"<certLabel>\" Certificate file: \"<certFilename>\".`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates a recovery card was registered.

Recommended Action No action is required.

SPM-3028

Message `Event: SPM-EE state changed, Info: EE State: <EE Status>.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates an encryption engine state has changed.

Recommended Action No action is required.

SPM-3029

Message `Event: KeyVault Connection Status: <status>, Info: KAC_Connect: <kac status>.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates the status of key vault.

Recommended Action No action is required.

SS Messages

SS-1000

Message `supportSave has uploaded support information to the host with IP address <host ip>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the **supportSave** command was used to transfer support information to a remote location.

Recommended Action No action is required.

SS-1001

Message `supportSave's upload operation to host IP address <host ip> aborted.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a file copy error occurred during execution of the **supportSave** command. Complete error information cannot always be displayed in this message because of possible errors in subcommands being executed by the **supportSave** command.

Recommended Action Check and correct the remote server settings and configuration. Execute the **supportFtp** command (as needed) to set the FTP or SCP parameters. After the problem is corrected, execute the **supportSave** command again.

SS-1002

Message `supportSave has stored support information to the USB storage device.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the **supportSave** command was used to transfer support information to an attached USB storage device.

Recommended Action No action is required.

SS-1003

Message `supportSave's operation to USB storage device aborted.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a USB operation error occurred during execution of the **supportSave** command. Complete error information cannot always be displayed in this message because of possible errors in subcommands being executed by the **supportSave** command.

Recommended Action Execute the **usbstorage** command to check the USB storage device settings. After the USB problem is corrected, execute the **supportSave** command again.

SS-1004

Message `One or more modules timed out during supportsave. Retry supportsave with -t option to collect all logs.`

Message Type LOG

Severity WARNING

Probable Cause Indicates a timeout in modules during the execution of the **supportSave** command.

Recommended Action Execute the **supportSave -t [2-5]** command to collect all logs.

SS-1005

Message `supportsave failed for the slot <Slot Number>. Reason: No IP connection.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that there is no IP connection between the active control processor (CP) and the blade in the specified slot.

Recommended Action Check for the IP connection between the active CP and the blade in the specified slot. After the IP connection is established, execute the **supportSave** command again.

SS-1006

Message `supportsave not collected for slot <Slot Number>. Reason: blade was not available to accept a supportsave request.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the supportsave request was not sent to the blade in the specified slot.

Recommended Action Restart the switch using the **reboot** command and then execute the **supportSave** command.

SS-1007

Message `supportsave failed for the slot <Slot Number>. Reason: No response from the blade in the specified slot for the given supportsave request.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that there was no response from the blade in the specified slot for the given supportsave request.

Recommended Action Restart the switch using the **reboot** command and then execute the **supportSave** command.

SS-1008

Message `supportsave failed for the slot <Slot Number>. Reason: BP supportsave timeout.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the specified slot has taken more time than expected to collect the supportsave logs.

Recommended Action Execute the **supportSave** command again.

SS-1009

Message `<slot number and its node name(BP/DP)> supportsave failed. Reason:No ISC connection for <slot number and its node name(BP/DP)>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that there is no Inter-Subsystem Communication (ISC) connection for the specified node slot.

Recommended Action Restart the switch using the **reboot** command and then execute the **supportSave** command.

SS-1010

Message `CORE/FFDC files have been uploaded to the host with IP address <host ip>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the **supportSave** command was used to transfer core and first failure data capture (FFDC) files to a remote location.

Recommended Action No action is required.

SS-1011

Message `CORE/FFDC files have been transferred to the USB storage device.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the **supportSave** command was used to transfer core and first failure data capture (FFDC) files to a USB storage Device.

Recommended Action No action is required.

SS-1012

Message `BP supportsave failed. The /mnt of Active CP does not have enough disk space to collect BP supportsave files.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a chassis with the blade processor (BP) does not have enough disk space in the secondary partition of the active CP to save the supportsave files, before uploading them to the remote host.

Recommended Action Manually clean up the secondary partition of the active CP to collect the supportsave files.

SS-1013

Message `supportSave's upload operation aborted. username or password is not provided.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the username or password parameters were not specified with the **supportSave** command in non-interactive mode.

Recommended Action Specify both username and password or neither of them. If no username and password are specified, anonymous FTP will be used to collect the supportsave files.

SSMD Messages

SSMD-1001

Message `Failed to allocate memory: (<function name>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified function has failed to allocate memory.

Recommended Action Check the memory usage on the switch using the **memShow** command.
Restart or power cycle the switch.

SSMD-1002

Message `Failed to initialize <module> rc = <error>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the initialization of a module within System Services Manager (SSM) has failed.

Recommended Action Download a new firmware using the **firmwareDownload** command.

SSMD-1003

Message `Failed to lock semaphore mutex: (<function name>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified function has failed to lock the mutex (semaphore).

Recommended Action Restart or power cycle the switch.

SSMD-1004

Message `Failed to unlock semaphore mutex: (<function name>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified function failed to unlock the mutex (semaphore).

Recommended Action Restart or power cycle the switch.

SSMD-1005

Message `SSM start up failed.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that Data Center Ethernet (DCE) SSM encountered an unexpected severe error during basic startup and initialization.

Recommended Action Restart or power cycle the switch.

If the problem persists, download a new firmware using the **firmwareDownload** command.

SSMD-1006

Message `Error while configuring ACL <ACL name> on interface <Interface name>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that an error occurred while programming a Ternary Content Addressable Memory (TCAM) entry on the specified interface.

Recommended Action Try again after some time. If the problem persists, execute the **supportSave** command and then restart or power cycle the switch.

SSMD-1007

Message `Error while removing ACL <ACL name> from interface <Interface name>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that an error occurred while programming a TCAM entry on the specified interface.

Recommended Action Try again after some time. If the problem persists, execute the **supportSave** command and then restart or power cycle the switch.

SSMD-1008

Message `Apptype TCAM Table full for Slot:<slot number> chip:<Chip number in the slot>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the application type TCAM table is full on the specified chip.

Recommended Action Remove the unused protocol-based VLAN classifiers and Layer 2 extended access control lists (ACLs).

SSMD-1200

Message `QoS failed programming ASIC <ASIC slot number>/<ASIC chip number> Multicast Rate Limit.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that DCE SSM encountered an unexpected error in programming the dataplane application-specific integrated circuit (ASIC) for enforcing the Multicast Rate Limit feature.

Recommended Action Delete and reapply the Quality of Service (QoS) Multicast Rate Limit policy using the **qos rcv-queue multicast rate-limit** command.

If the problem persists, restart or power cycle the switch.

SSMD-1201

Message `QoS failed programming ASIC <ASIC slot number>/<ASIC chip number> Multicast Tail Drop.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that DCE SSM encountered an unexpected error in programming the dataplane ASIC for enforcing the Multicast Tail Drop feature.

Recommended Action Delete and reapply the QoS Multicast Tail Drop policy using the **qos rcv-queue multicast threshold** command.

If the problem persists, restart or power cycle the switch.

SSMD-1202

Message `QoS failed programming interface 0x<Interface ID> 802.3x Pause flow control.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that DCE SSM encountered an unexpected error in programming the dataplane ASIC for enforcing interface 802.3x Pause flow control feature.

Recommended Action Delete and reapply the QoS 802.3x Pause flow control policy using the **qos flowcontrol** command.

If the problem persists, restart or power cycle the switch.

SSMD-1203

Message `QoS failed programming interface 0x<Interface ID> PFC flow control.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that DCE SSM encountered an unexpected error in programming the dataplane ASIC for enforcing interface Priority-based Flow Control (PFC) flow control feature.

Recommended Action Delete and reapply the QoS PFC flow control policy using the **qos flowcontrol pfc** command.

If the problem persists, restart or power cycle the switch.

SSMD-1204

Message `QoS failed initializing ASIC <ASIC slot number>/<ASIC chip number>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that DCE SSM encountered an unexpected error in initializing the dataplane ASIC QoS infrastructure.

Recommended Action Restart or power cycle the switch.

SSMD-1205

Message `CEE failed programming ETS policy for CEE Map <CEE Map name>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that DCE SSM encountered an unexpected error in programming the dataplane ASIC for enforcing the Converged Enhanced Ethernet (CEE) Map Enhanced Transmission Selection (ETS) feature.

Recommended Action Delete and reapply the CEE Map ETS policy using the **cee-map default** command.

If the problem persists, restart or power cycle the switch.

SSMD-1206

Message `CEE failed programming CoS to PGID policy for CEE Map <CEE Map name>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that DCE SSM encountered an unexpected error in programming the dataplane ASIC for enforcing the CEE Map Class of Service (CoS) to Priority Group ID (PGID) mapping feature.

Recommended Action Delete and reapply the CEE Map CoS to PGID policy using the **cee-map default** command.

If the problem persists, restart or power cycle the switch.

SSMD-1207

Message `QoS failed programming interface 0x<Interface ID> Default CoS.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that DCE SSM encountered an unexpected error in programming the dataplane ASIC for enforcing the interface Default CoS feature.

Recommended Action Delete and reapply the QoS interface Default CoS policy using the **qos cos** command.

If the problem persists, restart or power cycle the switch.

SSMD-1208

Message `QoS failed programming interface 0x<Interface ID> Trust.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that DCE SSM encountered an unexpected error in programming the dataplane ASIC for enforcing the interface Trust feature.

Recommended Action Delete and reapply the QoS interface Trust policy using the **qos trust cos** command.

If the problem persists, restart or power cycle the switch.

SSMD-1209

Message `QoS failed programming interface 0x<Interface ID> CoS Mutation map.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that DCE SSM encountered an unexpected error in programming the dataplane ASIC for enforcing the interface CoS Mutation mapping feature.

Recommended Action Delete and reapply the QoS interface CoS Mutation policy using the **qos cos-mutation** command.

If the problem persists, restart or power cycle the switch.

SSMD-1210

Message `QoS failed programming interface 0x<Interface ID> CoS to Traffic Class map.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that DCE SSM encountered an unexpected error in programming the dataplane ASIC for enforcing the CoS to Traffic Class mapping feature.

Recommended Action Delete and reapply the QoS interface CoS to Traffic Class policy using the **qos cos-traffic-class** command.

If the problem persists, restart or power cycle the switch.

SSMD-1211

Message `QoS failed programming ASIC <ASIC slot number>/<ASIC chip number> Scheduler Control.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that DCE SSM encountered an unexpected error in programming the dataplane ASIC for enforcing the packet Scheduler Control feature.

Recommended Action Delete and reapply the QoS packet Scheduler Control policy using the **qos queue scheduler** command.

If the problem persists, restart or power cycle the switch.

SSMD-1212

Message `QoS failed programming ASIC <ASIC slot number>/<ASIC chip number> Multicast Scheduler Control.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that DCE SSM encountered an unexpected error in programming the dataplane ASIC for enforcing the multicast packet Scheduler Control feature.

Recommended Action Delete and reapply the QoS multicast packet Scheduler Control policy using the **qos queue multicast scheduler** command.

If the problem persists, restart or power cycle the switch.

SSMD-1213

Message `QoS failed programming interface 0x<Interface ID> CoS Tail Drop Threshold.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that DCE SSM encountered an unexpected error in programming the dataplane ASIC for enforcing the interface CoS Tail Drop Threshold feature.

Recommended Action Delete and reapply the QoS CoS Tail Drop Threshold policy using the **qos rcv-queue** command.

If the problem persists, restart or power cycle the switch.

SSMD-1214

Message `QoS failed programming interface 0x<Interface ID> CoS Tail Drop Threshold.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that DCE SSM encountered an unexpected error in programming the dataplane ASIC for enforcing the interface CoS Tail Drop Threshold feature.

Recommended Action Delete and reapply the QoS CoS Tail Drop Threshold policy using the **qos rcv-queue** command.

If the problem persists, restart or power cycle the switch.

SSMD-1215

Message `QoS failed programming interface 0x<Interface ID> CoS Tail Drop Threshold.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that DCE SSM encountered an unexpected error in programming the dataplane ASIC for enforcing the interface CoS Tail Drop Threshold feature.

Recommended Action Delete and reapply the QoS CoS Tail Drop Threshold policy using the **qos rcv-queue** command.

If the problem persists, restart or power cycle the switch.

SSMD-1216

Message `QoS failed programming interface 0x<Interface ID> Pause.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that DCE SSM encountered an unexpected error in programming the dataplane ASIC for enforcing the interface Pause feature.

Recommended Action Delete and reapply the QoS Pause policy.

If the message persists, restart or power cycle the switch.

SSMD-1217

Message `QoS CEE could not comply with FCoE scheduler policy for CEE Map <CEE Map name>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that DCE SSM was unable to translate the CEE Map and Fibre Channel over Ethernet (FCoE) configuration into an ETS scheduler policy implementable by the dataplane ASIC.

Recommended Action Redefine CEE Map and FCoE into a configuration that translates into an ETS scheduler policy requiring eight or fewer traffic classes.

SSMD-1300

Message `CEE Map <ceemap> is created with precedence <precedence>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified CEE Map has been created.

Recommended Action No action is required.

SSMD-1301

Message `CEE Map <ceemap> is deleted.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified CEE Map has been deleted.

Recommended Action No action is required.

SSMD-1302

Message `CEE Map <ceemap> priority table <pg_ids> are <action>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the priority groups have been added to or removed from the specified CEE Map.

Recommended Action No action is required.

SSMD-1303

Message `CEE Map <ceemap> priority group <pg_id> with weight <PGID_weight> is created with PFC <pfc>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified priority group has been created.

Recommended Action No action is required.

SSMD-1304

Message `CEEM Map <ceemap> priority group <pg_id> is deleted.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified priority group has been deleted.

Recommended Action No action is required.

