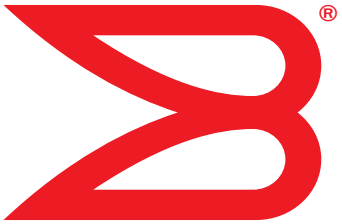
53-1004587-01
21 November 2016



Brocade Network OS

Message Reference

Supporting Network OS 7.1.0

BROCADE

© 2016 Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, Brocade Assurance, the B-wing symbol, ClearLink, DCX, Fabric OS, HyperEdge, ICX, MLX, MyBrocade, OpenScript, VCS, VDX, Vplane, and Vyatta are registered trademarks, and Fabric Vision is a trademark of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned may be trademarks of others.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. assume no liability or responsibility to any person or entity with respect to the accuracy of this document or any loss, cost, liability, or damages arising from the information contained herein or the computer programs that accompany it.

The product described by this document may contain open source software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit *http://www.brocade.com/support/oscd*.

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
Network OS Message Reference	53-1002082-01	New document	December 2010
Network OS Message Reference	53-1002341-01	Updated for Network OS v2.1.0: • Added new chapters: DCM, DOT1, FW, IGMP, L2SS, L3SS, PHP, PLAT, SS, VC, and VCS. • Added new messages: EM, FABR, FCOE, FVCS, HAM, HIL, LOG, MSTP, NSM, ONMD, PORT, RAS, RTWR, SEC, SFLO, SNMP, SSMD, SULB, and ZONE. • Deleted messages: CEE CONFIG, EANV, FABR, FVCS, HSL, LACP, MFIC, NSM, PORT, and TOAM.	September 2011

Title	Publication number	Summary of changes	Date
Network OS Message Reference	53-1002489-01	Updated for Network OS v2.1.1: • Added new chapters: AUTH, C2, ELD, RCS, and TS. • Added new messages: L2SS, PORT, SEC, and SSMD. • Modified messages: L2SS, SEC, and ZONE.	December 2011
Network OS Message Reference	53-1002559-01	Updated for Network OS v3.0.0: • Added new chapters: BL, BLL, C3, CHS, ERCP, ESS, FABS, FCMC, FCPH, FLOD, FSPF, FSS, HASM, HAWK, HLO, KTRC, L2AG, LSDB, MCAST_SS, MPTH, MS, NBFS, NS, OSPF, PDM, RTM, SCN, SLCD, SWCH, UCST, UPTH, VRRP, and WLV. • Added new messages: AUTH, C2, DCM, EM, FABR, FVCS, FW, HIL, IPAD, L2SS, MSTP, NSM, and ONMD. • Modified messages: DOT1, EANV, ELD, FCOE, HSL, IGMP, LOG, MSTP, NSM, ONMD, PHP, PLAT, PORT, RAS, RCS, RTWR, SEC, SFLO, SNMP, SS, SSMD, SULB, TOAM, TRCE, TS, VC, VCS, and ZONE. • Deleted chapters: HAM and L3SS.	September 2012
Network OS Message Reference	53-1002807-01	Updated for Network OS v3.0.1: • Added new chapter: LACP. • Added new messages: EM, PORT, RAS, SEC, TS, and VC. • Modified messages: BL, HASM, and SNMP. • Deleted messages: RTM.	December 2012
Network OS Message Reference	53-1002843-01	Updated for Network OS v4.0.0: • Added new chapters: BGP, CBR, LIC, PCAP, PIM, QOSD, and UDLD. • Added new messages: DCM, FCOE, FVCS, HASM, HIL, L2AG, LOG, MSTP, NSM, PORT, RAS, RTM, SFLO, SS, SSMD, SULB, TS, VC, and VRRP. • Modified messages: DCM, EM, FSS, FVCS, HASM, LACP, LOG, MCST, MSTP, NSM, PLAT, PORT, RAS, RTM, SEC, SFLO, SS, SSMD, TS, VC, and VCS. • Deleted messages: SEC and SSMD.	July 2013

Title	Publication number	Summary of changes	Date
Network OS Message Reference	53-1003121-01	Updated for Network OS v4.1.0: • Added new chapters: AG, DAD, HWK2, SRM, and TNLD. • Added new messages: BL, DCM, EM, FABR, FCOE, FSS, FW, HASM, L2AG, L2SS, NSM, RAS, SEC, and WLV. • Modified messages: FCOE, FVCS, FW, HASM, MSTP, NSM, SEC, and WLV.	February 2014
Network OS Message Reference	53-1003227-01	Updated for Network OS v4.1.1: • Added new messages: L2SS, NSM, and TNLD. • Modified messages: QOSD.	March 2014
Network OS Message Reference	53-1003319-01	Updated for Network OS v5.0.0: • Added new chapters: MM, OSPF6, and RPS. • Added new messages: FABR, FCPH, FSPF, FSS, FVCS, FW, HASM, HSL, NBFS, NSM, PIM, PLAT, RCS, SEC, SS, SWCH, and ZONE. • Modified messages: AG, FABR, FSPF, FVCS, HASM, MCST, NBFS, NS, NSM, RTM, SULB, and ZONE. • Deleted messages: FABR, RTM, SSMD, and ZONE.	August 2014
Network OS Message Reference	53-1003664-01	Updated for Network OS v6.0.0: • Added new chapters: CBR2 and WEBD. • Added new messages: BL, DCM, EM, FW, HASM, HIL, IPAD, L2AG, L2SS, QOSD, and SEC. • Modified messages: AG, FCOE, FVCS, LOG, PORT, RAS, and SEC. • Deleted messages: SSMD.	February 2015
Network OS Message Reference	53-1003777-01	Updated for Network OS v6.0.1: • Added new chapters: BFD, MAPS, OFMA, and OFMM. • Added new messages: CBR, DAD, DCM, FCOE, FCPH, FVCS, HASM, HSL, NSM, SEC, SSMD, SULB, TNLD, and VC. • Modified messages: DAD, NSM, SSMD, TNLD, and WLV. • Deleted messages: SSMD.	June 2015
Network OS Message Reference	53-1003777-02	Updated for Network OS v6.0.1a: • Added new chapters: PEM. • Modified messages: WEBD.	August 2015

Title	Publication number	Summary of changes	Date
Network OS Message Reference	53-1004080-01	Updated for Network OS v7.0.0: • Added new chapters: AQPH. • Added new messages: ARP, BL, CBR, CBR2, DCM, FABR, FVCS, HAWK, HSL, HWK2, L2AG, L2SS, LACP, LIC, NBFS, NS, NSM, TNLD, VCS, and ZONE. • Modified messages: HASM, L2SS, PEM, SSMD, and ZONE. • Deleted messages: ZONE-1012.	February 2016
Network OS Message Reference	53-1004373-01	Updated for Network OS v7.0.1: • Added new messages: HSL, MAPS, ONMD and TNLD. • Modified messages: NSM.	May 2016
Brocade Network OS Message Reference	53-1004587-01	Updated for Network OS v7.1.0: • Added new chapters: AL and DHCP. • Added new messages: CBR, CBR2, DCM, DOT1, L2SS, LOG, SEC, SRM, and VCS. • Modified messages: BL, HSL, SRM, TNLD, and WLV. • Deleted messages: HSL.	November 2016

Contents

Preface

In this chapter

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Brocade technical documentation.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used in the flow of the text to highlight specific words or phrases.

Format	Description
bold text	Identifies command names Identifies keywords and operands Identifies the names of user-manipulated GUI elements Identifies text to enter at the GUI
italic text	Identifies emphasis Identifies variables Identifies document titles
`courier font`	Identifies CLI output Identifies command syntax examples

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
Italic text	Identifies a variable.
Value	In Fibre Channel products, a fixed value provided as input to a command option is printed in plain text, for example, –show WWN.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ x | y | z }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options. In Fibre Channel products, square brackets may be used instead for this purpose.
x | y	A vertical bar separates mutually exclusive elements.
< >	Non-printing characters, for example, passwords, appear in angle brackets.
...	Repeat the previous element, for example, member[member...].
\	Indicates a “soft” line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

NOTE
In Brocade VCS Fabric technology® mode, interfaces are identified using switch/slot/port notation.

Notes, cautions, and warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the 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 a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

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.

Brocade resources

Visit the Brocade website to locate related documentation for your product and additional Brocade resources.

You can download additional publications supporting your product at www.brocade.com. Select the Brocade Products tab to locate your product, then click the Brocade product name or image to open the individual product page. The user manuals are available in the resources module at the bottom of the page under the Documentation category.

To get up-to-the-minute information, go to MyBrocade. You can register at no cost for a user ID and password.

Release notes are available onMyBrocade under Product Downloads.

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

Contacting Brocade Technical Support

As a Brocade customer, you can contact Brocade Technical Support 24x7 online, by telephone, or by e-mail. Brocade OEM customers contact their OEM/Solutions provider.

For product support information and the latest information on contacting the Technical Assistance Center, go to http://www.brocade.com/service-support/index.html

If you have purchased Brocade product support directly from Brocade, use one of the following methods to contact the Brocade Technical Assistance Center 24x7.

Online	Telephone
Preferred method of contact for non-urgent issues: • My Cases through MyBrocade • Software downloads and licensing tools • Knowledge Base	Required for Sev 1-Critical and Sev 2-High issues: • Continental US: 1-800-752-8061 • Europe, Middle East, Africa, and Asia Pacific: +800-AT FIBREE (+800 28 34 27 33) • For areas unable to access toll free number: +1-408-333-6061 • Toll-free numbers are available in many countries.

If you have purchased Brocade product support from a Brocade OEM/Solution Provider, contact your OEM/Solution Provider for all of your product support needs.

- OEM/Solution Providers are trained and certified by Brocade to support Brocade® products.
- Brocade provides backline support for issues that cannot be resolved by the OEM/Solution Provider.
- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information, contact Brocade or your OEM.
- For questions regarding service levels and response times, contact your OEM/Solution Provider.

Document feedback

To send feedback and report errors in the documentation you can use the feedback form posted with the document or you can e-mail the documentation team.

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. You can provide feedback in two ways:

- Through the online feedback form in the HTML documents posted on www.brocade.com.
- By sending your feedback to documentation@brocade.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

About This Document

In this chapter

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 Network OS v7.1.0, documenting all possible configurations and scenarios is beyond the scope of this document.

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

- Brocade VDX 2741
- Brocade VDX 2746
- Brocade VDX 6740
  - Brocade VDX 6740-48
  - Brocade VDX 6740-64
- Brocade VDX 6740T
  - Brocade VDX 6740T-48
  - Brocade VDX 6740T-64
  - Brocade VDX 6740T-1G
- Brocade VDX 6940-36Q
- Brocade VDX 6940-144S
- Brocade VDX 8770
  - Brocade VDX 8770-4
  - Brocade VDX 8770-8

What's new in this document

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

- New modules added:
  - AL messages
  - DHCP messages
- Information that was added:
  - CBR-1042
  - CBR2-1042
  - DCM-1015
  - DCM-1601
  - DOT1-1014
  - DOT1-1015
  - DOT1-1016
  - DOT1-1017
  - L2SS-1033
  - L2SS-1034
  - L2SS-1035
  - LOG-1013
  - SEC-3108
  - SEC-3109
  - SRM-1002
  - SRM-1003
  - SRM-1004
  - SRM-1005
  - SRM-1006
  - VCS-1011
  - VCS-1012
- Information that was modified:
  - BL-1052
  - HSL-1014
  - HSL-1015
  - SRM-1001
  - TNLD-1008
  - WLV-1004
- Information that was deleted:
  - HSL-1016

Chapter

1 Introduction to RASLog Messages

In this chapter

Overview of RASLog messages

RASLog messages log system events related to configuration changes or system error conditions. Messages are reported at various levels of severity ranging from informational (INFO) to escalating error levels (WARNING, ERROR, and CRITICAL). Network OS maintains two separate internal message storage repositories, SYSTEM and DCE. Table 1 shows the message types stored in each of the two repositories. A RASLog message can have one or more type attributes. For example, a message can be of type DCE, FFDC, and AUDIT. A message cannot have both LOG and DCE type attributes.

TABLE 1 Message type matrix

Message type	DCE message repository	SYSTEM message repository
LOG	No	Yes
DCE	Yes	No
CFFDC	Yes	Yes
FFDC	Yes	Yes
VCS	Yes	Yes
AUDIT	Yes	Yes

RASLog message types

Network OS supports five types of RASLog messages. The following sections describe in detail the message types.

System messages

System or LOG messages report significant system-level events or information and are also used to show the status of the high-level user-initiated actions. System messages are stored in a separate nonvolatile storage and are preserved across the firmware upgrade or downgrade. The system messages are forwarded to the console, to the configured syslog servers, and through the SNMP traps or informs to the SNMP management station.

The following is an example of a system message.

```
2011/08/23-22:58:12, [EM-1036], 4,, WARNING, VDX6720-24, Fan 1 is not accessible.
```

For information on displaying and clearing the system messages, refer to "Viewing and clearing the SYSTEM messages" on page 15.

DCE RASLog messages

DCE RASLog messages report error-related events and information in the protocol-based modules such as network service module (NSM), system services manager (SSM), and so on. DCE messages are stored in a separate nonvolatile storage and are preserved across the firmware upgrades. The DCE messages are forwarded to the console, to the configured syslog servers, and through the SNMP traps or informs to the SNMP management station.

NOTE

DCE messages are supported only in Network OS v3.0.0 and later. If you downgrade to an earlier firmware version, the DCE messages will be dropped.

The following is an example of a DCE message.

```
2012/05/30-21:25:55, [ONMD-1002], 59, M1 | DCE, INFO, sw0, LLDP global
configuration is changed.
```

For information on displaying and clearing the DCE RASLog messages, refer to "Viewing and clearing the DCE messages" on page 15.

VCS RASLog messages

VCS RASLog messages are supported in VCS fabrics only. The VCS RASLog messages are used to indicate events such as node removal and node join from the Brocade VCS fabric. When a switch generates a VCS RASLog message, it is forwarded to the system console, remote syslog, and SNMP management station.

The following is an example of a VCS RASLog message.

```
2011/08/26-12:40:01, [VCS-1003], 7013/3454, VCS, INFO, VDX6720-60, Event: VCS
node add, Coordinator IP: 10.17.10.31, VCS ID: 1, Status: rBridge ID 1
(10.17.10.32) added to VCS cluster., VcsFabAddRejoin, line: 1450, comp:dcmd,
ltime:2011/06/27-02:47:04:555942.
```

You can display the VCS RASLog messages using the **show logging raslog attribute VCS** command. For information on displaying the VCS RASLog messages, refer to "Displaying the VCS messages" on page 16.

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, firmware downloads, and configuration. Audit log messages are saved in the persistent storage. The storage has a limit of 1024 entries and will wrap around if the number of messages exceed the limit. The switch can be configured to stream Audit messages to the specified syslog servers. The Audit log messages are not forwarded to an SNMP management station.

The following is an example of an Audit log message.

```
AUDIT,2011/08/26-07:51:32 (GMT), [DCM-2001], INFO, DCMCFG,
root/none/127.0.0.1/rpc/cli,, VDX6720-24, Event: noscli start, Status: success,
Info: Successful login attempt through console from 127.0.0.1.
```

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.
- Status - The status of the event that occurred: success or failure.
- Event Info - Information about the event.

The three event classes described in Table 2 can be audited.

TABLE 2 Event classes of the Audit messages

Event class	Operand	Description
DCMCFG	CONFIGURATION	You can audit all the configuration changes in the Network OS.
FIRMWARE	FIRMWARE	You can audit the events occurring during the firmware download process.
SECURITY	SECURITY	You can audit any user-initiated security event for all management interfaces. For events that have an impact on the entire network, an audit is generated only for the switch from which the event was initiated.

You can enable event auditing by configuring the syslog daemon to send the events to a configured remote host using the **logging syslog-server** command. You can set up filters to screen out particular classes of events using the **logging auditlog class** command (the classes include SECURITY, CONFIGURATION, and FIRMWARE). All the Audit classes are enabled by default. The defined set of Audit messages are 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 19.

FFDC messages

First Failure Data Capture (FFDC) is used to capture failure-specific data when a problem or failure is first noted and before the switch reloads or the 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 by executing the **copy support** command. The data are used for debugging purposes. FFDC is intended for use by Brocade technical support.

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

The following is an example of an FFDC message.

```
2011/08/26-12:39:02, [HAM-1007], 2, FFDC, CRITICAL, VDX6720-24, Need to reboot the
system for recovery, reason: raslog-test-string0123456-raslog.
```

You can display the FFDC messages using the **show logging raslog attribute FFDC** command. For information on displaying the FFDC RASLog messages, refer to "Displaying the FFDC messages" on page 17.

CFFDC messages

Chassis wide FFDC (CFFDC) is used to capture FFDC data for every management module (MM) or line card (LC) in the entire chassis for failure analysis. This debug information is saved in a nonvolatile storage and can be retrieved by executing the **copy support** command. If FFDC is disabled, the CFFDC data is not captured even when a message with CFFDC attribute is logged.

The following is an example of a CFFDC message.

```
2013/10/14-10:36:51, [EM-1100], 28749, M2 | Active | CFFDC, CRITICAL, VDX8770-4,
Unit in L3 with ID 127 is faulted(119). 1 of 1 total attempt(s) at auto-recovery
is being made. Delay is 60 seconds.
```

Message severity levels

There are four levels of severity for messages, ranging from CRITICAL to INFO. In general, the definitions are wide ranging and are to be used as general guidelines for troubleshooting. In all cases, you must look at each specific error message description thoroughly before taking action. Table 3 lists the RASLog message severity levels.

TABLE 3 Severity levels of the RASLog messages

Severity level	Description
CRITICAL	Critical-level messages indicate that the software has detected serious problems that 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.
ERROR	Error-level messages represent an error condition that does not affect overall system functionality significantly. For example, error-level messages may indicate time-outs on certain operations, failures of certain operations after retries, invalid parameters, or failure to perform a requested operation.
WARNING	Warning-level messages highlight a current operating condition that must 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.
INFO	Info-level messages report the current non-error status of the system components; for example, detecting online and offline status of an interface.

RASLog message logging

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

- SYSTEM and DCE messages are saved to separate nonvolatile storage repositories.
- SYSTEM and DCE message logs can save a maximum of 4096 messages.
- The message log is implemented as a circular buffer. When more than the maximum entries are added to the log file, new entries overwrite the old entries.
- Messages are numbered sequentially from 1 through 2,147,483,647 (0x7fffffff). The sequence number continues to increase after the message log wraps around. The message sequence numbering is not split for the system and DCE message logs. The sequence number can be reset to 1 using the **clear logging raslog** command. However, the sequence number is not reset to 1 if you clear a particular message type, for example, DCE.
- Trace dump, FFDC, and core dump files can be uploaded to the FTP server using the **copy support ftp** command.
- Brocade recommends that you configure the system logging daemon (syslogd) facility as a management tool for error logs. For more information, refer to "System logging daemon" on page 5.

Configuring the syslog message destinations

You can configure a switch 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.

Network 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. All the RASLog messages are forwarded to the syslogd. Configuring for syslogd involves configuring the host, enabling syslogd on the Brocade model, and optionally, setting the facility level.

Configuring a syslog server

To configure the switch to forward all RASLog messages to the syslogd of one or more servers, perform the following steps.

1. Execute the **configure terminal** command to access the global configuration level of the CLI.

```
device# configure terminal
Entering configuration mode terminal
```

2. Execute the **logging syslog-server** *IP address* command to add a server to which the messages are forwarded. You can configure a syslog server in both IPv4 or IPv6 format. The following example is for configuring a syslog server with IPv4 address.

```
device(config)# logging syslog-server 192.0.2.2
```

You can configure up to four syslog servers to receive the syslog messages.

3. Execute the **show running-config logging syslog-server** command to verify the syslog configuration on the switch.

```
device# show running-config logging syslog-server
logging syslog-server 192.0.2.2
```

The following example configures a syslog server with an IPv6 address.

```
device# configure terminal
Entering configuration mode terminal
device(config)# logging syslog-server 2001:DB8::32
device(config)# exit
device# show running-config logging syslog-server
logging syslog-server 2001:db8::32
```

You can remove a configured syslog server using the **no logging syslog-server** *IP address* command.

Setting the syslog facility

The syslog facility is a configurable parameter that specifies the log file to which messages are forwarded. You must configure the syslog servers to receive system messages before you can configure the syslog facility.

To set the syslog facility, perform the following steps.

1. Execute the **configure terminal** command to access the global configuration level of the CLI.

```
device# configure terminal
Entering configuration mode terminal
```

2. Execute the **logging syslog-facility local** *log_level* command to set the syslog facility to a specified log file.

   The *log_leve*l specifies the syslog facility and can be a value from LOG_LOCAL0 through LOG_LOCAL7. The default syslog level is LOG_LOCAL7. The following example is for setting the syslog facility level to LOG_LOCAL2.

```
device(config)# logging syslog-facility local LOG_LOCAL2
```

3. Execute the **show running-config logging syslog-facility** command to verify the syslog facility configuration on the switch.

```
device# show running-config logging syslog-facility
logging syslog-facility local LOG_LOCAL2
```

You can reset the syslog facility to the default (LOG_LOCAL7) using the **no logging syslog-facility local** command.

System console

The system console displays all 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 message 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 **logging raslog console** command. All messages are still sent to the system message log, syslog (if enabled), and SNMP management station.

You can use the **logging raslog console** [**stop** [*minutes*] | **start**] command to disable and re-enable the RASLog messages from displaying on the system console.

Setting the RASLog console severity level

You can limit the types of messages that are logged to the console using the **logging raslog console** command. The RASLog messages displayed on the console are passed up to and above the configured severity level. For example, if you configure the console severity level to ERROR, then only ERROR and CRITICAL messages pass through. You can choose one of the following severity levels: INFO, WARNING, ERROR, or CRITICAL.The default severity level is INFO.

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

1. Execute the **configure terminal** command to access the global configuration level of the CLI.

   ```
   device# configure terminal
   Entering configuration mode terminal
   ```

2. Execute the **logging rbridge-id** *rbridge-id* **raslog console** *severity level* command to set the RASLog console severity level.

   The *severity level* can be one of the following: INFO, WARNING, ERROR, or CRITICAL. The severity level values are case-sensitive. For example, to set the console severity level to ERROR on switch 1, enter the following command.

   ```
   device(config)# logging rbridge-id 1 raslog console ERROR
   ```

You can reset the console severity level to the default (INFO) using the **no logging rbridge-id** *rbridge-id* **raslog console** command.

SNMP management station

When an unusual event, error, or a status change occurs on the device, an event notification is sent to the SNMP management station. Network OS v7.1.0 supports two types of event notifications: traps (in SNMPv1, SNMPv2c, and SNMPv3) and informs (in SNMPv3).

SNMP traps

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 possible severity levels are as follows:

- Critical
- Debug
- Error
- Info
- None
- Warning

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 Info, all traps with the severity level of Info, Warning, Error, and Critical are received.

NOTE

The Audit log 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, SNMPv2c, and SNMPv3 hosts to receive the traps. For more information, refer to "Configuring the SNMP (version 1 or version 2c) server host" on page 9.

SNMP informs

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 PDU. If the sender does not receive the SNMP response, the SNMP 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 SNMP 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. For more information, refer to "Configuring the SNMPv3 server" on page 9.

Port logs

The Network OS maintains an internal log of all port activity. Each switch maintains a log file for each port. Port logs are circular buffers that can save up to 8,000 entries per 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 across power cycles and reboots.

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

Configuring the SNMP server hosts

Network OS v7.1.0 supports SNMP version 1, version 2c, and version 3. Use the commands listed in Table 4 to configure the SNMPv1, SNMPv2c, and SNMPv3 hosts and their configurations.

TABLE 4 Commands for configuring SNMP server hosts

Command	Description
[**no**] **snmp-server host** {*ipv4 host* | *ipv6-host* | *dns*} *community-string* [**severity-level** [**None** | **Debug** | **Info** | **Warning** | **Error** | **Critical**] [**udp-port** *port_number*] [**version** [**1** | **2c**]	This command sets the destination IP addresses, version, community string (for version 1 and version 2c), and destination port for the traps. The **severity-level** option is used to filter the traps based on severity. The **no** form of the command changes the SNMP server host configurations to the default value.
[**no**] **snmp-server v3host** {*ipv4-host* | *ipv6-host* | **dns**} *username* [**notifytype** {**traps** | **informs**}] **engineid** *engine-id* **severity-level** [**None** | **Debug** | **Info** | **Warning** | **Error** | **Critical**] **udp-port** *port_number*	This command specifies the recipient of the SNMP version 3 notification option. The **severity-level** option is used to filter the traps or informs based on severity. Use the **no** form of the command to remove the specified host.

Configuring the SNMP (version 1 or version 2c) server host

To set the trap destination IP addresses, version (1 or 2c), community string for SNMP version 1 and version 2c, and the destination port for the SNMP traps, perform the following steps.

1. Execute the **configure terminal** command to access the global configuration level of the CLI.

```
device# configure terminal
Entering configuration mode terminal
```

2. Execute the following command to set the trap recipient with IP address 192.0.2.2, which receives all traps with the severity levels of Critical, Error, Info, and Warning.

```
device(config)# snmp-server host 192.0.2.2 public severity-level Info udp-port
162 version 1
```

NOTE

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

3. Execute the **do show running-config snmp-server** command to verify the configuration.

```
device(config)# do show running-config snmp-server
snmp-server contact "Field Support."
snmp-server location "End User Premise."
snmp-server sys-descr "Brocade VDX Switch."
snmp-server community ConvergedNetwork
snmp-server community OrigEquipMfr rw
snmp-server community "Secret C0de" rw
snmp-server community common
snmp-server community private rw
snmp-server community public
snmp-server host 192.0.2.2 public
 udp-port 162
 severity-level Info
```

Configuring the SNMPv3 server

Use the **snmp-server v3-host** command to specify the recipient of SNMP version 3 notifications: traps or informs. The following example explains the procedure to configure the recipient of the SNMPv3 informs.

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

1. Execute the **configure terminal** command to access the global configuration level of the CLI.

```
device# configure terminal
Entering configuration mode terminal
```

2. Execute the following command to set the inform recipient with IP address 192.0.2.2, which receives all traps with the severity levels of Critical, Error, Info, and Warning.

```
device(config)# snmp-server v3host 192.0.2.2 snmpadmin1 notifytype informs
engineid 80:00:05:23:01:AC:1A:01:79 severity-level Info udp-port 4425
```

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 **show running-config snmp-server** command to verify the configuration.

```
device# show running-config snmp-server
snmp-server contact "Field Support."
snmp-server location "End User Premise."
snmp-server sys-descr "Brocade VDX Switch."
snmp-server community ConvergedNetwork
snmp-server community OrigEquipMfr rw
snmp-server community "Secret C0de" rw
snmp-server community common
snmp-server community private rw
snmp-server community public
snmp-server user snmpadmin1 auth md5 auth-password
"5MmR2qGjoryjusN9GL5kUw==\n" priv DES priv-password
"2ThfbBNgPsCyI25tLI2yxA==\n" encrypted
snmp-server user snmpadmin2 groupname snmpadmin
snmp-server user snmpadmin3 groupname snmpadmin
snmp-server user snmpuser2
snmp-server user snmpuser3
snmp-server v3host 192.0.2.2 snmpadmin1
 udp-port 4425
 notifytype informs
 engineid 80:00:05:23:01:AC:1A:01:79
 severity-level Info
!
```

Commands for displaying, clearing, and configuring the message logs

Table 5 describes commands that you can use to view or configure various message logs. Most commands require the admin access level. For detailed information on required access levels and commands, refer to the *Network OS Command Reference*.

TABLE 5 Commands for viewing or configuring the message logs

Command	Description
clear logging auditlog	This command clears the Audit log messages from the local switch or the specified switches.
clear logging raslog	This command clears the error log messages from the local switch or the specified switches.

TABLE 5 Commands for viewing or configuring the message logs (Continued)

Command	Description
logging auditlog class	This command sets the event classes for Audit log messages.
logging raslog console	This command sets a filter based on the severity level for the messages to be displayed on the system console.
logging syslog-facility local	This command sets the syslog facility.
logging syslog-server	This command configures a syslog server to which the switch can forward the messages.
show logging auditlog	This command displays the Audit log messages on the local switch or the specified switches. **NOTE:** This command can be disruptive because it displays all the logs in the buffer continuously. Use **| more** to see output page by page.
show logging raslog	This command displays the error log message on the local switch, the specified switch, or interface module. The command includes options to filter the messages based on the message attribute and the severity level, and also to set the count of messages to display, and to display messages in reverse order. **NOTE:** This command can be disruptive because it displays all the logs in the buffer continuously. Use **| more** to see output page by page.
show running-config logging	This command is used to display the logging settings on the local switch.
show running-config logging auditlog class	This command displays the event class configured for the Audit log.
show running-config logging raslog	This command displays the RASLog console severity level on the local switch or the specified switch.
show running-config logging syslog-facility	This command displays the syslog facility level.

Displaying message content on the 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** *message_ID* command.

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

1. Log in to the switch as admin.
2. Use the **rasman message id** *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 EM-1059.

```
device# rasman message id EM-1059

Miscellaneous                                          EM-1059(7m)

MESSAGE
     EM-1059 - <Slot number or Switch> with ID <Blade Id> may not
     be supported on this platform, check 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) ver-
     sion 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.
```

Configuring system messages

This section provides information on configuring the system message logs.

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 **logging raslog message** *message_ID* **suppress** command to disable a RASLog message. For example, execute the following command to disable the NS-1001 message:

     ```
     switch:admin> logging raslog message NS-1001 suppress
     2012/07/20-13:28:37, [LOG-1007], 375, M1, INFO, switch, Log message
     NS-1001 RASLOG message has been disabled.
     ```

     Use the **show running-config logging raslog message** *message_ID* command to verify the status of the message.
   - Execute the **logging raslog 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 NSM module:

     ```
     switch:admin> logging raslog module NSM
     2012/07/20-13:28:37, [LOG-1007], 375,  CHASSIS, INFO, switch, Log Module
     NSM module RASLOG message has been suppress.
     ```

     Use the **show running-config logging raslog module** *module_ID* command to verify the status of the messages that belong to a module.

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 **no logging raslog message** *message_ID* **suppress** command to enable a single RASLog message that has been disabled. For example, execute the following command to enable the NS-1001 message that was previously disabled:

     ```
     switch:admin> no logging  raslog message NS-1001 suppress
     2012/07/20-13:24:43, [LOG-1008], 374, M1, INFO, switch, Log Module NS-1001
     RASLOG message has been enabled.
     ```

     Use the **show running-config logging raslog message** *message_ID* command to verify the status of the message.
   - Execute the **no logging raslog module** *module_ID* command to enable all messages in a module. For example, execute the following command to enable to all previously disabled the NSM messages:

     ```
     switch:admin> no logging  raslog module NSM
     2012/07/20-13:24:43, [LOG-1008], 374, M1, INFO, switch, Log Module NSM has
     been enabled.
     ```

     Use the **show running-config logging raslog 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 **logging raslog message** *message_ID* **severity** [**CRITICAL** | **ERROR** | **WARNING** | **INFO**] command to change the severity level of a message. For example, execute the following command to change the severity level of the SEC-1203 message to WARNING.

   ```
   switch:admin> logging raslog message SEC-1203 severity WARNING
   ```

3. Use the **show running-config logging raslog message** *message_ID* **severity** command to verify the severity of the message.

   ```
   switch:admin> show running-config logging raslog message SEC-1203 severity
   WARNING
   ```

Viewing and clearing the RASLog messages

You can display system message log using the **show logging raslog** command. This command provides options to filter the messages by attribute, message type, severity, or message count. You can also specify to display messages for a single module by using the **blade** option. Use the **clear logging raslog** command to delete the system messages.

Displaying the RASLog messages

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

1. Log in to the switch as admin.
2. Enter the **show logging raslog** command at the command line.

```
device# show logging raslog
NOS: v7.1.0
2012/06/04-22:57:00, [HASM-1108], 94,, INFO, VDX6720-24, All service instances
become active.

2012/06/04-22:57:03, [DCM-1002], 96,, INFO, VDX6720-24, PostBoot processing on
global config has started.

2012/06/04-22:57:05, [BL-1000], 100,, INFO, VDX6720-24, Initializing ports...

2012/06/13-05:10:22, [NSM-1004], 4428, DCE, INFO, sw0,  Interface Vlan 1 is
created.

2012/06/13-05:10:24, [DOT1-1013], 4435, DCE, INFO, sw0, DOT1X test timeout
value is set to 10.

2012/06/13-05:10:24, [ONMD-1002], 4437, DCE, INFO, sw0, LLDP global
configuration is changed.

2012/06/13-05:10:28, [RAS-2001], 4438,, INFO, sw0, Audit message log is
enabled.
[...]
```

Displaying the messages on an interface module

To display the saved messages for a specific interface module, line card (LC), or management module, perform the following steps.

1. Log in to the switch as admin.
2. Enter the **show logging raslog blade** command at the command line. You can filter messages based on the severity level using the **severity** option. The following example filters messages by the severity level of info.

```
device# show logging raslog blade LC2 severity info
NOS: v7.1.0
2012/05/29-11:43:06, [HASM-1004], 6919, L2, INFO, VDX8770-4, Processor
rebooted - Reset.

2012/05/29-11:43:06, [HASM-1104], 6920, L2, INFO, VDX8770-4, Heartbeat to M2
up.

2012/05/29-11:43:10, [HASM-1004], 6921, L2, INFO, VDX8770-4, Processor
rebooted - Reset.
2012/05/29-11:43:10, [HASM-1104], 6922, L2, INFO, VDX8770-4, Heartbeat to M2
up.
[...]
```

Clearing the RASLog messages

To clear the RASLog messages for a particular switch instance, perform the following steps.

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

Viewing and clearing the SYSTEM messages

This section provides information on viewing and clearing the SYSTEM messages saved on the switch memory.

Displaying the SYSTEM messages

To display the messages saved in the SYSTEM storage repository, perform the following steps.

1. Log in to the switch as admin.
2. Enter the **show logging raslog message-type SYSTEM** command at the command line.

```
device# show logging raslog message-type SYSTEM
NOS: v7.1.0

2011/09/14-04:52:05, [LOG-1003], 1,, INFO, VDX6720-60, SYSTEM error log has
been cleared.

2011/09/14-04:56:18, [DCM-1101], 2,, INFO, VDX6720-60, Copy running-config to
startup-config operation successful on this node.

2011/09/14-05:05:21, [RAS-1007], 5,, INFO, VDX6720-60, System is about to
reboot.
[...]
```

Clearing the SYSTEM messages

To clear the messages saved in the SYSTEM storage repository, perform the following steps.

1. Log in to the switch as admin.
2. Execute the **clear logging raslog message-type SYSTEM** command to clear all system messages from the local switch.

Viewing and clearing the DCE messages

This section provides information on viewing and clearing the DCE messages saved on the switch memory.

Displaying the DCE messages

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

1. Log in to the switch as admin.
2. Enter the **show logging raslog message-type DCE** command at the command line.

```
device# show logging raslog message-type DCE
```

```
NOS: v7.1.0
2012/05/30-21:25:34, [NSM-1004], 41, M1 | DCE, INFO, switch,  Interface Vlan
4093 is created.

2012/05/30-21:25:34, [NSM-1019], 42, M1 | DCE, INFO, switch,  Interface Vlan
4093 is administratively up.

2012/05/30-21:25:52, [DOT1-1013], 50, M1 | DCE, INFO, switch, DOT1X test
timeout has set to 10.

2012/05/30-21:25:52, [ONMD-1002], 59, M1 | DCE, INFO, switch, LLDP global
configuration is changed.

2012/05/30-21:25:53, [SSMD-1602], 63, M1 | DCE, INFO, switch, Class map
default is created.

2012/05/30-21:25:55, [NSM-1004], 58, M1 | DCE, INFO, switch,  Interface Vlan
1002 is created.

2012/05/30-21:25:55, [ONMD-1002], 59, M1 | DCE, INFO, switch, LLDP global
configuration is changed.

2012/05/30-21:25:59, [SSMD-1602], 63, M1 | DCE, INFO, switch, Class map
default is created

[...]
```

Clearing the DCE messages

To clear the DCE messages for a particular switch instance, perform the following steps.

1. Log in to the switch as admin.
2. Execute the **clear logging raslog message-type DCE** command to clear all DCE messages from the local switch.

Displaying the VCS messages

This section provides information on viewing the VCS messages saved on the switch memory.

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

1. Log in to the switch as admin.
2. Enter the **show logging raslog attribute VCS** command at the command line.

```
device# show logging raslog attribute VCS
NOS: v7.1.0
2012/06/05-03:00:18:101601, [VCS-1009], 8002/3929, VCS, INFO, VDX6720-60,
Event: VCS node disconnect, Coordinator IP: 192.0.2.15, VCS Id: 1, Status:
Rbridge-id 3 (192.0.2.2) disconnected from VCS cluster.

2012/06/05-03:04:11:621996, [VCS-1005], 8051/3935, VCS, INFO, VDX6720-60,
Event: VCS node rejoin, Coordinator IP: 192.0.2.15, VCS Id: 1, Status:
Rbridge-id 3 (192.0.2.2) rejoined VCS cluster.
[...]
```

Displaying the FFDC messages

This section provides information on viewing the FFDC messages saved on the switch memory.

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

1. Log in to the switch as admin.
2. Enter the **show logging raslog attribute FFDC** command at the command line.

```
device# show logging raslog attribute FFDC
NOS: v7.1.0
2012/06/15-10:39:02, [LOG-1002], 4496, FFDC, WARNING, VDX6720-24, A log
message was not recorded.

2012/06/15-10:39:18, [RAS-1001], 4496, FFDC, WARNING, VDX6720-24, First
failure data capture (FFDC) event occurred.
[...]
```

Displaying the description of the RASLog modules

To display the description of the RASLog modules, perform the following steps.

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

```
device# rasman description
RASModule ID   Description
-----------------------------------------------------
  KT      1    Kernel Test ID
  UT      2    User Test ID
  TRCE    3    Trace Subsystem (User)
  KTRC    4    Trace Subsystem (Kernel)
  LOG     5    RASLOG module
  CDR     6    Condor ASIC driver
[...]
```

Displaying RASLog messages in a module

To display the list of all RASLog messages in a module along with their message text, perform the following steps.

1. Log in to the switch as admin.
2. Enter the **rasman module name** *module_name* command at the command line. For example, execute the following command to display all messages in the AUTH module.

```
device# rasman module name AUTH
RAS Message ID  Severity  Message
-------------------------------------------------------------------
AUTH-1001       INFO      %s has been successfully completed.
AUTH-1002       ERROR     %s has failed.
AUTH-1003       INFO      %s type has been successfully set to %s.
AUTH-1004       ERROR     Failed to set %s type to %s.
AUTH-1005       ERROR     Authentication file does not exist: %d.
AUTH-1006       WARNING   Failed to open authentication configuration file.
AUTH-1007       ERROR     The proposed authentication protocol(s) are not
                          supported: port %d.
AUTH-1008       ERROR     No security license, operation failed.
```

```
[...]
```

Displaying RASLog messages by type

To display the list of RASLog messages based on the message type, perform the following steps.