SSMD-1305

Message `CEE Map <ceemap> priority group <pg_id> weight is changed from <PGID_weight_new> to <PGID_weight_old>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified priority group weight has been changed.

Recommended Action No action is required.

SSMD-1306

Message `CEE Map <ceemap> priority group <pg_id> is PFC <pfc_status>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified priority group PFC status has been changed.

Recommended Action No action is required.

SSMD-1307

Message `<acl_type> access list <acl_name> is created.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified access list has been created.

Recommended Action No action is required.

SSMD-1308

Message `<acl_type> access list <acl_name> is deleted.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified access list has been deleted.

Recommended Action No action is required.

SSMD-1309

Message `<acl_type> access list <acl_name> rule sequence number <rule_sq_no> is <action>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified access list rules were added to or removed from an existing policy.

Recommended Action No action is required.

SSMD-1310

Message `ACL <acl_name> configured on interface <InterfaceName>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified access list has been configured on the interface.

Recommended Action No action is required.

SSMD-1311

Message `ACL <acl_name> is removed from interface <InterfaceName>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified access list has been removed from the interface.

Recommended Action No action is required.

SSMD-1312

Message `<map_type> <map_name> assigned to interface <InterfaceName>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified user profile map has been assigned to the interface.

Recommended Action No action is required.

SSMD-1313

Message `<map_type> <map_name> removed from interface <InterfaceName>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified user profile map has been removed from the interface.

Recommended Action No action is required.

SSMD-1314

Message `CEE Map <ceemap> precedence changed from <precedence_old> to <precedence_new>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that precedence of the specified CEE Map has been changed.

Recommended Action No action is required.

SSMD-1315

Message `CEE Map <ceemap> is incompatible with current firmware. Resetting it to default.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified CEE Map is incompatible with the current firmware and therefore it is reset to the default.

Recommended Action No action is required.

SSMD-1316

Message `CEE Map <ceemap> is reset to default configuration.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified CEE Map is reset to the default using the **no cee-map** *name* command.

Recommended Action No action is required.

SSMD-1317

Message `ACL <acl_name> is being configured on interface <InterfaceName>. This operation could take a long time.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified access list is being configured on the interface.

Recommended Action No action is required.

SSMD-1318

Message

```
ACL <acl_name> is being removed from interface <InterfaceName>. This operation
could take a long time.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the specified access list is being removed from the interface.

Recommended Action

No action is required.

SULB Messages

SULB-1001

Message `Firmwaredownload command has started. (From v<current_version> To v<new_version>).`

Message Type AUDIT | LOG

Class FIRMWARE

Severity WARNING

Probable Cause Indicates that the **firmwareDownload** command has been entered. This process should take approximately 17 minutes. The process is set to time out after 30 minutes.

Recommended Action Do not fail over or power down the system during firmware upgrade. Allow the **firmwareDownload** command to continue without disruption. No action is required.

Run the **firmwareDownloadStatus** command for more information.

SULB-1002

Message `Firmwaredownload command has completed successfully.`

Message Type AUDIT | LOG

Class FIRMWARE

Severity INFO

Probable Cause Indicates that the **firmwareDownload** command has completed successfully and switch firmware has been updated.

Recommended Action No action is required. The **firmwareDownload** command has completed as expected.

Run the **firmwareDownloadStatus** command for more information. Run the **firmwareShow** command to verify the firmware versions.

SULB-1003

Message `Firmwarecommit has started.`

Message Type AUDIT | LOG

Class FIRMWARE

Severity INFO

Probable Cause Indicates that the **firmwareCommit** command has been entered.

Recommended Action No action is required. Run the **firmwareDownloadStatus** command for more information.

SULB-1004

Message `Firmwarecommit has completed.`

Message Type AUDIT | LOG

Class FIRMWARE

Severity INFO

Probable Cause Indicates that the **firmwareCommit** command has completed successfully.

Recommended Action No action is required. Run the **firmwareDownloadStatus** command for more information.

SULB-1005

Message `Current Active CP is preparing to failover.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the active control processor (CP) is about to reboot. The standby CP is taking over as the active CP.

Recommended Action No action is required. The **firmwareDownload** command is progressing as expected.

Run the **firmwareDownloadStatus** command for more information.

SULB-1006

Message `Forced failover succeeded. New Active CP is running new firmware.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the previous standby control processor (CP) has now become the active CP and is running the new firmware version.

Recommended Action No action is required. The **firmwareDownload** command is progressing as expected.

Run the **firmwareDownloadStatus** command for more information.

SULB-1007

Message `Standby CP reboots.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the standby control processor (CP) is rebooting with new firmware.

Recommended Action No action is required. The **firmwareDownload** command is progressing as expected.

Run the **firmwareDownloadStatus** command for more information.

SULB-1008

Message `Standby CP booted successfully with new firmware.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the standby control processor (CP) has rebooted successfully.

Recommended Action No action is required. The **firmwareDownload** command is progressing as expected.

Run the **firmwareDownloadStatus** command for more information.

SULB-1009

Message `Firmwaredownload command failed. Status: 0x<status code>, error: 0x<error code>.`

Message Type AUDIT | LOG

Class FIRMWARE

Severity INFO

Probable Cause Indicates that the **firmwareDownload** command failed. The additional *status code* and *error code* values provide debugging information.

The following table lists **firmwareDownload** status messages and status codes. Some of them will not be displayed in this RASLog message and are listed for completeness.

TABLE 7 Status messages and status codes

Status message	Status code
"Firmware download sanity check failed."	0x30
"Sanity check failed because system is non-redundant."	0x31
"Sanity check failed because firmware download is already in progress."	0x32
"Sanity check failed because Fabric OS is disabled on active CP."	0x33

TABLE 7 Status messages and status codes

Status message	Status code
"Sanity check failed because HAMD is disabled on active CP."	0x34
"Sanity check failed because firmware download process is already in progress."	0x35
"Sanity check failed because Fabric OS is disabled on standby CP."	0x36
"Sanity check failed because HAMD is disabled on standby CP."	0x37
"Firmware download failed on standby CP."	0x40
"Firmware download failed on standby CP."	0x41
"Firmware download failed on standby CP."	0x42
"Firmware commit failed on standby CP."	0x43
"Firmware download failed."	0x44
"Firmware download failed due to IPC error."	0x50
"Unable to check the firmware version on standby CP due to IPC error."	0x51
"Firmware download failed due to IPC error."	0x52
"Firmware download failed due to IPC error."	0x53
"Standby CP failed to reboot due to IPC error."	0x54
"Firmware commit operation failed due to IPC error."	0x55
"Unable to check the firmware version on standby CP due to IPC error."	0x56
"Unable to restore the original firmware due to standby CP timeout."	0x57
"Standby CP failed to reboot and was not responding."	0x58
"Unable to check the firmware version on standby CP due to IPC error."	0x59
"Sanity check failed because the firmware download operation is already in progress."	0x60
"Sanity check failed because the firmware download operation is already in progress."	0x61
NOT USED	0x62
"System error."	0x63
"Active CP forced failover succeeded. Now the standby CP becomes active CP."	0x64
"Standby CP booted up."	0x65
"Active and standby CP failed to gain HA synchronization within 10 minutes."	0x66
"Standby CP rebooted successfully."	0x67
"Standby CP failed to reboot."	0x68
"Firmware commit has started to restore the secondary partition."	0x69
"Local CP is restoring its secondary partition."	0x6a
"Unable to restore the secondary partition. Run the **firmwareDownloadStatus** and **firmwareShow** commands to see firmware status."	0x6b
"Firmware download has started on standby CP. It might take up to 10 minutes."	0x6c
"Firmware download has completed successfully on standby CP."	0x6d
"Standby CP reboots."	0x6e

TABLE 7 Status messages and status codes

Status message	Status code
"Standby CP failed to boot up."	0x6f
"Standby CP booted up with new firmware."	0x70
"Standby CP failed to boot up with new firmware."	0x71
"Firmware download has completed successfully on standby CP."	0x72
"Firmware download has started on standby CP. It might take up to 10 minutes. "	0x73
"Firmware download has completed successfully on standby CP."	0x74
"Standby CP reboots."	0x75
"Standby CP failed to reboot."	0x76
"Firmware commit has started on standby CP."	0x77
"Firmware commit has completed successfully on standby CP."	0x78
"Standby CP booted up with new firmware."	0x79
"Standby CP failed to boot up with new firmware."	0x7a
"Firmware commit has started on both active and standby CPs."	0x7b
"Firmware commit has completed successfully on both active and standby CPs."	0x7c
"Firmware commit failed on active CP."	0x7d
"The original firmware has been restored successfully on standby CP."	0x7e
"Unable to restore the original firmware on standby CP."	0x7f
"Standby CP reboots."	0x80
"Standby CP failed to reboot."	0x81
"Standby CP booted up with new firmware."	0x82
"Standby CP failed to boot up with new firmware."	0x83
"There was an unexpected reboot during the firmware download operation. The command is aborted."	0x84
"Standby CP was not responding. The command is aborted."	0x85
"Firmware commit has started on both active and standby CPs. Run the **firmwareDownloadStatus** and **firmwareShow** commands to see the firmware status."	0x86
"Firmware commit has started on the local CP. Run the **firmwareDownloadStatus** and **firmwareShow** commands to see the firmware status."	0x87
"Firmware commit has started on the remote CP. Run the **firmwareDownloadStatus** and **firmwareShow** commands to see the firmware status."	0x88
"Run the **firmwareDownloadStatus** and **firmwareShow** commands to see the firmware status."	0x89
"The **firmwareDownload** command has completed successfully."	0x8a
"The original firmware has been restored successfully."	0x8b
"Remote CP is restoring its secondary partition."	0x8c
"Local CP is restoring its secondary partition."	0x8d
"Remote CP is restoring its secondary partition."	0x8e

TABLE 7 Status messages and status codes

Status message	Status code
"Firmware download has started."	0x8f
"Firmware commit has started."	0x90
"Firmware download has completed successfully."	0x91
"Firmware commit has completed successfully."	0x92
"Firmware commit has started to restore the secondary partition."	0x93
"Firmware commit failed."	0x94
"The secondary partition has been restored successfully."	0x95
"Firmware is being downloaded to the blade. This step may take up to 10 minutes."	0xa0
"Firmware download timed out."	0xa1
"Reboot occurred during firmware download. Firmware commit will be started to recover the blade."	0xa2
"Blade rebooted during firmware commit. The operation will be restarted."	0xa3
"Firmware has been downloaded successfully. Blade is rebooting with the new firmware."	0xa4
"Blade has rebooted successfully."	0xa5
"New firmware failed to boot up. Run the **firmwareDownload** command again."	0xa6
"Firmware commit has started on the blade. This may take up to 10 minutes."	0xa7
"The **firmwareRestore** command is entered. System will reboot and a firmware commit operation will start upon bootup."	0xa8
"Switch is relocating the AP image."	0xa9
"The AP image is relocated successfully."	0xaa
"Switch reboots during relocating the AP image. The operation will be restarted."	0xab
"Blade failed to reboot with the original image. The **firmwareRestore** command failed."	0xac

The following table lists additional **firmwareDownload** error messages and error codes. The error code provide more details on the reason for firmware download failure.

TABLE 8 Error messages and error codes

Error message	Error code
"Image is up-to-date. No need to download the same version of firmware."	0xF
"Upgrade is inconsistent."	0x10
"OSRootPartition is inconsistent. For example: swap OSRootPartitions and reboot."	0x11
"Unable to access the required package list file. Check whether the switch is supported by the requested firmware. Also check the **firmwareDownload** help page for other possible failure reasons."	0x12
"The RPM package database is inconsistent. Contact your switch service provider for recovery."	0x13
"Out of memory."	0x14

TABLE 8 Error messages and error codes

Error message	Error code
"Failed to download RPM package."	0x15
"Unable to create firmware version file."	0x16
"Unexpected system error."	0x17
"Error in getting lock device for firmware download."	0x18
"Error in releasing lock device for firmware download."	0x19
"Firmware commit failed."	0x1a
"Firmware directory structure is not compatible. Check whether the firmware is supported on this platform."	0x1b
"Failed to load the Linux kernel image."	0x1c
"OSLoader is inconsistent."	0x1d
"New image has not been committed. Run the **firmwareCommit** or **firmwareRestore** command and then run the **firmwareDownload** command."	0x1e
"Firmware restore failed."	0x1f
"Both images are mounted to the same device."	0x20
"Unable to uninstall old packages."	0x21
"Firmware download is already in progress."	0x22
"Firmware download timed out."	0x23
"Out of disk space."	0x24
"Primary filesystem is inconsistent. Run the **firmwareRestore** command to restore the original firmware, or contact your switch service provider for recovery."	0x25
"The post-install script failed."	0x26
"Unexpected reboot."	0x27
"Primary kernel partition is inconsistent. Contact your switch service provider for recovery."	0x28
"The pre-install script failed."	0x29
"The platform option is not supported."	0x2a
"Failed to install RPM package."	0x2b
"Cannot downgrade directly to this version. Downgrade to an intermediate version and then download the desired version."	0x2c
"Invalid RPM package. Reload firmware packages on the file server."	0x2e
"Cannot downgrade due to presence of blade type 17. Remove or power off these blades before proceeding."	0x2f
"Cannot downgrade due to presence of blade type 24. Remove or power off these blades before "	0x30
"Cannot downgrade due to presence of long-distance ports in LS mode. Remove these settings before proceeding."	0x31
"Network is not reachable. Verify the IP address of the server is correct."	0x32

The following descriptions explain the causes of some common error messages:

- 0x15 - "Failed to download RPM package." If this error occurs immediately after firmware download is started, the firmware on the switch may be two releases older than the requested firmware. The firmware download operation supports firmware upgrades within two feature releases (a feature release is indicated by a major number and a minor number; for example, X.Y). In this case, you will need to upgrade to an intermediate version before downloading the desired version. If this error occurs in the middle of a firmware download, the firmware in the file server may be corrupted or there may be a temporary network issue. In this case, retry the **firmwareDownload** command. If the problem persists, contact your system administrator.
- 0x18 - "Error in getting lock device for firmware download". This error can be due to another firmware download is already in progress. Run the **firmwareDownloadStatus** command to verify that this is the case. Wait for the current session to finish before proceeding.
- 0x23 - "Firmware download timed out." This error may occur because the **firmwareDownloadStatus** command has not completed within the predefined timeout period. It is most often caused by network issues. If the problem persists, contact your system administrator.
- 0x24 - "Out of disk space." This error may occur because some core dump files have not been removed from the filesystem and are using up disk space. Remove these core dump files by using the **supportSave** command before proceeding.
- 0x29 - "The pre-install script failed." This error may be caused by an unsupported blade type. Remove or power off the unsupported blades before proceeding.
- 0x2e - "Invalid RPM package." This error may be caused by an inconsistent firmware image loaded on the file server. It may also be caused by temporary networking issues. Reload the firmware packages on the file server and then retry the **firmwareDownload** command. If the problem persists, contact your system administrator.

The following table lists the **firmwareDownload** state names and code values. They indicate where in the **firmwareDownload** process the error occurred.

TABLE 9 Upgrade state and code value

Upgrade state	Code
SUS_PEER_CHECK_SANITY	0x21
SUS_PEER_FWDL_BEGIN	0x22
SUS_SBY_FWDL_BEGIN	0x23
SUS_PEER_REBOOT	0x24
SUS_SBY_REBOOT	0x25
SUS_SBY_FABOS_OK	0x26
SUS_PEER_FS_CHECK	0x27
SUS_SELF_FAILOVER	0x28
SUS_SBY_FWDL1_BEGIN	0x29
SUS_SELF_FWDL_BEGIN	0x2a
SUS_SELF_COMMIT	0x2b
SUS_SBY_FWC_BEGIN	0x2c
SUS_SBY_COMMIT	0x2d
SUS_SBY_FS_CHECK	0x2e
SUS_ACT_FWC_BEGIN	0x2f

TABLE 9 Upgrade state and code value

Upgrade state	Code
SUS_PEER_RESTORE_BEGIN	0x30
SUS_SBY_RESTORE_BEGIN	0x31
SUS_PEER_FWC_BEGIN	0x32
SUS_PEER_FS_CHECK1	0x33
SUS_FINISH	0x34
SUS_COMMIT	0x35

Recommended Action

Run the **firmwareDownloadStatus** command for more information.

In a modular switch, when the **firmwareDownload** command fails, the command will synchronize the firmware on the two partitions of each CP by starting a firmware commit operation. Wait until this operation completes (about 10 minutes) before attempting another firmware download.

In a modular switch, when the **firmwareDownload** command fails, the two CPs may end up with different versions of firmware and they may not gain high availability (HA) sync. In this case, run the **firmwareDownload -s** command to upgrade the firmware on the standby CP to the same version as the active CP. Then retry the **firmwareDownload** command to download the desired version of firmware onto the CPs.

Refer to the *Fabric OS Troubleshooting Guide* for troubleshooting information.

SULB-1010

Message