1. Log in to the switch as admin.
2. Enter the **rasman type value** *message_type* command at the command line. For example, execute the following command to display all Audit messages.

```
device# rasman type value AUDIT
RAS Message ID   Severity  Message
-----------------------------------------------------------------
FCIP-1002        INFO       An IPsec/IKE policy was added
FCIP-1003        INFO       An IPsec/IKE policy was deleted
AUTH-1045        ERROR     Certificate not present in this switch in %s port
                           %d.
AUTH-1046        INFO      %s has been successfully completed.
AUTH-1047        ERROR     %s has failed.
AUTH-3001        INFO      Event: %s, Status: success, Info: %s type has been
                           changed from [%s] to [%s].
AUTH-3002        INFO      Event: %s, Status: success, Info: %s.
AUTH-3003        INFO      Event: %s, Status: success, Info: %s the PKI
                           objects.
[...]
```

Viewing, clearing, and configuring Audit log messages

This section provides information on viewing, clearing, and configuring the Audit log messages.

Displaying the Audit messages

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

1. Log in to the switch as admin.
2. Enter the **show logging auditlog** command at the command line.

   You can also display messages in reverse order using the **reverse** option.

```
device# show logging auditlog

0 AUDIT,2011/08/26-07:51:29 (GMT), [RAS-2001], INFO, SYSTEM,
NONE/root/NONE/None/CLI,, switch, Audit message log is enabled.

1 AUDIT,2011/08/26-07:51:29 (GMT), [RAS-2003], INFO, SYSTEM,
NONE/root/NONE/None/CLI,, switch, Audit message class configuration has been
changed to 2,6,4,.

2 AUDIT,2011/08/26-07:51:32 (GMT), [DCM-2001], INFO, DCMCFG,
root/none/127.0.0.1/rpc/cli,, VDX6720-24, Event: noscli start, Status:
success, Info: Successful login attempt through console from 127.0.0.1.

3 AUDIT,2011/08/26-07:51:34 (GMT), [DCM-2001], INFO, DCMCFG,
admin/admin/127.0.0.1/rpc/cli,, VDX6720-24, Event: noscli start, Status:
success, Info: Successful login attempt through console from 127.0.0.1.
```

```
4 AUDIT,2011/08/26-07:51:36 (GMT), [DCM-2002], INFO, DCMCFG,
admin/admin/127.0.0.1/rpc/cli,, VDX6720-24, Event: noscli exit, Status:
success, Info: Successful logout by user [admin].
[...]
```

Clearing the Audit messages

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

1. Log in to the switch as admin.
2. Execute the **clear logging auditlog** command to clear all messages on the switch memory.

Configuring event auditing

The Audit log classes SECURITY, CONFIGURATION, and FIRMWARE are enabled by default. You can enable or disable auditing of these classes using the **logging auditlog class** *class* command.

To configure and verify the event auditing, perform the following steps.

1. Execute the **configure terminal** command to access the global configuration level of the CLI.

   ```
   device# configure terminal
   Entering configuration mode terminal
   ```

2. Configure the event classes you want to audit. For example, to audit the CONFIGURATON class, execute the following command.

   You can choose one of the following event classes: CONFIGURATION, FIRMWARE, or SECURITY.

   ```
   device(config)# logging auditlog class CONFIGURATION
   ```

3. Execute the **show running-config logging auditlog class** command to verify the configuration.

   ```
   device# show running-config logging auditlog class
   logging auditlog class CONFIGURATION
   ```

Understanding the RASLog messages

This section provides information about reading the RASLog messages.

RASLog messages

The following example shows the format of a RASLog message.

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

The following example shows the sample messages from the error log.

```
2011/08/23-22:58:10, [IPAD-1000], 2,, INFO, VDX6720-24, SW/0 Ether/0 IPv4 DHCP
10.24.95.252/20 DHCP On.
```

```
2012/05/30-21:26:00, [FCOE-1035], 67, M1 | DCE, INFO, sw0, Virtual FCoE port 1/1/4
is online.
```

```
2011/08/26-12:39:02, [HAM-1007], 2, FFDC, CRITICAL, VDX6720-24, Need to reboot the
system for recovery, reason: raslog-test-string0123456-raslog.
```

```
2011/08/26-12:40:01, [VCS-1003], 7013/3454, VCS, INFO, VDX6720-60, Event: VCS
node add, Coordinator IP: 10.17.10.31, VCS ID: 1, Status: rBridge ID 1
(10.17.10.32) added to VCS cluster., VcsFabAddRejoin, line: 1450, comp:dcmd,
ltime:2011/06/27-02:47:04:555942.

2011/08/27-03:39:52, [HASM-1004], 127, L, INFO, chassis, Processor reloaded -
Reset.
```

The fields in the error message are described in Table 6.

TABLE 6 RAS message field description

Variable name	Description
Timestamp	The system time (UTC) when the message was generated on the switch. The RASLog subsystem supports an internationalized time stamp format base on the "LOCAL" setting.
Event ID	The Event ID is the message module and number. These values uniquely identify each message in the Network 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.
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 **firmware download** and increases up to a value of 2,147,483,647 (0x7fffffff). The sequence number continues to increase after the message log wraps around; that is, the oldest message in the log is deleted when a new message is added. The message sequence numbering is not split for the system and DCE message logs. The sequence number can be reset to 1 using the **clear logging raslog** command. However, the sequence number is not reset if you clear a particular message type, for example, DCE. 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 a DCE, FFDC, or VCS message. Messages may contain the following values: • DCE–Indicates a message generated by the protocol-based modules. • FFDC–Indicates that additional first failure data capture information has also been generated for this event. • VCS–Indicates a VCS message generated by a switch in the Brocade VCS fabric.
Severity	The severity level of the message, which can be one of the following: • CRITICAL • ERROR • WARNING • INFO
Switch name	The defined switch name or the chassis name of the switch. This value is truncated if it exceeds 16 characters in length.
Event-specific information	A text string explaining the error encountered and provides the parameters supplied by the software at runtime.

Audit event messages

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

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>/<app name>, <Reserved field for future
expansion>, <Switch name>, <Event-specific information>
```

The following is a sample Audit event message.

```
0 AUDIT,2011/08/26-07:51:32 (GMT), [DCM-2001], INFO, DCMCFG,
root/none/127.0.0.1/rpc/cli,, VDX6720-24, Event: noscli start, Status: success,
Info: Successful login attempt through console from 127.0.0.1.
```

The fields in the Audit event message are described in Table 7.

TABLE 7 Audit message field description

Variable name	Description
Sequence Number	The error message position in the log.
AUDIT	Identifies the message as an Audit message.
Timestamp	The system time (UTC) when the message was generated on the switch. The RASLog subsystem supports an internationalized time stamp format base on the “LOCAL” setting.
Event ID	The Event ID is the message module and number. These values uniquely identify each message in the Network 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 level of the message, which can be one of the following: • CRITICAL • ERROR • WARNING • INFO
Event Class	The event class, which can be one of the following: • DCMCFG • FIRMWARE • SECURITY
User ID	The user ID.
Role	The role of the user.
IP Address	The IP address.
Interface	The interface being used.
Application Name	The application name being used on the interface.
Reserved field for future expansion	This field is reserved for future use and contains a space character (null value).
Switch name	The defined switch name or the chassis name of the switch. This value is truncated if it is over 16 characters in length.
Event-specific information	A text string explaining the error encountered and provides the parameters supplied by the software at runtime.

Responding to a RASLog message

This section provides procedures on gathering information on RASLog messages.

Looking up a 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 8 on page 24) 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

The following are the common steps and questions to ask yourself when troubleshooting a system message:

- What is the current Network OS version?
- 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 **show logging raslog** command on each switch.
- Execute the **copy support** command.
- Document the sequence of events by answering the following questions:
  - What happened just before 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 Power-On Self-Test (POST) enabled?
- Are serial port (console) logs available?
- What and when were the last actions or changes made to the system?

Support

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

Panic dump, core dump, and FFDC data files

The Network OS creates panic dump files, core files, and FFDC data files when there are problems in the Network OS kernel. You can view files using the **show support** command. These files can build up in the persistent storage and may need to be periodically deleted or downloaded using the **copy support** command.

The software watchdog (SWD) process 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.

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 **show support** command to view these files or the **copy support ftp** command to send them to a host workstation using FTP. The panic dump files, core files, and FFDC data files are intended for support personnel use only.

Trace dumps

The Network OS produces trace dumps when problems are encountered within Network OS modules. The Network OS trace dump files are intended for support personnel use only. You can use the **copy support** command to collect trace dump files to a specified remote location to provide support when requested.

Using the copy support command

The **copy support** command is used to send the output of the RASLog messages, the trace files, and the output of the **copy support** command to an off-switch storage location through FTP. You can upload supportsave data from the local switch to an external host or you can save the data on an attached USB device. The **copy support** command runs a large number of dump and show commands to provide a global output of the status of the switch. Refer to the *Network OS Command Reference* for more information on the **copy support** command.

System module descriptions

Table 8 provides a summary of the system modules for which messages are documented in this reference guide; a module is a subsystem in the Network OS. Each module generates a set of numbered messages.

TABLE 8 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.
AL	AL module messages allow the user to identify which application has been started or stopped.
AQPH	AQPH messages indicate problems observed in the physical layer (PHY) transceivers chips.
ARP	The ARP module notifies events regarding both IPv4 (ARP) and IPv6 (ND) neighbor cache in the system.
AUTH	AUTH messages indicate problems with the authentication module of the Network OS.
BFD	BFD messages indicate whether the BFD session is Up or Down for the specified neighbors on the interface.
BGP	BGP messages indicate problems with the Border Gateway Protocol (BGP) module of the Network OS.
BL	BL messages are a result of faulty hardware, transient out-of-memory conditions, ASIC errors, or inconsistencies in the software state between an interface module and the environment monitor (EM) module.
BLL	Bloom is the name of the ASIC used as the building block for third-generation hardware platforms.
C2	C2 error messages indicate problems with the 8 Gbps-capable FC module of the Network OS.
C3	C3 error messages indicate problems with the 16 Gbps-capable FC module of the Network OS.
CBR	CBR error messages indicate problems with the ASIC driver of Network OS.
CHS	CHS messages report the problems in the management of the interface modules in the different slots of the chassis.
DAD	DAD messages report errors encountered during the DHCP Auto Deployment (DAD) process.
DCM	Distributed Configuration Manager (DCM) messages indicate major switch bootup events, user login or logout, and the configuration operations.
DHCP	The Dynamic Host Configuration Protocol (DHCP) messages indicate the status and operations performed in the DHCP server. The operation includes start, stop and restart of the DHCP server.
DOT1	DOT1 messages indicate problems with the 802.1x authentication module of the Network OS.
EANV	EANV messages indicate any issues associated with eAnvil ASIC operation and eAnvil ASIC driver operations.
ELD	End Loop Detection (ELD) messages notify a loop in the Layer 2 network and the status of the port on which the loop is detected.

TABLE 8 System module descriptions (Continued)

System module	Description
EM	The environmental monitor (EM) manages and monitors the various field-replaceable units (FRUs), including the port cards, 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 way of CLI commands, system light emitting diodes (LEDs), and status and alarm messages. EM also manages some component-related data.
ERCP	ERCP messages indicate any problems associated with Double Data Rate (DDR) errors.
ESS	Exchange Switch Support (ESS) error messages indicate problems with the ESS module of the Network OS. ESS is an SW_ILS mechanism utilized by switches to exchange vendor and support information.
FABR	FABR (network of Fibre Channel switches) 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	FABS messages indicate problems in the fabric system driver module.
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 Fibre Channel over Ethernet (FCoE) module of the Network OS.
FCPH	The Fibre Channel Physical Layer is used to send Fibre Channel traffic to and from the switch.
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. FSPF messages are about protocol errors.
FSS	The fabric state synchronization framework provides facilities by which the active management module can synchronize with the standby management module, enabling the standby management module 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 Network OS, implementing a related set of functionality. A service is a collection of components grouped together to achieve a modular software architecture.
FVCS	The Fabric Services VCS (FVCS) daemon provides fabric distribution services for VCS and Virtual Link Aggregation Group (vLAG).
FW	FW messages indicate the warnings when the temperature, voltage, fan speed, and switch status thresholds are exceeded for the switch subsystems.
HASM	HASM is the infrastructure for the High Availability System Management, which has the functionality to maintain the cluster of high availability switch platforms, deploy and start multiple service instances with active and standby redundancy in a distributed clustering environment, manage the state synchronizations, and the non-disruptive failovers between active and standby management modules, host the non-disruptive firmware upgrade context, and support the software watchdog and daemon restart.
HAWK	HAWK is a component that connects the fabric ASIC.

TABLE 8 System module descriptions (Continued)

System module	Description
HIL	HIL messages indicate any issues associated with the Hardware Independent Layer (HIL) for general platform components, such as Environmental Monitoring (EM), fan and power supply unit (PSU) subsystems, and other platform FRUs.
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.
HSL	HSL messages indicate problems with the Hardware Subsystem Layer (HSL) of the Network OS.
HWK2	HWK2 is a component that connects the fabric ASIC.
IGMP	IGMP messages indicate any issue associated with the Internet Group Management Protocol (IGMP) snooping feature.
IPAD	IPAD messages are generated by the IP admin demon.
KTRC	KTRC messages indicate any problem associated with the RAS-TRACE facility, which provide Brocade internal information to diagnose a failure.
L2AG	L2AG messages indicate problems with the Layer 2 system agent module. L2SS and L2AG together control the Layer 2 forwarding engine and are responsible for MAC learning, aging, and forwarding functionalities.
L2SS	L2SS messages indicate problems with the Layer 2 system manager module. L2SS and L2AG together control the Layer 2 forwarding engine and are responsible for MAC learning, aging, and forwarding functionalities.
LACP	LACP error messages indicate problems with the Link Aggregation Control Protocol module of the Network OS.
LIC	LIC messages indicate problems with the licensing module.
LOG	LOG messages describe events and problems associated with the RASLog and Audit log facilities.
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.
MCST	MCST messages indicate any problems associated with the Layer 2 and Layer 3.
MAPS	The MAPS module identifies and reports anomalies associated with the various error counters, thresholds, and resources monitored on the switch.
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.
MS	The Management Service (MS) enables the user to obtain information about the Fibre Channel fabric topology and attributes by providing a single management access point.
MSTP	MSTP messages indicate problems with Multiple Spanning Tree Protocol (MSTP) modules of the Network OS.
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.
NS	NS messages indicate problems with the simple Name Server module.

TABLE 8 System module descriptions (Continued)

System module	Description
NSM	NSM messages indicate problems with the interface management and VLAN management module of the Network OS.
OFMA	The openflow agent module is responsible to map openflow logical view to physical hardware. Any mapping error or unsupported constructs are logged by these messages.
OFMM	Openflow manager messages indicated any error in the flow, group, meter mod processing by the openflow subsystem. These include protocol error and VDX pipeline limitations along with internal error condition. Openflow protocol exchanges and connections are also logged through this module.
ONMD	ONMD messages indicate problems with the Operation, Administration and Maintenance module of the Network OS.
OSPF	OSPF messages indicate information or problems with the OSPF module of the Network OS.
OSPF6	OSPF6 messages indicate information or problems with the OSPF version 3 module of the Network OS.
PCAP	PCAP messages indicate the status or information about the packet capture module.
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 management module to the standby management module.
PEM	PEM messages indicate error or warning situation associated with event handling or action script execution.
PHP	PHP messages indicate any important information associated with the discovery and creation, deletion, and updating of the port profiles.
PIM	PIM messages indicate problems with the Protocol-Independent Multicast (PIM) module.
PLAT	PLAT messages indicate hardware problems.
PORT	PORT 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.
QOSD	QOSD messages indicate problems with the Quality of Service (QoS) module.
RAS	RAS messages notify when first failure data capture (FFDC) events are logged to the FFDC log, and size or roll-over warnings.
RCS	The reliable commit service (RCS) daemon generates log entries when it receives a request from the zoning or security server for passing data messages to switches. 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 or Security modules.
RTM	Route Manager (RTM) messages indicate status or errors while updating or maintaining the route and next-hop database.
RTWR	The reliable transport write (RTWR) and read daemon helps deliver data messages either to specific switches in the fabric or to all 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 Network OS.
SEC	SEC messages indicate security errors, warnings, or information during security-related data management or fabric merge operations. Administrators must watch for these messages to distinguish between internal switch and fabric operation errors and external attack.

TABLE 8 System module descriptions (Continued)

System module	Description
SFLO	sFlow is a standards-based sampling technology embedded within switches and routers, which is used to monitor high speed network traffic. 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 sflow daemon.
SLCD	SLCD messages provide wear level statistics of the western digital (WD) SiliconDrive 2 compact flash.
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 four management entities that can be configured to receive these traps or informs. SNMP messages indicate problems in the SNMP operations.
SRM	System Resource Monitor daemon monitors memory and CPU usage of all processes. The SRM message is generated when the available Low memory is below 100 MB.
SS	SS messages indicate problems during the execution of the **copy support** command.
SSMD	SSMD messages indicate problems with the System Services Module (SSM) of the Network OS.
SULB	The software upgrade library provides the **firmware download** command capability, which enables firmware upgrades as well as nondisruptive code load to the switches. SULB messages may display if there are any problems during the **firmware download** procedure.
SWCH	SWCH messages are generated by the switch driver module that manages a Fibre Channel switch instance.
TNLD	TNLD messages indicate status or problems with the Data Center Ethernet (DCE) tunnel manager of the Network OS.
TOAM	TRILL OAM (TOAM) messages indicate problems with the **l2traceroute** family of commands that help in VCS cluster data path troubleshooting.
TRCE	TRCE messages describe events and problems associated with the tracedump facility.
TS	Time Service (TS) provides switch time-synchronization by synchronizing all clocks in the network. The TS messages indicate information or errors during the switch time synchronization.
UCST	UCST is a part of the fabric shortest path first (FSPF) protocol that manages the unicast routing table.
UDLD	UDLD messages indicate problems with the UniDirectional Link Detection (UDLD) module of the Network OS.
UPTH	UPATH is a part of the FSPF protocol that uses the SPF algorithm to dynamically compute a unicast tree.
VC	VC messages indicate any important information related to the vCenter CLI and its plugins.
VCS	VCS messages indicate major events related to VCS cluster formation and node operations.
VRRP	VRRP messages indicate information or problems with the VRRP module of the Network OS.
WEBD	WEBD messages Indicate problems with the Web Tools module.

TABLE 8 System module descriptions (Continued)

System module	Description
WLV	Wolverine (WLV) ASIC is a component that connects the front-end port. WLV messages indicate failures in the front-end port.
ZONE	ZONE messages indicate any problems associated with the zoning features, including commands associated with aliases, zones, and configurations.

1 System module descriptions

Chapter 2

Audit Messages

AUTH Messages

DCM Messages

HASM Messages

LOG Messages

RAS Messages

SEC Messages

SULB Messages

TS Messages

Chapter 3

CFFDC Messages

EM Messages

Chapter 4

DCE Messages

ARP Messages

DOT1 Messages

ELD Messages

FCOE Messages

IGMP Messages

L2AG Messages

L2SS Messages

LACP Messages

LOG Messages

MCST Messages

MSTP Messages

NSM Messages

OFMA Messages

OFMM Messages

ONMD Messages

OSPF Messages

OSPF6 Messages

QOSD Messages

RPS Messages

RTM Messages

SFLO Messages

SSMD Messages

TOAM Messages

VRRP Messages

VRRP-2001

Chapter 5

FFDC Messages

AQPH Messages

AUTH Messages

BL Messages

BLL Messages

CBR Messages

CBR2 Messages

CHS Messages

EANV Messages

EM Messages

ERCP Messages

FABR Messages

FABS Messages

FCMC Messages

FCPH Messages

FLOD Messages

FSS Messages

HASM Messages

HAWK Messages

HIL Messages

HLO Messages

HWK2 Messages

IPAD Messages

LOG Messages

LSDB Messages

MPTH Messages

NBFS Messages

PDM Messages

PLAT Messages

RAS Messages

SCN Messages

SNMP Messages

SRM Messages

SS Messages

SWCH Messages

TRCE Messages

WEBD Messages

WLV Messages

Chapter

6

Log Messages

AG Messages

AL Messages

AQPH Messages

AUTH Messages

BFD Messages

BGP Messages

BL Messages

BLL Messages

C2 Messages

C3 Messages

CBR Messages

CBR2 Messages

CHS Messages

DAD Messages

DCM Messages

DHCP Messages

EANV Messages

EM Messages

ERCP Messages

ESS Messages

FABR Messages

FABS Messages

FCMC Messages

FCPH Messages

FLOD Messages

FSPF Messages

FSS Messages

FVCS Messages

FW Messages

HASM Messages

HAWK Messages

HIL Messages

HLO Messages

HSL Messages

HWK2 Messages

IPAD Messages

KTRC Messages

LIC Messages

LOG Messages

LSDB Messages

MAPS Messages

MM Messages

MPTH Messages

MS Messages

NBFS Messages

NS Messages

PCAP Messages

PDM Messages

PEM Messages

PHP Messages

PIM Messages

PLAT Messages

PORT Messages

QOSD Messages

RAS Messages

RCS Messages

RTWR Messages

SCN Messages

SEC Messages

SLCD Messages

SNMP Messages

SRM Messages

SS Messages

SULB Messages

SWCH Messages

TNLD Messages

TRCE Messages

TS Messages

UCST Messages

UDLD Messages

UPTH Messages

VC Messages

VCS Messages

WEBD Messages

WLV Messages

ZONE Messages

Chapter

7

VCS Messages

HASM Messages

SS Messages

SSMD Messages

SULB Messages

VCS Messages

Chapter 8

Network OS Messages

AG Messages

AG-1001

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

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
- 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.
- 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-1004

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

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 **copy support** command and contact your switch service provider.

AG-1006

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

Message Type LOG

Severity INFO

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

Recommended Action Execute the **show ag rbridge-id** {*rbridge-id* | **all**} command to verify the current status of the Access Gateway mode.

AG-1007

Message `FLOGI response not received for the N_Port <port> 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>.`

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 **copy support** command and contact your switch service provider.

AG-1009

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

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 **copy support** command and contact your switch service provider.

AG-1010

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

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 **copy support** command and contact your switch service provider.

AG-1011

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

Message Type LOG

Severity WARNING

Probable Cause Indicates that there was a failure sending a discover VF_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 **copy support** command and contact your switch service provider.

AG-1012

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

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 **copy support** command and contact your switch service provider.

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.

If the message persists, execute the **copy support** command and contact your switch service provider.

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 Run the **show fabric islports** command to display the status of all ports in the system and run **show running-config interface FibreChannel** to display a list of ports currently configured as N_Ports.

AG-1018

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

Message Type LOG

Severity ERROR

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

Recommended Action Run the **show fabric islports** command to display the status of all ports in the system and run **show running-config interface FibreChannel** to display a list of ports currently configured as N_Ports. Ensure the host is connected to a VF_Port.

AG-1020

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

Message Type LOG

Severity INFO

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

Recommended Action Execute the **show ag map***nport***rbridge-id** {*rbridge-id* | **all**} command to display the updated VF_Port-to-N_Port mapping.

AG-1026

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

Message Type LOG

Severity WARNING

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

Recommended Action Increase the number of allowed logins on the specified port.

If the message persists, execute the **copy support** command and contact your switch service provider.

AG-1029

Message `Disabling port <port> connected to fabric <port_wwn_str>. Ports to fabric <retain_wwn_str> remain online.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a misconfiguration.

Recommended Action Connect all ports in the switch to the same FC fabric.

AG-1030

Message `N-Port (ID: <port>) 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>.`

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>) 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-1034

Message `VF_Port cannot accept any more logins (<fport>).`

Message Type LOG

Severity INFO

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

Recommended Action No action is required.

AG-1038

Message `FCoE AG Ports going to different fabrics, Check N Port (<domain>/<blade>/<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-1040

Message `No N_Port(s) are currently Online in PG <PG that has no N ports 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 Check the status of the N_Ports in the port group.

AG-1041

Message `PG <pgid> has been <action>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the specified port group has been created or deleted.

Recommended Action No action is required.

AG-1042

Message `VF_Port to N_Port mapping has been updated for N_Port <buf>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the VF_Ports mapped to an N_Port have changed.

Recommended Action No action is required.

AG-1043

Message `VF_Port (<Rbridge-id>/<Slot>/<Port>) was forced logged out <Repeat count>(th) time due to reason: <Reason string>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the specified VF_Port is being forcefully logged out.

Recommended Action No action is required.

AL Messages

AL-1003

Message `Application <app name> is launched.`

Message Type LOG

Severity INFO

Probable Cause Indicates that an application is launched.

Recommended Action No action is required.

AL-1004

Message `Application <app name> is restarted.`

Message Type LOG

Severity INFO

Probable Cause Indicates that an application is restarted.

Recommended Action No action is required.

AL-1005

Message `Application <app name> is unexpected terminated.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that an application has terminated unexpectedly.

Recommended Action No action is required.

AL-1006

Message `Application <app name> is stopped.`

Message Type LOG

Severity INFO

Probable Cause Indicates that an application has been stopped by the user.

Recommended Action No action is required.

AQPH Messages

AQPH-1001

Message `Port <port number> reached warn temperature <temperature>.`

Message Type LOG | FFDC

Severity ERROR

Probable Cause Indicates that a particular chip temperature is slowly increasing.

Recommended Action No action is required.

AQPH-1002

Message `Port <port number> reached fail temperature <temperature>.`

Message Type LOG | FFDC

Severity ERROR

Probable Cause Indicates an internal switch hardware error. All the ports on the interface module or switch will be disrupted.

Recommended Action For a modular switch, execute the **slotpoweroff** command to power off the interface module.

For a compact switch, shut down the switch.

ARP Messages

ARP-1034

Message `System <messsage> Limits exceeded. System MAX Profile Limit <profile limit>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that system limits have exceeded.

Recommended Action Execute clear on all VRFs.

ARP-1035

Message `Clearing <messsage> on vrf <vrf name>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that clear is executed on the specified VRF.

Recommended Action No action is required.

ARP-1036

Message `Hardware <messsage> is <percentage> full. Hardware MAX is <hardware max>. Current count is <current count>.`

Message Type DCE

Severity WARNING

Probable Cause Indicates that hardware host table is almost full.

Recommended Action Execute clear on all VRFs.

ARP-1037

Message `Hardware <messsage> Limits exceeded. System MAX Profile Limit <profile limit>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that hardware limits have exceeded.

Recommended Action Execute clear on all VRFs.

ARP-1038

Message `Duplicate IP <IP Address> detected. New MAC-Address <New MAC-Address>, Old MAC-Address <Old MAC-Address>.`

Message Type DCE

Severity WARNING

Probable Cause Indicates that there is a duplicate IP configuration in the network.

Recommended Action No action is required.

AUTH Messages

AUTH-1001

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

Message Type LOG

Severity INFO

Probable Cause Indicates that the secret database has been updated using the **fcsp auth-secret** or **no fcsp auth-secret** 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 to update the secret database using the **fcsp auth-secret** or **no fcsp auth-secret** command has failed. The values for Operation type can be "set" or "remove".

Recommended Action Execute the **fcsp auth-secret** or **no fcsp auth-secret** command again.

Execute the **copy support** 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 parameter was set to a specified value. The data type can be either authentication type, DH group 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 **fcsp auth** command has failed to set the authentication configuration value. The data type can be either authentication type, DH group type, hash type, or policy type.

Recommended Action Execute the **fcsp auth** command.

Execute the **copy support** 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 security policy.

Recommended Action Reinitialize authentication using the **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands.

If the message persists, execute the **copy support** 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 local port.

Recommended Action Execute the **fcsp auth** command to make sure the local switch supports the following protocols: Fibre Channel Authentication Protocol (FCAP) or Diffie-Hellman Challenge Handshake Authentication Protocol (DH-CHAP).

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 security policy.

Recommended Action Reload or power cycle the switch.

If the message persists, execute the **copy support** 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 Make sure the entity at the other end of the link supports authentication.

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 **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands.

If the message persists, execute the **copy support** 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 security policy.

Recommended Action Reinitialize authentication using the **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands.

If the message persists, execute the **copy support** 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 security policy.

Recommended Action Reinitialize authentication using the **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands.

If the message persists, execute the **copy support** 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 security policy.

Recommended Action Reinitialize authentication using the **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands.

If the message persists, execute the **copy support** 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 **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands.

If the message persists, execute the **copy support** 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 that 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 **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands.

If the message persists, execute the **copy support** 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 **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands.

If the message persists, execute the **copy support** 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. The authentication may fail.

Recommended Action Reinitialize authentication using the **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands.

If the message persists, execute the **copy support** 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 (for example, DH group, hash value, or protocol type) from a receiving payload during the specified authentication phase. This error occurred because 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 **fcsp auth** command.

Reinitialize authentication using the **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands.

If the message persists, execute the **copy support** 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 a 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 **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands.

If the message persists, execute the **copy support** 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 certain phase. Usually this problem is transient. The authentication may fail.

The data type is a payload or structure that failed to get memory.

Recommended Action Reinitialize authentication using the **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands.

If the message persists, execute the **copy support** 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 during the specified authentication phase. Usually this problem is transient. The authentication may fail.

Recommended Action Reinitialize authentication using the **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands.

If the message persists, execute the **copy support** 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 **fcsp auth-secret** command.

Reinitialize authentication using the **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands.

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 (for example, challenge, nonce, or response data) for an authentication payload. This usually relates to an 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 **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands.

If the message persists, execute the **copy support** 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, which was not configured in the switch connection control (SCC) policy tried to connect to the port.

Recommended Action Add the entity World Wide Name (WWN) to the SCC policy using the **secpolicy defined-policy** command, then reinitialize authentication using the **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** 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 entity name in the payload is not in the correct format.

Recommended Action Reinitialize authentication using the **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands.

If the message persists, execute the **copy support** 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 an internal failure.

Usually this problem is transient. The authentication may fail.

Recommended Action Reinitialize authentication using the **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis disable** commands.

If the message persists, execute the **copy support** 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 **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis disable** commands.

If the message persists, execute the **copy support** 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.

Recommended Action Check the connection port for a possible security attack.

Reinitialize authentication using the **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis disable** commands.

If the message persists, execute the **copy support** 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 **fcsp auth** command, and then enable the port using the **no shutdown** 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 **fcsp auth** command, and then enable the port on neighboring switch using the **no shutdown** 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 **show fcsp auth-secret dh-chap** command and reinitialize authentication using the **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis disable** commands.

If the message persists, execute the **copy support** 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 **show fcsp auth-secret dh-chap** command and reinitialize authentication using the **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis disable** commands.

If the message persists, execute the **copy support** command and contact your switch service provider.

AUTH-1044

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

Message Type LOG | FFDC

Severity ERROR

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

Recommended Action Check the SFP and the cable. Then try to enable the port using the **no shutdown** command.

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 a authentication configuration parameter was set to a specified value. The data type can be either 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 has been updated using the **fcsp auth-secret** command.

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 **fcsp auth** command, and then enable the port using **no shutdown** 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 **fcsp auth** command, and then enable the port on the neighboring switch using **no shutdown** 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 **show fcsp auth-secret dh-chap** command and reinitialize authentication using the **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands.

If the message persists, execute the **copy support** command and contact your switch service provider.

AUTH-3007

Message `Event: <Event Name>, Status: failed, Info: Port <port number> disabled, because an authentication-reject was received 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 **show fcsp auth-secret dh-chap** and reinitialize authentication using the **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands.

If the message persists, execute the **copy support** 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 **show fcsp auth-secret dh-chap** and reinitialize authentication using the **shutdown** and **no shutdown** commands or the **chassis disable** and **chassis enable** commands.

If the message persists, execute the **copy support** command and contact your switch service provider.

BFD Messages

BFD-1001

Message `BFD Session UP for neighbor <NeighborIp> on Interface <InterfaceName>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Bidirectional Forwarding Detection (BFD) session for the specified neighbor is now up.

Recommended Action No action is required.

BFD-1002

Message `BFD Session DOWN for neighbor <NeighborIp> on Interface <InterfaceName> reason <DownReason>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Bidirectional Forwarding Detection (BFD) session for the specified neighbor is now down.

Recommended Action No action is required.

BGP Messages

BGP-1001

Message `<error message>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a configuration error.

Recommended Action Make sure to input or pass the right parameter through the CLI or other daemon.

BGP-1002

Message `<message>.`

Message Type LOG

Severity INFO

Probable Cause Indicates a Border Gateway Protocol (BGP) interface state change or external link-state database (LSDB) overflow notification.

Recommended Action No action is required.

BGP-1003

Message `<error message>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the length, format, or content of the received packet is incorrect.

Recommended Action Check the configuration at the local or remote node.

BGP-1004

Message `<message>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates a Border Gateway Protocol (BGP) interface state change or external link-state database (LSDB) overflow warning.

Recommended Action No action is required.

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 string> 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 interface module initiation failed because one or more of the internal ports were not online. The interface module is faulted.

Recommended Action Make sure that the interface module is seated correctly. If the interface module is seated correctly, reload or power cycle the interface module using the **power-off** and **power-on** commands.

Execute the **diag systemverification** command to verify that the interface module does not have hardware problems.

Execute the **diag post** command to make sure that Power-On Self-Test (POST) is enabled.

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

If the message persists, replace the interface module.

BL-1003

Message `Faulty interface module in <slot string>.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates a faulty interface module in the specified slot.

Recommended Action Make sure that the interface module is seated correctly. If the interface module is seated correctly, reload or power cycle the interface module using the **power-off** and **power-on** commands.

Execute the **diag systemverification** command to verify that the interface module does not have hardware problems.

Execute the **diag post** command to make sure that Power-On Self-Test (POST) is enabled.

If the message persists, replace the interface module.

BL-1004

Message `Suppressing interface module fault in <slot string>.`

Message Type FFDC | LOG

Severity CRITICAL

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

Recommended Action Reload or power cycle the interface module using the **power-off** and **power-on** commands.

Execute the **diag systemverification** command to verify that the interface module does not have hardware problems.

Execute the **diag post** command to make sure that Power-On Self-Test (POST) is enabled.

If the message persists, replace the interface module.

BL-1006

Message `Interface module <slot number> NOT faulted. Peer interface module <slot number> experienced abrupt failure.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the errors (mostly synchronization errors) on this interface module are harmless. Probably, the standby management module connected to the active management module has experienced transitory problems.

Recommended Action Execute the **show ha** command to verify that the standby management module is healthy. If the problem persists, remove and reinstall the faulty interface module.

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

BL-1007

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

Message Type LOG

Severity WARNING

Probable Cause Indicates that a failover occurred while an interface module was initializing on the previously active management module.

Recommended Action No action is required. The interface module is re-initialized. Because re-initializing an interface module is a disruptive operation and can stop I/O traffic, you must stop and restart the traffic during this process.

BL-1008

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

Message Type FFDC | LOG

Severity CRITICAL

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

Recommended Action Make sure that the interface module is seated correctly. If the interface module is seated correctly, reload or power cycle the interface module using the **power-off** and **power-on** commands.

Execute the **diag systemverification** command to verify that the interface module does not have hardware problems.

Execute the **diag post** command to make sure that Power-On Self-Test (POST) is enabled.

If the message persists, replace the interface module.

BL-1009

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

Message Type FFDC | LOG

Severity CRITICAL

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

Recommended Action

Make sure that the interface module is seated correctly. If the interface module is seated correctly, reload or power cycle the interface module using the **power-off** and **power-on** commands.

Execute the **diag systemverification** command to verify that the interface module does not have hardware problems.

Execute the **diag post** command to make sure that Power-On Self-Test (POST) is enabled.

If the message persists, replace the interface module.

BL-1010

Message

```
Interface module in <slot string> is 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 management module.

Recommended Action

No action is required. This interface module has been re-initialized. Because re-initializing an interface module is a disruptive operation and can stop I/O traffic, you must stop and restart the traffic during this process.

BL-1011

Message

```
Busy with emb-port int for chip <chip number> in minis <mini-switch number> on
interface module <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 management module 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.

Execute the **diag systemverification** command to verify that the interface module or switch does not have hardware problems.

Execute the **diag post** command to make sure that Power-On Self-Test (POST) is enabled.

For a modular switch, execute the **power-off** and **power-on** commands to power cycle the interface module.

For a compact switch, reload or power cycle the switch.

If the message persists, replace the interface module or the switch.

BL-1012

Message `bport <interface module port number> port int is disabled. Status=0x<interrupt status>; Port <port number> will be re-enabled in a 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 management module from becoming too busy. The interface module port number displayed in the message 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.

For a modular switch, execute the **power-off** and **power-on** commands to power cycle the interface module.

For a compact switch, reload or power cycle the switch.

If the message persists, replace the interface module or the switch.

BL-1013

Message `bport <interface module port number> port is faulted. Status=0x<interrupt status>; Port <port number> will be re-enabled in a 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 management module from becoming too busy. The interface module port number displayed in the message may not correspond to the 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.

For a modular switch, execute the **power-off** and **power-on** commands to power cycle the interface module.

For a compact switch, reload or power cycle the switch.

If the message persists, replace the interface module or the switch.

BL-1014

Message `bport <interface module 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 management module from becoming too busy. The interface module port number displayed in the message may not correspond to the user port number.

Recommended Action Make sure to capture the console output during this process.

For a modular switch, execute the **power-off** and **power-on** commands to power cycle the interface module.

For a compact switch, execute the **reload** command to reload the switch.

Execute the **diag systemverification** command to determine if there is a hardware error.

Execute the **diag post** command to make sure that Power-On Self-Test (POST) is enabled.

If there is a hardware error, the **power-off** or **power-on** command fails on the modular switch, or the errors are encountered again, replace the interface module or the switch.

BL-1015

Message `bport <interface module 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 management module from becoming too busy. The interface module port number displayed in the message may not correspond to the user port number.

Recommended Action Make sure to capture the console output during this process.

For a modular switch, execute the **power-off** and **power-on** commands to power cycle the interface module.

For a compact switch, execute the **reload** command to reload the switch.

Execute the **diag systemverification** command to determine if there is a hardware error.

Execute the **diag post** command to ensure that Power-On Self-Test (POST) is enabled.

If there is a hardware error, the **power-off** or **power-on** command fails on the modular switch, or the errors are encountered again, replace the interface module or the switch.

BL-1016

Message `Interface module port <port number> in <slot string> failed to enable.`

Message Type FFDC | LOG

Severity CRITICAL

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

Recommended Action Make sure that the interface module is seated correctly. If the interface module is seated correctly, reload or power cycle the interface module using the **power-off** and **power-on** commands.

Execute the **diag systemverification** command to verify that the interface module does not have hardware problems.

Execute the **diag post** command to make sure that Power-On Self-Test (POST) is enabled.

If the message persists, replace the interface module.

BL-1017

Message `<slot string> Initializing.`

Message Type LOG

Severity INFO

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

Recommended Action No action is required.

BL-1018

Message `<slot string> Initialization completed.`

Message Type LOG

Severity INFO

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

Recommended Action No action is required.

BL-1019

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

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified 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

Reload power cycle the switch.

Execute the **diag systemverification** command to verify that the switch does not have hardware problems.

Execute the **diag post** command to make sure that Power-On Self-Test (POST) is enabled.

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 were not online. The switch is faulted.

Recommended Action Reload or power cycle the switch.

Execute the **diag systemverification** command to verify that the switch does not have hardware problems.

Execute the **diag post** command to make sure that Power-On Self-Test (POST) is enabled.

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 `Interface module in <slot string> was reset before initialization completed. As a result the interface module is faulted.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that the interface module was reset before the initialization completed.

Recommended Action Reload or power cycle the interface module using the **power-off** and **power-on** commands. If the message persists, replace the interface module.

BL-1024

Message `All ports on the interface module in <slot string> will be reset as part of the firmware upgrade.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a recent firmware upgrade caused the interface module firmware to be upgraded and resulted in a cold upgrade. As part of the upgrade, all data path elements 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 a cold recovery.

Recommended Action Execute the **copy support** command and reload the switch.

Execute the **diag post** command to make sure Power-On Self-Test (POST) is enabled.

If the problem persists, replace the switch.

BL-1027

Message `Interface module in <slot string> 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 interface module failed to boot properly.

Recommended Action Reload or power cycle the interface module using the **power-off** and **power-on** commands. If the message persists, replace the interface module.

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 Reload or power cycle the switch. 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 data path elements were reset.

Recommended Action No action is required.

BL-1031

Message `Link timeout in internal port (slot <slot number>, port <port number>) caused interface module fault. Use power-off/power-on commands to recover it.`

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 interface module using the **power-off** and **power-on** commands.

BL-1032

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

Message Type LOG

Severity CRITICAL

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

Recommended Action Reload or power cycle the interface module using the **power-off** and **power-on** commands.

Execute the **diag systemverification** command to verify that the interface module does not have hardware problems.

Execute the **diag post** command to make sure that Power-On Self-Test (POST) is enabled.

If the message persists, replace the interface module.

BL-1033

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

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that the system has timed out waiting for the disable acknowledgment messages from the user ports.

Recommended Action Reload or power cycle the interface module using the **power-off** and **power-on** commands.

Execute the **diag systemverification** command to verify that the interface module does not have hardware problems.

Execute the **diag post** command to make sure that Power-On Self-Test (POST) is enabled.

If the message persists, replace the interface module.

BL-1034

Message `<slot string> CEE initialization completed.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified slot has completed initializing the Converged Enhanced Ethernet (CEE) ports.

Recommended Action No action is required.

BL-1037

Message `Faulting chip in <slot string>, miniS = <mini-switch 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 Execute the **diag systemverification** command to determine if there is a hardware error.

Execute the **diag post** command to make sure that Power-On Self-Test (POST) is enabled.

BL-1038

Message `Inconsistent FPGA image version detected, reload 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 Reload the switch. If the message persists, replace the switch.

BL-1039

Message `Inconsistent FPGA image version detected, faulting the interface module in <slot string>.`

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 interface module using the **power-off** and **power-on** commands. If the message persists, replace the interface module.

BL-1045

Message `mini SFP+ (SN: <mini SFP+ serial number>) is only supported in certain high port count interface modules, not interface module in slot <slot number of interface module that has the mini SFP+> with ID <Interface module ID of interface module that has the mini SFP+ that does not support it>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the mini (form factor) enhanced small form-factor pluggable (SFP+) transceiver is supported only by a certain type of interface module, but it can be inserted in other interface modules.

Recommended Action Replace the mini SFP+ transceiver with an SFP or SFP+ transceiver.

BL-1046

Message `<Slot number of interface module 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>). Reseat or replace the SFP.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that 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 the 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-1049

Message `Incompatibility with an active 12x40G LC detected, faulting the interface module in <slot string>.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that this line card (LC) is incompatible with one or more existing 12x40G LCs.

Recommended Action Power cycle all active 12X40G LCs and then power cycle the interface module using the **power-off** and **power-on** commands. Then power on all 12X40G LCs. After completing these steps, all LCs can interoperate with one another.

BL-1050

Message `Media is not supported on this platform( slot <slot number>, port <port number>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the media on the specified port is bad or incompatible with this platform.

Recommended Action Replace a different media on the specified port.

BL-1051

Message `The media is not verified for this platform (slot<slot number>, port <port number>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the media on the specified port is not verified with this platform.

Recommended Action Brocade recommends to use a supported media on this platform. You can still use an unsupported media at your own risk.

BL-1052

Message `FEC is enabled for 100G Interface <Interface_Num>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the Forward Error Correction (FEC) enforcement status for 100G interfaces.

Recommended Action No action is required.

BL-1053

Message `FEC is disabled for 100G Interface <Interface_Num>. Media <Is_SR4>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the Forward Error Correction (FEC) enforcement status for 100G interfaces along with a check for SR4 media.

Recommended Action No action is required.

BLL Messages

BLL-1000

Message `ASIC driver detected <slot string> port <port number> as faulty (reason: <reason code>).`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that an interface module regulation problem was reported on the specified slot. The interface module is faulted.

The reason codes are as follows:

- 1 = Available buffer overflow
- 2 = Backend port buffer timeout
- 3 = Backend port got shut down
- 4 = Embedded port buffer timeout
- 5 = Excessive busy mini buffer
- 6 = Excessive RCC VC on E_Port
- 7 = Excessive RCC VC on FL_Port
- 8 = Fail detection buffer tag error
- 9 = Fail detection TX parity error
- 10 = EPI CMEM interrupt error
- 11 = Checkpoint Middleware Interface (CMI) interrupt error
- 12 = Interrupt overrun
- 13 = FDET interrupt
- 14 = Interrupt suspended
- 15 = Filter LISTD error
- 16 = Unknown filter LIST error
- 17 = Wait for LPC open state
- 18 = Wait for Old port state
- 19 = Wait for Open init state
- 20 = TX parity error
- 21 = RAM parity error
- 22 = Built in Self Repair (BISR) or RAMINIT error

Recommended Action Make sure the interface module is seated correctly. If the interface module is seated correctly, reload or power cycle the interface module using the **power-off** and **power-on** commands.

Execute the **diag systemverification** command to verify that the interface module does not have hardware problems.

If the message persists, replace the interface module.

C2 Messages

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 interface module.

C2-1006

Message `S<slot number>,C<chip index>: Internal link errors have been reported, no hardware faults identified, continuing to monitor for errors: fault1:<fault1_count>, fault2:<fault2_count>, 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> (<interface module port number>): At next port state change, best effort QoS will be turned off automatically as it is no longer supported under this configuration.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that quality of service (QoS) will be turned off automatically at next port state change because best effort 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> (<interface module port number>): QoS overwrites vc-link-init idle. ARB will be used on the link.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that quality of service (QoS) overwrites the fill word IDLE used in 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> (<interface module port number>): vc-link-init arb overwrites fill word IDLE. ARB will be used on the link.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the **vc-link-init arb** 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 of faults has identified suspect hardware, interface module may need to be reset or replaced: fault1:<fault1_count>, fault2:<fault2_count>, 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 Whenever the error is observed persistently, power cycle the specified interface module using the **power-off** and **power-on** commands. If the problem persists, replace the interface module.

C2-1011

Message `S<slot number>,P<port number> (<interface port number>): Primitive received with Encoding errors, do AL_RESET.`

Message Type LOG

Severity WARNING

Probable Cause Indicates encoding errors on the internal links. This error can cause cyclic redundancy check (CRC) errors or frame loss.

Recommended Action Whenever the error is observed persistently, power cycle the specified interface module using the **power-off** and **power-on** commands. If the problem persists, check the backplane or replace the interface module.

C2-1012

Message `S<slot number>,P<port number> (<interface module port number>): Link Timeout on internal port ftx=<frame transmitted> tov=<real timeout value> (><expected timeout value>), interface module may need to be reset or replaced.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that above normal errors were observed in hardware that may or may not impact the data traffic.

Recommended Action Whenever the error is observed persistently, power cycle the specified interface module using the **power-off** and **power-on** commands. If the problem persists, replace the interface module.

C3 Messages

C3-1004

Message `<slot string>,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 Reload the system at the next maintenance window. If the problem persists, replace the interface module.

C3-1006

Message `<slot string>,C<chip index>: Various non-critical hardware errors were observed: fault1:0x<fault1_count>, fault2:0x<fault2_count>, 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.

C3-1010

Message `<slot string>,C<chip index>: Above normal hardware errors were observed: fault1:<fault1_count>, fault2:<fault2_count>, 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 Whenever this error is observed persistently, power cycle the specified interface module using the **power-off** and **power-on** commands. If the problem persists, replace the interface module.

C3-1011

Message `Detected a complete loss of credit on internal back-end VC: Slot <slot string>, Port <port number>(<interface module port number>) vc_no=<vc number> crd(s)lost=<credit(s)lost>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that all credits have been lost on the specified virtual channel (VC) and port.

Recommended Action No action is required. The link will be reset to recover the credits.

C3-1012

Message `<slot string>,P<port number>(<interface module 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 above normal errors were observed in hardware that may or may not impact the data traffic.

Recommended Action Whenever this error is observed persistently, power cycle the specified interface module using the **power-off** and **power-on** commands. If the problem persists, replace the interface module.

C3-1014

Message `Link Reset on internal Port <slot string>,P<port number>(<interface module 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 Whenever this error is observed persistently, power cycle the specified interface module using the **power-off** and **power-on** commands. If the problem persists, replace the interface module.

C3-1017

Message `Interface module in Slot-<slot string> failed due to unavailability of ports in the internal trunk.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified interface module failed due to unavailability of ports in the internal trunk.

Recommended Action Whenever this error is observed persistently, power cycle the specified interface module using the **power-off** and **power-on** commands. If the problem persists, replace the interface module.

C3-1019

Message `<slot string>,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 an internal error in the application-specific integrated circuit (ASIC) hardware that may degrade the data traffic.

Recommended Action Reload the system at the next maintenance window.

C3-1020

Message `<slot string>,P<port number>(<interface module port number>): Some non-critical CRC with good EOF errors were observed: 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 that some non-critical errors were detected in the hardware.

Recommended Action No action is required.

CBR Messages

CBR-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.

CBR-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 interface module or switch will be disrupted.

Recommended Action For a modular switch, execute the **power-off** and **power-on** commands to power cycle the interface module.

For a compact switch, reload or power cycle the switch.

CBR-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, check the connections and replace the SFPs and cables as needed.

CBR-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, check the connections and replace the SFPs and cables as needed.

CBR-1040

Message `The <feature name> table utilization is above 90 percentage threshold.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the number of entries in the feature has increased.

Recommended Action Monitor the number of entries in the feature and make sure it is below threshold value.

CBR-1041

Message `The <feature name> table utilization has gone below 90 percentage threshold.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of entries in the feature is below threshold value.

Recommended Action Monitor the number of entries in the feature.

CBR-1042

Message `Number of packets per second processed on BPQ <BPQ number> exceeded threshold.`

Message Type LOG

Severity INFO

Probable Cause Indicates that number of packets per second dispatched from this BPQ exceeded threshold.

Recommended Action Recheck configuration

CBR2 Messages

CBR2-1001

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.

CBR2-1002

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 interface module or switch will be disrupted.

Recommended Action For a modular switch, execute the **power-off** and **power-on** commands to power cycle the interface module.

For a compact switch, reload or power cycle the switch.

CBR2-1040

Message `The <feature name> table utilization is above 90 percentage threshold.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the number of entries in the feature has increased.

Recommended Action Monitor the number of entries in the feature and make sure it is below threshold value.

CBR2-1041

Message `The <feature name> table utilization has gone below 90 percentage threshold.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the number of entries in the feature is below threshold value.

Recommended Action Monitor the number of entries in the feature.

CBR2-1042

Message `Number of packets per second processed on BPQ <BPQ number> exceeded threshold.`

Message Type LOG

Severity INFO

Probable Cause Indicates that number of packets per second dispatched from this BPQ exceeded threshold.

Recommended Action Recheck configuration

CHS Messages

CHS-1002

Message `ki_gd_register_action failed with rc = <return value>.`

Message Type LOG | FFDC

Severity ERROR

Probable Cause Indicates an internal error.

Recommended Action Reload or power cycle 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 modular switch, execute the **power-off** and **power-on** commands to power cycle the interface module.

For a compact switch, reload or power cycle the switch.

CHS-1004

Message `Interface module attach failed during recovery, disabling slot = <slot number>, rval = <return value>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified interface module has failed during failover or recovery.

Recommended Action For a modular switch, execute the **power-off** and **power-on** commands to power cycle the interface module.

For a compact switch, reload 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 interface module attach operation has failed during failover or recovery.

Recommended Action For a modular switch, execute the **power-off** and **power-on** commands to power cycle the interface module.

For a compact switch, reload or power cycle the switch.

DAD Messages

DAD-1300

Message `DHCP Auto-Deployment firmware download start.`

Message Type LOG

Severity INFO

Probable Cause Indicates that DHCP automatic firmware download has started.

Recommended Action No action is required.

DAD-1301

Message `DHCP Auto-Deployment failed due to dual-MM HA sync timeout.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the DHCP Auto Deployment (DAD) process has failed because HA synchronization of the dual-management module has timed out.

Recommended Action No action is required.

DAD-1302

Message `DHCP Auto-Deployment failed during DHCP process.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the DHCP Auto Deployment (DAD) process failed because the dhclient is not getting the FTP server IP or the firmware path information.

Recommended Action No action is required.

DAD-1303

Message `Last firmware download session is in progress.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the previous firmware download session is still in progress.

Recommended Action No action is required.

DAD-1304

Message `Last firmware download session failed.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the last firmware download session has failed.

Recommended Action No action is required.

DAD-1305

Message `DHCP Auto-Deployment cluster formation timeout.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that not all nodes have completed DHCP Auto Deployment (DAD) before the current DAD session limit.

Recommended Action No action is required.

DAD-1306

Message `DHCP Auto-Deployment sanity check failed.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the DHCP Auto Deployment (DAD) sanity check has failed.

Recommended Action No action is required.

DAD-1307

Message `DHCP Auto-Deployment principle node ready.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the principle node is ready for the secondary node to join.

Recommended Action No action is required.

DAD-1308

Message `Current firmware skip firmware download.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the new firmware is already loaded on the switch and therefore there is no need to trigger firmware download.

Recommended Action No action is required.

DAD-1309

Message `DHCP Auto-Deployment session fail to start firmware download.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the DHCP Auto Deployment (DAD) session has failed to start firmware download.

Recommended Action No action is required.

DAD-1310

Message `DHCP Auto-Deployment firmware download completed successfully.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the DHCP Auto Deployment (DAD) process has completed successfully.

Recommended Action No action is required.

DAD-1311

Message `DHCP Auto-Deployment firmware download failed.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the DHCP Auto Deployment (DAD) process has failed.

Recommended Action No action is required.

DAD-1312

Message `DHCP Auto-Deployment node succeeded.`

Message Type LOG

Severity INFO

Probable Cause Indicates that DHCP Auto Deployment (DAD) succeeded on the node.

Recommended Action No action is required.

DAD-1313

Message `DHCP Auto-Deployment cluster partially succeeded.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that some of the nodes are not in the cluster before the DHCP Auto Deployment (DAD) session time limit.

Recommended Action No action is required.

DAD-1314

Message `DHCP Auto-Deployment cluster succeeded.`

Message Type LOG

Severity INFO

Probable Cause Indicates that DHCP Auto Deployment (DAD) succeeded on all nodes.

Recommended Action No action is required.

DAD-1315

Message `DHCP Auto-Deployment firmware mismatch.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the secondary node has a different firmware from the principle node.

Recommended Action No action is required.

DAD-1316

Message `DHCP Auto-Deployment running global configuration script.`

Message Type LOG

Severity INFO

Probable Cause Indicates that DHCP Auto Deployment (DAD) is running global configuration script.

Recommended Action No action is required.

DAD-1317

Message `DHCP Auto-Deployment complete global configuration script.`

Message Type LOG

Severity INFO

Probable Cause Indicates that DHCP Auto Deployment (DAD) has completed running global configuration script.

Recommended Action No action is required.

DAD-1318

Message `DHCP Auto-Deployment running local configuration script.`

Message Type LOG

Severity INFO

Probable Cause Indicates that DHCP Auto Deployment (DAD) is running local configuration script.

Recommended Action No action is required.

DAD-1319

Message `DHCP Auto-Deployment complete local configuration script.`

Message Type LOG

Severity INFO

Probable Cause Indicates that DHCP Auto Deployment (DAD) has completed running local configuration script.

Recommended Action No action is required.

DAD-1320

Message `DHCP Auto-Deployment running local command.`

Message Type LOG

Severity INFO

Probable Cause Indicates that DHCP Auto Deployment (DAD) is running local command.

Recommended Action No action is required.

DAD-1321

Message `DHCP Auto-Deployment complete local command.`

Message Type LOG

Severity INFO

Probable Cause Indicates that DHCP Auto Deployment (DAD) has completed running local command.

Recommended Action No action is required.

DAD-1322

Message `DHCP Auto-Deployment unexpected switch reboot.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that an unexpected switch reboot has occurred in the middle of the DHCP Auto Deployment (DAD) session.

Recommended Action No action is required.

DAD-1323

Message `DHCP Auto-Deployment parameter error.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that a parameter (*/etc/fabos/dad/dadparams*) error has occurred.

Recommended Action No action is required.

DAD-1324

Message `DHCP Auto-Deployment wait for principle node timeout.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the secondary node has not found the DHCP Auto Deployment (DAD) principle node in the cluster.

Recommended Action No action is required.

DAD-1325

Message `DHCP Auto-Deployment principle node in cluster is not in principle role.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the secondary node has found the DHCP Auto Deployment (DAD) principle node in the cluster, but the principle node is not in principle role.

Recommended Action No action is required.

DAD-1326

Message `DHCP Auto-Deployment timeout when wait for CLI ready.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the Network OS CLI has failed to start up.

Recommended Action No action is required.

DAD-1327

Message `DHCP Auto-Deployment timeout when running local command.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the local command was running for a long time.

Recommended Action No action is required.

DAD-1328

Message `DHCP Auto-Deployment secondary node timeout when joining cluster.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the secondary node was taking long time to join the cluster.

Recommended Action No action is required.

DAD-1329

Message `DHCP Auto-Deployment fail to copy running-config startup-config.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that DHCP Auto Deployment (DAD) has failed to copy the running configuration to the startup configuration.

Recommended Action No action is required.

DAD-1330

Message `DHCP Auto-Deployment secondary node fail to notify principle node.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the secondary node has failed to send update to the principle node.

Recommended Action No action is required.

DCM Messages

DCM-1001

Message `VCS ID is changed from <Previous Vcs Id> to <New Vcs Id>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the VCS ID has been changed.

Recommended Action No action is required.

DCM-1002

Message `PostBoot processing on <Configuration name> has started.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the PostBoot processing on the specified configuration group has started.

Recommended Action No action is required.

DCM-1003

Message `PostBoot processing on <Configuration name> is complete.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the PostBoot processing on the specified configuration group has been completed.

Recommended Action No action is required.

DCM-1004

Message `Configuration File Replay has started.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the configuration replay has started.

Recommended Action No action is required.

DCM-1005

Message `Configuration Replay is complete.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the configuration replay has been completed.

Recommended Action No action is required.

DCM-1006

Message `Event: <Event Name>, Status: <Command status>, User command: <ConfD hpath string>.`

Message Type AUDIT

Class DCMCFG

Severity INFO

Probable Cause Indicates that the user command has been executed successfully.

Recommended Action No action is required.

DCM-1007

Message `No Configuration File Replay.`

Message Type LOG

Severity INFO

Probable Cause Indicates that configuration file replay will not happen on this system boot up.

Recommended Action No action is required.

DCM-1008

Message `Configuration has been reset to default due to changes in configuration metadata.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the configuration schema has changed and therefore the old configuration cannot be retained.

Recommended Action Replay the saved configuration manually.

DCM-1009

Message `RBridge ID is set to <Rbridge-id>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the RBridge ID has changed to the specified value.

Recommended Action No action is required.

DCM-1010

Message `Operation of setting RBridge ID to <Rbridge-id> failed.`

Message Type LOG

Severity INFO

Probable Cause Indicates a failure while changing the RBridge ID.

Recommended Action No action is required.

DCM-1011

Message `VCS enabled: VCS ID is set to <New Vcs Id>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the VCS mode has been enabled.

Recommended Action No action is required.

DCM-1012

Message `VCS disabled: VCS ID is set to <New Vcs Id>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the VCS mode has been disabled.

Recommended Action No action is required.

DCM-1013

Message `Reset terminal timeout: <Timeout Reset Command>.`

Message Type AUDIT

Class DCMCFG

Severity INFO

Probable Cause Indicates that terminal timeout has been reset.

Recommended Action No action is required.

DCM-1014

Message `Error Node replace model mismatch, chassis disabled WWN: <switch_wwn>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the replacement switch model is different from the model of switch being replaced; this is not supported and therefore the chassis has been disabled.

Recommended Action Use the same switch model for replacement.

DCM-1015

Message `Switch is prepared for power-cycle. No CLIs will work henceforth. Reload or power cycle to make switch fully functional.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the database is shut down gracefully so that the node is power-cycle ready.

Recommended Action Reload or power cycle the switch to make it fully functional.

DCM-1101

Message `Copy running-config to startup-config operation successful on this node.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the running configuration has been copied to the startup configuration on the node.

Recommended Action No action is required.

DCM-1102

Message `Copy running-config to startup-config operation failed on this node.`

Message Type LOG

Severity INFO

Probable Cause Indicates failure to copy the running configuration to the startup configuration on the node.

Recommended Action No action is required.

DCM-1103

Message `Copy default-config to startup-config operation successful on this node.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the default configuration has been copied to the startup configuration on the node.

Recommended Action No action is required.

DCM-1104

Message `Copy default-config to startup-config operation failed on this node.`

Message Type LOG

Severity INFO

Probable Cause Indicates failure to copy the default configuration to the startup configuration on the node.

Recommended Action No action is required.

DCM-1105

Message `Copy of the downloaded config file to the current running-config has completed successfully on this node.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the downloaded configuration file has been copied to the current running configuration.

Recommended Action No action is required.

DCM-1106

Message `Copy of the downloaded config file to the current startup-config has completed successfully on this node.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the downloaded configuration file has been copied to the current startup configuration.

Recommended Action No action is required.

DCM-1107

Message `Startup configuration file has been uploaded successfully to the remote location.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the startup configuration file has been uploaded successfully.

Recommended Action No action is required.

DCM-1108

Message `Running configuration file has been uploaded successfully to the remote location.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the running configuration file has been uploaded successfully.

Recommended Action No action is required.

DCM-1109

Message `Error (<error string>) encountered while copying configuration to flash/USB.`

Message Type LOG

Severity INFO

Probable Cause Indicates a failure to copy configuration file to flash or USB storage device.

Recommended Action No action is required.

DCM-1110

Message `Last configuration replay complete.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a configuration was in progress during high availability (HA) failover and the configuration has been replayed.

Recommended Action No action is required.

DCM-1111

Message `Error (<error string>) last configuration replay failed.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that a configuration was in progress during high availability (HA) failover and the configuration replay has failed.

Recommended Action Reconfigure the failed command.

DCM-1112

Message `Running configuration file has been uploaded successfully to flash.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the running configuration file has been uploaded successfully.

Recommended Action No action is required.

DCM-1113

Message `Running configuration file has been uploaded successfully to USB.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the running configuration file has been uploaded successfully to a USB storage device.

Recommended Action No action is required.

DCM-1114

Message `Startup configuration file has been uploaded successfully to flash.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the startup configuration file has been uploaded successfully.

Recommended Action No action is required.

DCM-1115

Message `Startup configuration file has been uploaded successfully to USB.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the startup configuration file has been uploaded successfully.

Recommended Action No action is required.

DCM-1116

Message `System initialization is complete. NOS is ready to handle all commands.`

Message Type LOG

Severity INFO

Probable Cause Indicates that NOS is ready to handle all commands after system initialization completion.

Recommended Action No action is required.

DCM-1117

Message `File has been uploaded successfully to USB.`

Message Type LOG

Severity INFO

Probable Cause Indicates that file has been uploaded successfully to USB.

Recommended Action No action is required.

DCM-1118

Message `Copy of the downloaded config file to the current running-config has completed with errors on this node.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the downloaded configuration file encountered errors while being applied to the current running configuration.

Recommended Action Inspect the errors that were reported during the operation and fix or reconfigure failed commands.

DCM-1201

Message `FIPS Zeroize operation request received.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Federal Information Protection Standard (FIPS) Zeroize operation request has been received.

Recommended Action No action is required.

DCM-1202

Message `FIPS Zeroize operation: failed as VCS is enabled for this node.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the Federal Information Protection Standard (FIPS) Zeroize operation has failed because VCS is enabled on the node.

Recommended Action Execute the **no vcs enable** command to disable the VCS mode and then perform the Zeroize operation.

DCM-1203

Message `FIPS Zeroize operation: confirmed that VCS is not enabled for this node.`

Message Type LOG

Severity INFO

Probable Cause Indicates that VCS is not enabled on the node and therefore the Federal Information Protection Standard (FIPS) Zeroize operation will proceed.

Recommended Action No action is required.

DCM-1204

Message `FIPS Zeroize operation: all client sessions are notified that Zeroize in progress.`

Message Type LOG

Severity INFO

Probable Cause Indicates that all client sessions are notified about the Federal Information Protection Standard (FIPS) Zeroize operation in progress and the commands cannot be executed.

Recommended Action No action is required.

DCM-1205

Message `FIPS Zeroize operation: starting with cleanup for Zeroize.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the configuration files cleanup for Federal Information Protection Standard (FIPS) Zeroize has started.

Recommended Action No action is required.

DCM-1206

Message `FIPS Zeroize operation: starting prepare phase for Zeroize.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the prepare phase for Federal Information Protection Standard (FIPS) Zeroize has started, during which all the services will be shut down.

Recommended Action No action is required.

DCM-1207

Message `FIPS Zeroize operation: failed in prepare phase step for Zeroize.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Federal Information Protection Standard (FIPS) Zeroize operation has failed during the prepare phase.

Recommended Action No action is required.

DCM-1208

Message `FIPS Zeroize operation: Running Zeroize for secure deletion of the user configuration data.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Federal Information Protection Standard (FIPS) Zeroize operation is running for secure deletion of the user configuration data.

Recommended Action No action is required.

DCM-1209

Message `FIPS Zeroize operation: failed during secure deletion of the user configuration data.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the Federal Information Protection Standard (FIPS) Zeroize operation has failed during secure deletion of the user configuration data.

Recommended Action Refer to the reason code indicated in the **fips zeroize** command output for possible action.

DCM-1210

Message `FIPS Zeroize operation failed.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Federal Information Protection Standard (FIPS) Zeroize operation has failed.

Recommended Action No action is required.

DCM-1211

Message `FIPS Zeroize operation executed successfully.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Federal Information Protection Standard (FIPS) Zeroize operation has been executed successfully.

Recommended Action No action is required.

DCM-1212

Message `FIPS Zeroize operation failed. Node zeroizing or already zeroized.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Federal Information Protection Standard (FIPS) Zeroize operation has failed because the node is zeroizing or it was already zeroized.

Recommended Action No action is required.

DCM-1301

Message `Bare-Metal state is <Bare-Metal state>.`

Message Type LOG

Severity INFO

Probable Cause Indicates if the switch is in the bare-metal state.

Recommended Action No action is required.

DCM-1401

Message `Event-Handler: Exclusive run-mode action has been triggered and is active. Cluster formation operations will be paused.`

Message Type LOG

Severity INFO

Probable Cause Indicates that an activated event-handler that is configured with exclusive run-mode has been triggered. Cluster formation operations will be paused.

Recommended Action No action is required.

DCM-1402

Message `Event-Handler: Exclusive run-mode action has completed and is inactive. Cluster formation operations will be resumed.`

Message Type LOG

Severity INFO

Probable Cause Indicates that an activated event-handler that is configured with exclusive run-mode has completed. Cluster formation operations will be resumed.

Recommended Action No action is required.

DCM-1403

Message `Event-Handler: Action execution (Event-Handler: <Event-Handler Name>, Action Script: <Action Script Name>) timed out.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the action script associated with one of the VCS event-handlers timed out.

Recommended Action In case action script is going to take longer, reconfigure the event-handler activation action-timeout to a higher value.

DCM-1501

Message `Default config mode has been disabled on rbridgeId: <Rbridge Id>.`

Message Type LOG

Severity INFO

Probable Cause Indicates if default config mode has been disabled when a secondary node becomes principal.

Recommended Action No action is required.

DCM-1601

Message `Distributed logging has reached the maximum queue limit. The distributed log request will be ignored.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that distributed audit logging has reached the maximum queue limit due to a high volume of add log requests.

Recommended Action Lower the frequency of user sessions polling commands through all north-bound interfaces.

DCM-2001

Message `Event: <Event Name>, Status: success, Info: Successful login attempt through <connection method and IP Address>.`

Message Type AUDIT

Class DCMCFG

Severity INFO

Probable Cause Indicates that the log in was successful. An IP address is displayed when the login occurs over a remote connection.

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.

DCM-2002

Message `Event: <Event Name>, Status: success, Info: Successful logout by user [<User>].`

Message Type AUDIT

Class DCMCFG

Severity INFO

Probable Cause Indicates that the specified user has successfully logged out.

Recommended Action No action is required.

DCM-3005

Message `DCM ASSERT Service:<message>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates an internal failure in the distributed configuration manager (DCM).

Recommended Action Execute the **copy support** command and contact your switch service provider.

DCM-3010

Message `<Database Name> database integrity check timed out after <Timeout in minutes> minutes.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the database integrity check timeout has occured.

Recommended Action No action is required.

DCM-3051

Message `Encountered Database Corruption. System going down for auto-recovery.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the database operation failed because of database corruption. The system reloads for auto-recovery of the database.

Recommended Action No action is required.

DCM-3052

Message `Database Corruption was detected. Therefore, system was rebooted for recovery and may have taken longer than usual.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the last system reload was for auto-recovery of database because the database corruption was detected.

Recommended Action No action is required.

DCM-3053

Message `<Database name> database corruption was detected. The system will startup with the default configuration for this database.`

Message Type LOG

Severity INFO

Probable Cause Indicates that database corruption was detected. The system has auto-recovered with the default configuration applied.

Recommended Action No action is required.

DCM-4001

Message `Database schema conversion succeeded.`

Message Type LOG

Severity INFO

Probable Cause Indicates that after a firmware download, the database schema was successfully converted to the schema supported by the firmware.

Recommended Action No action is required.

DCM-4002

Message `Database schema conversion failed.`

Message Type LOG

Severity INFO

Probable Cause Indicates that after a firmware download, a failure was encountered in converting the database schema to the schema supported by the firmware.

Recommended Action No action is required.

DHCP Messages

DHCP-1001

Message `DHCP server started successfully.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Dynamic Host Configuration Protocol (DHCP) server has started successfully without errors.

Recommended Action No action is required.

DHCP-1002

Message `Unsupported platform to run DHCP server.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the command is supported only in Brocade VDX 6740T.

Recommended Action No action is required.

DHCP-1003

Message `Missing DHCP server configuration file.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the Dynamic Host Configuration Protocol (DHCP) server configuration file (/etc/dhcpd.conf) is missing in the setup.

Recommended Action Check the file system.

DHCP-1004

Message `Errors exist in DHCP server configuration file.`

Message Type LOG

Severity ERROR

Probable Cause The Dynamic Host Configuration Protocol (DHCP) server configuration file (/etc/dhcpd.conf) has potential errors which may fail to start the DHCP server.

Recommended Action Check the configuration file before invoking the server.

DHCP-1005

Message `DHCP server configuration is updated successfully.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Dynamic Host Configuration Protocol (DHCP) server configuration is updated successfully.

Recommended Action No action is required.

DHCP-1006

Message `DHCP IP address is configured on management interface.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the Dynamic Host Configuration Protocol (DHCP) client is enabled in the system which fails the server to invoke.

Recommended Action No action is required.

DHCP-1007

Message `DHCP server stop due to a switch joining a VCS cluster.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the Dynamic Host Configuration Protocol (DHCP) server has stopped due to a switch joining a Virtual Cluster Switching (VCS) cluster.

Recommended Action No action is required.

DHCP-1008

Message `Detected unexpected termination. DHCP server is restarted.`

Message Type LOG

Severity ERROR

Probable Cause Indicates unexpected termination of the Dynamic Host Configuration Protocol (DHCP) server.

Recommended Action No action is required.

DOT1 Messages

DOT1-1001

Message `802.1X is enabled globally.`

Message Type DCE

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 DCE

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 DCE

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 DCE

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 DCE

Severity INFO

Probable Cause Indicates that 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 DCE

Severity WARNING

Probable Cause Indicates that 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 RADIUS server. You can reconfigure the attributes on the RADIUS server using the **radius-server** command.

DOT1-1007

Message `No RADIUS server available for authentication.`

Message Type DCE

Severity CRITICAL

Probable Cause Indicates that there is no remote authentication dial-in user service (RADIUS) server available for authentication.

Recommended Action Check whether the configured RADIUS servers are reachable and are functioning.

DOT1-1008

Message `Port <port_name> is forcefully authorized.`

Message Type DCE

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 DCE

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 DCE

Severity INFO

Probable Cause Indicates that the specified port is set to auto mode.

Recommended Action No action is required.

DOT1-1011

Message `DOT1X_PORT_EAPOL_CAPABLE: Peer with MAC <mac1><mac2>.<mac3><mac4>.<mac5><mac6> connected to port <port_name> is EAPOL Capable.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the peer connected to the specified port is DOT1X-capable.

Recommended Action No action is required.

DOT1-1012

Message `DOT1X_PORT_EAPOL_CAPABLE: Peer connected to port <port_name> is NOT EAPOL capable.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the peer connected to the specified port is not DOT1X-capable.

Recommended Action No action is required.

DOT1-1013

Message `DOT1X test timeout value is set to <Updated test timeout value>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the DOT1X test timeout value has been changed to the specified value.

Recommended Action No action is required.

DOT1-1014

Message `802.1X Mac Authentication Bypass is enabled for port <port_name>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that 802.1X MAC authentication bypass is enabled on the specified port.

Recommended Action No action is required.

DOT1-1015

Message `802.1X Mac Authentication Bypass is disabled for port <port_name>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that 802.1X MAC authentication bypass is disabled on the specified port.

Recommended Action No action is required.

DOT1-1016

Message `802.1X Transition to Mac Authentication Bypass for port <port_name>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that 802.1X MAC authentication bypass is triggered on the specified port.

Recommended Action No action is required.

DOT1-1017

Message `802.1X Mac Authentication Bypass is reset for port <port_name>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that 802.1X MAC authentication bypass is reset on the specified port.

Recommended Action No action is required.

EANV Messages

EANV-1001

Message `Port <port number> port fault. Change the SFP transceiver 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.

EANV-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 this chip will be disabled.

Recommended Action Reload the system at the next maintenance window.

EANV-1003

Message `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 Reload the system at the next maintenance window.

EANV-1004

Message 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 No action is required. The software will recover from the error.

EANV-1005

Message C<chip index>,A<eanvil id>: Memory allocation failed.

Message Type LOG

Severity ERROR

Probable Cause Indicates memory allocation failure in the software.

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

EANV-1006

Message 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 not operational.

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

ELD Messages

ELD-1001

Message `Interface <InterfaceName> is shut down by edge loop detection (ELD) for loop in VLAN <VLAN ID>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that a loop has been detected by the edge loop detection (ELD) protocol on the specified interface. The interface has been shut down.

Recommended Action Identify and fix the Layer 2 bridging loop and then re-enable the interface using the **clear edge-loop-detection** command.

ELD-1002

Message `Interface <InterfaceName> is auto-enabled by edge loop detection (ELD).`

Message Type DCE

Severity INFO

Probable Cause Indicates that the interface on which a loop was detected has been auto-enabled based on the configured shutdown time.

Recommended Action No action is required.

EM Messages

EM-1001

Message `<FRU ID> is overheating: Shutting down.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that a field replaceable unit (FRU) is shutting down due to overheating. Overheating is mainly 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.

Execute the **show environment fan** command to verify that all fans are running at normal speeds. Replace fans that are missing or not performing at high enough speeds.

EM-1002

Message `System fan(s) status <fan FRU>.`

Message Type LOG | FFDC

Severity INFO

Probable Cause Indicates that a compact system has overheated and may shut down. All the fan speeds are dumped to the console.

Recommended Action Verify that the location temperature is within the operational range of the switch.

Execute the **show environment fan** command to verify that all fans are running at normal speeds. Replace fans that are missing or not performing at high enough speeds.

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 cannot be read or is invalid. The FRU is faulted.

Recommended Action Reload or power cycle the switch.

Execute the **diag systemverification** command to verify that the switch does not have hardware problems.