```
Firmwarecommit failed (status=0x<error code>).
```

Message Type

AUDIT | LOG

Class

FIRMWARE

Severity

INFO

Probable Cause

Indicates that the **firmwareCommit** command failed. The error code provides debugging information.

Recommended Action

If the failure is caused by an inconsistent filesystem, contact your switch service provider.

SULB-1011

Message

```
Firmwaredownload command failed. <error string>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates that the **firmwareDownload** command failed. The *error string* value indicates the reason for failure.

Recommended Action Run the **firmwareDownloadStatus** command for more information.

Refer to the *Fabric OS Troubleshooting Guide* for troubleshooting information.

SULB-1017

Message `Firmwaredownload failed in slot <Slot number>.`

Message Type AUDIT | LOG

Class FIRMWARE

Severity ERROR

Probable Cause Indicates that the **firmwareDownload** command failed on the specified blade. The error may be caused by the inconsistent application processor (AP) blade firmware stored on the active CP. It may also be caused by an internal Ethernet issue or by a persistent storage hardware failure.

Recommended Action Run the **slotShow** command. If the blade is in the FAULTY state, run the **slotPowerOff** and **slotPowerOn** commands to trigger another firmware download. If the blade is stuck in the LOADING state, remove and re-insert the blade to trigger another firmware download. If the problem persists, contact your switch service provider.

SULB-1018

Message `Firmwaredownload timed out in slot <Slot number>.`

Message Type AUDIT | LOG

Class FIRMWARE

Severity ERROR

Probable Cause Indicates that there may be error caused by the blade initialization issue after the new firmware is downloaded and the blade is rebooted. The error may also be caused by an internal Ethernet issue or by a persistent storage hardware failure.

Recommended Action Run the **slotShow** command. If the blade is in the FAULTY state, run the **slotPowerOff** and **slotPowerOn** commands to trigger another firmware download to the blade. If the blade is stuck in the LOADING state, remove and re-insert the blade to trigger another firmware download. If the problem persists, contact your switch service provider.

SULB-1020

Message `New firmware failed to boot in slot <Slot number>.`

Message Type AUDIT | LOG

Class FIRMWARE

Severity ERROR

Probable Cause Indicates that the BP blade is still running the old image even though it should reboot with the new image. This error may indicate that the new image has not been loaded correctly to the specified blade.

Recommended Action Run the **slotShow** command. If the blade is in a FAULTY state, run the **slotPowerOff** and **slotPowerOn** commands to trigger another firmware download to the blade. If the blade is stuck in LOADING state, remove and re-insert the blade to trigger another firmware download. If the problem persists, contact your switch service provider.

SULB-1021

Message `Firmware is being downloaded to the blade in slot <Slot number>.`

Message Type AUDIT | LOG

Class FIRMWARE

Severity WARNING

Probable Cause Indicates that the firmware is being loaded to the specified blade.

Recommended Action Run the **firmwareDownloadStatus** command to monitor the firmware download progress. After it finishes, run the **firmwareShow** command to verify the firmware versions.

SULB-1022

Message `The blade in slot <Slot number> has rebooted successfully with new firmware.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the blade in the specified slot has rebooted with new firmware. This is a normal step in the firmware download process.

Recommended Action Run the **firmwareDownloadStatus** command to monitor the firmware download progress.

SULB-1023

Message `The blade in slot <Slot number> has rebooted during firmwaredownload.`

Message Type AUDIT | LOG

Class FIRMWARE

Severity WARNING

Probable Cause Indicates that there may be an error caused by an unexpected disruption of the **firmwareDownload** command; for example, powering off and on of the indicated BP blade in the middle of a firmware download. The error may also be caused by persistent storage hardware failure or by a software error.

Recommended Action The **firmwareCommit** command will be started automatically after the blade boots up to repair the secondary partition. If at the end of the firmware commit, the blade firmware version is still inconsistent with the active CP firmware, firmware download will be restarted automatically on the blade. Run the **firmwareDownloadStatus** command to monitor the progress. If the problem persists, contact your switch service provider.

SULB-1024

Message `Firmware commit has completed on the blade in slot <Slot number>.`

Message Type AUDIT | LOG

Class FIRMWARE

Severity WARNING

Probable Cause Indicates that the **firmwareCommit** command has completed on the specified blade.

Recommended Action Run the **firmwareShow** command to verify the firmware versions. If the blade firmware is the same as the active CP firmware, the **firmwareDownload** command has completed successfully on the blade. However, if the firmware commit operation has been started to repair the secondary partition, at the end of the firmware commit, the blade firmware version may still be inconsistent with the active CP firmware. In this case, firmware download will automatically be restarted on the blade. Run the **firmwareDownloadStatus** command to monitor the progress.

SULB-1025

Message `The blade in slot <Slot number> will reboot with the new firmware.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that new firmware has been downloaded to the specified application processor (AP) blade and the AP blade will reboot to activate it.

Recommended Action Wait for the blade to reboot.

SULB-1026

Message `Firmware commit operation started on the blade in slot <Slot number>.`

Message Type AUDIT | LOG

Class FIRMWARE

Severity WARNING

Probable Cause Indicates that the **firmwareCommit** command has started on the specified blade. The operation may be a normal part of firmware download, or it may have started to repair the secondary partition of the blade if the secondary partition is corrupted.

Recommended Action Wait for the firmware commit operation to complete.

SULB-1030

Message `The switch has rebooted during relocating the internal firmware image.`

Message Type AUDIT | LOG

Class FIRMWARE

Severity WARNING

Probable Cause Indicates that there may be an error caused by an unexpected disruption of the **firmwareDownload** command; for example, by powering the switch off and on in the middle of a firmware download. The error may also be caused by persistent storage hardware failure or by a software error.

Recommended Action The **firmwareDownload** command will continue after the switch has rebooted. Run the **firmwareDownloadStatus** command to monitor progress. If the problem persists, contact your switch service provider.

SULB-1031

Message `The switch is relocating an internal firmware image.`

Message Type AUDIT | LOG

Class FIRMWARE

Severity WARNING

Probable Cause Indicates that the switch has rebooted with the new firmware and is relocating the application processor (AP) firmware.

Recommended Action Wait for the operation to complete.

SULB-1032

Message `Relocating an internal firmware image on the CP.`

Message Type AUDIT | LOG

Class FIRMWARE

Severity WARNING

Probable Cause Indicates that the switch has started firmware download to the co-CPU.

Recommended Action Wait for the operation to complete.

SULB-1033

Message `Switch has completed relocating the internal firmware image.`

Message Type AUDIT | LOG

Class FIRMWARE

Severity WARNING

Probable Cause Indicates that the firmware download process has completed normally on the switch.

Recommended Action Run the **firmwareShow** command to verify the firmware versions. Run the **switchShow** command to make sure the switch is enabled.

SULB-1034

Message `Relocation of internal image timed out.`

Message Type AUDIT | LOG

Class FIRMWARE

Severity ERROR

Probable Cause Indicates that there may be an error caused by the switch initialization issue after the internal image is relocated. It may also be caused by an internal Ethernet issue or by a persistent storage hardware failure.

Recommended Action Reboot the switch. This will cause the internal image to be relocated again. Use the **firmwareDownloadStatus** command to monitor the progress. If the problem persists, contact your switch service provider.

SULB-1035

Message `An error has occurred during relocation of the internal image.`

Message Type AUDIT | LOG

Class FIRMWARE

Severity ERROR

Probable Cause Indicates that an error has occurred during the relocation of the internal image. The error may be caused by inconsistent internal firmware image. It may also be caused by an internal Ethernet issue or a persistent storage hardware failure.

Recommended Action Reset the switch. This will cause the internal image to be relocated again. If the problem persists, contact your switch service provider.

SULB-1036

Message `<The Version being logged><Version String>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the version running in the system. This is generally logged before download and after download of the firmware to store version information.

Recommended Action No action is required.

SULB-1037

Message `HCL failed. Reboot the switch manually using the reboot command. However, it will disrupt the FC traffic.`

Message Type AUDIT | LOG | FFDC

Class FIRMWARE

Severity ERROR

Probable Cause Indicates that Hot Code Load (HCL) has failed. Many reasons, such as a domain not confirmed, can cause this failure.

Recommended Action Run the **reboot** command to reboot the switch manually.

SULB-1039

Message `CP has completed relocating the internal firmware image.`

Message Type AUDIT | LOG

Class FIRMWARE

Severity INFO

Probable Cause Indicates that the firmware download process has completed normally on the control processor (CP).

Recommended Action Run the **firmwareShow** command to verify the firmware versions.

SULB-1040

Message `An error has occurred during relocation of the internal image on the CP.`

Message Type AUDIT | LOG

Class FIRMWARE

Severity WARNING

Probable Cause Indicates that an error has occurred during the relocation of the internal image. The error may be caused by an inconsistent internal firmware image. It may also be caused by an internal Ethernet failure.

Recommended Action Run the **firmwareShow** command to verify the firmware versions. Run the **firmwareDownload** command again if the firmware is not updated.

This will cause the internal image to be relocated again. If the problem persists, contact your switch service provider.

SULB-1041

Message `Firmware has been activated successfully on standby CP.`

Message Type AUDIT | LOG

Class FIRMWARE

Severity INFO

Probable Cause Indicates that the **firmwareActivate** command has completed successfully on the standby control processor (CP).

Recommended Action No action is required. The **firmwareActivate** command has completed on the standby CP as expected.

Run the **firmwareShow** command to verify the firmware versions.

SULB-1042

Message `Firmwareactivate command has completed successfully.`

Message Type AUDIT | LOG

Class FIRMWARE

Severity INFO

Probable Cause Indicates that the **firmwareActivate** command has completed successfully and the switch firmware has been updated.

Recommended Action No action is required. The **firmwareActivate** command has completed as expected.

Run the **firmwareShow** command to verify the firmware versions.

SULB-1043

Message `Firmwareactivate command failed. <error string>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the **firmwareActivate** command failed. The *error string* value indicates the reason for failure.

Recommended Action Run the **firmwareShow** command to verify the firmware versions.

SULB-1044

Message `Firmwaredownload to secondary partition has completed successfully.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the **firmwareDownload** command to the secondary partition has completed successfully and the switch will come up with the updated firmware on reboot.

Recommended Action No action is required. The switch will auto-reboot with the downloaded firmware.

SULB-1050

Message `Firmwaredownload command continues.`

Message Type AUDIT | LOG

Class FIRMWARE

Severity INFO

Probable Cause Indicates that the **firmwareDownload** command is running on the standby control processor (CP) of the dual-CP system. This process should take approximately 17 minutes. The process is set to time out after 30 minutes.

Recommended Action Do not fail over or power down the system during firmware upgrade. Allow the **firmwareDownload** command to continue without disruption. No action is required.