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.

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 an interface module in the specified slot or the switch (for compact switches) is being shut down 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 **show environment fan** 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 interface module itself, replace the interface module.

Voltage problems on a interface module are likely a hardware problem on the interface module itself; replace the interface module.

EM-1006

Message `<FRU Id> has faulted. Sensor(s) below minimum limits.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the sensors show the voltage is below minimum limits. The switch or specified interface module is being shut down for environmental reasons; the voltage is too low.

Recommended Action If this problem occurs on an interface module, it usually indicates a hardware problem on the interface module; replace the interface module.

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 firmware version as a possible cause.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that an interface module inserted in the specified slot or the switch (for compact switches) is not compatible with the platform configuration (includes the firmware version). The interface module is faulted.

Recommended Action If the interface module is not compatible, upgrade the firmware or replace the interface module and make sure the replacement interface module is compatible with your management module type and firmware.

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 4 seconds.

Recommended Action Reseat the interface module. If the problem persists, replace the interface module.

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 4 seconds it could not be determined if it has powered down or not.

Recommended Action Reseat the interface module. If the problem persists, replace the interface module.

EM-1012

Message `<FRU Id> failed <state> state transition, unit faulted.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that a switch interface module or compact 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 Network OS configuration or hardware problems on the switch.

Recommended Action Reload or power cycle the switch.

Execute the **diag systemverification** command to verify that the switch does not have hardware problems.

If the problem 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 an field-replaceable unit (FRU).

Recommended Action 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, reload 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 message persists, execute the **copy support** command and contact your switch service provider.

EM-1020

Message `A problem was found on one or both CID cards (<The return code is for internal use only.>), run the CIDrecov tool to get more information and recovery options.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that a problem was found either accessing one (or both) of the CID cards or with the content of the data stored there. The content problem could be a corrupted data set or a mismatch between the two CID cards.

Recommended Action Execute the **CIDrecov** command to get details of the problems found and how to recover.

EM-1021

Message `A CID card has been inserted, a CID verification audit will be run to detect any mismatches or other problems.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the second CID card was enabled. Because the data may not match, the CID verification audit will be run.

Recommended Action If an EM-1020 follows, execute the **CIDrecov** command to get details of the problems found and how to recover. If not, no action is required.

EM-1022

Message `A CID card access problem has been encountered, please run the CIDrecov tool to get more information and recovery options.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a problem was encountered while accessing one (or both) of the 2 CID cards or with the content of the data stored there.

Recommended Action Execute the **CIDrecov** command to get details of the problems found and how to recover.

EM-1023

Message `Chassis fan airflow-direction <fan-direction> change is failed.`

Message Type LOG

Severity INFO

Probable Cause Indicates failure to change the fan airflow direction.

Recommended Action No action is required.

EM-1024

Message `Platform is not supported for changing the fan-airflow direction.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the platform is not supported for changing the configuration.

Recommended Action No action is required.

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 Chassis ID (CID) card field-replaceable unit (FRU) or the World Wide Name (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. This error 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. The return code is for internal use only.

Recommended Action If the problem persists, reload or power cycle the switch.

If the problem still persists, perform one of the following actions:

- For compact switches, replace the switch.
- For CID cards, run the CIDrecov tool to get more information.

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 error persists, check for loose or dirty connections. Remove all dust and debris prior to reseating the field-replaceable unit (FRU). Replace the FRU if it continues to fail.

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 interface module that is inserted, but the optical ejector switch is not latched. The interface module in the specified slot is treated as not inserted.

Recommended Action Close the ejector switch (completely screw in the optical (middle) thumbscrew on the switch fabric module(SFM)) if the field-replaceable unit (FRU) is intended for use. Refer to the appropriate *Hardware Reference Manual* for instructions on inserting the switch interface modules.

EM-1032

Message `<FRU Id> is faulted due to a PCI scan failure.`

Message Type LOG | FFDC

Severity ERROR

Probable Cause Indicates that the interface module in the specified slot has been marked as faulty because the peripheral component interconnect (PCI) scan during interface module validation failed.

Recommended Action Power cycle or reseat the interface module.

Execute the **diag systemverification** command to verify that the switch does not have hardware problems.

If the problem persists, replace the interface module.

EM-1033

Message `MM in <FRU Id> is reloading.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the standby management module has been detected to be in the reload process. The high availability (HA) feature will not be available. This message occurs every time the other management module reloads, 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 management module; however, if the failover was not intentional, it is recommended to find the reason for the failover.

Recommended Action If the standby management module was just reloaded, wait for the error to clear (execute the **show slots** command to determine if the errors are cleared). Watch for the EM-1047 message to verify that this error has cleared.

If the standby management module state changes to faulty or if it was not intentionally reloaded, check the error logs on the other management module (using the **show logging raslog** 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> is 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 **diag systemverification** command to verify that the switch does not have hardware problems.

If the problem persists, replace the FRU.

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 Chassis ID (CID) card, then the default WWN and IP addresses are used for the switch.

Recommended Action
Reseat the FRU card.

If the problem persists, reload or power cycle the switch.

Execute the **diag systemverification** command to verify that the switch does not have 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-1038

Message `Chassis fan airflow-direction changed to <fan-direction>`

Message Type LOG

Severity INFO

Probable Cause Indicates change of fan airflow direction.

Recommended Action No action is required.

EM-1042

Message `Important FRU header data for <FRU Id> is invalid.`

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 it is corrupted in the object database, which contains information about all the FRUs.

Recommended Action Reseat the FRU. If the problem persists, replace the FRU.

EM-1043

Message `Cannot power <FRU Id> <state (on or off)>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the specified field-replaceable unit (FRU) could not be powered on or off. The FRU is not responding to commands.

Recommended Action Reseat or replace the FRU.

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 interface module.

The new state can be one of the following:

- On - A port interface module is being powered on because more power is available (either a power supply was inserted or a port interface module was removed or powered down).
- Off - A port interface module has been powered down because of a (predicted) failure of the power supply.
- Down - A newly inserted port interface module was not powered on because there was not enough power available.

Recommended Action Refer to the *Hardware Reference Manual* of your switch for the number of power supplies required for redundancy.

EM-1046

Message `Error status received for interface module ID <id value> for <FRU Id>, <interface module incompatibility type: platform>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the specified interface module is incompatible.

Recommended Action If the interface module ID listed is incorrect, the field-replaceable unit (FRU) header for the interface module is corrupted and the interface module must be replaced.

If the error is due to platform, the interface module ID listed is not supported for that platform (management module) type. Remove the interface module from the chassis.

EM-1047

Message `MM in <FRU Id> is booting up.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the firmware in the specified management module is now in the boot process. This message usually follows the EM-1033 message. The new standby management module is in the process of reloading and has turned off the MM_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 the specified field-replaceable unit (FRU) is accessible on the I2C bus.

Recommended Action No action is required. This 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 the field-replaceable unit (FRU) of the specified type and location was 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 the field-replaceable unit (FRU) of the specified type and location was removed from the chassis.

Recommended Action Verify that the FRU was intended to be removed. Replace the FRU as soon as possible.

EM-1051

Message `<FRU Id>: Inconsistency detected, FRU re-initialized.`

Message Type LOG

Severity INFO

Probable Cause Indicates that an inconsistent state was found in the specified field-replaceable unit (FRU). This event occurs when the state of the FRU was changing during a failover. The FRU is reinitialized and traffic may have been disrupted.

Recommended Action No action is required.

EM-1059

Message `<FRU Id or Switch name> with ID <Interface module Id> may not be supported on this platform, check firmware version as a possible cause.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the interface module inserted in the specified slot or the switch (for compact switches) is not compatible with the switch configuration software. The interface module will not be completely usable.

The interface module may only be supported by a later (or earlier) version of the firmware.

Recommended Action Change the management module firmware or replace the interface module. Make sure the replacement is compatible with your switch type and firmware.

EM-1064

Message `<FRU 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 interface module has been powered off because a hardware application-specific integrated circuit (ASIC) error was detected, and you have selected to power off the problem interface module when such a condition occurred.

Recommended Action Execute the **copy support** command and contact your switch service provider.

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 4 minutes of receiving a request from the environmental monitor (EM). This event 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 Network OS configuration or hardware problems on the switch.

Recommended Action Reload or power cycle the switch.

If the message persists, execute the **copy support** command and contact your switch service provider.

EM-1069

Message `<FRU slot identifier> is being powered off.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified interface module has been intentionally powered off.

Recommended Action No action is required.

EM-1070

Message `<FRU slot identifier> is being powered on.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified interface module has been intentionally powered on.

Recommended Action No action is required.

EM-1080

Message `<FRU Id> is being faulted (<return code>) because it was so faulted before failover.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified interface module or fan was faulted prior to the most recent failover, and that state and reason code are being carried forward.

Recommended Action Reseat the FRU.

Execute the **diag systemverification** command to verify that the switch does not have hardware problems.

If the problem persists, replace the FRU.

EM-1081

Message `Unit in <Slot number or Switch> with ID <FRU Id> is faulted(<Fault>). This is a critical fault that requires the slot to be shutdown to avoid damage to the switch. Shutdown will happen in <Delay time in seconds> seconds.`

Message Type CFFDC | LOG

Severity CRITICAL

Probable Cause Indicates that a fault that has been determined to have the potential to cause serious damage to the switch has been detected.

Recommended Action Contact customer support.

EM-1082

Message `The switch with ID <FRU Id> is faulted(<Fault>). This is a critical fault that requires shutdown to avoid damage to the switch. Shutdown will happen in <Delay time in seconds> seconds.`

Message Type CFFDC | LOG

Severity CRITICAL

Probable Cause Indicates that a fault that has been determined to have the potential to cause serious damage to the switch has been detected.

Recommended Action Contact customer support.

EM-1083

Message `Unit in <Slot number or Switch> with ID <FRU Id> is faulted(<Fault>). This is a critical fault that requires the slot to be shutdown to avoid damage to the switch. Shutdown will happen NOW.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that a fault that has been determined to have the potential to cause serious damage to the switch has been detected.

Recommended Action Contact customer support.

EM-1084

Message `The switch with ID <FRU Id> is faulted(<Fault>). This is a critical fault that requires shutdown to avoid damage to the switch. Shutdown will happen NOW.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that a fault that has been determined to have the potential to cause serious damage to the switch has been detected.

Recommended Action Contact customer support.

EM-1100

Message `Unit in <Slot number or Switch> with ID <FRU Id> is faulted(<Fault>). <Current attempt number> of <Total number of attempts> total attempt(s) at auto-recovery is being made. Delay is <Delay time in seconds> seconds.`

Message Type CFFDC | LOG

Severity CRITICAL

Probable Cause Indicates that a fault that has been determined to be auto-recoverable has happened and recovery is being attempted.

Recommended Action If auto-recovery does not happen gracefully in a reasonable time frame, follow the user guide to recover the blade.

EM-1101

Message `Unit in <Slot number or Switch> with ID <FRU Id> is faulted(<Fault>). <Current attempt number> attempt(s) at auto-recovery were made without success.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that a fault that has been determined to be auto-recoverable has happened but recovery failed.

Recommended Action Follow the user guide to recover the blade.

EM-2003

Message `<FRU Id or switch for compact switches> has failed the POST tests. FRU is being faulted.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified 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 login ID is switch name for compact systems.

Recommended Action On modular systems, reseat the specified FRU.

On compact switches, reload or power cycle the switch.

If the problem persists:

- Execute the **diag systemverification** command to verify that the switch does not have hardware problems.
- On modular systems, replace the specified FRU; For compact switch, replace the switch.

ERCP Messages

ERCP-1000

Message `Multiple ECC errors are detected and the system will reload automatically.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that error checking and correction (ECC) errors occurred due to multi-bit corruption.

Recommended Action No action is required. The system will reload automatically to recover from the error.

ESS Messages

ESS-1008

Message `Fabric Name - <fabric_name> configured (received from domain <domain ID>).`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified fabric name has been 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 LOG

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 in the fabric.

ESS-1010

Message `Duplicate Fabric Name - <fabric_name> matching with FID <Fabric ID>.`

Message Type LOG

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.

FABR Messages

FABR-1001

Message `Interface <InterfaceName>, <segmentation reason>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the specified interface is isolated because of a segmentation resulting from mismatched configuration parameters.

Recommended Action Based on the segmentation reason displayed in the message, look for a possible mismatch of relevant parameters in the switches at both ends of the link.

FABR-1003

Message `Interface <InterfaceName>: 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. Execute the **show logging raslog** 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) transceiver. Replace the cable or SFP transceiver if necessary.

If the message persists, execute the **copy support** command and contact your switch service provider.

FABR-1004

Message `Interface: <InterfaceName>, 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 (IU) 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 Network 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 the message persists, execute the **copy support** command and contact your switch service provider.

FABR-1005

Message `<command sent>: interface <InterfaceName>: 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 an interface is about to go down.

Recommended Action No action is required. This message is often transitory.

If the message persists, execute the **copy support** 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 Network 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 Network OS.

Recommended Action If the message persists, execute the **copy support** 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 (IU). This message is rare and usually indicates a problem with the Network OS.

Recommended Action If the message persists, execute the **copy support** 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 RBridge ID state; the information unit (IU) 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 Network 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, execute the **copy support** 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 (EFP) state; cannot allocate RBridge IDs list due to a faulty EFP type. This message is rare and usually indicates a problem with the Network OS.

Recommended Action The fabric daemon will discard the EFP. The system will recover through the EFP retrial process.

If the message persists, execute the **copy support** 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 RBridge ID (RDI). The error description provides further details. This message is rare and usually indicates a problem with the Network OS.

Recommended Action If the message persists, execute the **copy support** 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 Network OS.

Recommended Action The fabric daemon will take proper action to recover from the error.

If the message persists, execute the **copy support** 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 Network OS.

Recommended Action The system will recover by failing over to the standby management module.

If the message persists, execute the **copy support** command and contact your switch service provider.

FABR-1014

Message `Interface <InterafceName> Disabled: RBridge IDs overlap. Insistent RBridge ID <RBridge ID> could not be obtained. Principal is trying to assign RBridge ID <RBridge ID>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the switch received an RBridge ID other than the one it requested. The interface was disabled because the requested insistent RBridge ID could not be obtained.

Recommended Action Change the RBridge ID of the local node (if applicable) using the **vcs rbridge-id** command. You can toggle the disabled port using the **fabric isl enable** and **no fabric isl enable** commands after the RBridge ID change.

FABR-1019

Message `Critical fabric size (<current RBridges>) exceeds supported configuration (<supported RBridges>).`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that this switch is a value-line switch and has exceeded the configured fabric size: that is, a specified limit to the number of RBridges. 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.

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 R_RDY primitive for flow control.

Recommended Action No action is required.

FABR-1030

Message `fabric: RBridge ID <new RBridge ID> (was <old RBridge ID>).`

Message Type LOG

Severity INFO

Probable Cause Indicates that the RBridge ID has changed.

Recommended Action No action is required.

FABR-1039

Message `Invalid RBridge ID zero received from principal switch (RBridge ID = <Principal RBridge id>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that an invalid RBridge ID zero has been received.

Recommended Action Check the reason for the principal switch to assign an invalid RBridge ID zero.

FABR-1041

Message `Port <Port that is being disabled> is disabled due to trunk protocol error.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that a link reset was received before the completion of the trunking protocol on the port.

Recommended Action Toggle the port using the **no fabric isl enable** and **fabric isl enable** commands.

The port may recover by re-initialization of the link.

If the message persists, execute the **copy support** command and contact your switch service provider.

FABR-1056

Message `Interface <InterfaceName> Disabled: Insistent RBridge ID <RBridge ID> could not be obtained. Principal is trying to assign RBridge ID <RBridge ID>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the switch received an RBridge ID other than the one it requested. The interface was disabled because the requested insistent RBridge ID could not be obtained.

Recommended Action RBridge ID conflict must be reconciled with the Principal configuration. Either set the RBridge ID of the local RBridge to match the configuration on the Principal using the **vcs rbridge-id** command, or remove the conflicting RBridge from the cluster using the **no vcs enable rbridge-id** command. If you remove the conflicting RBridge from the cluster, you will need to toggle the disabled port using the **no fabric isl enable** and **fabric isl enable** commands.

FABR-1057

Message `Switch <Switchname> will be taken offline and back online for RBridge Id auto configuration to take effect.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the specified switch has been bounced for the RBridge ID auto configuration to take effect on the unconfigured VCS switch.

Recommended Action No action is required.

FABR-1058

Message `<dportTestStatus>`

Message Type LOG

Severity INFO

Probable Cause Indicates the status of D_port test.

Recommended Action No action is required.

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 Network OS problem or file corruption. The *Description of memory need* variable specifies the memory size that was being requested. The value could be any whole number.

Recommended Action Reload 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 Network OS problem or file corruption.

Recommended Action Reload or power cycle the switch.

If the message persists, execute the **firmware download** 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 Network OS problem or file corruption.

Recommended Action Reload 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 Network OS problem or file corruption. The following is the possible value for the *function name and description of problem* variable:

fabsys_write: Unsupported write operation: process xxx

The xxx value is the process ID (PID), which could be any whole number.

Recommended Action Reload or power cycle the active management module (for modular systems) or the switch (for compact systems).

If the message persists, execute the **firmware download** 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 Network OS data problem on the switch. The following are the possible values for the *function name and description of problem* variable:

- 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, fail over or reload the switch.

If the message persists, execute the **firmware download** 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 Network OS has detected an invalid value in an object status field. This is usually an internal Network OS problem or file corruption.

Recommended Action Reload or power cycle the switch.

If the message persists, execute the **firmware download** command to update the firmware.

FABS-1008

Message `<Function name>: Media OID mapping failed.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Network OS was unable to locate a necessary object handle. This is usually an internal Network OS problem or file corruption.

Recommended Action Reload or power cycle the switch.

FABS-1009

Message `<Function name>: type is not media.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Network OS was unable to locate an appropriate object handle. This is usually an internal Network OS problem or file corruption.

Recommended Action Reload 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 Network OS detected an unknown event type. This is usually an internal Network OS problem or file corruption.

Recommended Action Reload or power cycle the switch.

If the message persists, execute the **firmware download** 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 Network OS message for a field-replaceable unit (FRU).

Recommended Action Reload or power cycle the management module or switch.

If the message persists, execute the **firmware download** command to update the firmware.

FABS-1013

Message `<Method name>[<Method tag number>]:Unknown interface module type 0x<Interface module type>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that an unrecognized type of interface module has been discovered in the system.

This error can be caused by one of the following reasons: an incorrect field-replaceable unit (FRU) header, inability to read the FRU header, or the interface module may not be supported by this platform or Network OS version.

Recommended Action Verify that the interface module is valid for use in this system and this version of Network OS.

Reseat the interface module.

If this is a valid interface module and reseating does not solve the problem, replace the interface module.

FABS-1014

Message `<Method name>[<Method tag number>]:Unknown FRU type 0x<FRU Object type>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that an unrecognized type of field-replaceable unit (FRU) has been discovered in the system.

This error can be caused by one of the following reasons: an incorrect FRU header, inability to read the FRU header, or the FRU may not be supported by this platform or Network OS version.

Recommended Action Verify that the FRU is valid for use in this system and this version of Network 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 that the specified field-replaceable unit (FRU) could not be enabled. This is usually an internal Network OS problem.

Recommended Action Remove and reinsert the FRU.

Reload or power cycle the management module or switch.

If the message persists, execute the **firmware download** command to update the firmware.

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 therefore failed to allocate new memory for an information unit (IU).

Recommended Action A compact switch will automatically reload.

For a modular switch, the active management module will automatically fail over and the standby management module become the active management module.

FCOE Messages

FCOE-1001

Message `calloc failed for <object>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates a memory failure.

Recommended Action Check the switch memory status using the **show process memory** command.

FCOE-1010

Message `Clean up of login failed for port:<port number>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates an invalid port number.

Recommended Action Execute the **copy support** command and restart the system. Contact your switch service provider.

FCOE-1019

Message `FLOGI ignored as FCMAP not configured on FCoE VLAN.`

Message Type DCE

Severity WARNING

Probable Cause Indicates that FCMAP is not configured on the Fibre Channel over Ethernet (FCoE) VLAN.

Recommended Action Configure FCMAP using the **fcmap** command.

FCOE-1020

Message `Login rejected by FC stack.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the login was rejected by the Fibre Channel (FC) stack.

Recommended Action No action is required. The device will try to login again.

FCOE-1022

Message `Max FCoE device login limit reached.`

Message Type DCE

Severity WARNING

Probable Cause Indicates that the switch has reached its maximum allowed Fibre Channel over Ethernet (FCoE) device limit.

Recommended Action Do not add any more FCoE devices to the switch.

FCOE-1023

Message `Too many logins on FCoE controller from Device MAC: <Enode MAC Address > , max allowed = <MAX_DEVS_PER_CTLR>.`

Message Type DCE

Severity WARNING

Probable Cause Indicates that the controller has reached its maximum allowed Fibre Channel over Ethernet (FCoE) login limit.

Recommended Action Log out some of the logged-in devices using one of the following commands: **no fcoeport default**, **shutdown**, and **clear fcoe login**, and then log in the new device.

You can view the list of logged-in devices using the **show fcoe login** command.

FCOE-1024

Message `FDISC received from Enode without prior FLOGI.`

Message Type DCE

Severity WARNING

Probable Cause Indicates that a fabric discovery (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 No action is required.

FCOE-1029

Message `Version mismatch between FIP FDISC and root VN port.`

Message Type DCE

Severity WARNING

Probable Cause Indicates that the FCoE Initialization Protocol (FIP) version does not match between the fabric login (FLOGI) and fabric discovery (FDISC) frames.

Recommended Action Make sure that the device that is trying to log in conforms to the FC-BB-5 standard.

FCOE-1030

Message `Version mismatch between FIP LOGO and root VN port.`

Message Type DCE

Severity WARNING

Probable Cause Indicates that the switch received an FCoE Initialization Protocol (FIP) logout (LOGO) request but the device logged in with a different FIP version.

Recommended Action Make sure that the device that is trying to log in conforms to the FC-BB-5 standard.

FCOE-1032

Message `The chassis is in WARM RECOVERING state.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the chassis is in a warm recovering state and therefore cannot perform the protocol-specific actions for the time being.

Recommended Action Wait until the chassis has fully recovered before you perform any operations.

FCOE-1034

Message `FIP/FCoE frame on priority <pkt_ctrlp->pri_in> for <Name of the following string> <MAC address or WWN of the source device> on interface <Interface Name> discarded because PFC/FCoE not enabled on this priority.`

Message Type DCE

Severity WARNING

Probable Cause Indicates that the specified priority is not priority-based flow control (PFC) or Fibre Channel over Ethernet (FCoE) enabled.

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-1035

Message `Virtual FCoE port <port number> is online.`

Message Type DCE

Severity INFO

Probable Cause Indicates an administrative action on the Fibre Channel over Ethernet (FCoE) port.

Recommended Action No action is required.

FCOE-1036

Message `Virtual FCoE port <port number> is offline.`

Message Type DCE

Severity INFO

Probable Cause Indicates an administrative action on the Fibre Channel over Ethernet (FCoE) port.

Recommended Action No action is required.

FCOE-1037

Message `Slot <slot_id> not ready in FCoE daemon.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the slot state has been detected as inconsistent during high availability (HA) failover.

Recommended Action No action is required.

FCOE-1038

Message `Interface module removed during FCoE port create. ifindex 0x<if_index> uport <uport_num>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the interface module was removed before the system could fully complete the online event for the interface module.

Recommended Action No action is required.

FCOE-1039

Message `<message> : 0x<ifIndex> : <mac1>:<mac2>:<mac3>:<mac4>:<mac5>:<mac6>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the login was rejected because there are no more VF ports available.

Recommended Action Increase the number of VF ports and try again.

FCOE-1040

Message `Interface <Port Channel Member Interface type><Port Channel Member Interface Name> of FCoE Provisioned Port Channel <FCOE Provisioned Port Channel> is CEE INCAPABLE.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the member interface of a FCoE provisioned port channel is no more CEE capable.

Recommended Action Check the reason for CEE failure. Execute the **shutdown** and **no shutdown** commands on the interface.

FCOE-1044

Message `Fcoe provisionig is already applied through fcoeport config. Ignoring FCoE provisioning through port-profile-port config.`

Message Type DCE

Severity WARNING

Probable Cause Indicates that FCoE provisioning is already applied through fcoeport configuration, therefore FCoE provisioning through port-profile-port configuration is ignored by the FCoE module.

Recommended Action No action is required.

FCOE-1045

Message `Fcoe port-profile-port provisioning of local logical SAN will not be allowed if the switch is in AG mode.`

Message Type DCE

Severity WARNING

Probable Cause Indicates that port-profile-port provisioning of local logical SAN will not be allowed if the switch is in AG mode.

Recommended Action No action is required.

FCOE-1046

Message `Default port-profile provisioning will not be allowed if the FCF/AG rbridge id is part of any fcf-groups.`

Message Type DCE

Severity WARNING

Probable Cause Indicates that port-profile-port provisioning of local logical SAN will not be allowed if the switch is in AG mode.

Recommended Action No action is required.

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 therefore failed to allocate new memory for a Fibre Channel driver instance.

The *function* 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 compact switch will automatically reload.

For a modular switch, the active management module will automatically fail over and the standby management module become the active management module.

FCPH-1003

Message `New port <Port Number> has same Port WWN [<Port WWN>] as old port <Port Number> and will be logged out 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 [<Port WWN>] as old port <Port Number> with pid 0x<Port PID> and will be logged out 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 `Old port <Port Number> has same Port WWN [<Port WWN>] as new port <Port Number> and will be logged out 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-1006

Message `NPIV port <Port Number>[pid:0x<Port PID>] has same Port WWN [<Port WWN>] as new port <Port Number> and will be logged out 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 N_Port ID virtualization (NPIV) port.

Recommended Action No action is required.

FCPH-1007

Message `Old port <Port Number>[pid:0x<Port PID>] has same Port WWN [<Port WWN>] as new NPIV port <Port Number> and will be logged out 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-1008

Message `Old NPIV port <Port Number>[pid:0x<Port PID>] has same Port WWN [<Port WWN>] as new NPIV port <Port Number> and will be logged out 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 NPIV port.

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 are the known LSR header types: 1 - Unicast and 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 that 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 RBridge ID: <RBridge number>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the received link state record (LSR) contained an invalid RBridge number.

Recommended Action No action is required; the LSR is discarded.

FLOD-1006

Message `Transmitting invalid RBridge ID: <RBridge number>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the transmit link state record (LSR) contained an invalid RBridge 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 **copy support** command and contact your service provider.

FSPF-1002

Message `Wrong neighbor ID (<RBridge ID>) in Hello message from interface <interface name> (<interface index>), expected ID = <RBridge ID>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the switch has received a wrong RBridge ID in the Hello message from its neighbor switch. This may happen when the RBridge ID for a switch has been changed.

Recommended Action No action is required.

FSPF-1003

Message `Remote RBridge ID <RBridge number> out of range, input port = <port number>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified remote RBridge 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 **firmware download** command. All current versions of the Network OS support FSPF version 2.

FSPF-1007

Message `ICL triangular topology is broken between the neighboring RBridges: <RBridge number> and <RBridge 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 Investigate the ICLs and reconnect the switches to form a triangular topology.

FSPF-1008

Message `ICL triangular topology is formed among the RBridges: <RBridge number> (self), <RBridge number>, and <RBridge 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-1013

Message `Exceeded maximum number of supported paths (16) to one or more remote RBridges.`

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 **show fabric route topology** and **show fabric route linkinfo** commands to get additional details about which remote domains are violating the maximum paths limit. Refer to the *Network 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 Execute the **copy support** 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 Execute the **copy support** 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 synchronization service (FSS) has dropped the update because an application has not set the transaction flag correctly.

Recommended Action Execute the **copy support** command and contact your switch service provider.

FSS-1004

Message `FSS out of memory (<memory allocation with number of bytes>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the system ran out of memory.

Recommended Action Check memory usage on the switch using the **show process memory** command.
Execute the **copy support** 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 synchronization service (FSS) device has failed.

Recommended Action If the message persists, execute the **copy support** 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 synchronization service (FSS) device.

Recommended Action If the message persists, execute the **copy support** command and contact your switch service provider.

FSS-1007

Message `<component name>: Faulty Ethernet connection.`

Message Type LOG | FFDC

Severity CRITICAL

Probable Cause Indicates that the Ethernet connection between the active and standby management modules is not healthy. The error occurs when the standby management module does not respond to a request from the active management module within 5 seconds. This usually indicates a problem with the internal Ethernet connection and a disruption of the synchronization process.

Recommended Action Execute the **copy support** command and contact your switch service provider.

FSS-1008

Message `FSS Error on service component [<service name><service instance>:<component name>]: <Error Message>.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that a fabric synchronization service (FSS) error has occurred.

Recommended Action Execute the **copy support** command and contact your switch service provider.

FSS-1009

Message `FSS Error on service instance [<service name><service instance>]: <Error Message>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that a fabric synchronization service (FSS) error has occurred.

Recommended Action Execute the **copy support** 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 synchronization service (FSS) error may have occurred.

Recommended Action No action is required.

FSS-1011

Message `All services complete the critical recoveries in <time taken for the critical service recovery> sec.`

Message Type LOG

Severity INFO

Probable Cause Indicates a non-disruptive failover with warm recovery.

Recommended Action If the time taken for critical service recovery is more than 8 seconds, contact your switch service provider.

FSS-1012

Message `FSS transport flow hitting the threhold (<number of waiting requests>:<the current xmb allocation size>:<total of KERNEL memory>:<total of ATOMIC memory>).`

Message Type LOG | FFDC

Severity CRITICAL

Probable Cause Indicates that the underlying transport is not healthy.

Recommended Action Execute the **copy support** command and contact your switch service provider.

FSS-1013

Message `FSS transport flow hitting OOM (<the current xmb allocation size>).`

Message Type LOG | FFDC

Severity CRITICAL

Probable Cause Indicates out of memory.

Recommended Action Execute the **copy support** command and contact your switch service provider.

FSS-1014

Message `FSS transport is being blocked for too long (<the current xmb allocation size>).`

Message Type LOG | FFDC

Severity CRITICAL

Probable Cause Indicates that fabric synchronization service (FSS) transport has been blocked for too long time.

Recommended Action Execute the **copy support** command and contact your switch service provider.

FVCS Messages

FVCS-1003

Message `Possible vLAG Split Detected vLAG - ifindex (<vLAG ifindex>), split RBridge(<split RBridge >).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the RBridge has left the cluster.

Recommended Action If the RBridge was not disabled on purpose, check if it is still connected to the cluster using the **show fabric isl** command.

FVCS-1004

Message `HA Sync Failure- THA API call Failed and Retries timed out rc (<API RC>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Transparent High Availability (THA) library state synchronization attempt has failed.

Recommended Action No action is required. If the message persists, execute the **copy support** command and contact your switch service provider.

FVCS-1005

Message `Protected Group <Protected Group ID> Configured Active vLAG ifindex mismatch detected (local 0x<Local Configured Active VLAG ifindex>, remote 0x<Remote Configured Active VLAG ifindex>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates that a Protected Group mismatch has been detected across RBridges due to potential misconfiguration.

Recommended Action Check to make sure the configured active Virtual Link Aggregation Group (vLAG) is the same across all RBridges for the specified Protected Group.

FVCS-1006

Message `Protected Group <Protected Group ID> Port-Channel mismatch detected (local: m1-0x<Local VLAG Member 1 ifindex>, m2-0x<Local VLAG Member 2 ifindex>, remote: m1-0x<Remote VLAG Member 1 ifindex>, m2-0x<Remote VLAG Member 2 ifindex>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates that a Protected Group mismatch has been detected across RBridges due to potential misconfiguration.

Recommended Action Check to make sure the Virtual Link Aggregation Groups (vLAG) member port-channel IDs are the same across all RBridges for the specified Protected Group.

FVCS-1007

Message `vLAG Config error, vLAG on remote RBridge connected to different end device - ifindex (<vLAG ifindex>), remote RBridge(<remote RBridge >).`

Message Type LOG

Severity ERROR

Probable Cause Configure common Port Channel with Links connected to different end devices .

Recommended Action Check the Port Channel configuratoin on remote RBridge. Cannot connect common vLAG links to different end devices

FVCS-2001

Message `FCS Primary Update Send attempt Failed - reason (<Failure Reason>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the remote switch has rejected the update. Refer to the failure reason for more details.

Recommended Action Execute the **show fabric isl** command to check the cluster connection status.

If the message persists, execute the **copy support** command and contact your switch service provider.

FVCS-2002

Message `Link State Update sent to Remote RBridge Failed - reason (<Failure Reason Code>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates a possible cluster infrastructure problem.

Recommended Action Execute the **show fabric isl** command to check the cluster connection status.

If the message persists, execute the **copy support** command and contact your switch service provider.

FVCS-2003

Message `Lag Configureation Update sent to Remote RBridge Failed - reason (<Failure Reason Code>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates a possible cluster infrastructure problem.

Recommended Action Execute the **show fabric isl** command to check the cluster connection status.

If the message persists, execute the **copy support** command and contact your switch service provider.

FVCS-2004

Message `FCS Commit stage Failed - cfg type <Configuration Type>, cfg tag <Configuration Tag>, domain <Source Domain>, reason (<Failure Reason Code>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the fabric configuration server (FCS) commit stage has failed. The failure reason can be one of the following:

- 7 - Memory allocation error
- 14 - Reliable Transport Write and Read (RTWR) send failure

Recommended Action Check the status of the virtual link aggregation group (vLAG) identified by the configuration tag.

If the message persists, execute the **copy support** command on both this RBridge and the remote RBridge specified by the domain field and contact your switch service provider.

FVCS-2005

Message `FCS Cancel stage Failed - cfg type <Configuration Type>, cfg tag <Configuration Tag>, domain <Source Domain>, reason (<Failure Reason Code>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the fabric configuration server (FCS) cancel stage has failed. The failure reason can be one of the following:

- 7 - Memory allocation error
- 14 - Reliable Transport Write and Read (RTWR) send failure

Recommended Action Check the status of the virtual link aggregation group (vLAG) identified by the configuration tag.

If the message persists, execute the **copy support** command on both this RBridge and the remote RBridge specified by the domain field and contact your switch service provider.

FVCS-2006

Message `FCS Transaction Hung - cfg type <Configuration Type>, cfg tag <Configuration Tag>, trans state<Trans State>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the update cannot be completed for an unknown reason.

Recommended Action Check the status of the virtual link aggregation group (vLAG) identified by the configuration tag.

If the message persists, execute the **copy support** command and contact your switch service provider.

FVCS-2007

Message `Fabric Hello Timeout: Inter-switch Frame Delivery problem - remote RBridge ID <Remote Domain>, port <Port>, reason (<Failure Reason Code>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates failure to send frames to the specified remote RBridge domain even after several retry attempts. The following are the possible failure reasons:

- 7 - Routing Problem
- 14 - Reliable Transport Write and Read (RTWR) send failure

Recommended Action Check the status of cluster and the specified remote RBridge domain.

If the problem persists, execute the **copy support** command on both this RBridge and the specified remote RBridge domain and contact your switch service provider.

FVCS-2008

Message `Recover from Fabric Hello Timeout - remote RBridge ID <Remote Domain>, port <Port>, failure cnt <Failure Count>.`

Message Type LOG

Severity INFO

Probable Cause Indicates recovery from previously detected problem with sending frames to the specified remote RBridge domain.

Recommended Action No action is required.

FVCS-3001

Message `Eth_ns Message Queue Overflow. Failed to send Update. MAC or MCAST database may be out of sync. Queue size = (<Queue Size>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Eth_ns (component of FVCS) that kept the MCAST and L2 databases in sync cannot send an update to the remote RBridges because its internal message queue is full. This error is due to a temporary congestion issue on the local RBridge.

Recommended Action The RBridge must leave and rejoin the fabric for synchronization of the MCAST and L2 databases.

FVCS-3002

Message `Eth_ns Message Queue Overflow. Failed to add received Update. MLD, MAC, or MCAST database may be out of sync. Queue size = (<Queue Size>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the Eth_ns (component of FVCS) that kept the MLD, MCAST, and L2 databases in sync cannot process an update received from the remote RBridge because its internal message queue is full. This error is due to a temporary congestion issue on the local RBridge.

Recommended Action No action is required. The MLD, L2, and MCAST databases will synchronize with the fabric after the local congestion issue is resolved.

FVCS-3003

Message `Local VRID config attempt failed. Existing VLAN_ID mismatch. VRID <VRID>, VRB_ID <VRB_ID>, New VLAN_ID <New VLAN_ID>, Existing VLAN_ID <Existing VLAN_ID>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates virtual router ID (VRID) configuration conflict.

Recommended Action Check existing VRID configurations.

FVCS-3004

Message `Local VRID config attempt failed. vmac mismatch. Existing_VMAC <Existing_VMAC>, VRID <VRID>, VLAN_ID <VLAN_ID>, New_VMAC <New_VMAC>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates virtual router ID (VRID) configuration conflict.

Recommended Action Check existing VRID configurations.

FVCS-3005

Message `Remote VRB_ID update failed. Existing VRID mismatch. VRB_ID <VRB_ID>, SRC_Domain <SRC_Domain> New VRID <New VRBID>, Existing VRID <Existing VRBID>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates virtual router ID (VRID) configuration conflict.

Recommended Action Check existing VRID configurations.

FVCS-3006

Message `Remote VRB_ID update failed. Existing VLAN_ID mismatch. VRB_ID <VRB_ID>, SRC_Domain <SRC_Domain> New VLAN_ID <New VLAN_ID>, Existing VLAN_ID <Existing VLAN_ID>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates virtual router ID (VRID) configuration conflict.

Recommended Action Check existing VRID configurations.

FVCS-3007

Message `Remote VRB_ID update failed. Existing VMAC mismatch. VLAN_ID <VLAN_ID>, SRC_Domain <SRC_Domain>, New VMAC <New VMAC>, Existing VMAC <Existing VMAC>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates virtual router ID (VRID) configuration conflict.

Recommended Action Check existing VRID configurations.

FVCS-3008

Message `MAC (L2) database out of sync, Down-level domain <Domain>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the current media access control (MAC) count is not supported on the specified downlevel domain.

Recommended Action Upgrade the firmware to Network OS v3.0.0 or later.

FVCS-3009

Message `Eth_ns buffer capacity exceeded - MAC or MCAST database may be out of sync.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the current media access control (MAC) count exceeds the supported limit.

Recommended Action Reduce the number of Ethernet devices in the fabric.

FVCS-3010

Message `Fab_STP Message Queue Overflow. Failed to send Update. MSTP may be out of sync. Queue size = (<Queue Size>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the fab_stp (component of FVCS) that keeps MSTP in sync cannot send an update to the remote RBridges because its internal message queue is full. This error is due to a temporary congestion issue on the local RBridge.

Recommended Action The RBridge must leave and rejoin the fabric for synchronization of the spanning tree databases.

FVCS-3011

Message `Fab_STP Message Queue Overflow. Failed to add received Update. Spanning tree (MSTP) database may be out of sync. Queue size = (<Queue Size>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the fab_stp (component of FVCS) that keeps MSTP in sync cannot process an update received from the remote RBridge because its internal message queue is full. This error is due to a temporary congestion issue on the local RBridge.

Recommended Action No action is required. MSTP will synchronize with the fabric after the local congestion issue is resolved.

FVCS-3012

Message `Eth_ns buffer capacity exceeded - MCAST (IGMP) database may be out of sync.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the current Internet Group Management Protocol (IGMP) data set exceeds the supported limit.

Recommended Action Reduce the number of memberships defined in the fabric.

FVCS-3013

Message `Eth_ns buffer capacity exceeded - MLD database may be out of sync.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the current Multicast Listener Discovery (MLD) data set exceeds the supported limit.

Recommended Action Reduce the number of memberships defined in the fabric.

FVCS-3014

Message `MAC database communication error - MAC information may be temporarily out of sync.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that MAC information might be out of sync across RBridges.

Recommended Action No action is required. The local RBridge will automatically attempt to recover.

FVCS-3015

Message `MAC database communication restored.`

Message Type LOG

Severity INFO

Probable Cause Indicates that MAC information will be re-synced.

Recommended Action No action is required. The local RBridge will automatically attempt to re-sync.

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 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 Respond to this message as is appropriate to the particular policy of the end-user installation. Typically, low temperatures means 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 may 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 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.

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.

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.