Run the **firmwareDownloadStatus** command for more information.

SULB-1051

Message `Detected hot-plug of Standby CP. Firmware from Active CP will automatically be synchronized to Standby CP.`

Message Type AUDIT | LOG

Class FIRMWARE

Severity INFO

Probable Cause Indicates that auto firmware synchronization has started because the standby control processor (CP) is hot-plugged.

Recommended Action No action is required. Firmware download has started on the standby CP.

SULB-1052

Message `Firmwaresync has failed.<return code>`

Message Type AUDIT | LOG

Class FIRMWARE

Severity ERROR

Probable Cause Indicated that auto firmware synchronization has failed.

Recommended Action Execute the **firmwareDownloadStatus** and **firmwareShow** commands to view firmware status. Execute the **haShow** command to view the HA state.

SULB-1053

Message `<message>`

Message Type AUDIT | LOG

Class FIRMWARE

Severity INFO

Probable Cause Indicated that auto firmware synchronization has completed.

Recommended Action No action is required.

SULB-1054

Message `Firmwaresync has started`

Message Type AUDIT | LOG

Class FIRMWARE

Severity INFO

Probable Cause Indicated that firmware synchronization has started.

Recommended Action No action is required.

SWCH Messages

SWCH-1001

Message `Switch is not in ready state - Switch enable failed, switch status= 0x<switch status>, c_flags = 0x<switch control flags>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the switch is enabled before it is ready.

Recommended Action If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

SWCH-1002

Message `Security violation: Unauthorized device <wwn name of device> tries to flogin to port <port number>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified device is not present in the authorized profile list.

Recommended Action Verify that the device is authorized to log in to the switch. If the device is authorized, execute the **secPolicyDump** command to verify whether the World Wide Name (WWN) of the specified device is listed. If it is not listed, execute the **secPolicyAdd** command to add this device to an existing policy.

SWCH-1003

Message `Slot ENABLED but Not Ready during recovery, disabling slot = <slot number>(<return value>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the slot state has been detected as inconsistent during failover or recovery.

Recommended Action For a bladed switch, execute the **slotPowerOff** and **slotPowerOn** commands to power cycle the blade.

For a non-bladed switch, reboot or power cycle the switch.

SWCH-1004

Message `Blade attach failed during recovery, disabling slot = <slot number>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified blade has failed during failover or recovery.

Recommended Action For a bladed switch, execute the **slotPowerOff** and **slotPowerOn** commands to power cycle the blade.

For a non-bladed switch, reboot or power cycle the switch.

SWCH-1005

Message `Diag attach failed during recovery, disabling slot = <slot number>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the diagnostic blade attach operation has failed during failover or recovery.

Recommended Action For a bladed switch, execute the **slotPowerOff** and **slotPowerOn** commands to power cycle the blade.

For a non-bladed switch, reboot or power cycle the switch.

SWCH-1006

Message

```
HA state out of sync: Standby CP (ver = <standby SWC version>) does not support
NPIV functionality. (active ver = <active SWC version>, NPIV devices = <'1' if
NPIV devices exist; Otherwise '0'>).
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that the standby control processor (CP) does not support N_Port ID Virtualization (NPIV) functionality, but the switch has some NPIV devices logged in to the fabric.

Recommended Action Load a firmware version on a standby CP that supports NPIV functionality using the **firmwareDownload** command.

SWCH-1007

Message

```
Switch port <port number> disabled due to \"<disable reason>\".
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the switch port is disabled due to the reason displayed in the message.

Recommended Action

Based on the disable reason displayed, take appropriate action to restore the port.

If the disable reason is "Insufficient frame buffers", reduce the distance or speed settings for the port to reduce the buffer requirement of the link. Alternatively, one or more ports in the port group must be disabled to make more buffers available for the link.

Refer to the *Fabric OS Administrator's Guide* for more information.

SWCH-1008

Message

```
<area string> are port swapped on ports that do not support port swap. Slot <slot
number> will be faulted.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the blade enabled with the port configuration that does not support port swap.

Recommended Action

Replace the blade with ports that support port swap. Then swap ports back to the port's default area.

Refer to the *Fabric OS Administrator's Guide* for more information on port swapping.

SWCH-1009

Message

```
Shared area having Trunk Area (TA) enabled on slot <slot number>. Shared areas
that have TA enabled will be persistently disabled.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the blade is enabled with a port configuration that had Trunk Area previously enabled on the shared area port.

Recommended Action

Disable Trunk Area on ports that had Trunk Area enabled previously. Refer to the *Fabric OS Administrator's Guide* for more information.

SWCH-1010

Message `Trunk Area (TA) enabled on slot <slot number> with switch not in PID format 1. TA enabled ports will be persistently disabled.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the blade is enabled with the port configuration that had Trunk Area enabled previously.

Recommended Action Disable Trunk Area on ports that had Trunk Area enabled previously. Refer to the *Fabric OS Administrator's Guide* for more information.

SWCH-1011

Message `HA out of sync: Stby CP (ver=<standby SWC version>) doesn't support Trunk Area functionality. (active ver=<active SWC version>, TA enabled on sw=<'1' if Trunk Area ports exist; Otherwise '0'>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the standby control processor (CP) does not support Trunk Area functionality, but the switch has some ports with Trunk Area enabled.

Recommended Action Load a firmware version on standby CP that supports Trunk Area functionality by using the **firmwareDownload** command.

SWCH-1012

Message `Trunk Area (<trunk area>) has been enabled for one or more ports.`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates that a Trunk Area has been enabled for one or more ports and the configuration file has been updated.

Recommended Action No action is required.

SWCH-1013

Message `Trunk Area has been disabled for one or more ports.`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates that a Trunk Area assignment has been disabled for one or more ports and the configuration file has been updated.

Recommended Action No action is required.

SWCH-1014

Message `All Trunk Areas have been disabled.`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates that all Trunk Areas have been disabled and the configuration file has been updated.

Recommended Action No action is required.

SWCH-1015

Message `<Function name> <Description of problem>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that an internal problem has been detected by the software. This is usually an internal Fabric OS problem or due to file corruption.

Recommended Action Reboot or power cycle the switch.

If the message persists, execute the **firmwareDownload** command to update the firmware.

SWCH-1016

Message `Device <wwn name of device> FDISC to port <port number>. Static persistent PID set and area requested not assigned to the device. Reject FDISC.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the static persistent port ID (PID) is set and the area requested is not assigned to the device.

Recommended Action This is an N_Port ID virtualization (NPIV) device and the static persistent PID is set on it, though the area cannot be assigned as requested. Remove the static binding to have the device come up with a different area by using the **wwnaddress --unbind** command.

SWCH-1017

Message `Device <wwn name of device> tries to FLOGI to port <port number>, reject FLOGI as persistent PID is set on the Loop device.`

Message Type LOG

Severity INFO

Probable Cause Indicates persistent port ID (PID) is set and static persistent PID is not supported on loop device.

Recommended Action Remove the WWN-PID binding using the **wwnaddress --unbind** command and re-enable the port.

SWCH-1018

Message `Device <wwn name of device> FLOGI to port <port number>, Static persistent PID set, Requested area <area> user bound to another port. Reject FLOGI.`

Message Type LOG

Severity INFO

Probable Cause Indicates a WWN-PID and port address binding collision.

Recommended Action The persistent PID is set on the device and the requested area cannot be assigned because it is user bound to a different port. Remove the WWN-PID binding using the **wwnaddress --unbind** command or remove the port address binding using the **portaddress --unbind** command and then re-enable the port.

SWCH-1019

Message `Device <wwn name of device> tries to FLOGI, reject FLOGI as persistent PID is set on device and port <port number> has user area <area> bound to it.`

Message Type LOG

Severity INFO

Probable Cause Indicates a WWN-PID and port address binding collision.

Recommended Action The persistent PID is set on the device and the requested area cannot be assigned because the port it is trying to log in through has a different area bound to it. Remove the WWN-PID binding using the **wwnaddress --unbind** command or remove the port address binding using the **portaddress --unbind** command and then re-enable the port.

SWCH-1020

Message `HA state out of sync: Standby CP (ver = <standby SWC version>) does not support QoS links to AG(Active CP version = <active SWC version>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the standby control processor (CP) does not support links to Access Gateway running quality of service (QoS).

Recommended Action Load a firmware version on the standby CP that supports QoS links to Access Gateway by using the **firmwareDownload** command.

SWCH-1021

Message `HA state out of sync: Standby CP (ver = <standby SWC version>) does not support Dynamic area on default switch (Active CP version = <active SWC version>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the standby control processor (CP) does not support dynamic area on the default switch.

Recommended Action Load a firmware version on the standby CP that supports dynamic area on the default switch by using the **firmwareDownload** command.

SWCH-1022

Message
```
Port:<port number> has been disabled due to port address conflict while enabling
FMS mode.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that the switch has ports with FICON Management Server (FMS) reserved areas (0xFE, 0xFF) that are not supported in FMS mode.

Recommended Action No action required. Refer to the *FICON Administrator's Guide* for more information.

SWCH-1023

Message
```
HA state out of sync: Standby CP (ver = <standby SWC version>) does not support
XISL use while fmsmode and/or lossless are enabled (Active CP version =<active SWC
version>).
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that the standby control processor (CP) does not support extended inter-switch link (XISL) while FICON Management Server (FMS) mode and Lossless are enabled.

Recommended Action Load a firmware version on standby CP that supports both XISL use and FMS mode and Lossless at the same time by using the **firmwareDownload** command.

SWCH-1024

Message
```
HA state out of sync: Standby CP (ver = <standby SWC version>) does not support
active's enforce_login policy (Active CP version =<active SWC version>).
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that the standby control processor (CP) does not enforce login policy of the active CP.

Recommended Action Configure the enforce login policy to a value that the standby CP supports.

SWCH-1025

Message
```
This Logical Switch has ports other than 16 Gbps-capable FC ports. Edge Hold Time
for these ports is unchanged and is <Edge Hold Time>.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that the edge hold time for the non 16 Gbps-capable FC ports is not the same as 16 Gbps-capable FC ports in the logical switch. The non 16 Gbps-capable FC ports use the edge hold time configured on the default switch.

Recommended Action To know the edge hold time configured for non 16 Gbps-capable FC ports, go to the default switch and execute the **configShow** command.

SWCH-1026

Message
```
HA state out of sync: Standby CP (ver = <standby SWC version>) does not support
auto csctl_mode (Active CP version = <active SWC version>).
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that the standby control processor (CP) does not support auto class-specific control (CS_CTL) mode.

Recommended Action Upgrade the standby CP firmware version to same level as active CP.

SWCH-1027

Message
```
HA state out of sync: Standby CP (ver = <standby SWC version>) does not support
NPIV Base device Logout functionality. (active ver = <active SWC version>).
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that the standby control processor (CP) does not support N_Port ID Virtualization (NPIV) base device logout functionality, but the switch has some ports with base device configured.

Recommended Action Load a firmware version on standby CP that supports NPIV Base device Logout functionality using the **firmwareDownload** command, or change the 'base logout' feature with the **portCfgNPIVPort** command.

SWCH-1028

Message `The base FLOGI device(PID: 0x<PID>)) has logged out from the port (Index <Port Index>).`

Message Type LOG

Severity INFO

Probable Cause Indicates that the FLOGI assigned N_Port logged out from the port and other N_Ports are still active on the port.

Recommended Action No action required.

SWCH-1029

Message `supportinfoclear --clear was issued<message>`

Message Type AUDIT

Class CLI

Severity INFO

Probable Cause Indicates all the default statistics with portlogs and errorlogs are cleared.

Recommended Action No action is required.

SWCH-1030

Message `Switch port <port number> statistics cleared.`

Message Type AUDIT

Class FABRIC

Severity INFO

Probable Cause Indicates that the switch port statistics have been cleared.

Recommended Action No action is required.

SYSC Messages

SYSC-1001

Message `Failed to run <Name of program that could not be run (string)>:<System internal error message (string)>.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that one of the programs would not run on the system during the boot sequence.

Recommended Action If the message is reported during a reboot after new firmware has been loaded, try reloading the firmware using the **firmwareDownload** command.

If the message persists, there may be a conflict between the two versions of firmware or the nonvolatile storage may be corrupted.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

SYSC-1002

Message `Switch bring-up timed out.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the system timed out during a reboot or failover sequence, waiting for one or more programs to register with system services or to fail over to active status.

Recommended Action The switch is in an inconsistent state and can be corrected only by a reboot or power cycle. Before rebooting the chassis, record the firmware version on the switch or control processor (CP) and run the **haDump** command. If this is a dual-CP switch, gather the output from the CP in which this log message appeared.

SYSC-1004

Message `Daemon <Daemon name to restart> restart successful.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a terminated daemon is restarted by the system automatically.

Recommended Action Execute the **supportSave** command to gather troubleshooting data. No further action is required.