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. Execute the **show environment power** 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 the power supply is installed correctly and that it is correctly seated in the chassis. If the problem persists, replace the faulty power supply.

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-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) transceiver 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) transceiver has risen above the high boundary.

Recommended Action Frequent fluctuations in temperature may indicate a deteriorating SFP transceiver. Replace the SFP transceiver.

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) transceiver has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action No action is required.

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) transceiver has fallen below the low boundary. The receive performance area measures the amount of incoming laser to help you determine if the SFP transceiver is in good working condition or not. If the counter often exceeds the threshold, the SFP transceiver is deteriorating.

Recommended Action Verify that the optical components are clean and functioning properly. Replace deteriorating cables or SFP transceivers. 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) transceiver has risen above the high boundary. The receive performance area measures the amount of incoming laser to help you determine if the SFP transceiver is in good working condition or not. If the counter often exceeds the threshold, the SFP transceiver is deteriorating.

Recommended Action Replace the SFP transceiver 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) transceiver 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 if the SFP transceiver is in good working condition or not. If the counter often exceeds the threshold, the SFP transceiver 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-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) transceiver has fallen below the low boundary. The transmit performance area measures the amount of outgoing laser to help you determine if the SFP transceiver is in good working condition or not. If the counter often exceeds the threshold, the SFP transceiver is deteriorating.

Recommended Action Verify that the optical components are clean and functioning properly. Replace deteriorating cables or SFP transceivers. 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) transceiver has risen above the high boundary. The transmit performance area measures the amount of outgoing laser to help you determine if the SFP transceiver is in good working condition or not. If the counter often exceeds the threshold, the SFP transceiver is deteriorating.

Recommended Action Replace the SFP transceiver.

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) transceiver 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 if the SFP transceiver is in good working condition or not. If the counter often exceeds the threshold, the SFP transceiver 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-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) transceiver voltage has fallen below the low boundary.

Recommended Action Verify that your optical components are clean and functioning properly. Replace deteriorating cables or SFP transceivers. 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) transceiver 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, replace the SFP transceiver.

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) transceiver 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-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) transceiver 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 transceiver 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) transceiver voltage has risen above the high boundary. High voltages indicate possible hardware failures.

Recommended Action Frequent voltage fluctuations are an indication that the SFP transceiver is deteriorating. Replace the SFP transceiver.

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) transceiver 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-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 **show logging raslog** 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-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 **show logging raslog** command to determine the IP address of the log in 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-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.

FW-1404

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 CPU or memory usage is above the configured threshold. If this message pertains to memory usage, then the usage is above 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 LOG

Severity INFO

Probable Cause Indicates that the memory usage is above low 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 LOG

Severity CRITICAL

Probable Cause Indicates that the memory usage is above the configured high threshold for memory usage.

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 configured high and medium thresholds for memory usage.

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 configured low and medium thresholds for memory usage.

Recommended Action No action is required.

FW-1409

Message `Current disk utilization is <Value> <Unit>. Deleting <File>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates high compact flash (CF) disk utilization.

Recommended Action No action is required.

FW-1410

Message `Disk usage is greater than 60 percent and max number of Core file limit [5] has been exceeded. Deleting the oldest core file: <File>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the maximum number of core file limit has been exceeded.

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 **show system monitor** 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 state change occurred because a policy is no longer violated.

Recommended Action No action is required.

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 **system-monitor** command.

Recommended Action Replace the faulty or missing power supplies.

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 **system-monitor** command.

Recommended Action Replace the faulty power supplies.

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 **system-monitor** command.

Recommended Action Replace the missing power supplies.

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 **system-monitor** command. A temperature sensor is faulty when the sensor value is not in the acceptable range.

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 **system-monitor** command. A fan is faulty when sensor value is not in the acceptable range.

Recommended Action Replace the faulty or deteriorating fans.

FW-1432

Message `Switch status change contributing factor Cid-Card: <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 Chassis ID (CID) cards is greater than or equal to the policy set by the **system-monitor** command.

Recommended Action Replace the faulty CID card.

FW-1433

Message `Switch status change contributing factor non-redundant MM : M<CP Number> <MM Status>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the switch is not in a healthy state. This occurred because the number of faulty management modules is greater than or equal to the policy set by the **system-monitor** command. The management modules are non-redundant.

Recommended Action Execute the **show firmware** command to verify if both the management modules have compatible firmware levels. Execute the **firmware download** command to install the same level of firmware to both management modules. Replace any faulty management modules.

If you reset the micro-switch (the latch on the management module) on the active management module before the heartbeat was up on a power cycle, and the management modules came up non-redundant, reload the management modules again to clear the problem.

FW-1434

Message `Switch status change contributing factor LC: <Number Bad> LC failures (<LC Numbers>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the switch is not in a healthy state. This occurred because the number of line card (LC) failures is greater than or equal to the policy set by the **system-monitor** command.

Recommended Action Replace the faulty LC.

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 usage is out of range. The policy was set using the **system-monitor** command.

Recommended Action Execute the **clear support** command to clear the kernel flash.

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 **chassis enable** command to bring the switch online.

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 if the event was planned. If the event was planned, no action is required. If the event was not planned, check with your system administrator on the hardware state change.

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 an FRU is inserted but not powered on.

Recommended Action Verify if the event was planned. If the event was planned, no action is required. If the event was not planned, check with your system administrator on the hardware state change.

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 if the event was planned. If the event was planned, no action is required. If the event was not planned, check with your system administrator on the hardware state change.

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 if the event was planned. If the event was planned, no action is required. If the event was not planned, check with your system administrator on the hardware state change.

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-1447

Message `Switch status change contributing factor SFM: <Number Bad> SFM 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 switch fabric module (SFM) failures is greater than or equal to the policy set by the **system-monitor** command.

Recommended Action Replace the faulty SFM.

FW-1500

Message `Mail overflow - Alerts being discarded.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a mail alert overflow condition has occurred.

Recommended Action Resolve or disable the mail alert using the **system-monitor-mail fru** 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-1510

Message `<Area string> threshold exceeded: Port <Port number> disabled.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified port is now disabled because the link on this port had multiple link failures that exceed Fabric Watch (FW) threshold on the port. The link failures occurred due to one of following reasons:

- Physical and hardware problems on the switch.
- Loss of synchronization.
- Hardware failures.
- A defective small form-factor pluggable (SFP) transceiver or faulty cable.

Protocol errors indicates cyclic redundancy check (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 transceiver and the cable and enable the port using the **no shutdown** command.

FW-3101

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 cyclic redundancy checks (CRCs) 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. A low number of invalid CRCs means the switch is functioning normally.

FW-3102

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 cyclic redundancy checks (CRCs) that the port experiences has risen above the high boundary.

Recommended Action This error generally indicates an deteriorating fabric hardware. Check small form-factor pluggable (SFP) transceivers, cables, and connections for faulty hardware. Verify that all optical hardware is clean.

FW-3103

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 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.

Recommended Action Respond to this message as is appropriate to the particular policy of the end-user installation. Frequent fluctuations in CRC errors generally indicate an aging fabric. Check the small form-factor pluggable (SFP) transceivers, cables, and connections for faulty hardware. Verify that all optical hardware is clean.

FW-3104

Message `<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 lower threshold boundary to a value within the acceptable range.

Recommended Action Respond to this message as is appropriate to the particular policy of the end-user installation. Frequent fluctuations in CRC errors generally indicate an aging fabric. Check small form-factor pluggable (SFP) transceivers, cables, and connections for faulty hardware. Verify that all optical hardware is clean.

FW-3105

Message `<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 upper threshold boundary to a value within the acceptable range.

Recommended Action Respond to this message as is appropriate to the particular policy of the end-user installation. Frequent fluctuations in CRC errors generally indicate an aging fabric. Check small form-factor pluggable (SFP) transceivers, cables, and connections for faulty hardware. Verify that all optical hardware is clean.

FW-3107

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 Abnormal Frame termination frames 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. A low number of abnormal frame termination errors means the system is operating normally.

FW-3108

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 abnormal frame termination frames that the port experiences has risen above the high boundary. Flapping interfaces during the traffic flow can generate this error.

Recommended Action Check all loose connections in the fabric.

FW-3109

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 abnormal frame termination frames that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action Respond to this message as is appropriate to the particular policy of the end-user installation. Check all loose connections in the fabric.

FW-3110

Message `<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 abnormal frame termination frames that the port experiences crossed lower threshold boundary to a value within the acceptable range.

Recommended Action Respond to this message as is appropriate to the particular policy of the end-user installation. Check all loose connections in the fabric.

FW-3111

Message `<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 abnormal frame termination frames that the port experiences has dropped below upper threshold boundary to a value within the acceptable range.

Recommended Action Respond to this message as is appropriate to the particular policy of the end-user installation. Check all loose connections in the fabric.

FW-3113

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 frames with symbol error that the port experiences has fallen below the low boundary.

Recommended Action Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of symbol errors means the system is operating normally.

FW-3114

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 frames with symbol error that the port experiences has risen above the high boundary. Flapping interfaces or loose connections can cause this error.

A high number of symbol errors indicate a deteriorated device, cable, or hardware.

Recommended Action Check your small form-factor pluggables (SFPs), cables, and connections for faulty hardware. Verify that all optical hardware is clean.

FW-3115

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 frames with symbol error that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action Respond to this message as is appropriate to the particular policy of the end-user installation. Check all cables and form factors in the system.

FW-3116

Message `<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 frames with symbol error that the port experiences crossed lower threshold boundary to a value within the acceptable range.

Recommended Action Respond to this message as is appropriate to the particular policy of the end-user installation. Check all cables and form factors in the system.

FW-3117

Message `<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 frames with symbol error that the port experiences has dropped below upper threshold boundary to a value within the acceptable range.

Recommended Action Respond to this message as is appropriate to the particular policy of the end-user installation. Check all cables and form factors in the system.

FW-3119

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 inter frame gap violation errors that the port experiences has fallen below the low boundary.

Recommended Action Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of inter frame gap errors means the system is operating normally.

FW-3120

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 inter frame gap violation errors that the port experiences has risen above the high boundary. Flapping interfaces during the traffic flow can generate this error. Congestion or transmitting multiple frames without an inter frame gap.

Recommended Action Check loose connections and congestion in the fabric.

FW-3121

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 inter frame gap violation errors that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action Respond to this message as is appropriate to the particular policy of the end-user installation. Check loose connections and congestion in the fabric.

FW-3122

Message `<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 inter frame gap violation errors that the port experiences crossed lower threshold boundary to a value within the acceptable range.

Recommended Action Respond to this message as is appropriate to the particular policy of the end-user installation. Check loose connections and congestion in the fabric.

FW-3123

Message `<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 inter frame gap violation errors that the port experiences has dropped below upper threshold boundary to a value within the acceptable range.

Recommended Action Respond to this message as is appropriate to the particular policy of the end-user installation. Check loose connections and congestion in the fabric.

HASM Messages

HASM-1000

Message `Daemon <Component name> terminated. System initiated reload/failover for recovery.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that the software watchdog detected termination of a daemon and the system will reload or failover to recover.

Recommended Action After the system reloads, execute the **copy support** command and contact your switch service provider.

HASM-1001

Message `An unexpected failover event occured.`

Message Type LOG | FFDC

Severity CRITICAL

Probable Cause Indicates an unexpected failure on active. The setup will go through system reload for recovery.

Recommended Action After the system reloads, execute the **copy support** command and contact your switch service provider.

HASM-1002

Message `Error happens on service instance <Service type name> <Service instance name>: <Error message> (Critical).`

Message Type LOG | FFDC

Severity CRITICAL

Probable Cause Indicates software failure.

Recommended Action Execute the **copy support** command and reload the system manually to recover.

HASM-1003

Message `Error happened on service instance <Service type name> <Service instance name>: <Error message>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates a software error such as mismatch in the fabric synchronization service (FSS) configuration.

Recommended Action Execute the **copy support** command and reload the system manually to recover.

HASM-1004

Message `Processor reloaded - <Reboot Reason>.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the system has been reloaded either because of a user action or an error. The switch reload can be initiated by one of the following commands: **firmware download**, **fastboot**, **ha failover**, and **reload**. Some examples of errors that may initiate this message are hardware errors, software errors, compact flash (CF) errors, or memory errors. The reason for reload can be any 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
- Reload:API
- Reload:HAM
- EMFault:EM

Recommended Action Check the error log on both management modules for additional messages that may indicate the reason for the switch reload.

HASM-1005

Message `The standby peer has not booted up yet.`

Message Type LOG

Severity WARNING

Probable Cause Indicates peer node boot failure.

Recommended Action Execute the **copy support** command and check the network connectivity and the peer node boot status.

HASM-1006

Message `Heartbeat down detected on standby, reboot the standby.`

Message Type LOG | FFDC

Severity CRITICAL

Probable Cause Indicates heavy CPU load on active or standby.

Recommended Action Execute the **copy support** command.

HASM-1012

Message `HA State starts to sync.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the high availability (HA) state for the active management module starts to sync with the HA state of the standby management module. If the standby management module is healthy, the system may become in sync (see HASM-1100), and the failover afterwards will expect to be nondisruptive.

Recommended Action No action is required.

HASM-1013

Message `Restartable daemon (<Component name>) terminated prematurely. System initiated failover/reload for recovery.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that a restartable daemon terminated before the system has booted up completely.

Recommended Action After the system reloads, execute the **copy support** command and contact your switch service provider.

HASM-1014

Message `Daemon (<Component name>) terminated while the system was booting up.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that a daemon terminated before the system has booted up completely.

Recommended Action Execute the **copy support** command and reload the system manually to recover.

HASM-1015

Message `Error happens on service instance <Service type name> <Service instance name>: <Error message> (Critical, reboot to recover).`

Message Type LOG | FFDC

Severity CRITICAL

Probable Cause Indicates software failure.

Recommended Action Execute the **copy support** command after the system boots up.

HASM-1019

Message `Firmware operation (<operation code>) was aborted due to disconnection of the peer node.`

Message Type LOG | VCS

Severity WARNING

Probable Cause Indicates that the peer node has been reloaded or disconnected due to a software error.

Recommended Action No action is required. Firmware commit will be started automatically to repair the compact flash (CF) partitions in the system.

HASM-1020

Message `Firmware operation (<operation code>) was aborted due to timeout.`

Message Type LOG | FFDC | VCS

Severity WARNING

Probable Cause Indicates that the firmware operation took too long to complete due to CPU overload or other software errors.

Recommended Action No action is required. Firmware commit will be started automatically to repair the compact flash (CF) partitions in the system.

HASM-1021

Message `Firmware operation (<operation code>) was aborted manually.`

Message Type LOG | VCS

Severity WARNING

Probable Cause Indicates that the specified firmware operation was aborted manually.

Recommended Action No action is required.

HASM-1022

Message `Failed to fork firmware child process.`

Message Type LOG | VCS

Severity WARNING

Probable Cause Indicates that the firmware operation could not be started due to a software error.

Recommended Action Execute the **copy support** command and contact your switch service provider.

HASM-1023

Message `There is no HA connection between the MMs due to firmware incompatibility.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the firmware in the management modules are not compatible.

Recommended Action Upgrade the firmware on the standby management module to be the same as the active management module.

HASM-1024

Message `Firmware is not available at <Firmware path on MM> on MM.`

Message Type LOG | VCS

Severity WARNING

Probable Cause Indicates that the firmware for the line card (LC) is not available in the management module compact flash (CF) card. This event can be due to firmware corruption.

Recommended Action Execute the **copy support** command and contact your switch service provider.

HASM-1025

Message `HA is disconnected between the MMs due to incompatible features.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a feature is enabled and it is not compatible with the firmware running on the standby management module.

Recommended Action Upgrade the firmware on the standby management module to be the same as the active management module before enabling the feature.

HASM-1026

Message `The last reboot is due to Kernel Panic in <Module name>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the system has reloaded due to kernel panic in the specified module.

Recommended Action Execute the **copy support** command and contact your switch service provider.

HASM-1027

Message `The secondary switch needs linecard power-cycle for the connector configuration to take effect.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a static port breakout operation has completed and the line card (LC) needs to be power cycled for the changes to take effect.

Recommended Action Power cycle the LC whose 40 Gigabit Ethernet port has been broken out by using the **power-off linecard** and **power-on linecard** commands for the changes to take effect.

HASM-1028

Message `The secondary switch needs reload or linecard power-cycle for the port-group configuration to take effect.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a static port group operation has completed and the line card (LC) needs to be power cycled for the changes to take effect.

Recommended Action Power cycle the linecard whose port group configuration has been changed to performance mode by using the **power-off linecard** and **power-on linecard** commands for the changes to take effect.

HASM-1029

Message `The secondary switch needs to be rebooted for the new hardware profile configuration to take effect.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the secondary node has taken on a new hardware profile configuration from primary database upon rejoining the cluster.

Recommended Action The secondary switch need to be rebooted for the new profile configuration to take effect.

Execute the **reload system** command to reboot the secondary switch.

HASM-1030

Message `Failed to find the custom KAP profile specified. Use the default KAP profile instead.`

Message Type LOG

Severity INFO

Probable Cause Indicates failure to find the custom Keep-alive Protocol (KAP) profile specified in the user configuration. It will instead use the default KAP profile to boot up the switch.

Recommended Action Verify the hardware KAP profile configuration. This is likely an error condition.

HASM-1100

Message `HA State is in sync.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the high availability (HA) state for the active management module is in synchronization with the HA state of the standby management module. If the standby management module is healthy, the failover will be nondisruptive.

Recommended Action No action is required.

HASM-1101

Message `HA State out of sync.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the high availability (HA) state for the active management module is out of synchronization with the HA state of the standby management module. If the active management module failover occurs when the HA state is out of sync, the failover is disruptive.

Recommended Action If this message was logged as a result of a user-initiated action, no action is required.

Execute the **ha dump** command to diagnose the problem.

If the problem persists, execute the **copy support** command and contact your switch service provider.

HASM-1102

Message `Heartbeat misses to <slot/partition> reached threshold.`

Message Type LOG

Severity INFO

Probable Cause Indicates that either the active management module Ethernet Media Access Controller (EMAC) or the indicated interface module is down. The active management module will run a diagnostic test on the EMAC and will wait for the interface module to reset it if it is down.

Recommended Action No action is required.

HASM-1103

Message `Heartbeat to <slot/partition> down.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the active management module has detected that the indicated interface module is down. This event may happen as a result of one of the following conditions: an operator-initiated action such as **firmware download**, if the interface module is reset or removed, or an error occurred in the interface module.

Recommended Action Monitor the interface module for a few minutes. If this message is due to reloading of the interface module, a message indicating heartbeat up will be displayed after the interface module has reloaded successfully.

If the interface module does not successfully connect to the active management module after 10 minutes, reload the interface module by ejecting the interface module and reseating it.

HASM-1104

Message `Heartbeat to <slot/partition> up.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the active management module has detected that the specified interface module is up. This message indicates that the interface module is ready to start up services and it is typically displayed when the interface module boots up.

Recommended Action No action is required. This message indicates that the interface module is healthy.

HASM-1105

Message `Switch bring-up timed out.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the system timed out during a reload or failover sequence, waiting for one or more programs to register with system services or to fail over to active status.

Recommended Action If the switch is in an inconsistent state, reload or power cycle the chassis. Before reloading the chassis, record the firmware version on the switch or management module and execute the **ha dump** command. If this is a dual-management module switch, gather the output from the management module in which this log message appeared.

HASM-1106

Message `Reset the standby management module.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the standby management module is being reset due to loss of heartbeat. This message is typically seen when the standby management module has been reloaded. Note that in certain circumstances a management module may experience a double reset and reload twice. A management module can recover automatically even if it has reloaded twice.

Recommended Action No action is required.

HASM-1107

Message `Take over the active management module.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a failover occurred and the standby management module takes over the active management module.

Recommended Action No action is required.

HASM-1108

Message `All service instances become active.`

Message Type LOG

Severity INFO

Probable Cause Indicates that all service instances became active. Active is an intermediate stage in the boot process.

Recommended Action No action is required.

HASM-1109

Message `The system is ready for configuration replay.`

Message Type LOG

Severity INFO

Probable Cause Indicates that all line cards (LCs) are online and the system is ready for configuration replay.

Recommended Action No action is required.

HASM-1110

Message `Configuration replay has completed on the system.`

Message Type LOG

Severity INFO

Probable Cause Indicates that configuration replay has completed.

Recommended Action No action is required.

HASM-1111

Message `Configuration replay has completed on <slot/partition>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that configuration replay has completed on the specified slot or partition.

Recommended Action No action is required.

HASM-1112

Message `<FC or MC> mode on standby, mismatch with active. Reload the standby for mode recovery.`

Message Type FFDC | LOG

Severity WARNING

Probable Cause Indicates that fabric cluster (FC) or management cluster (MC) mode conversion did not synchronize to the standby management module.

Recommended Action No action is required.

HASM-1120

Message `Current version <firwmare version string>.`

Message Type LOG | VCS

Severity INFO

Probable Cause Indicates the current firmware version string.

Recommended Action No action is required.

HASM-1121

Message `New version <firmware version string>.`

Message Type LOG | VCS

Severity INFO

Probable Cause Indicates the new firmware version string after firmware download.

Recommended Action No action is required.

HASM-1130

Message `The Ethernet PHY for slot <slot/partition> was reset successfully.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that there was no Ethernet connection between the active management module and the specified line card (LC). Subsequently, the PHY in the LC was reset automatically and the connection has been recovered.

Recommended Action No action is required.

HASM-1131

Message `reset the Ethernet PHY for slot <slot/partition> (<error code>>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that there was no Ethernet connection between the active management module and the specified line card (LC). The active management module attempted to recover the connection by resetting the PHY in the LC but failed.

Recommended Action Execute the **copy support** command and contact your switch service provider.

HASM-1132

Message `Reset the Ethernet PHY for slot <slot/partition> (<reset return code>>) on standby.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that there was no Ethernet connection between the standby management module and the specified line card (LC). The standby management module attempted to recover the connection by resetting the PHY in the LC.

Recommended Action Execute the **copy support** command and contact your switch service provider.

HASM-1200

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.

HASM-1201

Message `<Software component>:<Software component Process ID> failed to refresh (<Current time>:<Refresh time>, kill-<signal killed>).`

Message Type FFDC | LOG

Severity WARNING

Probable Cause Indicates that one of the 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.

HASM-1202

Message `Detected termination of hasmd process <HASM Process ID>.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the High Availability System Management (HASM) daemon has terminated unexpectedly.

Recommended Action Copy the warning message along with any core file information and contact your switch service provider.

HASM-1203

Message `Reboot timeout in ISSU, collect ha trace.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the blade node took too long to reboot in the In Service Software Upgrade (ISSU) process.

Recommended Action Execute the **copy support** command and contact your switch service provider.

HAWK Messages

HAWK-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 interface module or switch will be disrupted.

Recommended Action For a modular switch, execute the **power-off** and **power-on** commands to power cycle the interface module.

For a compact switch, reload or power cycle the switch.

HAWK-1003

Message `<test string>`

Message Type LOG

Severity WARNING

Probable Cause Indicates that too many loss of synchronizations are detected on the backplane port.

Recommended Action Verify that all switch fabric modules (SFMs) and line cards (LCs) are securely fastened.

HIL Messages

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 RPMs) has fallen below the minimum threshold.

Recommended Action Replace the fan field-replaceable unit (FRU). Refer to the *Hardware Reference Manual* of your switch for instructions to replace the fan FRU.

HIL-1301

Message `A 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 may overheat the switch.

Recommended Action Replace the affected fan FRU immediately. Refer to the *Hardware Reference Manual* of your switch for instructions to replace the fan FRU.

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 the switch. This message is often preceded by a low fan speed message.

Recommended Action Replace the affected fan FRUs immediately. Refer to the *Hardware Reference Manual* of your switch for instructions to replace the fan FRU.

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-1505

Message `High temperature (<measured temperature> C), fan speed increasing per environmental specifications.`

Message Type LOG

Severity INFO

Probable Cause Indicates that temperature in the system has risen above the warning threshold and the fan speed has been increased to prevent overheating of the system.

Recommended Action Execute the **show environment fan** command to verify that all fans are working properly.

Make sure that the area is well ventilated and the room temperature is within operational range of your switch. Refer to the *Hardware Reference Manual* of 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 temperature in the system has risen above the critical threshold.

Recommended Action Execute the **show environment fan** 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 the room temperature is within operational range of your switch. Refer to the *Hardware Reference Manual* of your switch for the operational temperature range.

HIL-1510

Message `Current temperature (<measured temperature> C) is below shutdown threshold. System shut down cancelled.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that temperature in the system has dropped below the critical threshold; the system will continue operation.

Recommended Action To help prevent future problems, execute the **show environment fan** command to verify all fans are working properly.

Make sure that the area is well ventilated and the room temperature is within operational range of your switch. Refer to the *Hardware Reference Manual* of your switch for the operational temperature range.

HIL-1511

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-1512

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-1521

Message `<Slot Identifier>, high temperature (<measured temperature>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the temperature of the specified interface module has risen above the warning threshold.

Recommended Action Execute the **show environment fan** command to verify that all 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* of your switch for the operational temperature range.

HIL-1522

Message `<Slot Identifier>, 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 the specified interface module has risen above the critical threshold. This usually follows a high temperature message.

Recommended Action Execute the **show environment fan** command to verify that all fans are working properly.

Make sure that the area is well ventilated and the room temperature is within operational range of your switch. Refer to the *Hardware Reference Manual* of your switch for the operational temperature range.

If the message persists, replace the interface module.

HIL-1523

Message `<Slot Identifier>, unit shutting down.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that the temperature of the specified interface module was above the maximum threshold for at least two minutes and therefore it has been shut down to prevent damage. This message usually follows a high temperature warning message.

Recommended Action Execute the **show environment fan** command to verify that all fans are working properly.

Make sure that the area is well ventilated and the room temperature is within the operational range of your switch. Refer to the *Hardware Reference Manual* of your switch for the operational temperature range.

If the message persists, replace the faulty interface module.

HIL-1524

Message `<Slot Identifier> is below shutdown threshold. Blade shut down cancelled.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the temperature of the specified interface module has dropped below the critical threshold; the system will continue operation.

Recommended Action To help prevent future problems, execute the **show environment fan** command to verify that all fans are working properly.

Make sure that the area is well ventilated and the room temperature is within operational range of your switch. Refer to the *Hardware Reference Manual* of your switch for the operational temperature range.

HIL-1605

Message `High temperature (<measured temperature> C), fan speed increasing per environmental specifications.`

Message Type LOG

Severity INFO

Probable Cause Indicates that temperature in the system has risen above the threshold and therefore the fan speed has been increased to prevent overheating of the system.

Recommended Action No action is required.

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 the Network 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 the Network 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>, RBridge = <rBridge 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 RBridge 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.

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 **copy support** command and contact your switch service provider.

HSL-1001

Message `Failed to acquire the system MAC address pool.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates the failure to acquire the system address. This error is caused by other system errors.

Recommended Action Execute the **show logging raslog** command to view the error log for other system errors and correct the errors.

HSL-1004

Message `Incompatible SFP transceiver 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-1006

Message `Failed to get the kernel page size <PageSize> bytes for the Memory Map (MMap).`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that there is not enough contiguous kernel memory.

Recommended Action Execute the **show logging raslog** command to view the error log for other system errors and correct the errors.

HSL-1009

Message `Failed to create Brocade trunk interface <InterfaceName>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates failure to create Brocade trunk because the hardware resources are exhausted.

Recommended Action Do not exceed the maximum trunk configuration allowed by the system.

HSL-1010

Message `Reached max VRBIDs usage, VRB-ID allocation failed in ASIC.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that maximum VRBIDs have been used.

Recommended Action No action is required.

HSL-1011

Message `Resource limit reached, <Number of resources to be freed.> resources are required for the virtual-fabric entry.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that maximum resources have been used.

Recommended Action No action is required.

HSL-1012

Message `Interface <DeviceName> is link up`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Layer 3 interface is up.

Recommended Action No action is required.

HSL-1013

Message `Interface <DeviceName> is link down`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Layer 3 interface is down.

Recommended Action No action is required.

HSL-1014

Message `Tunnel IVF/EVF tables in asic are <ExmUsage> percent full. Current usage = <ExmCurrentUsage>, Max number of entries = <ExmMaxEntries>`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that application-specific integrated circuit (ASIC) tables are close to full utilization.

Recommended Action Additional tunnel,VLAN provisioning will fail due to lack of resources.

HSL-1015

Message `Tunnel IVF/EVF tables in asic are <ExmUsage> percent full. Current usage = <ExmCurrentUsage>, Max number of entries = <ExmMaxEntries>`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that additional tunnel, VLAN can be provisioned.

Recommended Action No action is required.

HWK2 Messages

HWK2-1002

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 interface module or switch will be disrupted.

Recommended Action For a modular switch, execute the **power-off** and **power-on** commands to power cycle the interface module.

For a compact switch, reload or power cycle the switch.

HWK2-1003

Message `<test string>`

Message Type LOG

Severity WARNING

Probable Cause Indicates that too many loss of synchronizations are detected on the backplane port.

Recommended Action Verify that all switch fabric modules (SFMs) and line cards (LCs) are securely fastened.

IGMP Messages

IGMP-1001

Message `MsgQ enqueue failed (rc: <rc>).`

Message Type DCE

Severity ERROR

Probable Cause Indicates an internal inter-process communication (IPC) failure due to the scalability scenario.

Recommended Action Reduce the number of groups and MRouter ports.

IGMP-1002

Message `IPC with McastSS failed (message-id: <message-id>, rc: <rc>).`

Message Type DCE

Severity ERROR

Probable Cause Indicates an internal inter-process communication (IPC) failure due to the scalability scenario.

Recommended Action Reduce the number of groups and MRouter ports.

IGMP-1003

Message `MRouter eNS update from a VCS RBridge (ID:<rbid>) running lower firmware version.`

Message Type DCE

Severity ERROR

Probable Cause Indicates an older message update.

Recommended Action Upgrade the VCS RBridge firmware to the latest build.

IGMP-1004

Message `IGMP maximum VLANs enabled. Cannot enable IGMP on <vlan>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the number of VLANs on which Internet Group Multicast Protocol (IGMP) can be enabled has reached the maximum limit. Therefore, IGMP cannot be enabled on the specified VLAN.

Recommended Action No action is required.

IGMP-1005

Message `IGMP snooping enabled on total <vlan> VLANs. Maximum limit reached.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the number of VLANs on which Internet Group Multicast Protocol (IGMP) can be enabled has reached the maximum limit.

Recommended Action No action is required.

IGMP-1006

Message `IGMP snooping enabled on <vlan>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the Internet Group Multicast Protocol (IGMP) is enabled on a particular VLAN.

Recommended Action No action is required.

IPAD Messages

IPAD-1000

Message `IP Config change: Entity:<Type of managed entity>/<Instance number of managed entity> Interface:<Type of network interface>/<Instance number of network interface> Adresss family:<Protocol address family> Source of change:<Source of address change> Address:<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 LOG

Severity INFO

Probable Cause Indicates that the switch name has been changed.

Recommended Action No action is required.

IPAD-1003

Message `libipadm: <error message> <error message specific code>.`

Message Type LOG | FFDC

Severity ERROR

Probable Cause Indicates that the IP admin library has encountered an unexpected error.

Recommended Action Execute the **copy support** command and contact your switch service provider.

IPAD-1004

Message `Unable to set the host name due to /etc/hosts file corruption.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the */etc/hosts* file was inconsistent and it could not be recovered.

Recommended Action Execute the **copy support** command and contact your switch service provider.

IPAD-1005

Message `The /etc/hosts file was inconsistent but has been recovered successfully.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the */etc/hosts* file was inconsistent but it was recovered.

Recommended Action No action is required.

IPAD-1006

Message `Chassis name has been successfully changed to <Chassis name>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the chassis name has been changed.

Recommended Action No action is required.

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 **copy support** 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 **copy support** 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 **copy support** 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 **copy support** command and reload the switch. If the problem persists, contact your switch service provider.

L2AG Messages

L2AG-1001

Message `Linux socket error - error reason: <reason>, socket name: <sockname>, error name <errorname>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that an error has occurred in the Linux socket.

Recommended Action Reload or power cycle the switch.

L2AG-1002

Message `Initialization error : <reason>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the Layer 2 Agent (L2AGT) has encountered an error during initialization.

Recommended Action Reload or power cycle the switch.

L2AG-1003

Message `Message Queue Error : Message queue create failed.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the Layer 2 Agent (L2AGT) has encountered system service manager (SSM) message queue errors.

Recommended Action Reload or power cycle the switch.

L2AG-1004

Message `FDB error: Error in creating AVL tree.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the Layer 2 Agent (L2AGT) has encountered an error while initializing the AVL tree.

Recommended Action Reload or power cycle the switch.

L2AG-1005

Message `MAC-address-table hash failed even after two attempts for slot <slot> chip <chip>.`

Message Type DCE

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 Reload or power cycle the switch.

L2AG-1006

Message `MAC-address-table on slot <Slot_id> chip <Chip_id> is 95 percent full.`

Message Type DCE

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 **clear mac-address-table dynamic** command or wait until the old entries age out.

L2AG-1007

Message `MAC-address-table on slot <Slot_id> chip <Chip_id> is less than 90 percent full.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the media access control (MAC) address table is less than 90 percent full.

Recommended Action No action is required. The Layer 2 Agent (L2AGT) will start learning the entries.

L2AG-1008

Message `MAC-address-table on slot <Slot_id> chip <Chip_id> is 95 percent full [Dynamic/Static MAC's: <fdb_count>; ACL MAC's: <Acl_count>].`

Message Type DCE

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 **clear mac-address-table dynamic** command or wait until the old entries age out.

L2AG-1009

Message `L2 H/W tables have reached capacity. Few ACL/MAC entries may not be configured in H/W, resulting in flooding.`

Message Type DCE

Severity INFO

Probable Cause Indicates that some of the Layer 2 hardware tables are full.

Recommended Action Clear some of the entries using the **clear mac-address-table dynamic** command or wait until the old entries age out.

L2AG-1010

Message `ERROR: Mac Vlan Classification table is Full. Add Failed for Vlan <ivid> Mac <mac1>:<mac2>:<mac3>:<mac4>:<mac5>:<mac6> on <ifname>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the Layer 2 classifier hardware table is full.

Recommended Action Remove the existing MAC VLAN entries and reconfigure.

L2AG-1011

Message `Mgr-Agt Checksum Mismatch reached the threshold for Slot:<slot-id>. Requesting the MAC Refresh from L2 Manager.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the MAC entries may be out of synchronization between the Layer 2 Manager and the Layer 2 Agent.

Recommended Action No action is required.

L2AG-1012

Message `FDB Programming is done for Slot:<slot-id>. Sending Fabric Ready to NSM via L2 Manager.`

Message Type DCE

Severity INFO

Probable Cause Indicates that all the forwarding databases (FDBs) are programmed in exm table. Sending the Fabric Ready notification to network service module (NSM) through Layer 2 Manager.

Recommended Action No action is required.

L2SS Messages

L2SS-1001

Message `Linux socket error - error reason: <reason>, socket name: <sockname>, error name <errorname>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that an error has occurred in the Linux socket.

Recommended Action Reload or power cycle the switch.

L2SS-1002

Message `Initialization error: <reason>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the Layer 2 system (L2SYS) has encountered an error during initialization.

Recommended Action Reload or power cycle the switch.

L2SS-1003

Message `Message Queue Error: Failed to create a Message Queue.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the Layer 2 system (L2SYS) has encountered system service manager (SSM) message queue errors.

Recommended Action Reload or power cycle the switch.

L2SS-1004

Message `FDB error: Error in creating the AVL tree.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the Layer 2 system (L2SYS) has encountered an error while initializing the AVL tree.

Recommended Action Reload or power cycle the switch.

L2SS-1005

Message `MAC-address-table hash failed even after two attempts for slot <slot> chip <chip>.`

Message Type DCE

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 Reload or power cycle the switch.

L2SS-1006

Message `MAC-address-table is 95 percent full.`

Message Type DCE

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 **clear mac-address-table dynamic** 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 DCE

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) will start learning the entries.

L2SS-1008

Message `Adding Internal MAC <mac1>:<mac2>:<mac3>:<mac4>:<mac5>:<mac6> VID <Vid> as a static MAC.`

Message Type DCE

Severity INFO

Probable Cause Indicates that a static media access control (MAC) is overriding an internal MAC entry (VRRP/SVI).

Recommended Action No action is required.

L2SS-1009

Message `Fabric-wide Layer 2 flush command issued.`

Message Type DCE

Severity INFO

Probable Cause Indicates that a fabric-wide Layer 2 flush command is issued and the entire Layer 2 forwarding table will be cleared.

Recommended Action No action is required.

L2SS-1010

Message `Fabric-wide l2 flush completed, status - <command status>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the entire Layer 2 forwarding table has been cleared.

Recommended Action No action is required.

L2SS-1011

Message `Security violation occured on interface <Ifname> with Mac <mac1><mac2>.<mac3><mac4>.<mac5><mac6> Vlan <vid>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the number of Media Access Control (MAC) addresses allowed on the specified interface has reached the maximum limit. Based on the configured action, the interface is either shut down or the MAC learning is restricted.

Recommended Action No action is required.

L2SS-1012

Message `Failed to create Tunnel <Ifid>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that tunnel creation was unsuccessful.

Recommended Action Technical support is required.

L2SS-1013

Message `Failed to delete Tunnel <Ifid>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that tunnel deletion was unsuccessful.

Recommended Action Technical support is required.

L2SS-1014

Message `Failed to handle Tunnel-Vlan association, Tunnel <Ifid> not found.`

Message Type DCE

Severity INFO

Probable Cause Indicates that tunnel VLAN association handling was unsuccessful.

Recommended Action Technical support is required.

L2SS-1015

Message `Failed to handle Tunnel-Vlan disassociation, Tunnel <Ifid> not found.`

Message Type DCE

Severity INFO

Probable Cause Indicates that tunnel VLAN disassociation handling was unsuccessful.

Recommended Action Technical support is required.

L2SS-1016

Message `Failed to associate Tunnel <Ifid> to Vlan <Vid>, Vlan not present.`

Message Type DCE

Severity INFO

Probable Cause Indicates that tunnel VLAN association was unsuccessful.

Recommended Action Technical support is required.

L2SS-1017

Message `Failed to disassociate Tunnel <Ifid> from Vlan <Vid>, Vlan not present.`

Message Type DCE

Severity INFO

Probable Cause Indicates that tunnel VLAN disassociation was unsuccessful.

Recommended Action Technical support is required.

L2SS-1018

Message `Failed to configure Remote VM MAC <mac1><mac2>.<mac3><mac4>.<mac5><mac6> for Tunnel <ifid> on Vlan <vid>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that configuring remote Virtual Machine (VM) Media Access Control (MAC) on the tunnel was unsuccessful.