SYSC-1005

Message

```
Daemon <Daemon name to restart> is not restarted (Reason: <Restart failure
reason>).
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that a terminated daemon is not restarted, either because a restart limit is reached or a restart action fails.

Recommended Action

Execute the **supportSave** command to gather troubleshooting data. Execute the **reboot** or **haFailover** command to recover the system.

SYSM Messages

SYSM-1001

Message `No memory.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates the switch has run out of system memory.

Recommended Action Run the **memShow** command to view the switch memory usage.

Reboot or power cycle the switch.

Run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

SYSM-1002

Message `<number>, Switch: <Switch number>.`

Message Type LOG

Severity INFO

Probable Cause Indicates a user has executed either the **switchShutdown** or **switchReboot** command. All services are brought down for a logical switch.

Recommended Action No action is required if the **switchShutdown** or **switchReboot** command was executed intentionally. If the **switchShutdown** command was run, you must run the **switchStart** command to restart traffic on the logical switch.

SYSM-1003

Message `<number>, Switch: <start reason>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the user executed the **switchStart** or **switchReboot** command. All services are brought back up after a temporary shutdown of the logical switch.

Recommended Action No action is required if the **switchStart** command was executed intentionally. Because reinitializing a switch is a disruptive operation and can stop I/O traffic, you may have to stop and restart the traffic during this process.

SYSM-1004

Message `Failed to retrieve current chassis configuration option, ret=<Unknown>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates there was a failure to read configuration data from the World Wide Name (WWN) card.

Recommended Action Verify that the WWN card is present and operational and the affected control processor (CP) is properly seated in its slot.

SYSM-1005

Message `CP blade in slot <Slot number> failed to retrieve current chassis type.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates there was a failure to read the chassis type from the system.

Recommended Action Verify the control processor (CP) blade is operational and is properly seated in its slot.

SYSM-1006

Message `CP blade in slot <Slot number> is incompatible with the chassis type.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates this chassis type is not compatible with the control processor (CP) blade.

Recommended Action Use the CP blade on a compatible chassis.

SYSM-1007

Message `PERMITTING USE OF INCOMPATIBLE CHASSIS FOR CP IN SLOT <Slot number>. DATA ERRORS MAY RESULT.`

Message Type LOG

Severity WARNING

Probable Cause Indicates an override of the incompatible control processor (CP) or chassis check. This message is for engineering use only.

Recommended Action Delete the /var/chassis_backplane_override file and reboot the CP.

TAPE Messages

TAPE-1001

Message `Key acquisition for <Pool or Container> <Begins or Complete>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the key acquisition for the pool or the container has begun or is complete.

Recommended Action No action is required.

TRCE Messages

TRCE-1001

Message

```
Trace dump available<slot on which the trace dump occurs>! (reason: <cause of
trace dump: PANIC DUMP, WATCHDOG EXPIRED, MANUAL, TRIGGER>).
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that trace dump files have been generated on the switch or the specified slot. The cause for the dump can be one of the following:

- PANICDUMP: Generated by panic dump.
- WATCHDOG EXPIRED: Generated by hardware watchdog expiration.
- MANUAL: Generated manually by issuing the **tracedump -n** command.
- TRIGGER: Triggered by a specific Message ID generated by CRITICAL RASLog message.

Recommended Action Execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

TRCE-1002

Message

```
Trace dump<optional slot indicating on which slot the dump occurs> automatically
transferred to address ' <FTP target designated by user> '.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that a trace dump has occurred on the switch or the specified slot, and the trace dump files were automatically transferred from the switch to the specified FTP server.

Recommended Action No action is required.

TRCE-1003

Message

```
Trace dump<optional slot indicating on which slot the dump occurs> was not
transferred due to FTP error.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates that a trace dump has occurred on the switch or the specified slot, but the trace dump files were not automatically transferred from the switch due to reasons such as an FTP error, wrong FTP address, FTP site is down, and network is down.

Recommended Action Execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

TRCE-1004

Message `Trace dump<slot on which the trace dump occurs> was not transferred because trace auto-FTP disabled.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that trace dump files have been created on the switch or the specified slot, but the trace dump files were not automatically transferred from the switch because auto-FTP is disabled.

Recommended Action Execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

TRCE-1005

Message `FTP Connectivity Test failed due to error.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the connectivity test to the FTP host failed because of reasons such as a wrong FTP address, FTP site is down, or network is down.

Recommended Action Execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

TRCE-1006

Message `FTP Connectivity Test succeeded to FTP site ' <FTP target configured by users> '.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a connectivity test to the FTP host has succeeded.

Recommended Action No action is required.

TRCE-1007

Message `Notification of this MM has failed. Parameters temporarily out of sync with other MM.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the active control processor (CP) is unable to alert the standby CP of a change in trace status. This message is only applicable to bladed switches.

Recommended Action This message is often transitory. Wait a few minutes and try the command again.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

TRCE-1008

Message `Unable to load trace parameters.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the active control processor (CP) is unable to read the stored trace parameters.

Recommended Action Reboot the CP (dual-CP system) or restart the switch.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

TRCE-1009

Message `Unable to alert active MM that a dump has occurred.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the control processor (CP) is unable to communicate trace information to active CP. This message is only applicable to bladed switches.

Recommended Action Execute the **haShow** command to verify that the current management module is standby and the active management module is active.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

TRCE-1010

Message `Traced fails to start.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the trace daemon (traced), which is used for transferring the trace files has failed to start. The trace capability within the switch is unaffected. The system automatically restarts the traced facility after a brief delay.

Recommended Action Reboot the CP (dual-CP system) or restart the switch.

If the message persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

TRCE-1011

Message `Trace dump manually transferred to target ' <optional string to indicate which slot the trace dump is transferred> ': <result>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the trace dump files were transferred manually to the specified slot.

Recommended Action No action is required.

TRCE-1012

Message `The system was unable to retrieve trace information from slot <Slot number of the interface module on which the attempt was made>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the system was unable to retrieve trace information from the specified slot because there is no communication between the main system and the slot.

Recommended Action Check that the interface module is enabled and retry the command. If the interface module is already enabled, execute the **supportSave** command and contact your switch service provider.

TRCE-1013

Message

```
Trace dump <slot on which the trace dump occurs> was not transferred as FIPS mode
is enabled.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that a trace dump has occurred on the switch or the specified slot, but the trace dump files were not automatically transferred from the switch because FIPS mode is enabled on the switch.

Recommended Action

No action is required.

TRCK Messages

TRCK-1001

Message `Successful login by user <User>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the track change feature recorded a successful login.

Recommended Action No action is required.

TRCK-1002

Message `Unsuccessful login by user <User> after <login_fail_cnt> overall login failure attempts.`

Message Type LOG

Severity INFO

Probable Cause Indicates the track change feature recorded a failed login. This occurs if the user name or password is entered incorrectly.

Recommended Action Normally, this message indicates a typing error by an authorized user. If this message occurs repeatedly, it may indicate an unauthorized user trying to gain access to a switch. When secure mode is enabled on the fabric, the IP address of a failed login is reported to the error log.

TRCK-1003

Message `Logout by user <User>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the track change feature recorded a successful logout.

Recommended Action No action is required.

TRCK-1004

Message `Config file change from task:<task>`

Message Type LOG

Severity INFO

Probable Cause Indicates the track change feature recorded a configuration change for the switch. The track change feature records any change to the configuration file in nonvolatile memory, including a configuration download. This message is not generated for a configuration upload. All configuration changes occur through the parity data manager (PDM) server, so the PDMIPC is the only task possible.

Recommended Action No action is required. Run the **configShow** command to view the configuration file.

TRCK-1005

Message `Track-changes on.`

Message Type LOG

Severity INFO

Probable Cause Indicates the track change feature has been enabled.

Recommended Action No action is required. Run the **trackChangesSet 0** command if you want to disable the track change feature.

TRCK-1006

Message `Track-changes off.`

Message Type LOG

Severity INFO

Probable Cause Indicates the track change feature has been disabled.

Recommended Action No action is required. Run the **trackChangesSet 1** command if you want to enable the track changes feature.

TS Messages

TS-1001

Message

```
NTP Query failed: <error code>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that a Network Time Protocol (NTP) query to the configured external clock server failed. Local clock time on the principal or primary fabric configuration server (FCS) switch is used for fabric synchronization.

This message may be logged during temporary operational issues such as IP network connection issues to the external clock server. If the message does not recur, it can be ignored.

Recommended Action

Execute the **tsClockServer** command to verify that the configured external clock server is available and functional. If that external clock server is not available, choose another clock server.

TS-1002

Message

```
<Type of clock server used> Clock Server used instead of <Type of clock server
configured>: locl: 0x<Reference ID of LOCL> remote: 0x<Reference ID of external
clock server>.
```

Message Type

LOG

Severity

INFO

Probable Cause

Indicates the fabric time synchronization was sourced from an alternate clock server instead of the configured clock server. The clock server used can be one of the following type:

- LOCL - Local clock on the principal or primary FCS switch.
- External - External Network Time Protocol (NTP) server address configured.

This message may be logged during temporary operational issues such as IP network connection issues to the external clock server or the fabric is configured for external time synchronization but the principal or primary fabric configuration server (FCS) does not support the feature. If the message does not recur, it can be ignored.

Recommended Action

Execute the **tsClockServer** command to verify that the principal or primary FCS switch has the clock server IP configured correctly, and the configured clock server is accessible to the switch and functional. If the principal or primary FCS does not support the feature, either choose a different switch for the role or reset the clock server to LOCL.

TS-1006

Message `<message>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a time service event is occurring or has failed. The message can be one of the following:

- Init failed. Time Service exiting - Initialization error, but the time server exits.
- Synchronizing time of day clock - Usually logged during temporary operational issues when the clock goes out of synchronization. For example, when a time update packet is missed due to fabric reconfiguration or role change of the principal or primary fabric configuration server (FCS) switch. If the message does not recur, it can be ignored.
- Validating time update - Usually logged during temporary operational issues when a time update packet cannot be validated in a secure fabric. For example, during fabric reconfiguration or role change of the primary FCS switch. If the message does not recur, it can be ignored.

Recommended Action No action is required.

TS-1007

Message `<message>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a switch is trying to set the clock server, which is not the primary fabric configuration server (FCS) across the fabric. A consistent FCS policy must be implemented across the fabric.

Recommended Action Execute the **secPolicyShow** command to verify that the FCS policy is consistent across the fabric.

TS-1008

Message `<New clock server used> Clock Server used instead of <Old server configured>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the source of fabric time synchronization distributed from the principal or primary fabric configuration server (FCS) switch was changed to another configured clock server. This happens when the Network Time Protocol (NTP) query to the current active external clock server failed.

Recommended Action No action is required.

UCST Messages

UCST-1003

Message `Duplicate Path to Domain <domain ID>, Output Port = <port number>, PDB pointer = 0x<value>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that duplicate paths were reported to the specified domain from the specified output port. The *PDB pointer* value displayed in the message is the address of the path database and provides debugging information.

Recommended Action No action is required.

UCST-1007

Message `Inconsistent route detected: Port = <port number>, should be <port number>.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the switch detected an inconsistency in the routing database between the routing protocol and the hardware configuration. The first port number displayed is what the hardware has configured and the second port number displayed is what the protocol is using.

Recommended Action Run the **switchDisable** command and then the **switchEnable** command to reset the routing database. Run the **uRouteShow** command to display the new routing tables.

UCST-1020

Message `Static route (input-area: <port number>, domain: <domain ID> output-area: <port number>) has been ignored due to platform limitation.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the configured static route cannot be applied to the routing database because of a platform limitation.

Recommended Action No action is required.

UCST-1021

Message `In-order delivery option has been enabled.`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates that in-order delivery (IOD) option has been enabled on the switch. This option guarantees in-order delivery of frames during fabric topology changes.

Recommended Action No action is required.

UCST-1022

Message `In-order delivery option has been disabled.`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates that in-order delivery (IOD) option has been disabled on the switch. This may cause out-of-order delivery of frames during fabric topology changes.

Recommended Action No action is required.

UCST-1023

Message `Dynamic Load Sharing option has been enabled`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates that Dynamic Load Sharing (DLS) option has been enabled on the switch. This will move existing routes to a new redundant path when this path becomes available.

Recommended Action No action is required.

UCST-1024

Message `Dynamic Load Sharing option has been disabled.`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates that Dynamic Load Sharing (DLS) option has been disabled on the switch.

Recommended Action No action is required.

UCST-1026

Message `LossLess-DLS option has been enabled.`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates that the NoFrameDrop option has been enabled. This will help minimize frame loss during fabric topology changes.

Recommended Action No action is required.

UCST-1027

Message `LossLess-DLS option has been disabled.`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates that the NoFrameDrop option has been disabled. This may cause higher frame loss during fabric topology changes.

Recommended Action No action is required.

UCST-1028

Message `E_Port Balance Priority option has been enabled by <functionName>.`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates that priority is given to make sure that E_Port bandwidth demand is balanced.

Recommended Action No action is required.

UCST-1029

Message `E_Port Balance Priority option has been disabled by <functionName>.`

Message Type AUDIT | LOG

Class CFG

Severity INFO

Probable Cause Indicates that priority is no longer given to balanced E_Port bandwidth demand when balancing routes.

Recommended Action No action is required.

UPTH Messages

UPTH-1001

Message `No minimum cost path in candidate list.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the switch is unreachable because no minimum cost path (MPATH) exists in the candidate list (domain ID list).

Recommended Action No action is required. This error will end the current shortest path first (SPF) computation.

UPTH-1002

Message `Domain <domain ID> is unreachable because the enabled TI zone is not compatible with the fabric configuration.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the specified switch is unreachable because the traffic isolation (TI) zone and the fabric configuration are incompatible.

Recommended Action Clear all TI zones and then create a valid TI zone for your fabric configuration. Refer to the *Fabric OS Administrator's Guide* for more information on TI zoning.

VDR Messages

VDR-2001

Message `<message>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Field-Programmable Gate Array (FPGA) parity error threshold exceeded.

Recommended Action Power cycle the switch.

VS Messages

VS-1001

Message `No virtual PWWN assignment for the device <Login device PWWN>, port <Switch port> or (AG <AG NWWN> port <AG port>).`

Message Type LOG

Severity INFO

Probable Cause Indicates that the device with the virtual Port World Wide Name (PWWN) feature enabled tried to log in but there is no mapping for the device, port, or Access Gateway (AG) port.

Recommended Action Execute the **fapwwn** command to map the device, port, or AG port. You can ignore this message if the virtual PWWN is not required.

VS-1002

Message `The Virtual PWWN assignment for the device <Login device PWWN>, port <Switch port> (AG <AG NWWN> port <AG port>) is timed out.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the virtual Port World Wide Name (PWWN) association has timed out.