Recommended Action Technical support is required.

L2SS-1019

Message `Failed to remove Remote VM MAC <mac1><mac2>.<mac3><mac4>.<mac5><mac6> for Tunnel <ifid> on Vlan <vid>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that removing remote Virtual Machine (VM) Media Access Control (MAC) on the tunnel was unsuccessful.

Recommended Action Technical support is required.

L2SS-1020

Message `MAC move detected across interface(s) <InterfaceList> for MAC <mac1>:<mac2>:<mac3>:<mac4>:<mac5>:<mac6>, VLAN <Vlan ID>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the MAC address is flapping across multiple interfaces.

Recommended Action No action is required.

L2SS-1021

Message `Rate limiting frequent MAC move detection logs. No more logs will be reported.`

Message Type DCE

Severity INFO

Probable Cause Indicates that MAC move logging has been stopped to avoid flooding.

Recommended Action Use "mac-move-detect log reset-count" to know if MAC moves are still happening

L2SS-1022

Message `MAC move detection and Virtual fabric can not co-exist. Disabling MAC move.`

Message Type DCE

Severity INFO

Probable Cause Indicates that Virtual fabric was enabled after enabling MAC move detection.

Recommended Action Disable Virtual fabric to enable MAC move detection again.

L2SS-1023

Message `ENS Checksum Mismatch reached maximum threshold(<max_threshold>) for Rbridge:<rbridge-id>. Requesting MAC refresh from Rbridge:<rbridge-id>.`

Message Type DCE

Severity WARNING

Probable Cause Indicates that the MAC entries may be out of synchronization with the specified RBridge.

Recommended Action No action is required.

L2SS-1024

Message `Repeated mac move detected for Mac <mac1><mac2>.<mac3><mac4>.<mac5><mac6> Vlan <vid>, interface <Ifname> shut down.`

Message Type DCE

Severity INFO

Probable Cause Indicates port shut down due to repeated mac move.

Recommended Action No action is required.

L2SS-1025

Message `Shut down recovery for interface <interface>`

Message Type DCE

Severity INFO

Probable Cause Indicates port shut recover due to multiple ports getting shut.

Recommended Action No action is required.

L2SS-1026

Message `Edge Loop Detection (ELD) has triggered mac-address-table refresh`

Message Type DCE

Severity INFO

Probable Cause Indicates that Edge Loop Detection (ELD) has detected loop and triggered mac-address-table refresh.

Recommended Action No action is required.

L2SS-1027

Message `Edge Loop Detection (ELD) has triggered mac-address-table refresh for interface <interface>`

Message Type DCE

Severity INFO

Probable Cause Indicates that Edge Loop Detection (ELD) has detected loop and triggered mac-address-table refresh for specified interface.

Recommended Action No action is required.

L2SS-1028

Message `Received Join Done Message from FabVCS.`

Message Type DCE

Severity INFO

Probable Cause Indicates that Join Done message has been received from the Fabric Services Virtual Cluster Switching (FVCS). Process the message and send an update to the Layer 2 Agent to program all the forwarding database (FDB) entries.

Recommended Action No action is required.

L2SS-1029

Message `Notify NSM about Fabric Ready.`

Message Type DCE

Severity INFO

Probable Cause Indicates that Join Done message has been received from all the slots. Sending Fabric Ready notification to the network service module (NSM).

Recommended Action No action is required.

L2SS-1030

Message `Sending the Join Done message to Slot: <slot-id>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that Join Done message has been received from the Fabric Services Virtual Cluster Switching (FVCS). Notifying the specified slot about the Join Done message.

Recommended Action No action is required.

L2SS-1031

Message `Received Join done response message from Slot:<slot-id>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that Join Done response message has been received from the specified slot. Sending Fabric Ready notification to the network service module (NSM), if response is received from all the slots.

Recommended Action No action is required.

L2SS-1032

Message `ENS Checksum Mismatch reached maximum threshold(<max_threshold>) for Rbridge:<rbridge-id>. Requesting MAC refresh from Rbridge:<rbridge-id>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the MAC entries may be out of synchronization with the specified RBridge.

Recommended Action No action is required.

L2SS-1033

Message `Mac Authentication is enabled for interface <Ifname>`

Message Type DCE

Severity INFO

Probable Cause Indicates that a port is enabled for MAC authentication.

Recommended Action No action is required.

L2SS-1034

Message `Mac Authentication is disabled for interface <Ifname>`

Message Type DCE

Severity INFO

Probable Cause Indicates that a port is disabled for MAC authentication.

Recommended Action No action is required.

L2SS-1035

Message `Mac loop detection algorithm has chosen interface <Ifname> has candidate for shutdown`

Message Type DCE

Severity INFO

Probable Cause Indicates port is probable candidate for which is causing loop.

Recommended Action No action is required.

LACP Messages

LACP-1001

Message `<module> Error opening socket (<error>).`

Message Type DCE

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 version using the **firmware download** command.

LACP-1002

Message `<message> <message>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that an error occurred in the Link Aggregation Control Protocol (LACP) daemon.

Recommended Action Take action specific to the error message.

LACP-1003

Message `Port-channel <PortChannelKey> up in defaulted state.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified port channel is up in the defaulted state.

Recommended Action No action is required.

LACP-1004

Message `Port-channel <PortChannelKey> down from defaulted state.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified port channel is down from the defaulted state.

Recommended Action No action is required.

LACP-1005

Message `vLAG multiple partners detected on Port-channel <PortChannelKey> .`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the specified virtual link aggregation group (vLAG) is connected to multiple partners across the VCS.

Recommended Action No action is required.

LIC Messages

LIC-1001

Message `Out of memory in module <Function name>.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that an unexpected internal memory allocation failure has occurred.

Recommended Action Try the operation again. If this operation fails, reload or fail over the switch.

LIC-1015

Message `Failed to read License Identifier from hardware. Licenses will be invalid. (error code=<Number>)`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates that access to World Wide Name (WWN) card has failed.

Recommended Action Reload or power cycle the switch, or replace the platform hardware.

LOG Messages

LOG-1000

Message `Previous message has repeated <repeat count> times.`

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 **copy support** command and contact your switch service provider.

LOG-1002

Message `A log message was not recorded.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a log 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 **copy support** command and contact your switch service provider.

LOG-1003

Message `SYSTEM error log has been cleared.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the persistent system 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 WARNING

Probable Cause Indicates that the specified message has been flooding and was blocked.

Recommended Action Reload the switch. If the message persists, execute the **copy support** 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 `DCE error log has been cleared.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the persistent DCE error log has been cleared.

Recommended Action No action is required.

LOG-1008

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-1009

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-1010

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 message has been enabled for syslog logging.

Recommended Action No action is required.

LOG-1011

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 message has been disabled from syslog logging.

Recommended Action No action is required.

LOG-1012

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.

LOG-1013

Message `Log message <Log message ID that has been enabled to generate a raslog> is re-enabled, <Number of message were blocked before re-neable.> messages were blocked before the re-enabled.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a message has been flooded and has been blocked. Now its re-enabled to generate raslog.

Recommended Action No action required.

LSDB Messages

LSDB-1001

Message `Link State ID <link state ID> out of range.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified link state database ID is out of the acceptable range. The valid *link state ID* is the same as the valid RBridge ID, whose range is 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 the local link state database reached the maximum incarnation.

An "incarnation" is a progressive number that identifies the most recent version of the link state record (LSR). The switch generates its local link state record 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, RBridge <local RBridge>.`

Message Type FFDC | LOG

Severity CRITICAL

Probable Cause Indicates that there is no local link state record (LSR) entry in the link state database. 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 LSR. The switch generates its local LSR when first enabled. By disabling and enabling the switch, a new local link state record is generated.

Recommended Action Execute the **chassis disable** and **chassis enable** commands. A new local link state record is generated during the switch enable.

LSDB-1004

Message `No Link State Record for RBridge <local RBridge>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates there is no link state record (LSR) for the specified local RBridge.

Recommended Action No action is required. The other switch will pass the LSR after the fabric is stable.

MCST Messages

MCST-1001

Message `Socket Error: <op> (<reason>) for socket <sockname> the error code<errorname>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that an error has occurred in the Linux socket.

Recommended Action Reload or power cycle the switch.

MCST-1002

Message `Socket Error: <op> sock name <sock> Error <error> type <type> seq <seq> pid <pid>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the specified error has occurred while processing the hardware abstraction layer (HAL) message.

Recommended Action Reload or power cycle the switch.

MCST-1003

Message `Learning error: <op> (<reason>) - VLAN <vid> MAC/group <address>.`

Message Type DCE

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 Reload or power cycle the switch.

MCST-1004

Message `NSM error: <op> (<reason>) for VLAN <vid> port <port>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the multicast subsystem (mcast_ss) has encountered an error during a network service module (NSM) event.

Recommended Action Reload or power cycle the switch.

MCST-1005

Message `Message error: Invalid message type <type> expecting <value1> or <value2> or <value3>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the type of the message received from the driver is invalid.

Recommended Action Reload or power cycle the switch.

MCST-1006

Message `Message error: <op> (<reason>)Invalid message length <length> expecting <length1>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the length of the message received from the driver is invalid.

Recommended Action Reload or power cycle the switch.

MCST-1007

Message `Initialization error: <op> (<reason>).`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the multicast subsystem (mcast_ss) has encountered an error during initialization.

Recommended Action Reload or power cycle the switch.

MCST-1008

Message `HAL error: <op> (<reason>) - VLAN <vid> MAC/group <address>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the multicast subsystem (mcast_ss) has encountered the hardware abstraction layer (HAL) errors.

Recommended Action Reload or power cycle the switch.

MCST-1009

Message `L2SS error: <op> (<reason>) VLAN <vid> MAC <mac address>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the multicast subsystem (mcast_ss) has encountered the Layer 2 subsystem (L2SS) related errors.

Recommended Action Reload or power cycle the switch.

MCST-1010

Message `Message Queue error: <op> (<reason>) TYPE <type>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the multicast subsystem (mcast_ss) has encountered the message queue errors.

Recommended Action Reload or power cycle the switch.

MCST-1011

Message `IDB error: <op> (<reason>) port index <port-index> not found for VLAN ID <vlan-id>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the specified port index is invalid.

Recommended Action If there is an impact on the data path, reload or power cycle the switch. Refer to the *Network OS Administrator's Guide* for instructions to verify the data path.

MCST-1012

Message `IDB error: <op> (<reason>) VLAN ID <vid> not found.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the specified VLAN ID (VID) is invalid.

Recommended Action If there is an impact on the data path, reload or power cycle the switch. Refer to the *Network OS Administrator's Guide* for instructions to verify the data path.

MCST-1013

Message `Snooping DB error: <op> (<reason>) Group not found - VLAN <vid> group <group address>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the group address lookup for the specified VLAN has failed.

Recommended Action Reload or power cycle the switch.

MCST-1014

Message `Snooping DB error: <op> (<reason>) MAC not found - VLAN <vid> MAC-addr <MAC address>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the media access control (MAC) address lookup for the specified VLAN has failed.

Recommended Action Reload or power cycle the switch.

MCST-1015

Message `HSL error: <op> (<reason>) failed for message <message> VLAN <vid> MAC <MAC address> mgid <mgid> CPU <cpu>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the specified hardware subsystem layer (HSL) related operation has failed.

Recommended Action Reload or power cycle the switch.

MCST-1016

Message `Message error: <op> (<reason>) <length> (<length1>).`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the length of the message received from the driver is invalid.

Recommended Action Reload or power cycle the switch.

MCST-1017

Message `Learning error: <op> (<reason>) Invalid number <port> for ifindex <ifindex>.`

Message Type DCE

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 Reload or power cycle the switch.

MCST-1018

Message `Memory Alloc Error: <op> (<reason>) type <memtype>/<memsize>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the multicast subsystem (mcast_ss) has encountered an error during the memory allocation.

Recommended Action Reload or power cycle the switch.

MCST-1019

Message `Ptree Error: <op> (<reason>) VLAN <vid> MAC/group <address>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the multicast subsystem (mcast_ss) has encountered an error during the Ptree operation.

Recommended Action Reload or power cycle the switch.

MCST-1020

Message `List Error: <op> (<reason>) VLAN <vid> MAC <mac address> group <group address>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the multicast subsystem (mcast_ss) has encountered an error during the List operation.

Recommended Action Reload or power cycle the switch.

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 |

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 |

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 |

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 |

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 |

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 |

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 |

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 |

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 |

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 |

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 |

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 |

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 |

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 |

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 |

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 |

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 |

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 |

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 |

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 |

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 |

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 |

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 |

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 |

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 |

Severity WARNING

Probable Cause Indicates that the dashboard has been cleared.

Recommended Action No action is required.

MAPS-1204

Message `MAPS has started monitoring.`

Message Type LOG |

Severity INFO

Probable Cause Indicates that MAPS has started monitoring the system.

Recommended Action Make sure the configuration change is expected.

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 VDX 2740 switch.

Recommended Action Execute the **copy support** 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 the 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 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.

MS Messages

MS-1021

Message `MS WARMBOOT failure (FSS_MS_WARMINIT failed. Reason=<failure reason>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates that fabric synchronization service (FSS) warm recovery failed during the warm initialization phase of the switch reload.

Recommended Action If the message persists, execute the **copy support** command and contact your switch service provider.

MSTP Messages

MSTP-1001

Message `<message>: <message>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the system has failed to allocate memory.

Recommended Action Check the memory usage on the switch using the **show process memory** command.

Reload or power cycle the switch.

MSTP-1002

Message `<message>: <message>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the system has failed to initialize.

Recommended Action Reload or power cycle the switch.

MSTP-1003

Message `<message>: <message>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates a connection, transfer, or receiving error in the socket.

Recommended Action If this is a modular switch, execute the **ha failover** command. If the problem persists or if this is a compact switch, download a new firmware version using the **firmware download** command.

MSTP-1004

Message `Received BPDU on PortFast enable port. Shutting down Interface <message>`

Message Type DCE

Severity ERROR

Probable Cause Indicates that a port on which PortFast is enabled has received a bridge protocol data unit (BPDU). The port has been disabled.

Recommended Action Disable the PortFast feature on the port using one of the following commands:

- For Rapid Spanning Tree Protocol (RSTP), execute the **no spanning-tree edgeport** command.
- For Spanning Tree Protocol (STP), execute the **no spanning-tree portfast** command.

After disabling the PortFast feature, execute the **no shutdown** command to re-enable the port.

MSTP-2001

Message `<message>.`

Message Type DCE

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 DCE

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 DCE

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 DCE

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 DCE

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> bridge priority is changed from <priority_old> to <priority_new>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified Multiple Spanning Tree Protocol (MSTP) instance priority has been modified.

Recommended Action No action is required.

MSTP-3001

Message `Could not restore spanning tree protocol settings from startup-config. Spanning tree is configured in shutdown state.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that allocation of logical bridge ID has failed. The VCS cluster formation could be in progress.

Recommended Action Wait for cluster formation to complete and then enable the Spanning Tree Protocol using the **no spanning-tree shutdown** command. You may have to execute the **shutdown** command followed by the **no shutdown** command from protocol spanning-tree submode.

MSTP-3002

Message `Could not restore spanning tree state for interface <ifName>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that allocation of logical port ID has failed. The VCS cluster formation could be in progress.

Recommended Action Wait for cluster formation to complete and then enable the spanning tree on the interface. You may have to execute the **spanning-tree shutdown** command followed by the **no spanning-tree shutdown** command from interface submode.

MSTP-3003

Message `Could not restore spanning tree state for interface <ifName>. Maximum port count reached.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the system ran out of port ID space, probably due to stale entries in the system. The maximum port count for STP and PVST is 1 through 255, and for RSTP, MSTP, and RPVST the maximum port count is 1 through 4095.

Recommended Action Shut down spanning tree on interfaces that are no longer required using the **spanning-tree shutdown** command and try the operation again.

NBFS Messages

NBFS-1001

Message `Duplicate E_Port SCN from interface <interface name> (<interface index>) 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:

- NB_ST_DOWN - The neighbor is down.
- NB_ST_INIT - The neighbor is initializing.
- NB_ST_DB_EX - The neighbor and the switch are exchanging data from their link state record (LSR) databases.
- NB_ST_DB_ACK_WT - The neighbor is waiting for the switch to acknowledge the LSR database.
- NB_ST_DB_WT - The LSR database is in the waiting state; synchronization is in process.
- NB_ST_FULL - The neighbor is in the finishing state.

Recommended Action No action is required.

NBFS-1002

Message `Wrong input: <state name> to neighbor FSM, state <current state name>, interface <interface name> (<interface index>).`

Message Type FFDC | LOG

Severity ERROR

Probable Cause Indicates that a wrong input was sent to the neighbor finite state machine (NBFSM). NBFSM states are as follows:

- NB_ST_DOWN - The neighbor is down.
- NB_ST_INIT - The neighbor is initializing.
- NB_ST_DB_EX - The neighbor and the switch are exchanging data from their link state record (LSR) databases.
- NB_ST_DB_ACK_WT - The neighbor is waiting for the switch to acknowledge the LSR database.
- NB_ST_DB_WT - The LSR database is in the waiting state; synchronization is in process.
- NB_ST_FULL - The neighbor is in the finishing state.

If this error occurs repeatedly, then there is a problem in the protocol implementation between two switches.

Recommended Action Execute the **show fabric route neighbor-state** command to check the neighbor state of the port listed in the message. If the neighbor state is NB_ST_FULL, then this message can safely be ignored. Otherwise, execute the **shutdown** and **no shutdown** commands to reset the port.

NBFS-1003

Message `DB_XMIT_SET flag not set in state <current state name>, input <state name>, interface <interface name> (<interface index>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that 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:

- NB_ST_DOWN - The neighbor is down.
- NB_ST_INIT - The neighbor is initializing.
- NB_ST_DB_EX - The neighbor and the switch are exchanging data from their link state record (LSR) databases.
- NB_ST_DB_ACK_WT - The neighbor is waiting for the switch to acknowledge the LSR database.
- NB_ST_DB_WT - The LSR database is in the waiting state; synchronization is in process.
- NB_ST_FULL - The neighbor is in the finishing state.

Recommended Action No action is required. The Network OS automatically recovers from this problem.

NBFS-1004

Message `Wrong input: <state name> to neighbor FSM, state <current state name>, interface <interface name> (<interface index>).`

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 **show fabric route neighbor-state** 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, toggle the interface by using the **shutdown** and **no shutdown** commands to refresh the port.

NBFS-1005

Message `FSPF experiencing link issues on interface <interface name> (<interface index>) in state <current state name> (<state change number>).`

Message Type LOG

Severity INFO

Probable Cause Indicates that fabric shortest path first (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 **show fabric route neighbor-state** command to check the neighbor state of the port listed in the message. If the state is Full, then this message can safely be ignored. Otherwise, please check the **show interface stats brief** 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 any faulty or bad equipment such as cables or optics.

NBFS-1006

Message `FSPF link dead timer expired on interface <interface name> (<interface index>) in state <state name> (<state number>).`

Message Type LOG

Severity INFO

Probable Cause Indicates that the link's FSPF dead timer has expired due to not receiving any of the appropriate inter-switch FSPF control frames.

Includes the current state of the link's neighbor finite state machine (NBFSM). The reported state indicates where in the FSPF synchronization protocol the link was when the timer expired and the link was reset. The possible state values are:

- 0 - Down
- 1 - Init
- 2 - Database Exchange
- 3 - Database Acknowledge Wait
- 4 - Database Wait
- 5 - Full

When a link's dead timer expires, the link and all its trunk members are bounced. This forces the link to either reform or stay offline if the neighbor is not ready to bring up the link yet.

Recommended Action

Run the **show fabric isl** and **show fabric route neighbor-state** commands to check the current state of the link. If the link is in the Full state, then this message can safely be ignored as the link has recovered. Otherwise, toggle the interface by using the **shutdown** and **no shutdown** commands to refresh the port. If the problem is observed more than once, there may be problems with the optics and/or cables and may need to be replaced.

NS Messages

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 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, administrators can check and remove devices with a duplicated WWN.

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-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-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 DCE

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 DCE

Severity INFO

Probable Cause Indicates that the specified interface has gone offline because one of the protocol dependency is unresolved.

Recommended Action Check for the reason codes using the **show interface** command and resolve the protocol dependencies.

NSM-1003

Message `Interface <InterfaceName> is link down.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified interface has gone offline because the link was down.

Recommended Action Check whether the connectivity is proper and the remote link is up.

NSM-1004

Message `Interface <InterfaceName> is created.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified logical interface has been created.

Recommended Action No action is required.

NSM-1007

Message `Chassis is <status>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the chassis has been enabled or disabled.

Recommended Action No action is required.

NSM-1009

Message `Interface <InterfaceName> is deleted.`

Message Type DCE

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 DCE

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 DCE

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 DCE

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 DCE

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 DCE

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 DCE

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 DCE

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 DCE

Severity INFO

Probable Cause Indicates that the specified 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 DCE

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 DCE

Severity INFO

Probable Cause Indicates that the interface administrative status has changed to up.

Recommended Action No action is required.

NSM-1020

Message `Interface <InterfaceName> is administratively down.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the interface administrative status has changed to down.

Recommended Action No action is required.

NSM-1021

Message `Interface IP overlap with management IP <ipAddr> ifname:<ifname>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the IP address configured on the interface overlaps with the management IP address.

Recommended Action Change the interface IP address using the **ip address** command.

NSM-1022

Message `FCoE configuration has been <Option> on interface <InterfaceName>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the Fibre Channel over Ethernet (FCoE) configuration has been enabled or disabled on the specified interface.

Recommended Action No action is required.

NSM-1023

Message `RBridge ID <RBridgeId> has joined Port-channel <PortChannelKey>. Port-channel is a vLAG with RBridge IDs <RBridgeList>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified RBridge has joined the virtual link aggregation group (vLAG).

Recommended Action No action is required.

NSM-1024

Message `RBridge ID <RBridgeId> has left Port-channel <PortChannelKey>. Port-channel is a vLAG with RBridge IDs <RBridgeList>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified RBridge has left the virtual link aggregation group (vLAG).

Recommended Action No action is required.

NSM-1025

Message `RBridge ID <RBridgeId> has left Port-channel <PortChannelKey>. Port-channel has only RBridge ID <RbridgeList> and is no longer a vLAG.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the virtual link aggregation group (vLAG) no longer exists.

Recommended Action No action is required.

NSM-1026

Message `<SFPType> transceiver for interface <InterfaceName> is inserted.`

Message Type DCE

Severity INFO

Probable Cause Indicates that a (SFP/CFP2) transceiver has been inserted in the specified interface.

Recommended Action No action is required.

NSM-1027

Message `<SFPType> transceiver for interface <InterfaceName> is removed.`

Message Type DCE

Severity INFO

Probable Cause Indicates that a transceiver (SFP or CFP2) has been removed from the specified interface.

Recommended Action No action is required.

NSM-1028

Message `Incompatible SFP transceiver for interface <InterfaceName> is detected.`

Message Type DCE

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.

NSM-1029

Message `Failed to read SFP transceiver for interface <InterfaceName>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates failure to read the small form-factor pluggable (SFP) transceiver for 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.

NSM-1030

Message `Interface <InterfaceName> is administratively down due to speed mismatch in port-channel.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified interface has gone down due to mismatching speed in the port-channel.

Recommended Action Set the correct speed for the interface using the **speed** command.

NSM-1031

Message `Session <SessionNumber> is created.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified session has been created.

Recommended Action No action is required.

NSM-1032

Message `Session <SessionNumber> is deleted.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified session has been deleted.

Recommended Action No action is required.

NSM-1033

Message `Session <SessionNumber> configuration is deleted.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified session configuration has been deleted.

Recommended Action No action is required.

NSM-1034

Message `Session <SessionNumber> configuration is added.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified session configuration has been added.

Recommended Action No action is required.

NSM-1035

Message `Description for Session <SessionNumber> is added.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the session description has been added.

Recommended Action No action is required.

NSM-1036

Message `Description for Session <SessionNumber> is deleted.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the session description has been deleted.

Recommended Action No action is required.

NSM-1037

Message `Interface <InterfaceName> is administratively down due to <LinkSpeed> link configured on Brocade Trunk.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified interface has gone down because a 1 Gbps link has been configured on the Brocade trunk.

Recommended Action Remove the 1 Gbps link from the Brocade trunk or change the 1 Gbps small form-factor pluggable (SFP) transceiver.

NSM-1038

Message `Private VLAN mode changed from <Mode_old> to <Mode_new> for interface <InterfaceName>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the interface private VLAN mode has been changed.

Recommended Action No action is required.

NSM-1039

Message `Unsupported Brocade-branded SFP transceiver for interface <InterfaceName> is detected.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that an unsupported Brocade-branded small form-factor pluggable (SFP) transceiver has been inserted in the specified interface.

Recommended Action Use a Brocade-branded SFP transceiver for the interface because the digital diagnostics will not be supported.

NSM-1040

Message `Interface <InterfaceName> is unprovisioned.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified logical interface has been unprovisioned.

Recommended Action No action is required.

NSM-1041

Message `Interface <InterfaceName> is provisioned.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified logical interface has been provisioned.

Recommended Action No action is required.

NSM-1042

Message `Unqualified SFP transceiver for interface <InterfaceName> is detected.`

Message Type DCE

Severity WARNING

Probable Cause Indicates that an unqualified Brocade-branded small form-factor pluggable (SFP) transceiver has been inserted in the specified interface.

Recommended Action Use a qualified Brocade-branded SFP transceiver for the interface because the digital diagnostics will not be supported.

NSM-1043

Message `Unsupported SFP transceiver for interface <InterfaceName> is detected.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that an unsupported small form-factor pluggable (SFP) transceiver has been inserted in the specified interface.

Recommended Action Use a qualified Brocade-branded SFP transceiver for the interface because the digital diagnostics will not be supported.

NSM-1044

Message `IP unnumbered intf <InterfaceName> vrf must be same as donor inttf <InterfaceName>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that IP unnumbered interface Virtual Routing and Forwarding (VRF) is not same as the donor interface VRF.

Recommended Action Make sure that both unnumbered interface VRF and donor interface VRF are same.

NSM-1045

Message `<SFPType> transceiver for interface <InterfaceName> is inserted.`

Message Type DCE

Severity INFO

Probable Cause Indicates that a transceiver (SFP or CFP2) has been inserted in the specified interface.

Recommended Action No action is required.

NSM-1046

Message `<SFPType> transceiver for interface <InterfaceName> is removed.`

Message Type DCE

Severity INFO

Probable Cause Indicates that a transceiver (SFP or CFP2) has been removed from the specified interface.

Recommended Action No action is required.

NSM-1047

Message `Port-channel configuration change made during maintenance-mode is not supported.`

Message Type DCE

Severity WARNING

Probable Cause Indicates that maintenance mode is entered.

Recommended Action Make sure that the port-channel configuration is not changed during maintenance mode.

NSM-1048

Message `If port-channel config changes were made while in maintenance-mode, please remove and reconfigure the port-channel and member intf.`

Message Type DCE

Severity WARNING

Probable Cause Indicates that maintenance mode is exited.

Recommended Action If port-channel configuration changes were made while in maintenance mode, then remove and reconfigure the port-channel and member interface.

NSM-1700

Message `Tunnel <TunnelName> creation failed.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the tunnel creation was unsuccessful.

Recommended Action Technical support is required.

NSM-1701

Message `VNI mapping for VLAN <VLAN> was unsuccessful.`

Message Type DCE

Severity INFO

Probable Cause Indicates that system could not map VNI to the VLAN for a VxLAN tunnel.

Recommended Action Technical support is required.

NSM-1702

Message `Enabling flooding for <TunnelName> was unsuccessful.`

Message Type DCE

Severity INFO

Probable Cause Indicates that system could not enable flooding for the specific tunnel.

Recommended Action Technical support is required.

NSM-2000

Message `Port-profile <ProfileName> activation succeeded.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the profile activation was successful.

Recommended Action No action is required.

NSM-2001

Message `Port-profile <ProfileName> activation failed, reason <Reason>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the profile activation was unsuccessful.

Recommended Action Check the configuration and port-profile status using the **show port-profile status** command. Execute the **copy support** command and contact your switch service provider.

NSM-2002

Message `Port-profile <ProfileName> deactivation succeeded.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the profile deactivation was successful.

Recommended Action No action is required.

NSM-2003

Message `Port-profile <ProfileName> deactivation failed, reason <Reason>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the profile deactivation was unsuccessful.

Recommended Action Check the configuration and port-profile status using the **show port-profile status** command. Execute the **copy support** command and contact your switch service provider.

NSM-2004

Message `Port-profile <ProfileName> application succeeded on <InterfaceName>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the profile application was successful.

Recommended Action No action is required.

NSM-2005

Message `Port-profile <ProfileName> application failed on <InterfaceName>, reason <Reason>, removing any applied configuration.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the profile application on the specified interface was unsuccessful.

Recommended Action Check the configuration and port-profile status using the **show port-profile status** command. Execute the **copy support** command and contact your switch service provider.

NSM-2006

Message `Port-profile <ProfileName> removed successfully on <InterfaceName>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified port-profile has been removed successfully.

Recommended Action No action is required.

NSM-2007

Message `Interface <InterfaceName> became port-profile-port.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the port-profile configuration mode has been enabled on the specified interface using the **port-profile-port** command.

Recommended Action No action is required.

NSM-2008

Message `Interface <InterfaceName> became non-port-profile-port.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the port-profile configuration mode has been disabled on the specified interface using the **no port-profile-port** command.

Recommended Action No action is required.

NSM-2010

Message `Interface <InterfaceName> could not become non-port-profile-port.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the port-profile configuration mode could not be disabled on the specified interface using the **no port-profile-port** command.

Recommended Action Check the configuration and port-profile status using the **show port-profile status** command. Execute the **copy support** command and contact your switch service provider.

NSM-2011

Message `Port-profile <ProfileName> removal failed on <InterfaceName>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the specified port-profile could not be removed.

Recommended Action Execute the **copy support** command and contact your switch service provider.

NSM-2012

Message `MAC <ProfileMac> is associated to port-profile <ProfileName>.`

Message Type DCE

Severity INFO

Probable Cause Indicates successful association of the Virtual Machine (VM) Media Access Control (MAC) address with the specified port-profile.

Recommended Action No action is required.

NSM-2013

Message `MAC <ProfileMac> is disassociated from port-profile <ProfileName>.`

Message Type DCE

Severity INFO

Probable Cause Indicates successful disassociation of the Virtual Machine (VM) Media Access Control (MAC) address from the specified port-profile.

Recommended Action No action is required.

NSM-2014

Message `VLAN sub-profile for port-profile <ProfileName> is created.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the VLAN sub-profile has been created successfully.

Recommended Action No action is required.

NSM-2015

Message `Access VLAN <VlanId> is configured for port-profile <ProfileName>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the untagged VLAN has been configured for the specified port-profile.

Recommended Action No action is required.

NSM-2016

Message `Access VLAN is deleted from port-profile <ProfileName>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the untagged VLAN has been removed from the specified port-profile.

Recommended Action No action is required.

NSM-2017

Message `Port-profile <ProfileName> is configured for switching properties.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the switching properties have been configured on the specified port-profile using the **switchport** command.

Recommended Action No action is required.

NSM-2018

Message `Switching properties are removed for port-profile <ProfileName>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the switching properties have been removed from the specified port-profile using the **no switchport** command.

Recommended Action No action is required.

NSM-2019

Message `The <ModeName> mode is configured for port-profile <ProfileName>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified mode has been configured for the port-profile using the **switchport mode** command.

Recommended Action No action is required.

NSM-2020

Message `The <ModeName> mode is de-configured for port-profile <ProfileName>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified mode has been removed for the port-profile using the **switchport mode** command.

Recommended Action No action is required.

NSM-2021

Message `The tagged VLANs <TaggedVlanStr> are configured for port-profile <ProfileName>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified tagged VLANs are configured in the VLAN sub-profile.

Recommended Action No action is required.

NSM-2022

Message `The tagged VLANs <TaggedVlanStr> are removed for port-profile <ProfileName>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified tagged VLANs have been removed from the VLAN sub-profile.

Recommended Action No action is required.

NSM-2023

Message `The tagged VLANs except <TaggedVlanStr> are configured for port-profile <ProfileName>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that except the specified tagged VLANs, all other tagged VLANs are configured in the VLAN sub-profile.

Recommended Action No action is required.

NSM-2024

Message `All VLANs are configured as tagged VLANs for port-profile <ProfileName>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that all the available tagged VLANs are configured in the specified VLAN sub-profile.

Recommended Action No action is required.

NSM-2025

Message `All tagged VLANs are removed for port-profile <ProfileName>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that all the available tagged VLANs have been from the specified VLAN sub-profile.

Recommended Action No action is required.

NSM-2026

Message `Native VLAN <VlanId> is configured to port-profile <ProfileName>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the native VLAN has been configured for the specified port-profile.

Recommended Action No action is required.

NSM-2027

Message `Native VLAN is deleted from port-profile <ProfileName>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the native VLAN has been removed from the specified port-profile.

Recommended Action No action is required.

NSM-2028

Message `FCoE sub-profile for port-profile <ProfileName> is created.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the Fibre Channel over Ethernet (FCoE) sub-profile has been created for the specified port-profile.

Recommended Action No action is required.

NSM-2029

Message `FCoE port is configured successfully for port-profile <ProfileName>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the Fibre Channel over Ethernet (FCoE) port has been configured for the specified port-profile.

Recommended Action No action is required.

NSM-2030

Message `FCoE port is removed successfully for port-profile <ProfileName>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the Fibre Channel over Ethernet (FCoE) port has been removed from the specified port-profile.

Recommended Action No action is required.

NSM-2031

Message `Port-profile <ProfileName> is created.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified port-profile has been created successfully.

Recommended Action No action is required.

NSM-2032

Message `Port-profile <ProfileName> is removed.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified port-profile has been removed successfully.

Recommended Action No action is required.

NSM-2033

Message `VLAN sub-profile for port-profile <ProfileName> is deleted.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the VLAN sub-profile has been deleted successfully.

Recommended Action No action is required.

NSM-2034

Message `FCoE sub-profile for port-profile <ProfileName> is deleted.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the Fibre Channel over Ethernet (FCoE) sub-profile has been deleted successfully.

Recommended Action No action is required.

NSM-2035

Message `Non-profiled-macs on profiled ports will be <allowflag>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the non-profiled media access control (MAC) entries on the profiled port will be allowed or dropped.

Recommended Action No action is required.

NSM-2036

Message `Association of MAC address: <MAC> failed. Reason : <Reason>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that an error occurred during port-profile to media access control (MAC) association.

Recommended Action Check the configuration and port-profile status using the **show port-profile status** command. Execute the **copy support** command and contact your switch service provider.

NSM-2037

Message `De-Association of MAC address: <MAC> failed. For Port-profile : <Reason>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that an error occurred during port-profile to media access control (MAC) de-association.

Recommended Action Check the configuration and port-profile status using the **show port-profile status** command. Execute the **copy support** command and contact your switch service provider.

NSM-2038

Message `Bulk MAC association is Success for port-profile: <ProfileName>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that all media access control (MAC) entries are successfully associated with the specified port-profile.

Recommended Action No action is required.

NSM-2039

Message `Bulk MAC de-association is Success for port-profile: <ProfileName>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that all media access control (MAC) entries are successfully de-associated with the specified port-profile.

Recommended Action No action is required.

NSM-2040

Message `Ctag <Ctag> is associated with Virtual Fabric <virtual fabric> for port-profile: <ProfileName>.`

Message Type DCE

Severity INFO

Probable Cause Indicates successful association of the c-tag with virtual fabric on the specified port-profile.

Recommended Action No action is required.

NSM-2041

Message `MAC <Mac> is associated with Virtual Fabric <virtual fabric> for port-profile: <ProfileName>.`

Message Type DCE

Severity INFO

Probable Cause Indicates successful association of Media Access Control (MAC) with virtual fabric on the specified port-profile.

Recommended Action No action is required.

NSM-2042

Message `Ctag <Ctag> is deassociated with Virtual Fabric <virtual fabric> for port-profile: <ProfileName>.`

Message Type DCE

Severity INFO

Probable Cause Indicates successful disassociation of the c-tag with virtual fabric on the specified port-profile.

Recommended Action No action is required.

NSM-2043

Message `MAC <Mac> is deassociated with Virtual Fabric <virtual fabric> for port-profile: <ProfileName>.`

Message Type DCE

Severity INFO

Probable Cause Indicates successful disassociation of Media Access Control (MAC) with virtual fabric on the specified port-profile.

Recommended Action No action is required.

NSM-2044

Message `Domain: <DomainName> creation successful.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified domain is created.

Recommended Action No action is required.

NSM-2045

Message `Domain deletion <DomainName> successful.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified domain is deleted.

Recommended Action No action is required.

NSM-2046

Message `Profile: <ProfileName> addition to domain <DomainName> successful.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the port-profile is added to the specified domain.

Recommended Action No action is required.

NSM-2047

Message `Profile <ProfileName> deletion from domain <DomainName> successful.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the port-profile is deleted from the specified domain.

Recommended Action No action is required.

NSM-2048

Message `VLAN classifier mac-group <group_id> is created.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified VLAN classifier MAC group has been created.

Recommended Action No action is required.

NSM-2049

Message `DAD failed for IPv6 address <IPv6 Address> on interface <Interface name>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the DHCP Auto Deployment (DAD) process failed for the specified IPv6 address.

Recommended Action Delete the rejected IPv6 address and configure a corrected IPv6 address.

NSM-2050

Message `Netdevice creation failed for interface <Interface name>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the system could not create a netdevice for the specified interfacce.

Recommended Action No action is required.

NSM-2051

Message `Port-profile <ProfileName> application failed on <InterfaceName>, for vlan <Vlan>, reason <Reason>`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the profile application on the specified interface was unsuccessful.

Recommended Action Check the configuration and port-profile status using the **show port-profile status** command. Execute the **copy support** command and contact your switch service provider.

NSM-2052

Message `Unnumbered Intf's peer ipv4 addr <IPv4 Address> is overlapped and can't be added on interface <InterfaceName>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that invalid peer address is received.

Recommended Action change unnumbered peer ipv4 address.

OFMA Messages

OFMA-1001

Message `Openflow Agent Ready Meta: <meta>`

Message Type DCE

Severity INFO

Probable Cause Indicates that a new controller is connected.

Recommended Action No action is required.

OFMM Messages

OFMM-1001

Message `OpenFlow controller connected at <address>:<port>, mode: <mode>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that an OpenFlow controller has been connected.

Recommended Action No action is required.

OFMM-1002

Message `OpenFlow controller disconnected from <address>:<port>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that an OpenFlow controller has been disconnected.

Recommended Action No action is required.

OFMM-1003

Message `Lost connection to OpenFlow controller <address>:<port>.`

Message Type DCE

Severity WARNING

Probable Cause Indicates that the connection to an OpenFlow controller was unexpectedly lost.

Recommended Action If unexpected, make sure that the controller is operating properly.

OFMM-1004

Message `Failed to connect to OpenFlow controller <Controller address>:<Controller port>, file=<Certificate/key file name>, error=<Error: 1=network, 2=CA certificate, 3=switch certificate, 4=switch private key, 5=other>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates network connectivity or certificate/key load error.

Recommended Action For a network error, make sure that the management network connection is properly configured, the controller address and port are set correctly, and the controller is operating properly. For a certificate/key load error, make sure that the certificate or key has been properly created or imported onto the switch. For any other error, consult the trace logs for details.

OFMM-1005

Message `Certificate verification error at depth=<depth>, issuer=<issuer>, subject=<subject>, err=<SSL error>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the SSL OpenFlow connection failed due to certificate verification error.

Recommended Action Make sure that the switch certificate and key have been properly created and signed by the Certificate Authority (CA). Also, make sure that the CA certificate has been imported onto the switch, and the controller has been properly configured with the switch and CA certificates.

OFMM-1006

Message `Flow/Group/Meter mod addition failed controller=<conn_id>, err_code= <err_code_str> [<err_code>], err_type= <err_type_str> [<err_type>].`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the flow, group, or meter mod addition failed.

Recommended Action Re-check the contruction of the mod. This could be either due to protocol error or pipeline limitation. Check the error type for the category of the mod that is flow, group, or meter. The code gives specific insight on the reason for failure.

ONMD Messages

ONMD-1000

Message `LLDP is enabled.`

Message Type DCE

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 DCE

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 DCE

Severity INFO

Probable Cause Indicates that the Link Layer Discovery Protocol (LLDP) global configuration has been changed.

Recommended Action No action is required.

0NMD-1003

Message `LLDP is enabled on interface <InterfaceName>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the Link Layer Discovery Protocol (LLDP) is enabled on the specified interface.

Recommended Action No action is required.

0NMD-1004

Message `LLDP is disabled on interface <InterfaceName>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the Link Layer Discovery Protocol (LLDP) is disabled on the specified interface.