Recommended Action No action is required.

VS-1003

Message `Could not find Virtual PWWN config file for the switch.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the configuration file is corrupted or accidently removed.

Recommended Action Restart the switch and download the configuration using the **configDownload** command.

VS-1004

Message `Could not find Virtual PWWN config file for the switch.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the virtual Port World Wide Name (PWWN) feature has been enabled for the first time on the switch or the configuration file was corrupted or accidently removed.

Recommended Action Creating a new default configuration file. Execute the **configDownload** command to download any of your earlier configurations for the virtual PWWN feature.

VS-1005

Message `Virtual PWWN config version mismatch detected.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the virtual Port World Wide Name (PWWN) configuration present on the switch is not of the same Fabric OS version.

Recommended Action Converting the virtual PWWN configuration to the current Fabric OS version. No action is required.

VS-1006

Message `Virtualization services failed to initialize due to lack of enough memory.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the system has run out of memory.

Recommended Action No action is required.

VS-1007

Message `FSS Registration failed for virtualization services.`

Message Type LOG

Severity INFO

Probable Cause Indicates failure in the virtualization service daemon (vsd) startup because vsd has failed to register with Fabric OS State Synchronization (FSS).

Recommended Action No action is required.

VS-1008

Message `Virtualization services failed to create timer.`

Message Type LOG

Severity INFO

Probable Cause Indicates failure in the virtualization service daemon (vsd) startup because vsd has failed to create a timer.

Recommended Action No action is required.

WEBD Messages

WEBD-1001

Message `Missing or Invalid Certificate file -- HTTPS is configured but could not be started.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the Secure Sockets Layer (SSL) certificate file is either invalid or absent.

Recommended Action Install a valid certificate file.

WEBD-1002

Message `Missing or Invalid Key file -- HTTPS is configured but could not be started.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the Secure Sockets Layer (SSL) key file is either invalid or absent.

Recommended Action Install a valid key file.

WEBD-1004

Message `HTTP server and weblinker process will be restarted due to configuration change.`

Message Type LOG

Severity INFO

Probable Cause Indicates the Hypertext Transfer Protocol (HTTP) server configuration has changed.

Recommended Action No action is required.

WEBD-1005

Message `HTTP server and weblinker process will be restarted for logfile truncation.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the size of the Hypertext Transfer Protocol (HTTP) log file exceeded the maximum limit.

Recommended Action No action is required.

WEBD-1006

Message `HTTP server and weblinker restarted due to logfile truncation.`

Message Type LOG

Severity INFO

Probable Cause Indicates the size of the Hypertext Transfer Protocol (HTTP) log file exceeded the maximum limit.

Recommended Action No action is required.

WEBD-1007

Message `HTTP server and weblinker process will be restarted due to change of IP Address.`

Message Type LOG

Severity INFO

Probable Cause Indicates the IP address of the switch changed and the Hypertext Transfer Protocol (HTTP) server is restarted.

Recommended Action No action is required.

WEBD-1008

Message `HTTP server and weblinker process cannot be started.`

Message Type LOG | FFDC

Severity WARNING

Probable Cause Indicates a rare error condition in which the built-in recovery process has failed to restore Hypertext Transfer Protocol (HTTP) services. The problem often results from invalid configuration of Secure Sockets Layer (SSL) certificates, but there can be more than one reason for such a failure.

Recommended Action Verify the certification file; there may be a mismatch involved.

WEBD-1009

Message `HTTPS is disabled due to invalid certificate.`

Message Type LOG

Severity INFO

Probable Cause Indicates a condition where HTTPS cannot be enabled since certificate file is invalid and HTTP is enabled

Recommended Action No action is required.

XTUN Messages

XTUN-1000

Message `FTNL Tunnel <VE Port (Tunnel) Number> Missed Data frame:I/T/L:<FC Initiator ID>/<FC Target ID>/<FCP Logical Unit Number>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a missed frame with one or more Fibre Channel Protocol (FCP) data information units during a SCSI write or read operation.

Recommended Action If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

XTUN-1001

Message `FTNL Tunnel <VE Port (Tunnel) Number> Memory allocation failed tracker <Number that represents the calling source module>/<Line number in that source file>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a memory allocation failure.

Recommended Action Contact your vendor's customer support for assistance.

XTUN-1002

Message `FTNL Tunnel <VE Port (Tunnel) Number> Exchange timeout:I/T/L:<FC Initiator ID>/<FC Target ID>/<FCP Logical Unit Number>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the Fibre Channel Protocol (FCP) exchange has timed out.

Recommended Action If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

XTUN-1003

Message `FTNL Tunnel <VE Port (Tunnel) Number> Message Transmission failed:I/T/L/E:<FC Initiator ID>/<FC Target ID>/<FCP Logical Unit Number>/<Error return value>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a message transmission failure.

Recommended Action If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

XTUN-1004

Message `FTNL Tunnel <VE Port (Tunnel) Number> Exchange aborted:I/T/L:<FC Initiator ID>/<FC Target ID>/<FCP Logical Unit Number>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the Fibre Channel Protocol (FCP) exchange has been aborted by the initiator.

Recommended Action If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

XTUN-1005

Message `FCP emulation for Tunnel/Initiator/Target/LUN:<VE Port (Tunnel) Number>/<FC Initiator ID>/<FC Target ID>/<FCP Logical Unit Number> may not be optimal.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Fibre Channel Protocol (FCP) emulation is in FastWrite mode and could also be in Tape Pipelining mode.

Recommended Action For disk devices, no action is required. For tape devices, device rediscovery is required.

XTUN-1006

Message

```
FCIP FC frame drop due to transmit timeout on slot=<FX8-24 Slot Number (0 for 7800
and 7840)> DP=<FX8-24/7840 DP Number (or 0 if 7800)> BLS=<Blaster Image Number (0
or 1)> DR=<FC Descriptor Ring Number> Frames Dropped=<Number of FC frames that
were dropped>.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that a Fibre Channel (FC) Send frame timeout occurred and the frames were dropped from the SW queue.

Recommended Action

This error indicates that there is a slow draining device or a hung Blaster TX Descriptor Ring.

XTUN-1007

Message

```
FCIP FC frame drop due to truncated receive on slot=<FX8-24 Slot Number (0 for
7800 and 7840)> DP=<FX8-24/7840 DP Number (or 0 if 7800)> BLS=<Blaster Image
Number (0 or 1)> DR=<FC Descriptor Ring Number> Frames Dropped=<Number of FC
frames that were dropped>.
```

Message Type

LOG

Severity

ERROR

Probable Cause

Indicates that a Fibre Channel (FC) Received frame event was posted, but the frame was dropped due to an invalid receive length. This error occurs only on faulty hardware.

Recommended Action

Contact your vendor's customer support for assistance.

XTUN-1008

Message

```
FCIP Control block memory usage slot=<FX8-24 Slot number (0 for 7800 or 7840)>
DP=<FX8-24/7840 DP number (or 0 if 7800)> Allocated=<The total allocated bytes
from the pool> Free=<The total free bytes remaining in the pool> Total=<The total
size of the pool>.
```

Message Type

LOG

Severity

WARNING

Probable Cause

Indicates that the control block memory pool has crossed the usage threshold. This message is generated when a significant amount of control block memory has been allocated from the free pool. This memory is limited and you should monitor for events that indicate that greater than 80 percent of the pool has been allocated.

Recommended Action

Contact your vendor's customer support for assistance.

XTUN-1009

Message

```
FCIP OSTP <Number of FCP write commands that were purged> Write blocks purged due
to PLOGI slot=<FX8-24 Slot number (0 for 7800 or 7840)> DP=<FX8-24/7840 DP number
(or 0 if 7800)> SFID=<SFID of the initiator> DFID=<DFID of the tape device>
SID/DID/Lun=0x<SID of the initiator>/<DID of the tape device>/<The tape device LUN
number>.
```

Message Type LOG

Severity ERROR

Probable Cause Indicates that more than one outstanding write command that were purged due to the receipt of a new PLOGI sequence. This can indicate missing blocks on the currently mounted tape. If the tape job resumed after this error, you must confirm the integrity of the data on the tape.

Recommended Action Contact your vendor's customer support for assistance.

XTUN-1996

Message

```
FTRACE buffer <FTRACE Trace Buffer Number> on slot <FX8-24 Slot Number (0 for 7800
and 7840)> DP <FX8-24/7840 DP Number (or 0 if 7800)> has been cleared.
```

Message Type LOG

Severity INFO

Probable Cause Indicates that a CLI command or **supportSave** operation freed the trace buffer back into the FTRACE free pool.

Recommended Action No action is required.

XTUN-1997

Message

```
FTRACE buffer <FTRACE Trace Buffer Number> on slot <FX8-24 Slot number (0 for 7800
or 7840)> dp <FX8-24/7840 DP number (or 0 if 7800)> has been triggered.
```

Message Type LOG

Severity WARNING

Probable Cause Indicates that a programmed trigger event has been detected.

Recommended Action If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

XTUN-1998

Message `FTRACE buffer <FTRACE Trace Buffer Number> has been cleared.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a CLI command or **supportSave** operation freed the trace buffer back into the FTRACE free pool.

Recommended Action No action is required.

XTUN-1999

Message `FTRACE buffer <FTRACE Trace Buffer Number> has been triggered.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a programmed trigger event has been detected.

Recommended Action If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

XTUN-2000

Message `FCIP Tunnel <VE Port (Tunnel) Number> UP.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified Fibre Channel over IP (FCIP) tunnel is up.

Recommended Action No action is required.

XTUN-2001

Message `FCIP Tunnel <VE Port (Tunnel) Number> DOWN (<Reason>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified Fibre Channel over IP (FCIP) tunnel has gone down.

Recommended Action If the tunnel has not been administratively disabled or deleted, a possible network error or disruption has occurred.

XTUN-2002

Message `FCIP Tunnel <VE Port (Tunnel) Number> Circuit <Circuit Number> UP.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified circuit is up.

Recommended Action No action is required.

XTUN-2003

Message `FCIP Tunnel <VE Port (Tunnel) Number> Circuit <Circuit Number> DOWN (<Reason>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified circuit has gone down, and the tunnel will also be down if this is the last circuit available.

Recommended Action If the tunnel or circuit has not been administratively disabled or deleted, a possible network error or disruption has occurred.

XTUN-2004

Message `FCIP Tunnel <VE Port (Tunnel) Number> <Priority Class>-Pri QoS UP.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified quality of service (QoS) for this tunnel is up. This applies to the data classes only. When the F-Class comes online, the tunnel itself is marked as up.

Recommended Action No action is required.

XTUN-2005

Message `FCIP Tunnel <VE Port (Tunnel) Number> <Priority Class>-Pri QoS DOWN (<Reason>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified quality of service (QoS) for this tunnel has gone down. This applies to the data classes only. If the F-Class goes down, the tunnel itself is marked as down.

Recommended Action If tunnel or circuit has not been administratively disabled or deleted, a possible network error or disruption has occurred.

XTUN-2006

Message `FCIP Tunnel <VE Port (Tunnel) Number> CREATED (<Originator>).`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified tunnel has been successfully created.

Recommended Action No action is required.

XTUN-2007

Message `FCIP Tunnel <VE Port (Tunnel) Number> Circuit <Circuit Number> CREATED (<Originator>).`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified circuit has been successfully created.

Recommended Action No action is required.

XTUN-2008

Message `IKEv2: <Reason>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the status of an IKEv2 session has changed.

Recommended Action No action is required.

XTUN-2009

Message `IPsec: <Reason>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the status of an Internet Protocol security (IPsec) association has changed.

Recommended Action No action is required.

XTUN-2010

Message `SPD: <Reason>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the status of an SPD entry has changed.

Recommended Action No action is required.

XTUN-2011

Message `FIPS: <Reason>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the status of the module FIPS compliance has changed.

Recommended Action No action is required.

XTUN-2020

Message `FCIP Tunnel <VE Port (Tunnel) Number> DELETED (<Originator>).`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified Fibre Channel over IP (FCIP) tunnel has been administratively deleted.

Recommended Action No action is required.

XTUN-2021

Message `FCIP Tunnel <VE Port (Tunnel) Number> Circuit <Circuit Number> DELETED (<Originator>).`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified circuit has been administratively deleted.

Recommended Action No action is required.

XTUN-2022

Message `FCIP Tunnel <VE Port (Tunnel) Number> MODIFIED (<Originator>).`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified Fibre Channel over IP (FCIP) tunnel has been administratively modified.

Recommended Action No action is required.

XTUN-2023

Message `FCIP Tunnel <VE Port (Tunnel) Number> MODATTR (<Attribute change description>).`

Message Type LOG

Severity INFO

Probable Cause Indicates that the attribute is modified. In most cases, the attribute value is modified within the specified Fibre Channel over IP (FCIP) tunnel.

Recommended Action No action is required.

XTUN-2024

Message `FCIP Tunnel <VE Port (Tunnel) Number> Circuit <Circuit Number> MODIFIED (<Originator>).`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified circuit has been administratively modified.

Recommended Action No action is required.

XTUN-2025

Message `FCIP Tunnel <VE Port (Tunnel) Number> Circuit <Circuit Number> MODATTR (<Attribute change description>).`

Message Type LOG

Severity INFO

Probable Cause Indicates that the attribute is modified. In most cases, the attribute value is modified within the specified circuit.

Recommended Action No action is required.

XTUN-4104

Message `FTNL Tunnel <VE Port Number>.<Tunnel Group Number> (<Tunnel Id>) <Priority Class>-Pri QoS UP.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified quality of service (QoS) for this tunnel group is up. This applies to the data classes only. When the Control/F-Class comes online, the tunnel group itself is marked as up.

Recommended Action No action is required.

XTUN-4105

Message `FTNL Tunnel <VE Port Number>.<Tunnel Group Number> (<Tunnel Id>) <Priority Class>-Pri QoS DOWN (<Reason>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified quality of service (QoS) for this tunnel group has gone down unexpectedly. This applies to the data classes only. If the Control/F-Class goes down, the tunnel group itself is marked as down.

Recommended Action If tunnel or circuit has not been administratively disabled or deleted, a possible network error or disruption has occurred.

XTUN-4106

Message `FTNL Tunnel <VE Port Number>.<Tunnel Group Number> (<Tunnel Id>) <Priority Class>-Pri QoS CREATED.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified tunnel has been successfully created.

Recommended Action No action is required.

XTUN-4107

Message `FTNL Tunnel <VE Port Number>.<Tunnel Group Number> (<Tunnel Id>) Circuit <Circuit Number> <Priority Class>-Pri QoS CREATED.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified circuit has been successfully created.

Recommended Action No action is required.

XTUN-4115

Message `FTNL Tunnel <VE Port Number>.<Tunnel Group Number> (<Tunnel Id>) <Priority Class>-Pri QoS DOWN (<Reason>).`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified quality of service (QoS) for this tunnel group has gone down. The tunnel group is non-active or this is expected. This applies to the data classes only. If the Control/F-Class goes down, the tunnel group itself is marked as down.

Recommended Action If tunnel or circuit has not been administratively disabled or deleted, a possible network error or disruption has occurred.

XTUN-4120

Message `FTNL Tunnel <VE Port Number>.<Tunnel Group Number> (<Tunnel Id>) <Priority Class>-Pri QoS DELETED.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified extension over IP Tunnel has been administratively deleted.

Recommended Action No action is required.

XTUN-4121

Message `FTNL Tunnel <VE Port Number>.<Tunnel Group Number> (<Tunnel Id>) Circuit <Circuit Number> <Priority Class>-Pri QoS DELETED.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified circuit has been administratively deleted.

Recommended Action No action is required.

XTUN-4122

Message `FTNL Tunnel <VE Port Number>.<Tunnel Group Number> (<Tunnel Id>) <Priority Class>-Pri QoS MODIFIED.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified Tunnel has been administratively modified.

Recommended Action No action is required.

XTUN-4123

Message `FTNL Tunnel <VE Port Number>.<Tunnel Group Number> (<Tunnel Id>) <Priority Class>-Pri QoS MODATTR (<Attribute change description>).`

Message Type LOG

Severity INFO

Probable Cause Indicates that the attribute is modified. In most cases, the attribute value is modified within the specified in the extension over IP Tunnel.

Recommended Action No action is required.

XTUN-4124

Message `FTNL Tunnel <VE Port Number>.<Tunnel Group Number> (<Tunnel Id>) Circuit <Circuit Number> <Priority Class>-Pri QoS MODIFIED.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified circuit has been administratively modified.

Recommended Action No action is required.

XTUN-4125

Message `FTNL Tunnel <VE Port Number>.<Tunnel Group Number> (<Tunnel Id>) Circuit <Circuit Number> <Priority Class>-Pri QoS MODATTR (<Attribute change description>).`

Message Type LOG

Severity INFO

Probable Cause Indicates that the attribute is modified. In most cases, the attribute value is modified within the specified circuit.

Recommended Action No action is required.

XTUN-4126

Message `FTNL Tunnel <VE Port Number>.<Tunnel Group Number> (<Tunnel Id>) Circuit <Circuit Number> <Priority Class>-Pri QoS UP.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified circuit is up for the QoS specified.

Recommended Action No action is required.

XTUN-4127

Message `FTNL Tunnel <VE Port Number>.<Tunnel Group Number> (<Tunnel Id>) Circuit <Circuit Number> <Priority Class>-Pri QoS DOWN (<Reason>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified circuit has gone down unexpectedly, and the tunnel will also be down if this is the last circuit available.

Recommended Action If the tunnel or circuit has not been administratively disabled or deleted, a possible network error or disruption has occurred.

XTUN-4137

Message `FTNL Tunnel <VE Port Number>.<Tunnel Group Number> (<Tunnel Id>) Circuit <Circuit Number> <Priority Class>-Pri QoS DOWN (<Reason>).`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified circuit has gone down. The tunnel group is non-active or this is expected. The tunnel will also be down if this is the last circuit available.

Recommended Action If the tunnel or circuit has not been administratively disabled or deleted, a possible network error or disruption has occurred.

ZEUS Messages

ZEUS-1001

Message `Port <port number> port fault. Change the SFP or check cable.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a deteriorated small form-factor pluggable (SFP) transceiver, an incompatible SFP transceiver pair, or a faulty cable between the peer ports.

Recommended Action Verify that compatible SFP transceivers are used on the peer ports, the SFP transceivers have not deteriorated, and the Fibre Channel cable is not faulty. Replace the SFP transceivers or the cable if necessary.

ZEUS-1002

Message `Port <port number> chip faulted due to internal error.`

Message Type LOG | FFDC

Severity ERROR

Probable Cause Indicates an internal error. All ports on the blade or switch will be disrupted.

Recommended Action To recover a bladed system, execute the **slotPowerOff** and **slotPowerOn** commands on the blade. To recover a non-bladed system, execute the **fastBoot** command on the switch.

ZEUS-1003

Message `S<slot number>,C<chip index>: HW ASIC Chip error type = 0x<chip error type>.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates an internal error in the application-specific integrated circuit (ASIC) hardware that may degrade the data traffic.

Recommended Action Reboot the system at the next maintenance window. If the problem persists, replace the blade.

ZEUS-1004

Message `S<slot number>,C<chip index>: Invalid DMA ch pointer, chan:<Channel number>, good_addr:0x<Good address> bad_addr:0x<Bad address>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates an internal error in the application-specific integrated circuit (ASIC) hardware that may degrade the data traffic.

Recommended Action Reboot the system at the next maintenance window. If the problem persists, replace the blade.

ZEUS-1005

Message `S<slot number>,C<chip index>,A<zeus id>: Memory allocation failed.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a memory allocation failure in the software.

Recommended Action Restart the system at the next maintenance window. If the problem persists, replace the control processor (CP) blade.

ZEUS-1015

Message `Port re-initialized due to Link Reset failure on internal Port S<slot number>,P<port number>(<blade port number>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the port was re-initialized due to link reset failure.

Recommended Action When this error is observed persistently, power cycle the specified blade using the **slotPowerOff** and **slotPowerOn** commands. If the problem persists, replace the blade.

ZEUS-1016

Message `Port is faulted due to port re-initialization failure on internal Port S<slot number>,P<port number>(<blade port number>) with reason <port fault reason>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the specified port failed due to port re-initialization failure.

Recommended Action When this error is observed persistently, power cycle the specified blade using the **slotPowerOff** and **slotPowerOn** commands. If the problem persists, replace the blade.

ZEUS-1028

Message `Detected excessive Link resets on the port in a second. Slot <slot number>, Port <port number>(<blade port number>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the port received excessive link resets from peer port within 1 second and that exceeded threshold.

Recommended Action When this error is observed persistently, change the small form-factor pluggable (SFP) transceiver or cable on the peer port to which this port is connected.

ZONE Messages

ZONE-1002

Message `WWN zoneTypeCheck or zoneGroupCheck warning(<warning string>) at port(<port number>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a zone filter or zone group check failure occurred. The frame filter logic reported a failure when creating or adding the zone groups during port login (PLOGI) trap processing. This message usually indicates problems when adding the content-addressable memory (CAM) entries before the filter setup.

Recommended Action If the problem persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

ZONE-1003

Message `zone(<current zone>) contains (<domain id>, <port number>) which does not exist.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the port zone member that is targeted for the local switch contains a nonexistent port. The specified port number in the effective zoning configuration (displayed in the error message) is out of range.

Recommended Action Edit the zone database and change the port number to a viable value in the effective configuration.

ZONE-1004

Message `Base PID: 0x<Base PID>, Port Index: <Port Index>, Port: <Slot/Port>: enforcement changed to Session-based HARD Zoning.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the zoning enforcement has changed to session-based hard zoning due to one of the following conditions:

- The zone has a mix of WWN and domain,index (D,I) members.
- The Source Identifier (S_ID) list of the hardware-enforced zoning exceeded the S_ID limit.

Recommended Action No action is required.

ZONE-1007

Message `Ioctl (<function>) in (<error message>) at port (<port number>) returns code (<error string>) and reason string (<reason string>).`

Message Type LOG

Severity INFO

Probable Cause Indicates that frame filter logic reported a failure during the specified I/O Control (IOCTL) call. This is usually a programming error when adding CAM entries before the filter setup.

Recommended Action Avoid this problem in the following ways:

- Avoid having too many hosts zoned with a set of target devices at a single port.
- Avoid having too many zones directed at a single port group on the switch.

ZONE-1010

Message `Duplicate entries in zone (<zone name>) specification.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that there are duplicate entries in the specified zone object. This message occurs only when enabling a zone configuration.

Recommended Action Check the members of the zone using the **cfgShow** command. Delete the duplicate member using the **zoneRemove** command.

ZONE-1013

Message `QuickLoop not supported.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the QuickLoop feature is not supported in the current version of Fabric OS. QuickLoop zones are not supported in Fabric OS version 4.x or later. Even if the QuickLoop zoning configuration is enabled on the switch, it will not be supported.

Recommended Action Edit the zone database to remove the QuickLoop zoning definition in the effective configuration.

ZONE-1015

Message `Not owner of the current transaction <transaction ID>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a zoning change operation is not allowed because the zoning transaction is opened by another task. Indicates concurrent modification of the zone database by multiple administrators.

Recommended Action Wait until the previous transaction is completed. Verify that only one administrator is working with the zone database at a time.

ZONE-1017

Message `FA Zone(<zone name>) contains incorrect number of Initiator and Target devices.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the fabric assist (FA) zoning configuration has more than one initiator. This is because of incorrect entries in the FA zoning configuration.

Recommended Action Edit the zone database to make sure that only one initiator is set for each FA zone configuration.

ZONE-1019

Message