Recommended Action No action is required.

0NMD-1005

Message `Feature Mismatch: <Feature>, will re-negotiate.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the content of the specified feature does not match with the link partner.

Recommended Action Change the feature setting at both ends of the link to match.

0NMD-1006

Message `Timed out waiting for LLDP PDUs on <InterfaceName> from MAC address <MacAddress>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that Link Layer Discovery Protocol (LLDP) PDUs are not recevied from the neighbor for the configured period of time.

Recommended Action No action is required.

0NMD-1007

Message `Received First LLDP PDU on <InterfaceName> from MAC address <MacAddress> after LLDP RX enabled or timeout.`

Message Type DCE

Severity INFO

Probable Cause Indicates that Link Layer Discovery Protocol (LLDP) PDUs are being received from the neighbor.

Recommended Action No action is required.

0NMD-1008

Message `Received shutdown LLDP PDUs with TTL=0 on <InterfaceName> from MAC address <MacAddress>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that shutdown Link Layer Discovery Protocol (LLDP) PDUs are received.

Recommended Action No action is required.

OSPF Messages

OSPF-1001

Message `<error message>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates a configuration error.

Recommended Action Make sure to input or pass the right parameter through CLI or other daemon.

OSPF-1002

Message `<message>.`

Message Type DCE

Severity INFO

Probable Cause Indicates an open shortest path first (OSPF) interface state change or external link-state database (LSDB) overflow notification.

Recommended Action No action is required.

OSPF-1003

Message `<error message>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the length, format, or content of the received packet is incorrect.

Recommended Action Check configuration at the local or remote node.

OSPF6 Messages

OSPF6-1001

Message `<error message>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates a configuration error.

Recommended Action Make sure to input or pass the right parameter through CLI or other daemon.

OSPF6-1002

Message `<message>.`

Message Type DCE

Severity INFO

Probable Cause Indicates an open shortest path first version 3(OSPFv3) interface state change or external link-state database (LSDB) overflow notification.

Recommended Action No action is required.

OSPF6-1003

Message `<error message>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the length, format, or content of the received packet is incorrect.

Recommended Action Check configuration at the local or remote node.

PCAP Messages

PCAP-1001

Message `Packet capture enabled on the <Port name> interface.`

Message Type LOG

Severity INFO

Probable Cause Indicates that packet capture is enabled on the specified interface.

Recommended Action No action is required.

PCAP-1002

Message `Packet capture disabled on the <Port name> interface.`

Message Type LOG

Severity INFO

Probable Cause Indicates that packet capture is disabled on the specified interface.

Recommended Action No action is required.

PCAP-1003

Message `Packet capture disabled globally.`

Message Type LOG

Severity INFO

Probable Cause Indicates that packet capture is disabled globally on the switch.

Recommended Action No action is required.

PCAP-1004

Message `<filename> file is created. Location is flash://<filename>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified .pcap file has been created.

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 due to a missing configuration file during the installation.

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

If the message persists, execute the **copy support** 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 **firmware download** command to reinstall the firmware.

If the message persists, execute the **copy support** 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 Restart or power cycle the switch.

If the message persists, execute the **copy support** 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 **firmware download** command to reinstall the firmware.
If the message persists, execute the **copy support** 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 **firmware download** command to reinstall the firmware.
If the message persists, execute the **copy support** command and contact your switch service provider.

PDM-1009

Message `Cannot update Port Config Data.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the parity data manager (PDM) system call for setting port configuration (setCfg) failed.

Recommended Action Execute the **firmware download** command to reinstall the firmware.
If the message persists, execute the **copy support** 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 **firmware download** command to reinstall the firmware.

If the message persists, execute the **copy support** 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 **firmware download** command to reinstall the firmware.

If the message persists, execute the **copy support** 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 **firmware download** command to reinstall the firmware.

If the message persists, execute the **copy support** 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 **firmware download** command to reinstall the firmware.

If the message persists, execute the **copy support** command and contact your switch service provider.

PDM-1014

Message `Access sysmod failed.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a system call to sysMod failed.

Recommended Action Execute the **firmware download** command to reinstall the firmware.
If the message persists, execute the **copy support** 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 **firmware download** command to reinstall the firmware.
If the message persists, execute the **copy support** command and contact your switch service provider.

PDM-1019

Message `File path or trigger is too long.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a line in the *pdm.conf* file is too long.

Recommended Action Execute the **firmware download** command to reinstall the firmware.
If the message persists, execute the **copy support** command and contact your switch service provider.

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 **firmware download** command to reinstall the firmware.

If the message persists, execute the **copy support** command and contact your switch service provider.

PEM Messages

PEM-1001

Message `Action execution (Profile: <profilename>, Event: <eventname>) timed out.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the action script associated with one of the Programmable Event Manager (PEM) profile timed out.

Recommended Action In case action script is going to take longer, reconfigure the default timeout to a higher value.

PHP Messages

PHP-1001

Message `<PHP Script message>.`

Message Type LOG

Severity INFO

Probable Cause Indicates a user-defined informative message.

Recommended Action No action is required.

PHP-1002

Message `<PHP Script message>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates a user-defined warning message.

Recommended Action No action is required.

PHP-1003

Message `<PHP Script message>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a user-defined error message.

Recommended Action No action is required.

PHP-1004

Message `<PHP Script message>.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates a user-defined critical message.

Recommended Action No action is required.

PIM Messages

PIM-1001

Message `<message> init failed.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that an internal failure occurred during sub-system initialization.

Recommended Action Make sure the switch has enough memory to initialize the sub-system.

PIM-1002

Message `<message> on port <port number>. PIM enable failed.`

Message Type LOG

Severity ERROR

Probable Cause Indicates an issue while enabling PIM on interface.

Recommended Action Verify port configuration and status.

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 reload automatically.

If the system does not reload, execute the **reload** command.

Execute the **copy support** command and contact your switch service provider.

PLAT-1001

Message `MM<Identifies which MM (1 or 2) is doing the reset> resetting other MM (double reset may occur).`

Message Type LOG

Severity INFO

Probable Cause Indicates that the other management module is being reset. This message is typically generated by a management module that is in the process of becoming the active management module. Note that in certain circumstances a management module may experience a double reset and reload twice. A management module can recover automatically even if it has reloaded twice.

Recommended Action No action is required.

PLAT-1002

Message `MM<Identifies which MM (1 or 2) is generating the message>: <Warning message> hk_fence 0x<MM Housekeeping Fence register. Contents are platform-specific> mm_ha 0x<MM HA register. Contents are platform-specific> mm_status 0x<MM Status register. Contents are platform-specific>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that one of the management modules cannot access the inter-integrated circuit (I2C) subsystem because of an error condition or being isolated from the I2C bus.

Recommended Action Reload the management module if it does not reload automatically. Reseat the management module if reloading does not solve the problem. If the problem persists, replace the management module.

PLAT-1004

Message `Turning off Fan <Fan Number> because of airflow direction mismatch.`

Message Type LOG | FFDC

Severity CRITICAL

Probable Cause Indicates that the specified fan field-replaceable unit (FRU) has been turned off because it is incompatible with the system airflow direction policy.

Recommended Action Replace the fan FRU. Refer to the *Hardware Reference Manual* of your switch for instructions to replace the fan FRU.

PLAT-1005

Message `Unable to read EEPROM for Global airflow direction. Setting to default Port side intake.`

Message Type LOG | FFDC

Severity CRITICAL

Probable Cause Indicates a failure to read the electrically erasable programmable read-only memory (EEPROM) to determine the airflow direction of the fans. Therefore, setting the airflow direction to be from the port side of the system.

Recommended Action Execute the **copy support** command and contact your switch service provider.

PLAT-1006

Message `Unable to read EEPROM for Global airflow direction. Shutting off Fans now.`

Message Type LOG

Severity CRITICAL

Probable Cause Indicates a failure to read the electrically erasable programmable read-only memory (EEPROM) to determine the airflow direction of the fans. The fans will be shut down.

Recommended Action Execute the **copy support** command and contact your switch service provider.

PLAT-1007

Message `Turning off Fan <Fan Number> because of airflow direction <Global airflow direction>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified fan is turned off because of an incorrect airflow direction.

Recommended Action Replace the fan field-replaceable units (FRUs) in such a manner that the air flows in the same direction, that is, towards the port side or away from the port side of the system. Refer to the *Hardware Reference Manual* of your switch for instructions to replace the fan FRU.

PLAT-1008

Message `Unable to read EEPROM for Global airflow direction.`

Message Type LOG

Severity ERROR

Probable Cause Indicates a failure to read the electrically erasable programmable read-only memory (EEPROM) and therefore unable to determine the global airflow direction of the fans.

Recommended Action Execute the **copy support** command and contact your switch service provider.

PLAT-1009

Message `Unable to read EEPROM Valid Signature for Global airflow direction.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the content read from electrically erasable programmable read-only memory (EEPROM) is invalid and therefore unable to determine the global airflow direction of the fans.

Recommended Action Execute the **copy support** command and contact your switch service provider.

PLAT-1011

Message `Switch has older FPGA revision <Current FPGA revision>. FPGA revision <Available FPGA revision> is available.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the **firmware download** command has downloaded a latest FPGA that is not activated yet.

This log is specific to platform EN4023 and Brocade VDX 2746. This log will not appear in other platforms.

Recommended Action To activate the latest FPGA, power on reset the switch by doing one of the two steps: physically reseat the switch from the chassis or execute the command 'service -vr' from CMM CLI.

PORT Messages

PORT-1003

Message `Port <port number> Faulted because of many Link Failures.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the specified port is disabled because of multiple link failures on the port that have exceeded the threshold internally set on the port. This problem is related to the hardware.

Recommended Action Check and replace (if necessary) the hardware attached to both the ends of the specified port, including:

- The small form-factor pluggable (SFP)
- The cable (fiber-optic or copper inter-switch link (ISL))
- The attached devices

After checking the hardware, execute the **no shutdown** 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 that the specified port cannot be enabled because other ports in the same group have used the buffers of this port group. This happens when other ports are configured to be long distance.

Recommended Action To enable the specified port, perform one of the following actions:

- Reconfigure the other E_Ports so that they are not long distance.
- Change the other E_Ports so that they are not E_Ports.

This will free some buffers and allow the port to be enabled.

PORT-1011

Message `An SFP transceiver for interface Fibre Channel <interface tuple string> is removed.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a small form-factor pluggable (SFP) transceiver has been removed from the specified port.

Recommended Action No action is required.

PORT-1012

Message `An SFP transceiver for interface Fibre Channel <interface tuple string> is inserted.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a small form-factor pluggable (SFP) transceiver has been inserted into the specified port.

Recommended Action No action is required.

PORT-1013

Message `An incompatible SFP transceiver for interface Fibre Channel <interface tuple string> is inserted.`

Message Type LOG

Severity INFO

Probable Cause Indicates that an incompatible small form-factor pluggable (SFP) transceiver has been inserted into the specified port.

Recommended Action No action is required.

PORT-1014

Message `Interface Fibre Channel <interface tuple string> is online.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified Fibre Channel interface has come online after the protocol dependencies are resolved.

Recommended Action No action is required.

PORT-1015

Message `Interface Fibre Channel <interface tuple string> is link down.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified Fibre Channel interface has gone offline because the link is down.

Recommended Action Check whether the connectivity is proper and the remote link is up.

PORT-1016

Message `Interface Fibre Channel <interface tuple string> is administratively up.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the administrative status of the specified Fibre Channel interface has changed to up.

Recommended Action No action is required.

PORT-1017

Message `Interface Fibre Channel <interface tuple string> is administratively down.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the administrative status of the specified Fibre Channel interface has changed to down.

Recommended Action No action is required.

QOSD Messages

QOSD-1000

Message `QoS initialized successfully.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Data Center Ethernet (DCE) QoS has been initialized.

Recommended Action No action is required.

QOSD-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 **show process memory** command.

Restart or power cycle the switch.

QOSD-1005

Message `QoS startup failed.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the Data Center Ethernet (DCE) QoS 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 version using the **firmware download** command.

QOSD-1006

Message `Interface <interface_name> is not allowed to come up as ISL because of Long Distance ISL restriction. Shutting down interface.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the interface could not come up as inter-switch link (ISL) because only regular ISL is allowed for 2 Km and 5 Km distant links. The interface has been automatically shut down.

Recommended Action No action is required.

QOSD-1007

Message `sFlow profile <sflow-profile-name> is not present.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the specified sFlow profile is not configured on the system.

Recommended Action No action is required.

QOSD-1008

Message `Classmap <class-map_name> is already applied on RBridge in dir <direction> through policy-map <policy-map_name>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the specified class-map is already applied on the RBridge.

Recommended Action No action is required.

QOSD-1500

Message `<BUM_protocol_name> traffic rate has been exceeded on interface <interface_name>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the broadcast, unknown unicast, and multicast (BUM) monitor routine has detected a rate violation.

Recommended Action No action is required.

QOSD-1501

Message `<BUM_protocol_name> traffic rate returned to conforming on interface <interface_name>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that broadcast, unknown unicast, and multicast (BUM) storm control has detected that the traffic rate has returned to the normal limit on the specified interface.

Recommended Action No action is required.

QOSD-1502

Message `<BUM_protocol_name> traffic rate has been exceeded interface <interface_name>. Interface will be shut down.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the broadcast, unknown unicast, and multicast (BUM) monitor routine has detected a rate violation. The interface has been shut down.

Recommended Action Disable BUM storm control on the interface using the **no storm-control ingress** command; then re-enable the interface (using the **no shutdown** command) and BUM storm control (using the **storm-control ingress** command).

QOSD-1600

Message `Tail drops detected on interface <interface_name>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that tail drops are detected on the specified interface.

Recommended Action No action is required.

QOSD-1601

Message `RED drops detected on interface <interface_name>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that red drops are detected on the specified interface.

Recommended Action No action is required.

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 **copy support** 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 **copy support** 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 **copy support** 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 **copy support** 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 `Software detected OOM: module id <Module id> failed to allocate <Memory size> byte(s) of memory.`

Message Type LOG | FFDC

Severity WARNING

Probable Cause Indicates that the system ran out of memory.

Recommended Action Execute the **copy support** command and contact your switch service provider.

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-2006

Message `Audit log message storage has wrapped around.`

Message Type LOG | AUDIT

Class RAS

Severity INFO

Probable Cause Indicates that audit log message storage has wrapped around.

Recommended Action No action is required.

RAS-2007

Message `Audit log message storage has reached 75 percentage of limit.`

Message Type LOG | AUDIT

Class RAS

Severity INFO

Probable Cause Indicates that audit log message storage is 75% full.

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 **usb off** 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 `File <filename/directory> removed from USB storage.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified file or directory has been removed from the USB storage.

Recommended Action No action is required.

RAS-3006

Message `Log messages have been blocked from displaying on console for <Number of minutes> minutes.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the RASLog messages were disabled from displaying on the console for the specified duration by using the **logging raslog console stop** [*minutes*] command.

Recommended Action No action is required.

RAS-3007

Message `Logging messages to console has been enabled.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the RASLog console timer has expired.

Recommended Action No action is required.

RAS-3008

Message `Logging messages to console has been reset by user.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the RASLog messages were re-enabled to display on the console by using the **logging raslog console start** command.

Recommended Action No action is required.

RAS-3009

Message `Please log out all of the CLI sessions and log back in before enabling the USB storage device.`

Message Type LOG

Severity WARNING

Probable Cause User sessions created after usb is turned on needs to be logged out once usb is turned off.

Recommended Action Please log out of all user sessions. The **show user** command can be used to check for active user sessions.

RCS Messages

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 a few minutes and retry the command.

Check memory usage on the switch using the **show process memory** command.

Reload 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 **show ha** command to view the HA state.

Run the **ha disable** and **ha enable** commands.

Investigate for routing issue or check the cabling, and re-enable the disabled E_ports to attempt another exchange of RCS-capable information.

Run the **firmware download** 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 acquire change authorization (ACA) phase, wait for several minutes and 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 RBridge and if the application data is compatible.

RCS-1006

Message `State <RCS phase>, Application <Application Name> AD<Administrative RBridge>, RCS CM. RBridge <RBridge 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 RBridge rejected the reliable commit service (RCS) phase initiated by an application on the local switch.

- If the reject phase is acquire change authorization (ACA), the remote RBridge 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 RBridge does not have the license to support the specified application.

Recommended Action If the reject is in ACA phase, wait for several minutes and then retry operation.

If the reject is in the SFC phase, check if the application license exists for the RBridge and if the application data is compatible.

RCS-1007

Message `Zone DB size and propagation overhead exceeds RBridge <RBridge 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 RBridge cannot handle the zone database being committed.

Recommended Action Reduce the zone database size by deleting some zones. Refer to the *Network OS Administrator's Guide* for instructions to delete a zone.

RCS-1008

Message `RBridge <RBridge number> Lowest Max Zone DB size.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified RBridge has the lowest memory available for the zone database in the fabric. The zone database must be smaller than the memory available on this RBridge.

Recommended Action Reduce the zone database size by deleting some zones. Refer to the *Network OS Administrator's Guide* for instructions to delete a zone.

RCS-1010

Message `RBridge <RBridge number> is RCS incapable. Disabled <Number of E_ports disabled> E_port(s) connected to this RBridge.`

Message Type LOG

Severity ERROR

Probable Cause Indicates inability to retrieve RCS-capable information for the specified RBridge due to some potential routing issues.

Recommended Action 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 RBridge <RBridge number> is RCS incapable. Configure this RBridge as RCS capable.`

Message Type LOG

Severity ERROR

Probable Cause Indicates inability to retrieve RCS-capable information for the specified RBridge due to some potential routing issues.

Recommended Action Investigate for routing issue or check the cabling, and re-enable the disabled E_ports to attempt another exchange of RCS-capable information.

RPS Messages

RPS-1001

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

Message Type DCE

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 **show process memory** command.
Reload or power cycle the switch.

RPS-1750

Message `Route Map <Route_map_name> is bound on interface <interface_name>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified route map has been applied to the specified interface.

Recommended Action No action is required.

RPS-1751

Message `Route Map <Route_map_name> binding on interface <interface_name> failed.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the specified route map was not instantiated on the specified interface.

Recommended Action No action is required.

RPS-1752

Message `Route Map <Route_map_name> is unbound from interface <interface_name>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified route map has been removed from the specified interface.

Recommended Action No action is required.

RPS-1753

Message `Route Map <Route_map_name> unbinding from interface <interface_name> failed.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the specified route map was not removed from the specified interface.

Recommended Action No action is required.

RPS-1754

Message `Route Map <Route_map_name> stanza sequence number <Stanza_sequence_number> binding to interface <interface_name> failed.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that a newly created stanza on an already active route map was unable to be instantiated.

Recommended Action No action is required.

RTM Messages

RTM-1001

Message `Initialization error: <messsage>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the route management (RTM) has encountered an error during initialization.

Recommended Action Reload or power cycle the switch.

RTM-1002

Message `RTM(<messsage>): Max route limit(<maximum limit>) reached.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the route management (RTM) has reached its maximum capacity.

Recommended Action Reduce the number of routes or next hops using the **clear ip route** command.

RTM-1022

Message `Clear Routes success.`

Message Type DCE

Severity INFO

Probable Cause Indicates that IP routes are cleared by the route management (RTM).

Recommended Action No action is required.

RTM-1032

Message `System <messsage> Route Limits exceeded. Current Profile Routes Limit <routes limit>. Configured Routes <configured routes>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates system limits have exceeded.

Recommended Action execute clear on all vrfs.

RTM-1033

Message `System Next-Hop limits exceeded. Current Profile Nexthop <profile nexthop>. Configured Next-Hops <configured nexthops>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the route management (RTM) has reached its maximum nexthop capacity.

Recommended Action Reduce the number of routes or next hops using the **clear ip route** command.

RTM-1037

Message `<messsage>`

Message Type DCE

Severity INFO

Probable Cause Indicates Graceful Restart Done.

Recommended Action No action is required.

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 Write and Read (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 Execute the **reload** command to restart the switch.

RTWR-1002

Message `RTWR <error message: Maximum retries exhausted> 0x<port>, 0x<RBridge>, 0x<retry count>, 0x<status>, 0x<process ID>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that Reliable Transport Write and Read (RTWR) has exhausted the maximum number of retries for sending data to the specified RBridge.

Recommended Action Execute the **show fabric all** command to verify that the specified RBridge ID is online.

If the switch with the specified RBridge ID is offline, enable the switch using the **chassis enable** command.

If the message persists, execute the **copy support** command and contact your switch service provider.

RTWR-1003

Message `<module name>: RTWR retry <number of times retried> to RBridge <RBridge ID>, iu_data <first word of iu_data>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the number of times Reliable Transport Write and Read (RTWR) has failed to get a response and retried.

Recommended Action Execute the **show fabric all** command to verify that the specified RBridge ID is reachable.

If the message persists, execute the **copy support** 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 reload the switch. In this case, execute the **copy support ftp** command to send the core files using FTP to a secure server location.

If the message persists, execute the **copy support** command and contact your switch service provider.

SEC Messages

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 that a member parameter in the **secpolicy defined-policy** command is invalid (for example, it may include an invalid character, such as an asterisk). A valid switch identifier (WWN, RBridge ID, or switch name) must be provided as a member parameter in the **secpolicy defined-policy** command.

Recommended Action Execute the **secpolicy defined-policy** command using a valid switch identifier (WWN, RBridge 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 that the input list has an invalid member.

Recommended Action Verify the member names and input the correct information.

SEC-1036

Message `Device name <device name> is invalid due to a missing colon.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that one or more device names mentioned in the **secpolicy defined-policy** command does not have the colon character (:).

Recommended Action Execute the **secpolicy defined-policy** command with a properly formatted device name parameter.

SEC-1037

Message `Invalid WWN format <invalid WWN>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the World Wide Name (WWN) entered in the policy member list had an invalid format.

Recommended Action Execute the command again using the standard WWN format, that is, 16 hexadecimal digits grouped as eight colon separated pairs. For example: 50:06:04:81:D6:F3:45:42.

SEC-1038

Message `Invalid domain <RBridge ID>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that an invalid RBridge ID was entered.

Recommended Action Verify that the RBridge ID is correct. If RBridge ID is not correct, execute the command again using the correct RBridge ID.

SEC-1044

Message `Duplicate member <member ID> in (<List>).`

Message Type LOG

Severity ERROR

Probable Cause Indicates that 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 duplicate members.

SEC-1071

Message `No new security policy data to apply.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that there are no changes in the defined security policy database to be activated.

Recommended Action Verify that the security event was planned. Change some policy definitions and execute the **secpolicy activate** command to activate the policies.

SEC-1180

Message `Added account <user name> with <role name> authorization.`

Message Type LOG

Severity INFO

Probable Cause Indicates that 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 that the specified account has been deleted.

Recommended Action No action is required.

SEC-1184

Message `<configuration> configuration change, action <action>, server ID <server>, VRF <vrf>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified action is applied to remote AAA (RADIUS/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 that the switch database was enabled or disabled as the secondary authentication, authorization, and accounting (AAA) mechanism when the remote authentication dial-in user service (RADIUS) or Lightweight Directory Access Protocol (LDAP) is the primary 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 that a switch connection control (SCC) security violation was reported. The specified unauthorized switch attempts to join the fabric.

Recommended Action Check the switch connection control policy (SCC) policy to verify the switches are 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 using the **secpolicy defined-policy scc_policy member-entry** command. 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-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 that a Simple Network Management Protocol (SNMP) security violation was reported. The specified unauthorized host attempted to perform an SNMP write operation.

Recommended Action Check the WSNMP policy (read/write SNMP 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 that a Simple Network Management Protocol (SNMP) security violation was reported. The specified unauthorized host attempted to perform an SNMP read operation.

Recommended Action Check the RSNMP policy (read-only SNMP policy) to verify the hosts that are 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 that a Hypertext Transfer Protocol (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 that a serial or modem login security violation was reported. An incorrect password was used while trying to log in through a serial or modem connection; the log in 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 that a login security violation was reported. The wrong password was used while trying to log in through the specified connection method; the log in failed. The violating IP address is displayed in the message.

Recommended Action Verify that the specified IP address is being used by a valid switch administrator. Use the correct password.

SEC-1197

Message `Changed account <user name>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified account has changed.

Recommended Action No action is required.

SEC-1199

Message `Security violation: Unauthorized access to serial port of switch <switch instance>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that 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 was made on the console. If so, add the switch World Wide Name (WWN) to the serial policy using the **secpolicy defined-policy scc_policy member-entry** command. 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-1203

Message `Login information: Login successful via TELNET/SSH/RSH. IP Addr: <IP address>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the remote log in of the specified IP address was successful.

Recommended Action No action is required.

SEC-1204

Message `Root access mode is configured to <Mode>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the root access mode is changed.

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-1205

Message `Login information: User [<User>] Last Successful Login Time : <last_successful_login_time> and Fail count : <fail_count>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the last successful login time and the failed attempt count for the specified user.

Recommended Action No action is required.

SEC-1206

Message `Login information: User [<User>] Last Successful Login Time : <last_successful_login_time>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the last successful login time for the specified user.

Recommended Action No action is required.

SEC-1307

Message `<RADIUS/TACACS+/LDAP server identity> server <server> authenticated user account '<username>'.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified AAA (RADIUS/TACACS+/LDAP) server responded to a switch request after some servers timed out.

Recommended Action If the message appears frequently, reconfigure the list of servers so that the responding server is the first server on the list.

SEC-1308

Message `All <RADIUS/TACACS+/LDAP server identity> servers failed to authenticate user account '<username>'.`

Message Type LOG

Severity INFO

Probable Cause Indicates that all servers in the remote AAA (RADIUS/TACACS+/LDAP) service configuration have failed to respond to a switch request within the configured timeout period.

Recommended Action Verify that the switch has proper network connectivity to the specified AAA (RADIUS/TACACS+/LDAP) servers and the servers are correctly configured.

SEC-1312

Message `<Message>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the password attributes have been changed.

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-1313

Message `The password attributes parameters were set to default values.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the password attributes were set to default values.

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-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 the specified switch is being disabled on the specified port because of a switch connection control (SCC) policy violation.

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 using the **secpolicy defined-policy scc_policy member-entry** command, then attempt to join the switch with the fabric.

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 that the IP filter policy enforcement failed because of an internal system failure.

Recommended Action Execute the **copy support** command and contact your switch service provider.

SEC-1334

Message `local security policy <Event name>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified event has occurred.

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.

SEC-1335

Message `local security policy <Event name> WWN <Member WWN>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified event has occurred.

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.

SEC-1336

Message `Missing file <file name> is replaced with default configuration.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified file is missing and it has been replaced with the default file.

Recommended Action No action is required.

SEC-1337

Message `Failed to access file <file name> and reverted the configuration.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified file was not accessible.

Recommended Action No action is required.

SEC-1338

Message `Accounting message queue 90 percent full, some messages may be dropped.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the server is unreachable.

Recommended Action No action is required.

SEC-1339

Message `Accounting message queue within limits all messages will be processed.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the server is now reachable.

Recommended Action No action is required.

SEC-3014

Message `Event: <Event Name>, Status: success, Info: <Event related info> <Event option> server <Server Name> vrf <VRF> for AAA services.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the AAA (RADIUS/TACACS+) server configuration has been changed manually.

Recommended Action Verify that the RADIUS/TACACS+ configuration was changed intentionally. If the RADIU/TACACS+ configuration was changed intentionally, no action is required. If the RADIUS/TACACS+ configuration was not changed intentionally, take appropriate action as defined by your enterprise security policy.

SEC-3016

Message `Event: <Event Name>, Status: success, Info: Attribute [<Attribute Name>] of <Attribute related info> server <server ID> vrf <VRF> changed <Attribute related info, if any>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the specified attribute of the remote AAA (RADIUS/TACACS+) server has been changed manually.

Recommended Action Verify that the attribute was changed intentionally. If the attribute was changed intentionally, no action is required. If the attribute was not changed intentionally, 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 to New Value>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the specified password attribute has been changed.

Recommended Action Verify that the password attribute was changed intentionally. If the password attribute was changed intentionally, no action is required. If the password attribute was not changed intentionally, take appropriate action as defined by your enterprise security policy.

SEC-3019

Message `Event: <Event Name>, Status: success, Info: Password attributes set to default values.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the password attributes are set to default values.

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-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 that the log in was successful. An IP address is displayed when the login occurs over a remote connection.

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-3021

Message `Event: <Event Name>, Status: failed, Info: Failed login attempt through <connection method and IP Address>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the log in attempt has failed.

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-3022

Message `Event: <Event Name>, Status: success, Info: Successful logout by user [<User>].`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that 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 the number of failed log in attempts due to incorrect password has exceeded the allowed limit; the account has been locked.

Recommended Action The administrator can 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 that the password was changed for the specified user.

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-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 that a new user account was created.

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-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 that the user account role has been changed.

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-3027

Message `Event: <Event Name>, Status: success, Info: User account [<User Name>] [<Changed Attributes>].`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the user account properties were changed.

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-3028

Message `Event: <Event Name>, Status: success, Info: User account [<User Name>] deleted.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the specified user account has been deleted.

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-3030

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

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the certificate authority (CA) certificate was imported successfully using the **certutil import ldapca** command.

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-3034

Message `Event: AAA Authentication Login Mode Configuration, Status: success, Info: Authentication configuration changed from <Previous Mode> to <Current Mode>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the authentication configuration has been changed.

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-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 that the specified IP filter policies have been saved.

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-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 that the specified IP filter policies have not been saved.

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-3037

Message `Event: ipfilter, Status: success, Info: <IP Filter Policy> ipfilter policy activated.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the specified IP filter policy has been activated.

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-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 that the specified IP filter policy failed to activate.

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-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 that 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-3045

Message `Zeroization has been executed on the system.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that 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 that there was a change in the Federal Information Protection Standard (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-3049

Message `Status of bootprom access is changed using prom-access disable CLI: <Access Status>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the status of Boot PROM has changed using **prom-access disable** command. By default, the Boot PROM is accessible.

Recommended Action No action is required.

SEC-3051

Message `The license key <Key> is <Action>.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that the specified license key has been 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 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 has been deleted.

Recommended Action No action is required.

SEC-3067

Message `Event: <Event Name>, Status: success, Info: Telnet Server is shutdown.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the Telnet server in the switch is shut down.

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-3068

Message `Event: <Event Name>, Status: success, Info: Telnet Server is started.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the Telnet server in the switch is started.

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-3069

Message `Event: <Event Name>, Status: success, Info: SSH Server is shutdown.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the SSH server in the switch is shut down.

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-3070

Message `Event: <Event Name>, Status: success, Info: SSH Server is started.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the SSH server in the switch is started.

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-3071

Message `Event: <Event Name>, Status: success, Info: SSH Server Key Exchange Algorithm is configured to DH Group 14.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the SSH server key exchange algorithm is configured to DH group 14.

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-3072

Message `Event: <Event Name>, Status: success, Info: SSH Server Key Exchange Algorithm is restored to default.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the SSH server key exchange algorithm is restored to default.

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-3073

Message `Event: <Event Name>, Status: success, Info: Login banner message is set to '<Banner>'.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the login banner message is set.

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-3074

Message `Event: <Event Name>, Status: success, Info: Login banner message is removed.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the login banner message is removed.

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-3075

Message `Event: <Event Name>, Status: success, Info: '<Type of cipher (LDAP/SSH)>' cipher list is configured.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the specified Lightweight Directory Access Protocol (LDAP) or SSH cipher list is configured.

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-3076

Message `Event: <Event Name>, Status: success, Info: '<Type of cipher (LDAP/SSH)>' cipher list is removed.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the specified Lightweight Directory Access Protocol (LDAP) or SSH cipher list is removed.

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-3077

Message `Event: <Event Name>, Status: success, Info: SSH Server Rekey Interval is configured to <RekeyInterval>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the SSH server periodic rekeying is enabled with configured interval.

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-3078

Message `Event: <Event Name>, Status: success, Info: SSH Server Rekey Interval is removed.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the SSH server periodic rekeying is disabled.

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-3079

Message `Event: <Event Name>, Status: success, Info: SSH Server Cipher is configured to <Cipher>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the SSH server cipher is changed to configured value.

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-3080

Message `Event: <Event Name>, Status: success, Info: SSH Server Cipher is restored to default.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the SSH server cipher is restored to default.

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-3081

Message `Event: <Event Name>, Status: success, Info: SSH Client Cipher is configured to <Cipher>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the SSH client cipher is changed to configured value.

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-3082

Message `Event: <Event Name>, Status: success, Info: SSH Client Cipher is restored to default.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the SSH client cipher is restored to default.

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-3083

Message `Event: <Event Name>, Status: success, Info: Root access mode is restored to default (SSH/Telnet/Console).`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the root access mode is restored to default (SSH/Telnet/Console).

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-3084

Message `Event: <Event Name>, Status: success, Info: Root access mode is configured to <mode>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the root access mode is changed to the configured value.

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-3085

Message `Event: <Event Name>, Status: success, Info: Root account is <status>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the root account is enabled or disabled.

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-3086

Message `Event: <Event Name>, Status: success, Info: Standby Telnet server is <status>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the standby Telnet server in the switch is started or shutdown.

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-3087

Message `Event: <Event Name>, Status: success, Info: Standby SSH server is <status>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the standby SSH server in the switch is started or shutdown.

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-3088

Message `Event: <Event Name>, Status: success, Info: SSH <Key Type> Key <status>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the SSH key is generated or deleted.

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-3089

Message `Event: <Event Name>, Status: success, Info: Crypto key is generated.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the Crypto key is generated.

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-3090

Message `Event: <Event Name>, Status: success, Info: Crypto key is deleted.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the Crypto key is deleted.

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-3091

Message `Event: <Event Name>, Status: success, Info: Crypto CA Trustpoint is created.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the Crypto CA Trustpoint is created.

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-3092

Message `Event: <Event Name>, Status: success, Info: Crypto CA Trustpoint is deleted.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the Crypto CA Trustpoint is deleted.

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-3093

Message `Event: <Event Name>, Status: success, Info: Crypto CA Trustpoint - Keypair associated.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the Crypto CA Trustpoint and keypair are associated.

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-3094

Message `Event: <Event Name>, Status: success, Info: Crypto CA Trustpoint - Keypair disassociated.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the Crypto CA Trustpoint and keypair are disassociated.

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-3095

Message `Event: <Event Name>, Status: success, Info: Crypto CA Trustpoint is authenticated.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the CA certificate of the Crypto CA Trustpoint is imported.

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-3096

Message `Event: <Event Name>, Status: success, Info: Crypto CA Trustpoint is unauthenticated.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the CA certificate of the Crypto CA Trustpoint is deleted.

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-3097

Message `Event: <Event Name>, Status: success, Info: Crypto CA Trustpoint is enrolled.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the Crypto CA Trustpoint Certificate Signing Request (CSR) is generated and exported.

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-3098

Message `Event: <Event Name>, Status: success, Info: Crypto CA Trustpoint certificate is imported.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the Crypto CA Trustpoint identity certificate is imported.

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-3099

Message `Event: <Event Name>, Status: success, Info: Crypto CA Trustpoint certificate is deleted.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the Crypto CA Trustpoint identity certificate is deleted.

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-3100

Message `Event: <Event Name>, Status: success, Info: SSH Server MAC is configured to <MAC>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the SSH server MAC is changed to the configured value.

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-3101

Message `Event: <Event Name>, Status: success, Info: SSH Client MAC is configured to <MAC>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the SSH client MAC is changed to the configured value.

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-3102

Message `Event: <Event Name>, Status: success, Info: SSH Client Kex is configured to <Kex>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the SSH client Kex is changed to configured value.

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-3103

Message `Event: <Event Name>, Status: success, Info: SSH Server Key Exchange is configured to <Kex>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the SSH server key exchange (Kex) is changed to the configured value.

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-3104

Message `Event: <Event Name>, Status: success, Info: SSH Server instance is started on <Vrfname> VRF.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the SSH server instance is started on given VRF.

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-3105

Message `Event: <Event Name>, Status: success, Info: SSH Server instance is stopped on <Vrfname> VRF.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the SSH server instance is stopped on given VRF.

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-3106

Message `Event: <Event Name>, Status: success, Info: Telnet Server instance is started on <Vrfname> VRF.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the Telnet server instance is started on given VRF.

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-3107

Message `Event: <Event Name>, Status: success, Info: Telnet Server instance is stopped on <Vrfname> VRF.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the Telnet server instance is stopped on given VRF.

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-3108

Message `Event: <Event Name>, Status: success, Info: SSH Server MaxSession is configured to <MaxSessions>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the Secure Shell (SSH) server MaxSession multiplexing is enabled with the configured count.