```
Transaction Commit failed. Reason code <reason code> (<Application reason>) -
\"<reason string>\".
```

Message Type LOG

Severity ERROR

Probable Cause Indicates that reliable commit service (RCS) had a transmit error. RCS is a protocol used to transmit changes to the configuration database within a fabric.

Recommended Action

Often this message indicates a transitory problem. Wait a few minutes and retry the command.

Make sure your changes to the zone database are not overwriting the work of another administrator.

Execute the **cfgTransShow** command to determine if there is any outstanding transaction running on the local switches.

If the problem persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

ZONE-1022

Message `The effective configuration has changed to <Effective configuration name>. <AD Id>`

Message Type LOG

Severity INFO

Probable Cause Indicates that the effective zone configuration has changed to the specified zone name.

Recommended Action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-1023

Message `Switch connected to port (<port number>) is busy. Retrying zone merge.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the switch is retrying the merge operation. This usually occurs if the switch on the other side of the port is busy.

Recommended Action If the problem persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

ZONE-1024

Message `<Information message>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the **cfgSave** command has completed successfully.

Recommended Action No action is required.

ZONE-1026

Message `port <port number> Out of CAM entries.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the total number of entries of S_ID CAM is above the limit while creating or adding a zone group. The maximum number of CAM entries allowed depends on the application-specific integrated circuit (ASIC).

Recommended Action If hardware zoning enforcement is preferred, edit the zoning database to have zoned port IDs (PIDs) for that port.

ZONE-1027

Message `Zoning transaction aborted <error reason>. <AD Id>`

Message Type LOG

Severity INFO

Probable Cause Indicates the zoning transaction was aborted because of a variety of potential errors. The *error reason* variable can be one of the following conditions:

- Zone Merge Received: The fabric is in the process of merging two zone databases.
- Zone Config update Received: The fabric is in the process of updating the zone database.
- Bad Zone Config: The new configuration is not viable.
- Zoning Operation failed: A zoning operation failed.
- Shell exited: The command shell has exited.
- Unknown: An error was received for an unknown reason.
- User Command: A user aborted the current zoning transaction.
- Switch Shutting Down: The switch is currently shutting down.

Most of these error conditions are transitory.

Recommended Action Try again after some time. Verify that only one administrator is modifying with the zone database at a time.

ZONE-1028

Message `Commit zone DB larger than supported - <zone db size> greater than <max zone db size>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the zone database size is greater than the limit allowed by the fabric. The limit of the zone database size depends on the lowest level switch in the fabric. Older switches have less memory and force a smaller zone database for the entire fabric.

Recommended Action Execute the **cfgSize** command to view the zone database size information. Edit the zone database to keep it within the allowable limit for the specific switches in your fabric.

ZONE-1029

Message `Restoring zone cfg from flash failed - bad config saved to <config file name> [<return code>].`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the zone configuration restored from the flash memory was faulty. This error will save the faulty zone configuration in the zoned core file directory.

Recommended Action If the problem persists, execute the **supportFtp** command (as needed) to set up automatic FTP transfers; then execute the **supportSave** command and contact your switch service provider.

ZONE-1034

Message `A new zone database file is created.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a new zone database file has been created.

Recommended Action No action is required.

ZONE-1036

Message `Unable to create <config file name>: error message <System Error Message>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the Fabric OS cannot create the zone configuration file. Typically, the zone configuration is too large for the memory available on the switch.

Recommended Action Reduce the size of the zone database and retry the operation.

ZONE-1037

Message `Unable to examine <config file name>: error message <System Error Message>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the Fabric OS cannot examine the zone configuration file. Typically, the zone configuration is too large for the memory available on the switch.

Recommended Action Reduce the size of the zone database and retry the operation.

ZONE-1038

Message `Unable to allocate memory for <config file name>: error message <System Error Message>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the Fabric OS cannot allocate enough memory for the zone configuration file. Typically, the zone configuration is too large for the memory available on the switch.

Recommended Action Reduce the size of the zone database and retry the operation.

ZONE-1039

Message `Unable to read contents of <config file name>: error message <System Error Message>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the Fabric OS cannot read the zone configuration file. Typically, the zone configuration is too large for the memory available on the switch.

Recommended Action Reduce the size of the zone database and retry the operation.

ZONE-1040

Message `Merged zone database exceeds limit.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Fabric OS cannot read the merged zone configuration file. Typically, the zone configuration is too large for the memory available on the switch.

Recommended Action Reduce the size of the zone database and retry the operation.

ZONE-1041

Message `Unstable link detected during merge at port (<Port number>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates a possible unstable link or faulty cable.

Recommended Action Verify that the small form-factor pluggable (SFP) transceiver and the cable at the specified port are not faulty. Replace the SFP and the cable, if necessary.

ZONE-1042

Message `The effective configuration has been disabled. <AD Id>`

Message Type LOG

Severity INFO

Probable Cause Indicates that the effective zone configuration has been disabled.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-1043

Message `The Default Zone access mode is set to No Access.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Default Zone access mode is set to No Access.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-1044

Message `The Default Zone access mode is set to All Access.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Default Zone access mode is set to All Access.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-1045

Message `The Default Zone access mode is already set to No Access.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Default Zone access mode is already set to No Access.

Recommended Action No action is required.

ZONE-1046

Message `The Default Zone access mode is already set to All Access.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Default Zone access mode is already set to All Access.

Recommended Action No action is required.

ZONE-1048

Message `ZONE ACA is rejected on the standby.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the standby zoning component did not receive a syncdump command from the primary side.

Recommended Action Synchronize the standby control processor (CP) using the **haSyncStart** command.

ZONE-1049

Message `ZONE AD-DefZone conflict detected while system initialization.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that there is an Admin Domain (AD) Default Zone conflict.

Recommended Action Verify that the default zoning mode for AD0 is set to No Access using the **defzone --show** command. If the default zoning mode is not set to No Access, execute the **defzone --noaccess** command and then execute the **cfgsave** command to commit the default zone mode change.

ZONE-1054

Message `Default Zone All Access mode is set with Frame Redirection zones.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Default Zone All Access mode will not grant all access behavior when the frame redirection zones are defined.

Recommended Action Remove frame redirection zones or set the Default Zone access mode to No Access using the **defzone --noaccess** command.

ZONE-1057

Message `TI Zone <TI zone name> has domain <Domain ID of switch with version pre6.4.0> running pre FOS6.4.0 firmware. TI member (Domain <Domain ID of higher port index>, Index <Higher port index>) is not supported.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that an unsupported port index (> 511) is present in the TI zone path or the routing may not be set up correctly.

Recommended Action Remove the port index from the TI zone using the **zone --remove** *name* command.

ZONE-1058

Message `Domain <Domain ID of the switch that becomes unreachable> present in TI zone <TI zone name> became unreachable due to failover disabled mode.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the domain present in the TI zone path is unreachable. This occurs if the TI zone paths are unavailable or the TI zone is set up incorrectly.

Recommended Action Verify that the paths defined by TI zones are online or remove the domain from the TI zone using the **zone --delete** *name* command.

ZONE-1059

Message `Unexpected TI routing behavior or a potentially unroutable TI configuration has been detected on local domain <Domain ID of the local Logical Switch where the error was detected>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the current fabric topology and TI zone configuration may result in an unroutable condition or an unexpected routing behavior.

Recommended Action Execute the **zone --showTIerrors** command on the specified switch to report the conflicting configuration details.

ZONE-1060

Message `Non-TI and TI failover-enabled traffic restricted to domain <Domain ID> due to TI failover-disabled zoning.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that only TI failover-disabled paths remain to reach the specified domain causing non-TI and TI failover traffic disruption.

Recommended Action Add or restore the non-TI or TI failover-enabled inter-switch links (ISLs) to the specified domain.

ZONE-1061

Message `Some trunk members are missing from failover disabled active TI zones.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that some members in the trunk group are not added to the failover-disabled TI zone. This will result in traffic disruption if the trunk member goes down.

Recommended Action If any trunk member is included in the TI failover-disabled zone path, then always add all members from that group. Execute the **zone --showTItrunkerrors** command on the switch to find the missing trunk members in the TI zone.

ZONE-1062

Message `Defined and Effective zone configurations are inconsistent.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the defined and effective configurations are different.

Recommended Action Execute the **cfgEnable** command to make both the configurations consistent.

ZONE-1064

Message `Failed to update client capability to ESS (Exchange Switch Support) after maximum number of retries - return code <Failed return code>. Failing sync dump to standby CP.`

Message Type LOG

Severity INFO

Probable Cause Indicates that Exchange Switch Support (ESS) is unable to update its capability. Failed to send the sync dump to standby control processor (CP).

Recommended Action Verify that HA synchronization has failed using the **haShow** command. If HA synchronization has failed, execute the **haSyncStart** command on active CP to resynchronize the HA state.

ZONE-1065

Message `Zoning operation (<function>) at port index (<port index>) returns code (<error code>). Port reset required.`

Message Type LOG

Severity WARNING

Probable Cause Indicates hardware and software zoning enforcement is out of sync.

Recommended Action Toggle the port using the **portDisable** and **portEnable** commands in order to recover zoning enforcement.

ZONE-1066

Message `Zoning operation failed to complete on the local switch - code <Error Code>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates an IPC error occurred between Name Server and Zone Server.

Recommended Action The switch is in an inconsistent state and can be corrected only by a reboot or power cycle.

Upon reboot, if switch is unable to join the fabric due to a zone conflict, issue **cfgClear** command.

If there is an enabled-configuration, commit **cfgClear** operation by issuing **cfgDisable**.

If there is no enabled-configuration, commit **cfgClear** operation by issuing **cfgSave**.

ZONE-3001

Message

```
Event: <Event Name>, Status: success, Info: <Zone object type> \"<Zone object
member list>\" added to <Zone object set type> \"<Zone object set name>\".
```

Message Type AUDIT

Class ZONE

Severity INFO

Probable Cause Indicates that a new zone object member or members have been added to the specified zone object set.

The *zone object type* variable can be an alias, zone member, zone, or zone configuration. The string "..." appears at the end of the *zone object member list* variable if the list was truncated in the message.

Recommended Action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3002

Message

```
Event: <Event Name>, Status: success, Info: <Zone object set type> \"<Zone object
set name>\" created with <Zone object type> \"<Zone object member list>\".
```

Message Type AUDIT

Class ZONE

Severity INFO

Probable Cause Indicates that a new zone object set was created and the specified zone object member or members were added to the zone object set.

The *zone object type* variable can be an alias, zone member, zone, or zone configuration. The string "..." appears at the end of the *zone object member list* variable if the list was truncated in the message.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3003

Message

```
Event: <Event Name>, Status: success, Info: <Zone object type> \"<Zone object
name>\" deleted.
```

Message Type AUDIT

Class ZONE

Severity INFO

Probable Cause Indicates that the specified zone object has been deleted.

The *zone object type* variable can be an alias, zone member, zone, or zone configuration.

Recommended Action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3004

Message

```
Event: <Event Name>, Status: success, Info: <Zone object type> \"<Zone object
member list>\" removed from <Zone object set type> \"<Zone object set name>\".
```

Message Type AUDIT

Class ZONE

Severity INFO

Probable Cause Indicates that the specified zone object member or members have been removed from the specified zone object set.

The *zone object type* variable can be an alias, zone member, zone, or zone configuration. The string "..." appears at the end of the *zone object member list* variable if the list was truncated in the message.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3005

Message `Event: <Event Name>, Status: success, Info: All zone information cleared from transaction buffer.`

Message Type AUDIT

Class ZONE

Severity INFO

Probable Cause Indicates that all the zone information has been cleared from the transaction buffer.

Recommended Action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3006

Message `Event: <Event Name>, Status: success, Info: Current zone configuration disabled. <AD Id>`

Message Type AUDIT

Class ZONE

Severity INFO

Probable Cause Indicates that the current zone configuration has been disabled.

Recommended Action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3007

Message `Event: <Event Name>, Status: success, Info: Zone configuration \"<Zone configuration>\" enabled. <AD Id>`

Message Type AUDIT

Class ZONE

Severity INFO

Probable Cause Indicates that the specified zone configuration has been enabled.

Recommended Action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3008

Message `Event: <Event Name>, Status: success, Info: Current zone configuration saved to MRAM. <AD Id>`

Message Type AUDIT

Class ZONE

Severity INFO

Probable Cause Indicates that the current zone configuration has been successfully saved to magnetoresistive random access memory (MRAM).

Recommended Action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3009

Message `Event: <Event Name>, Status: success, Info: <Event Description>.`

Message Type AUDIT

Class ZONE

Severity INFO

Probable Cause Indicates that the specified zone transaction has been successful.

Recommended Action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3010

Message `Event: <Event Name>, Status: success, Info: Zone object \"<Zone object name>\" copied to new zone object \"<New Zone object name>\".`

Message Type AUDIT

Class ZONE

Severity INFO

Probable Cause Indicates that the specified zone object has been copied to a new zone object.

Recommended Action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3011

Message `Event: <Event Name>, Status: success, Info: Zone object \"<Zone object name>\" expunged.`

Message Type AUDIT

Class ZONE

Severity INFO

Probable Cause Indicates that the specified zone object has been expunged.

Recommended Action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3012

Message `Event: <Event Name>, Status: success, Info: Zone object \"<Zone object name>\" renamed to \"<New Zone object name>\".`

Message Type AUDIT

Class ZONE

Severity INFO

Probable Cause Indicates that the specified zone object has been renamed.

Recommended Action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3013

Message `Event: <Event Name>, Status: success, Info: <Admin domain type> <Admin domain name> has been activated.`

Message Type AUDIT

Class FABRIC

Severity INFO

Probable Cause Indicates that the specified Admin Domain (AD) has been activated.

Recommended Action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3014

Message

```
Event: <Event Name>, Status: success, Info: \"<AD object member list>\" added to
<AD object set type> \"<AD object set name>\".
```

Message Type AUDIT

Class FABRIC

Severity INFO

Probable Cause Indicates that the specified new Admin Domain (AD) object member or members have been added to an AD object set.

The *AD object set type* variable can be an AD alias or AD member. The string "..." appears at the end of the *AD object member list* variable if the list was truncated in the message.

Recommended Action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3015

Message

```
Event: <Event Name>, Status: success, Info: AD configurations applied.
```

Message Type AUDIT

Class FABRIC

Severity INFO

Probable Cause Indicates that the saved Admin Domain (AD) configurations are enforced.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3016

Message

```
Event: <Event Name>, Status: success, Info: All AD definitions cleared.
```

Message Type AUDIT

Class FABRIC

Severity INFO

Probable Cause Indicates that all Admin Domain (AD) definitions and all zone configurations under them have been cleared.

Recommended Action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3017

Message `Event: <Event Name>, Status: success, Info: <AD object set type> \"<AD object set name>\" created with \"<AD object member list>\".`

Message Type AUDIT

Class FABRIC

Severity INFO

Probable Cause Indicates the specified Admin Domain (AD) has been created.

The *AD object set type* variable can be an AD alias or AD member. The string "..." appears at the end of the *AD object member list* if the list was truncated in the message.

Recommended Action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3018

Message `Event: <Event Name>, Status: success, Info:<AD object type> <AD object name> has been deactivated.`

Message Type AUDIT

Class FABRIC

Severity INFO

Probable Cause Indicates that the specified Admin Domain (AD) object has been deactivated.

Recommended Action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3019

Message `Event: <Event Name>, Status: success, Info: <AD object type> \"<AD object name>\" deleted.`

Message Type AUDIT

Class FABRIC

Severity INFO

Probable Cause Indicates that the specified Admin Domain (AD) object has been deleted.

Recommended Action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3020

Message

```
Event: <Event Name>, Status: success, Info: \"<AD object member list>\" removed
from <AD object set type> \"<AD object set name>\".
```

Message Type AUDIT

Class FABRIC

Severity INFO

Probable Cause Indicates that the specified Admin Domain (AD) member or members have been removed from the AD.

Recommended Action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3021

Message

```
Event: <Event Name>, Status: success, Info: AD object \"<AD object name>\" renamed
to \"<New AD object name>\".
```

Message Type AUDIT

Class FABRIC

Severity INFO

Probable Cause Indicates that the specified Admin Domain (AD) has been renamed.

Recommended Action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3022

Message

```
Event: <Event Name>, Status: success, Info: Current AD configuration saved to
flash.
```

Message Type AUDIT

Class FABRIC

Severity INFO

Probable Cause Indicates that the current Admin Domain (AD) configuration has been saved to flash memory.

Recommended Action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3023

Message `Event: <Event Name>, Status: Failure, Info: AD Apply operation failed due to transaction conflict.`

Message Type AUDIT

Class FABRIC

Severity INFO

Probable Cause Indicates that the **ad --apply** command has failed because of a transaction conflict.

Recommended Action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3024

Message `Command: <Command Name>, Status: success, Info: executed. <AD Id>`

Message Type AUDIT

Class FABRIC

Severity INFO

Probable Cause Indicates that the **ad --transabort** command has completed successfully in the specified Admin Domain (AD).

Recommended Action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3025

Message `Command: <Command Name> Info: executed. In AD <AD Id>.`

Message Type AUDIT

Class FABRIC

Severity INFO

Probable Cause Indicates that the **ad --exec** command was executed in the specified Admin Domain (AD).

Recommended Action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

ZONE-3026

Message

```
Event: <Event Name>, Status: success, Info: Zone object \"<Zone object name>\"
replaced with \"<New Zone object name>\".
```

Message Type

AUDIT

Class

ZONE

Severity

INFO

Probable Cause

Indicates that the specified zone object has been replaced.

Recommended Action

Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.