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-3109

Message `Event: <Event Name>, Status: success, Info: SSH Server MaxSession is removed.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the Secure Shell (SSH) server MaxSession is disabled.

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-3501

Message `Role '<Role Name>' is changed.`

Message Type AUDIT | LOG

Class SECURITY

Severity INFO

Probable Cause Indicates that attributes of the specified role have been changed.

Recommended Action No action is required.

SFLO Messages

SFLO-1001

Message `sFlow is <state> globally.`

Message Type DCE

Severity INFO

Probable Cause Indicates that sFlow is enabled or disabled globally.

Recommended Action No action is required.

SFLO-1002

Message `sFlow is <state> for port <name>.`

Message Type DCE

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 DCE

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 DCE

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 DCE

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 DCE

Severity INFO

Probable Cause Indicates that the sFlow 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 DCE

Severity INFO

Probable Cause Indicates that the specified sFlow collector is either configured or not configured.

Recommended Action No action is required.

SFLO-1008

Message `All the sFlow collectors are unconfigured.`

Message Type DCE

Severity INFO

Probable Cause Indicates that none of the sFlow collectors are configured.

Recommended Action No action is required.

SFLO-1009

Message `Socket Operation Failed while connecting with the collector address.`

Message Type DCE

Severity WARNING

Probable Cause Indicates that the connection to the sFlow collector server failed.

Recommended Action Reconfigure the sFlow collector using the **sflow collector** command.

SFLO-1010

Message `sFlow profile is created with name <name> and sampling rate <sample_rate>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified sFlow profile has been created.

Recommended Action No action is required.

SFLO-1011

Message `sFlow profile with name <name> is deleted.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified sFlow profile has been deleted.

Recommended Action No action is required.

SFLO-1012

Message `sFlow profile with name <name> is updated with sampling rate <sample_rate>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the sampling rate has been updated for the specified sFlow profile.

Recommended Action No action is required.

SFLO-1013

Message `sFlow profile with name <name> is in use. Cannot be deleted.`

Message Type DCE

Severity WARNING

Probable Cause Indicates that the specified sFlow profile is in use and therefore it cannot be deleted.

Recommended Action No action is required.

SFLO-1014

Message `<message>.`

Message Type DCE

Severity INFO

Probable Cause Indicates the sFlow configuration details.

Recommended Action No action is required.

SFLO-1015

Message `Max no. of profiles (<message>) already configured.`

Message Type DCE

Severity INFO

Probable Cause Indicates the sFlow configuration details.

Recommended Action No action is required.

SLCD Messages

SLCD-1001

Message `CF life percentage used up is between 90 - 95 on card No. <CF Card number in integer>, Actual percentage <life span of CF used up in percentage>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the compact flash (CF) life span left over is a little more than 5 percent as reported by the CF wear leveling statistics.

Recommended Action The CF card must be replaced as soon as possible. Contact your switch service provider for the CF card replacement.

SLCD-1002

Message `CF life span percentage is between 95 - 99 on card No. <CF Card number in integer>, Actual percentage <Life span used up on CF in percentage>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the compact flash (CF) life span left over is between 1 and 5 percent as reported by the CF wear leveling statistics.

Recommended Action The CF card must be replaced immediately for proper functioning. Contact your switch service provider for the CF card replacement.

SLCD-1003

Message `CF life span percentage left is less than 1 on card No. <CF Card number in integer>, Actual percentage <Life span used up on CF card in percentage>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the compact flash (CF) life span left over is less than 1 percent as reported by the CF wear leveling statistics.

Recommended Action A new CF card is required for proper functioning of the chassis. Contact your switch service provider for the CF card replacement.

SLCD-1004

Message `CF life span percentage left on Card No <CF Card number in integer> is - <Life span left on CF card in percentage>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the available life span of the compact flash (CF) as reported by the CF wear leveling statistics.

Recommended Action No action is required.

SLCD-1005

Message `Spare Blocks percentage left on Card No. <CF Card number in integer> is between 5-10,Actual percentage is - <Spare Blocks left in percentage>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the spare blocks percentage left on the compact flash (CF) card is between 5 and 10 percent as reported by the CF wear leveling statistics.

Recommended Action The CF card must be replaced as soon as possible. Contact your switch service provider for the CF card replacement.

SLCD-1006

Message `Spare Blocks percentage left on CF Card No. <CF Card number in integer> is between 1-5,Actual percentage is - <Spare Blocks left in percentage>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the spare blocks percentage left on the compact flash (CF) card is between 1 and 5 percent as reported by the CF wear leveling statistics.

Recommended Action The CF card must be replaced immediately for proper functioning. Contact your switch service provider for the CF card replacement.

SLCD-1007

Message `Spare Blocks percentage left on CF Card No. <CF Card number in integer> are less than 1,Actual percentage is - <Spare Blocks left in percentage>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the spare blocks percentage left on the compact flash (CF) card is less than 1 percent as reported by the CF wear leveling statistics.

Recommended Action A new CF card is required for proper functioning of the chassis. Contact your switch service provider for the CF card replacement.

SLCD-1008

Message `Spare Blocks percentage left on CF Card No. <CF Card number in integer> are - <Spare Blocks left in percentage>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the percentage of the spare blocks left on the compact flash (CF) card as reported by the CF wear leveling statistics.

Recommended Action No action is required.

SLCD-1009

Message `Unable to get Wear leveling stats for CF card No. <CF Card number in integer>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that wear leveling data cannot be retrieved from the attached compact flash (CF) card.

Recommended Action Check the availability and healthiness of the CF card immediately for proper functioning.

SLCD-1010

Message `CF wear leveling daemon Failed to find any western digital (WD) CF cards attached.`

Message Type LOG

Severity ERROR

Probable Cause Indicates an error in enumerating the attached compact flash (CF) cards.

Recommended Action Check the availability and connection to the CF cards immediately for proper functioning.

SLCD-1011

Message `CF life percentage used for card No. <CF Card number in integer> is <life span of CF used up in percentage>.`

Message Type LOG

Severity INFO

Probable Cause Indicates the used life span of the compact flash (CF) card as reported by the CF wear leveling statistics.

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. 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 using the **show interface management** command. If the specified reason is an initialization failure, reload the switch.

SNMP-1002

Message `SNMP <Error Details> initialization failed.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the initialization of the Simple Network Management Protocol (SNMP) service failed and you will not be able to query the switch through SNMP.

Recommended Action Reload 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 Simple Network Management Protocol (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 using the **snmp-server community** command.

SNMP-1004

Message `Incorrect SNMP configuration.`

Message Type FFDCLOG

Severity ERROR

Probable Cause Indicates that the Simple Network Management Protocol (SNMP) configuration is incorrect and the SNMP service will not work correctly.

Recommended Action Change the SNMP configuration using the **config snmp-server** command.

SNMP-1005

Message `SNMP configuration attribute, <Changed attribute>, <String Value>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Simple Network Management Protocol (SNMP) configuration has changed. The parameter that was modified is displayed along with the old and new values of that parameter.

Recommended Action Execute the **show running-config snmp-server** command to view the new SNMP configuration.

SRM Messages

SRM-1001

Message `CPU usage reached <percentage of current cpu usage> percent, exceeded the threshold.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the CPU usage exceeded the configured threshold and therefore triggered the alert action.

Recommended Action Execute the **show process cpu** command for more information.

SRM-1002

Message `The system memory is at <current low memory usage> kB and is below the threshold.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the system low memory usage exceeded the configured threshold and therefore triggered the alert action.

Recommended Action Execute the **show process memory** command for more information. Check for memory leak, if suspected.

SRM-1003

Message `High memory usage reached <current high memory usage> kB, exceeded the threshold.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the system high memory usage exceeded the configured threshold and therefore triggered the alert action.

Recommended Action Execute the **show process memory** command for more information.

SRM-1004

Message `Process <process name> PID <PID > memory usage reached <current memory usage in Kbytes> Kbytes and has exceeded the alarm threshold.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the process-based memory usage exceeded the configured alarm threshold and therefore triggered the alert action.

Recommended Action Execute the **show process memory** command for more information. Check for memory leak, if suspected.

SRM-1005

Message `Process <process name> PID <PID > memory usage reached <current memory usage in Kbytes> Kbytes and has exceeded the critical threshold.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the process-based memory usage exceeded the configured critical threshold and therefore triggered the alert action.

Recommended Action Execute the **show process memory** command for more information.

SRM-1006

Message `High memory usage reached <current high memory usage> kB, triggerring HA failover for recovery.`

Message Type LOG | FFDC

Severity CRITICAL

Probable Cause Indicates that the system high memory usage exceeded the configured threshold and therefore triggered the alert action.

Recommended Action No action is required. This will trigger high availability (HA) failover automatically.

SS Messages

SS-1000

Message `Copy support upload operation is completed.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the **copy support** command was used to transfer the support information to a remote location.

Recommended Action No action is required.

SS-1001

Message `Copy support upload operation has been aborted.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a file copy error occurred during execution of the **copy support** command. Complete error information cannot always be displayed in this message because of possible errors in the subcommands being executed by the **copy support** command.

The file copy error can occur due to one of the following reasons:

- Could not connect to remote host
- Could not connect to remote host - timed out
- Transfer failed
- Transfer failed - timed out
- Directory change failed
- Directory change failed - timed out
- Malformed URL
- Usage error
- Error in login configuration file
- Session initialization failed
- Unknown remote host error

Recommended Action Check and correct the remote server settings and configuration and then execute the **copy support** command again.

If the problem persists, contact your system administrator.

SS-1002

Message `Copy support has stored support information to the USB storage device.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the **copy support** command was used to transfer support information to an attached USB storage device.

Recommended Action No action is required.

SS-1003

Message `Copy support operation to USB storage device aborted.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a USB operation error occurred during execution of the **copy support** command. Complete error information cannot always be displayed in this message because of possible errors in subcommands being executed by the **copy support** command.

Recommended Action Make sure that the attached USB device is enabled.

Execute the **usb on** command to enable an attached USB device. After the USB problem is corrected, execute the **copy support** command again.

SS-1004

Message `One or more modules timed out during copy support. Retry copy support with timeout option to collect all modules.`

Message Type LOG

Severity WARNING

Probable Cause Indicates timeout in modules during execution of the **copy support** command.

Recommended Action Execute the **copy support** command again.

SS-1010

Message `Copy support timeout multiplier is set to <Timeout Multiplier> due to higher CPU load average. Copy support may take more time to complete.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the CPU load average is above normal. The copy support operation may take longer time than usual.

Recommended Action No action is required.

SS-1011

Message `Copy support upload operation failed. Reason: <Failure reason>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a file copy error occurred during execution of the **copy support** command.

The file copy error can occur due to one of the following reasons:

- Could not connect to remote host
- Could not connect to remote host - timed out
- Transfer failed
- Transfer failed - timed out
- Directory change failed
- Directory change failed - timed out
- Malformed URL
- Usage error
- Error in login configuration file
- Session initialization failed
- Unknown remote host error

Recommended Action Check and correct the remote server settings and configuration and then execute the **copy support** command again.

If the problem persists, contact your system administrator.

SS-1012

Message `Copy support upload Operation started.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the copy support upload operation has started.

Recommended Action No action is required.

SS-1013

Message `Previous Copy support upload operation aborted abnormaly. please run copy support group BASIC.`

Message Type LOG | FFDC

Severity WARNING

Probable Cause Indicates that the copy support upload operation has aborted abnormaly.

Recommended Action No action is required.

SS-1014

Message `Insufficient physical memory(<Physical Memory free space > MB) for copy support.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that physical memory is below minimum requirement for copy support.

Recommended Action No action is required.

SS-1015

Message `Insufficient CF Memory(<CF free space > MB) for copy support.`

Message Type LOG

Severity WARNING

Probable Cause Indiactes that CF Memory is below minimum requirement for copy support.

Recommended Action No action is required.

SS-1016

Message `Copy support module <Module name>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the copy support operation has started on the specified module.

Recommended Action No action is required.

SS-1017

Message `Copy support group <Group name> could not be found.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the copy support could not find the group name given by the user.

Recommended Action No action is required.

SS-2000

Message `Copy support started on rbridge-id <rbridge-id>.`

Message Type VCS | LOG

Severity INFO

Probable Cause Indicates that the copy support operation has started on the specified RBridge.

Recommended Action No action is required.

SS-2001

Message `Copy support completed on rbridge-id <rbridge-id>.`

Message Type VCS | LOG

Severity INFO

Probable Cause Indicates that the copy support operation has completed successfully on the specified RBridge.

Recommended Action No action is required.

SS-2002

Message `Copy support failed on rbridge-id <rbridge-id>.`

Message Type VCS | LOG

Severity INFO

Probable Cause Indicates that the copy support operation has failed on the specified RBridge.

Recommended Action Check and correct the remote server settings and configuration and then execute the **copy support** command again.

If the problem persists, contact your system administrator.

SSMD Messages

SSMD-1001

Message `Failed to allocate <Memory size> bytes of memory.`

Message Type DCE

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 **show process memory** command.
Reload or power cycle the switch.

SSMD-1002

Message `Failed to lock mutex.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that System Services Manager (SSM) component has failed to lock the mutex.

Recommended Action Reload or power cycle the switch.

SSMD-1003

Message `Failed to unlock mutex.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that System Services Manager (SSM) component has failed to unlock the mutex.

Recommended Action Reload or power cycle the switch.

SSMD-1004

Message `SSM startup failed.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the Data Center Ethernet (DCE) System Services Manager (SSM) has encountered an unexpected severe error during basic startup and initialization.

Recommended Action Reload or power cycle the switch.

If the problem persists, download a new firmware version using the **firmware download** command.

SSMD-1136

Message `Ethertype Based VLAN Classifier Table is full on Chip <Slot Number>/<Slot Chip Number>:<Chip Core Number>.`

Message Type DCE

Severity WARNING

Probable Cause Indicates that Ethertype-based VLAN classifier table is full.

Recommended Action Clean up the unused Ethertype-based VLAN classifiers to add new ones.

SSMD-1236

Message `MAC Based VLAN Classifier Table is full on Chip <Slot Number>/<Slot Chip Number>:<Chip Core Number>.`

Message Type DCE

Severity WARNING

Probable Cause Indicates that MAC-based VLAN classifier table is full.

Recommended Action Clean up the unused MAC-based VLAN classifiers to add new ones.

SSMD-1400

Message `<ACL Type> access list <ACL Name> is created.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified access list has been created.

Recommended Action No action is required.

SSMD-1402

Message `<ACL Type> access list <ACL Name> is deleted.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified access list has been deleted.

Recommended Action No action is required.

SSMD-1404

Message `<ACL Type> access list <ACL Name> rule sequence number <rule_sq_no> is <action>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the access list rules are added to or removed from an existing policy.

Recommended Action No action is required.

SSMD-1405

Message `<ACL Type> access list <ACL Name> configured on interface <Interface Name> at <Direction> by <Configuration source>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified access list has been configured on the interface.

Recommended Action No action is required.

SSMD-1406

Message `<ACL Type> access list <ACL Name> is removed from interface <Interface Name> at <Direction> by <Configuration source>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified access list has been removed from the interface.

Recommended Action No action is required.

SSMD-1407

Message `<ACL Type> access list <ACL Name> active on interface <Interface Name> at <Direction>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified access list has been configured on the interface.

Recommended Action No action is required.

SSMD-1408

Message `<Number of ACL Rules> rules added to <ACL Type> access list <ACL Name>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified rules are added to the access control list (ACL).

Recommended Action No action is required.

SSMD-1436

Message `<ACL Type> access list <ACL Name> partially active on interface <Interface Name> at <Direction>.`

Message Type | DCEVCS

Severity WARNING

Probable Cause Indicates that the specified access control list (ACL) was not fully instantiated into the ternary content addressable memory (TCAM).

Recommended Action Remove the specified ACL and other unused ACLs that are applied using the **no ip access-group***name***[in|out]** command, and then instantiate ACL into TCAM again.

SSMD-1437

Message `<ACL Type> access list <ACL Name> inactive on interface <Interface Name> at <Direction>.`

Message Type | DCEVCS

Severity WARNING

Probable Cause Indicates the specified access control list (ACL) was not instantiated into the ternary content addressable memory (TCAM).

Recommended Action Remove the specified ACL and other unused ACLs that are applied using the **no ip access-group***name***[in|out]** command, and then instantiate ACL into TCAM again.

SSMD-1438

Message `<ACL Type> access list <ACL Name> configured on interface <Interface Name> at <Direction> has rule(s) which are not supported on this platform.`

Message Type | DCEVCS

Severity WARNING

Probable Cause Indicates that the specified access control list (ACL) has rules which are not supported on this platform.

Recommended Action Remove unsupported rules using the **no seq** *0-4294967290* command in the ACL context.

SSMD-1439

Message `Rule with sequence number <ACL Rule Sequence number> of <ACL Type> access list <ACL Name> configured on interface <Interface Name> at <Direction> is not supported on this platform.`

Message Type | DCEVCS

Severity WARNING

Probable Cause Indicates that the specified access control list (ACL) has rules which are not supported on this platform.

Recommended Action Remove unsupported rules using the **no seq** *0-4294967290* command in the ACL context.

SSMD-1536

Message `<Table Mode> <Feature Name> Table is full at <Table Type> on Chip <Slot Number>/<Slot Chip Number>:<Chip Core Number>.`

Message Type DCE

Severity WARNING

Probable Cause Indicates that MAC-based VLAN classifier table is full.

Recommended Action Clean up the unused MAC-based VLAN classifiers to add new ones.

SSMD-1571

Message `Error <Error code> Creating region Feature:<Logical Device ID> Region:<Region ID> Chip:0x<Chip Index>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the application-specific integrated circuit (ASIC) driver has returned an error.

Recommended Action Execute the **copy support** command and contact your switch service provider.

SSMD-1900

Message `Security sub-profile is created for port-profile <Profile name>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that a security sub-profile has been created for the specified port-profile.

Recommended Action No action is required.

SSMD-1901

Message `ACL <ACL name> is configured successfully for security sub-profile of port-profile <Profile name>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified access control list (ACL) has been configured for the security sub-profile.

Recommended Action No action is required.

SSMD-1902

Message `ACL <ACL name> is removed successfully for security sub-profile of port-profile <Profile name>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the specified access control list (ACL) has been removed for the security sub-profile.

Recommended Action No action is required.

SSMD-1915

Message `Security sub-profile is deleted for port-profile <Profile name>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the security sub-profile has been deleted.

Recommended Action No action is required.

SULB Messages

SULB-1000

Message `The firmware download command has been started.`

Message Type AUDIT | LOG

Class FIRMWARE

Severity WARNING

Probable Cause Indicates that firmware download has started.

Recommended Action No action is required.

SULB-1100

Message `Firmware <firmware operations: install, swap, reboot, commit, recover> begins on <slot/partition>.`

Message Type AUDIT | LOG

Class FIRMWARE

Severity INFO

Probable Cause Indicates that the specified firmware operation has started on the specified slot or partition.

Recommended Action No action is required.

SULB-1101

Message `Firmware <firmware operations: install, swap, reboot, commit, recover> ends on <slot/partition>.`

Message Type AUDIT | LOG

Class FIRMWARE

Severity INFO

Probable Cause Indicates that the specified firmware operation has completed successfully on the specified slot or partition.

Recommended Action No action is required.

SULB-1102

Message `Firmware <firmware operations: install, swap, reboot, commit, recover> failed on <slot/partition> with error (<error code>).`

Message Type AUDIT | LOG

Class FIRMWARE

Severity WARNING

Probable Cause Indicates that the specified firmware operation has failed on the specified slot or partition. The error code indicates the reason for the failure.

The following table lists the error codes that provide more details on why the firmware operation failed.

TABLE 9 Error messages and error codes

Error message	Error code
"Upgrade is inconsistent."	0x10
"OSRootPartition is inconsistent."	0x11
"Unable to access the package list file. Check whether the file name is specified properly."	0x12
"Red Hat package manager (RPM) package database is inconsistent. Contact your service provider for recovery."	0x13
"Out of memory."	0x14
"Failed to download RPM package. Check if the firmware image is accessible."	0x15
"Unable to create firmware version file."	0x16
"Unexpected system error."	0x17
"Another firmware download is in progress."	0x18
"Error in releasing lock device."	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. Contact your service provider to assistance."	0x1c
"OSLoader is inconsistent.	0x1d
"New image has not been committed. Execute the **firmware commit** command or the **firmware restore** and **firmware download** commands."	0x1e
"**firmware restore** is not needed."	0x1f
"Images are not mounted properly."	0x20
"Unable to uninstall old packages. Contact your service provider for assistance."	0x21
"**firmware download** has timed out."	0x23
"Out of disk space."	0x24
"Primary filesystem is inconsistent. Execute the **firmware restore** to restore the original firmware, or contact your service provider for recovery."	0x25

TABLE 9 Error messages and error codes

Error message	Error code
"The post-install script failed."	0x26
"Reload (partition) failed."	0x27
"Primary kernel partition is inconsistent. Contact your service provider for recovery."	0x28
"The pre-install script failed."	0x29
"Failed to install RPM package."	0x2b
"Cannot downgrade directly to this version. Downgrade to an intermediate version and then download the desired version."	0x2c
"Failed to validate firmware signature."	0x3e
"Failed to swap the firmware partitions."	0x40
"Failed to load the PROM image. Contact your service provider for assistance."	0x41

Recommended Action Execute the **show firmwaredownloadstatus** command for more information. Restart the firmware operation if needed.

SULB-1103

Message `Firmware download completed successfully on <slot/partition>.`

Message Type AUDIT | LOG

Class FIRMWARE

Severity INFO

Probable Cause Indicates that firmware download has completed successfully on the specified slot or partition.

Recommended Action No action is required.

Execute the **show firmwaredownloadstatus** command for more information. Execute the **show version** to verify the firmware version.

SULB-1104

Message `Firmware download <failed or failed but recovered> on <node name> with error (<error code>).`

Message Type AUDIT | LOG

Class FIRMWARE

Severity CRITICAL

Probable Cause Indicates that firmware download has failed on the specified slot. The error code indicates the reason for the failure.

The following table lists the error codes that provide more details on why the firmware operation failed.

TABLE 10 Error messages and error codes

Error message	Error code
"Upgrade is inconsistent."	0x10
"OSRootPartition is inconsistent."	0x11
"Unable to access the package list file. Check whether the file name is specified properly."	0x12
"Red Hat package manager (RPM) package database is inconsistent. Contact your service provider for recovery."	0x13
"Out of memory."	0x14
"Failed to download RPM package. Check if the firmware image is accessible."	0x15
"Unable to create firmware version file."	0x16
"Unexpected system error."	0x17
"Another firmware download is in progress."	0x18
"Error in releasing lock device."	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. Contact your service provider to assistance."	0x1c
"OSLoader is inconsistent.	0x1d
"New image has not been committed. Execute the **firmware commit** command or the **firmware restore** and **firmware download** commands."	0x1e
"**firmware restore** is not needed."	0x1f
"Images are not mounted properly."	0x20
"Unable to uninstall old packages. Contact your service provider for assistance."	0x21
"**firmware download** has timed out."	0x23
"Out of disk space."	0x24
"Primary filesystem is inconsistent. Execute the **firmware restore** to restore the original firmware, or contact your service provider for recovery."	0x25
"The post-install script failed."	0x26
"Reload (partition) failed."	0x27
"Primary kernel partition is inconsistent. Contact your service provider for recovery."	0x28
"The pre-install script failed."	0x29
"Failed to install RPM package."	0x2b
"Cannot downgrade directly to this version. Downgrade to an intermediate version and then download the desired version."	0x2c
"Failed to validate firmware signature."	0x3e
"Failed to swap the firmware partitions."	0x40
"Failed to load the PROM image. Contact your service provider for assistance."	0x41

Recommended Action Execute the **show firmwaredownloadstatus** command for more information. Execute the **power-off** and **power-on** commands on the slot for recovery.

SULB-1105

Message `Firmware upgrade session (<session ID>: <session subject>) starts.`

Message Type AUDIT | LOG | VCS

Class FIRMWARE

Severity WARNING

Probable Cause Indicates that firmware upgrade has started.

Recommended Action No action is required.

SULB-1106

Message `Firmware upgrade session (<session ID>: <session subject>) completes.`

Message Type AUDIT | LOG | VCS

Class FIRMWARE

Severity WARNING

Probable Cause Indicates that firmware upgrade has completed successfully.

Recommended Action Execute the **show firmwaredownloadstatus** command for more information.

SULB-1107

Message `Firmware upgrade session (<session ID>: <session subject>) failed but recovered.`

Message Type LOG | VCS

Severity WARNING

Probable Cause Indicates that firmware upgrade has failed but was recovered.

Recommended Action Execute the **show firmwaredownloadstatus** command for more information. Execute the **firmware download** command again if needed.

SULB-1108

Message `Firmware upgrade session (<session ID>: <session subject>) failed.`

Message Type LOG | VCS

Severity CRITICAL

Probable Cause Indicates that firmware upgrade has failed.

Recommended Action Execute the **show firmwaredownloadstatus** command for more information. Execute the **firmware download** command again if needed.

SULB-1109

Message `Firmware upgrade session (<session ID>: <session subject>) aborted.`

Message Type LOG | VCS

Severity CRITICAL

Probable Cause Indicates that firmware upgrade has been aborted.

Recommended Action Execute the **firmware download** command again if needed.

SULB-1110

Message `Firmware upgrade session (<session ID>: <session subject>) has completed the installation successfully.`

Message Type LOG | VCS

Severity WARNING

Probable Cause Indicates that firmware upgrade has completed.

Recommended Action No action is required.

SULB-1111

Message `Logical chassis firmware download begins on rbridge-id <rbridge IDs>.`

Message Type LOG | VCS

Severity WARNING

Probable Cause Indicates that firmware upgrade has started.

Recommended Action No action is required.

SULB-1112

Message `Logical chassis firmware download has completed installation on rbridge-id <rbridge IDs>.`

Message Type LOG | VCS

Severity WARNING

Probable Cause Indicates that firmware upgrade has completed successfully.

Recommended Action No action is required.

SULB-1113

Message `Logical chassis firmware download will be aborted due to failover on rbridge-id <rbridge IDs>.`

Message Type LOG | VCS

Severity WARNING

Probable Cause Indicates that firmware upgrade failed.

Recommended Action Execute the **firmware recover** or **firmware activate** command.

SULB-1114

Message `Firmware installation has completed successfully on rbridge-id <rbridge IDs>. Please run 'firmware activate' for firmware activation.`

Message Type LOG | VCS

Severity INFO

Probable Cause Indicates that firmware upgrade has completed.

Recommended Action Execute the **firmware activate** command to activate the firmware.

SULB-1200

Message `Logical-chassis Firmware Auto-upgrade has started on remote node <rbridge id>.`

Message Type LOG | VCS

Severity INFO

Probable Cause Indicates that firmware auto-upgrade on remote node has started.

Recommended Action No action is required.

SULB-1201

Message `Logical-chassis Firmware Autdo-upgrade is in progress on remote node <rbridge id>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that firmware auto-upgrade on remote node is in progress.

Recommended Action No action is required.

SULB-1202

Message `Logical-chassis Firmware Auto-upgrade failed on remote node <rbridge id>.`

Message Type LOG | VCS

Severity ERROR

Probable Cause Indicates that firmware auto-upgrade failed on the remote node.

Recommended Action No action is required.

SULB-1203

Message `Logical-chassis Firmware download completed on remote node <rbridge id>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that firmware download has completed on the remote node.

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 failure to enable the switch because it is not in the ready state.

Recommended Action If the message persists, execute the **copy support** 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 **show secpolicy** command to verify whether the specified device World Wide Name (WWN) is listed. If it is not listed, execute the **secpolicy defined-policy** 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 modular switch, execute the **power-off** and **power-on** commands to power cycle the interface module.

For a compact switch, reload or power cycle the switch.

SWCH-1004

Message `Interface module attach failed during recovery, disabling slot = <slot number>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified interface module has failed during failover or recovery.

Recommended Action For a modular switch, execute the **power-off** and **power-on** commands to power cycle the interface module.

For a compact switch, reload 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 interface module attach operation has failed during failover or recovery.

Recommended Action For a modular switch, execute the **power-off** and **power-on** commands to power cycle the interface module.

For a compact switch, reload or power cycle the switch.

SWCH-1007

Message `Switch port <port number> disabled due to \"<disable reason>\".`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the specified switch port is disabled due to the reason displayed in the message.

Recommended Action Take corrective action to restore the port based on the disable reason displayed in the message and then execute the **shutdown** and **no shutdown** commands.

SWCH-1021

Message `HA state out of sync: Standby MM (ver = <standby SWC version>) does not support Dynamic area on default switch (Active MM version = <active SWC version>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the standby management module does not support the dynamic area on the default switch.

Recommended Action Load a firmware version in which the standby management module supports the dynamic area on the default switch using the **firmware download** command.

SWCH-1023

Message `HA state out of sync: Standby MM (ver = <standby SWC version>) does not support active's enforce_login policy (Active MM version =<active SWC version>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the standby management module does not enforce login policy of the active management module.

Recommended Action Configure the enforce login policy to a value that the standby management module supports.

SWCH-1024

Message `Rebooting the standby, received a duplicate update for port [<Port Number>]`

Message Type LOG | FFDC

Severity INFO

Probable Cause Indicates that the standby CP received duplicate port create event for a port which is probably due to LC coming online while syncing the backup MM. The standby CP reboots automatically to ensure sync and attain normal state. This is a rare occurrence.

Recommended Action No Action is required.

TNLD Messages

TNLD-1000

Message `TunnelMgr initialized successfully.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Data Center Ethernet (DCE) tunnel manager has been initialized.

Recommended Action None

TNLD-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 **show process memory** command.

Restart or power cycle the switch.

TNLD-1005

Message `TunnelMgr startup failed.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the Data Center Ethernet (DCE) tunnel manager 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 version using the **firmware download** command.

TNLD-1006

Message `Tunnel <tunnel ID> creation failed.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the tunnel creation was unsuccessful.

Recommended Action Technical support is required.

TNLD-1007

Message `Tunnel <tunnel ID> deletion failed.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the tunnel deletion was unsuccessful.

Recommended Action Technical support is required.

TNLD-1008

Message `Tunnel Termination and Origination Table in Asic have reached high watermark.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that tunnel resource is full. No more tunnels can be created in the system.

Recommended Action Technical support is required.

TNLD-2001

Message `NSX controller pushed more than <Safe Ucast_Macs_Remote limit> Ucast_Macs_Remote objects. This may result in unexpected traffic behavior.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the switch may be connecting to NSX controllers having huge number of configurations which are beyond scale capacity of the switch. There could be traffic loss or unexpected behavior.

Recommended Action Update configurations in NSX controller accordingly.

TNLD-2011

Message `Delete duplicate Mcast_Macs_Remote entry; MAC=\"<Multicast MAC>\", logical_switch=\"<Logical_Switch name>\".`

Message Type LOG

Severity ERROR

Probable Cause Indicates an unexpected error while communicating to the VMware NSX controller.

Recommended Action Undo all operations and try again.

TNLD-2012

Message `Local MAC \"<MAC address>\" already exists in Ucast_Macs_Remote table; skipping write to Ucast_Macs_Local.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that Layer 2 system (L2SYS) has notified a MAC entry that was learned from the VMware NSX controller.

Recommended Action Undo all operations and try again.

TNLD-2013

Message `Failed to cleanup Overlay Gateway Configuration during reconcile.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that cleanup of tunnels or local MAC entries has failed in the back-end.

Recommended Action Undo all operations and try again.

TNLD-2014

Message `Tunnel id conflict detected for one or more tunnels. Automatic recovery initiated.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that tunnel ID conflict is detected for one or more tunnels.

Recommended Action The system initiates automatic recovery.

TOAM Messages

TOAM-1000

Message `Cannot run this command because VCS is disabled.`

Message Type DCE

Severity INFO

Probable Cause Indicates inability to run the TRILL OAM (TOAM) commands because VCS is disabled.

Recommended Action To run the TOAM commands, enable VCS using the **vcs enable** command.

TOAM-1003

Message `Initilization error: <reason>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that TRILL OAM (TOAM) has encountered an error during initialization.

Recommended Action Reload or power cycle the switch.

TRCE Messages

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 If the message persists, execute the **copy support** 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 **copy support** 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 management module was unable to alert the standby management module of a change in the trace status. This message is only applicable to modular switches.

Recommended Action This message is often transitory. Wait a few minutes and try the command again.

If the message persists, execute the **copy support** 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 management module is unable to read the stored trace parameters.

Recommended Action Reload the switch or the chassis.

If the message persists, execute the **copy support** 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 standby management module is unable to communicate trace information to the active management module. This message is only applicable to modular switches.

Recommended Action Execute the **show ha** command to verify that the current management module is standby and the active management module is active.

If the message persists, execute the **copy support** 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 If the message persists, reload the switch or the chassis.

Execute the **copy support** 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 **copy support** command and contact your switch service provider.

TS Messages

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 that the switch 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 switch clock.
- 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. If the message does not recur, it can be ignored.

Recommended Action Execute the **show ntp status** command to verify that the switch clock server IP address is configured correctly. Verify if this clock server is accessible to the switch and functional. If it is not accessible or functional, configure an accessible and functional clock server or reset the clock server to local clock server (LOCL).

TS-1008

Message `<New clock server used> Clock Server used instead of <Old server configured>. System time changed from <Old time> to <New time>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the source of switch time synchronization was changed to another configured clock server because the Network Time Protocol (NTP) query to the current active external clock server failed.

Recommended Action No action is required. New clock server synchronization will adjust the clock time.

TS-1009

Message `Event: change time: attempt.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates an attempt to change the switch time.

Recommended Action No action is required.

TS-1010

Message `Event: change time: <success or fail>, Info: <result detail>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates the status of the switch time change.

Recommended Action No action is required.

TS-1011

Message `Event: change time zone: attempt.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates an attempt to change the time zone.

Recommended Action No action is required.

TS-1012

Message `Event: change time zone: <success or fail>, Info: <result detail>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates the status of the time zone change.

Recommended Action No action is required.

TS-1013

Message `Event: Clock Server change, Status: success, Info: <New clock server used> Clock Server used instead of <Old server configured>. System time changed from <Old time> to <New time>.`

Message Type AUDIT

Class SECURITY

Severity INFO

Probable Cause Indicates that the clock server and the system time have been changed.

Recommended Action No action is required.

UCST Messages

UCST-1003

Message `Duplicate Path to RBridge <RBridge 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 RBridge from the output port. The *PDB pointer* value displayed in the message is the address of the path database (PDB) and provides debugging information.

Recommended Action No action is required.

UDLD Messages

UDLD-1000

Message `UDLD is enabled.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the UniDirectional Link Detection (UDLD) protocol is enabled globally.

Recommended Action No action is required.

UDLD-1001

Message `UDLD is disabled.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the UniDirectional Link Detection (UDLD) protocol is disabled globally.

Recommended Action No action is required.

UDLD-1002

Message `UDLD Hello time has changed.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the UniDirectional Link Detection (UDLD) Hello time has been changed.

Recommended Action No action is required.

UDLD-1003

Message `UDLD Multiplier timeout has changed.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the UniDirectional Link Detection (UDLD) timeout multiplier value has been changed.

Recommended Action No action is required.

UDLD-1004

Message `UDLD is enabled on interface <InterfaceName>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the UniDirectional Link Detection (UDLD) protocol is enabled on the specified interface.

Recommended Action No action is required.

UDLD-1005

Message `UDLD is disabled on interface <InterfaceName>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the UniDirectional Link Detection (UDLD) protocol is disabled on the specified interface.

Recommended Action No action is required.

UDLD-1006

Message `Link status on interface <InterfaceName> is down. Unidirectional link detected.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the specified interface has been detected as a unidirectional link. The interface is blocked.

Recommended Action Action must be taken to fix the unidirectional link.

UDLD-1007

Message `Link status on interface <InterfaceName> is up. Bidirectional link detected.`

Message Type LOG

Severity INFO

Probable Cause Indicates that UniDirectional Link Detection (UDLD) PDUs are being received on a link that was considered unidirectional.

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 (RBridge ID list).

Recommended Action No action is required. This error will end the current shortest path first (SPF) computation.

VC Messages

VC-1000

Message `vCenter <vCenterName> configuration is added.`

Message Type LOG

Severity INFO

Probable Cause Indicates that a new vCenter configuration was added.

Recommended Action No action is required.

VC-1001

Message `vCenter <vCenterName> configuration is changed.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified vCenter configuration has been updated.

Recommended Action No action is required.

VC-1002

Message `vCenter <vCenterName> configuration is deleted.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified vCenter configuration has been deleted.

Recommended Action No action is required.

VC-1003

Message `vCenter <vCenterName> configuration has been activated successfully.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified vCenter configuration has been activated.

Recommended Action No action is required.

VC-1004

Message `vCenter <vCenterName> configuration has been deactivated successfully.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the specified vCenter configuration has been deactivated.

Recommended Action No action is required.

VC-1005

Message `Login to vCenter <vCenterName> failed (attempt(s) <failedAttempts>) - check credentials for user <userName>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that the vCenter login failed due to invalid credentials.

Recommended Action Enter the correct username and password for the vCenter.

VC-1006

Message `vCenter <vCenterName> periodic discovery interval has been changed to <interval> minutes.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the periodic discovery timer interval has been changed for the specified vCenter.

Recommended Action No action is required.

VC-1007

Message `vCenter <vCenterName>: ignore-delete-all-response has been changed to <ignore_count> cycles.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the vCenter ignore invalid discovery cycle count has been changed.

Recommended Action No action is required.

VC-1008

Message `Ignoring no data from vCenter <url> - cycle: <ignore_count>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the cycle for which no data is received from vCenter has been ignored.

Recommended Action No action is required.

VC-1009

Message `No data received from vCenter <url>, proceeding with discovery after specified <ignore_count> cycles.`

Message Type LOG

Severity WARNING

Probable Cause Indicates proceeding with discovery after receiving invalid data from vCenter.

Recommended Action No action is required.

VC-1010

Message `vCenter <vCenterName> : ignore-delete-all-response value has been changed to ALWAYS.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the vCenter ignore invalid discovery cycle count has been changed to "always".

Recommended Action No action is required.

VC-1011

Message `vCenter <url> : ignoring invalid discovery - ALWAYS.`

Message Type LOG

Severity WARNING

Probable Cause Indicates the cycle for which there was an invalid discovery has been ignored.

Recommended Action No action is required.

VC-1100

Message `START: <discType> discovery of virtual assets from vCenter <vCenterName> @ <url>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the discovery of assets has started for the specified vCenter.

Recommended Action No action is required.

VC-1101

Message `END: <discType> discovery of virtual assets from vCenter <vCenterName> @ <url>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the discovery of assets has completed for the specified vCenter.

Recommended Action No action is required.

VC-1103

Message `Connect to vCenter <vCenterName> failed @ <url> : <failureReason>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that connection to vCenter failed.

Recommended Action Ensure reachability to vCenter, and check vCenter credentials and vCenter version.

VC-1104

Message `vCenter profile <profile> creation failed : <failureReason>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that port-profile creation has failed.

Recommended Action Ensure that port-profiles can be created on the switch.

VCS Messages

VCS-1001

Message `Event: VCS cluster create, Coordinator IP: <Coordinator's Public IP>, VCS ID: <VCS Id>, Status: <Cluster status>.`

Message Type LOG | VCS

Severity INFO

Probable Cause Indicates that the VCS cluster has been created due to the initial VCS logical-chassis enable on two or more nodes where a VCS cluster of the same VCS ID did not exist before.

Recommended Action No action is required.

VCS-1002

Message `Event: VCS cluster create, Coordinator IP: <Coordinator's Public IP>, VCS ID: <VCS Id>, Status: VCS cluster failed to be created, Reason: <Error Reason>.`

Message Type LOG | VCS

Severity ERROR

Probable Cause Indicates that the VCS cluster failed to be created. Refer to the reason code for the cause of the error.

Recommended Action Refer to reason code for possible action.

VCS-1003

Message `Event: VCS node add, Coordinator IP: <Coordinator's Public IP>, VCS ID: <VCS Id>, Status: rBridge ID <RBridge-id of Added Switch> (<IP of Added Switch>) added to VCS cluster.`

Message Type LOG | VCS

Severity INFO

Probable Cause Indicates that a logical-chassis node has been added to the VCS cluster. The node was added because the VCS logical-chassis is enabled on a node that was not a member of the VCS cluster.

Recommended Action No action is required.

VCS-1004

Message `Event: VCS node add, Coordinator IP: <Coordinator's Public IP>, VCS ID: <VCS Id>, Status: rBridge ID <RBridge-id of Switch That Failed To Be Added> (<IP of Switch That Failed To Be Added>) failed to be added to VCS cluster, Reason: <Error Reason>.`

Message Type LOG | VCS

Severity ERROR

Probable Cause Indicates that a logical-chassis node failed to be added to the VCS cluster. Refer to the reason code for the cause of the error.

Recommended Action Refer to reason code for possible action.

VCS-1005

Message `Event: VCS node rejoin, Coordinator IP: <Coordinator's Public IP>, VCS ID: <VCS Id>, Status: rBridge ID <RBridge-id of Rejoined Switch> (<IP of Rejoined Switch>) rejoined VCS cluster.`

Message Type LOG | VCS

Severity INFO

Probable Cause Indicates that the logical-chassis node has gone offline and returned online without any configuration changes.

Recommended Action No action is required.

VCS-1006

Message `Event: VCS node rejoin, Coordinator IP: <Coordinator's Public IP>, VCS ID: <VCS Id>, Status: rBridge ID <RBridge-id of Switch That Failed To Rejoin> (<IP of Switch That Failed To Rejoin>) failed to rejoin VCS cluster, Reason: <Error Reason>.`

Message Type LOG | VCS

Severity ERROR

Probable Cause Indicates that the logical-chassis node has failed to rejoin the existing VCS cluster. Refer to the reason code for the cause of the error.

Recommended Action Refer to reason code for possible action.

VCS-1007

Message `Event: VCS node remove, Coordinator IP: <Coordinator's Public IP>, VCS ID: <VCS Id>, Status: rBridge ID <RBridge-id of Removed Switch> (<IP of Removed Switch>) removed from VCS cluster.`

Message Type LOG | VCS

Severity INFO

Probable Cause Indicates that VCS is disabled on the node that was part of a VCS cluster.

Recommended Action No action is required.

VCS-1008

Message `Event: VCS node remove, Coordinator IP: <Coordinator's Public IP>, VCS ID: <VCS Id>, Status: rBridge ID <RBridge-id of Switch That Failed To Be Removed> (<IP of Switch That Failed To Be Removed>) failed removal from VCS cluster, Reason: <Error Reason>.`

Message Type LOG | VCS

Severity ERROR

Probable Cause Indicates that a logical-chassis node failed to be removed from the VCS cluster. Refer to the reason code for the cause of the error.

Recommended Action Refer to reason code for possible action.

VCS-1009

Message `Event: VCS node disconnect, Coordinator IP: <Coordinator's Public IP>, VCS ID: <VCS Id>, Status: rBridge ID <RBridge-id of Switch That Disconnected> (<IP of Switch That Disconnected >) disconnected from VCS cluster.`

Message Type LOG | VCS

Severity INFO

Probable Cause Indicates that the heartbeat loss to a logical-chassis node occurred because the node was reloaded or all interswitch links (ISLs) to the node are down.

Recommended Action If you had issued the **reload** command, no action is required. If for another reason, check the state of the disconnected node and the ISLs to the disconnected node.

VCS-1010

Message `Event: Pending DB commit, Coordinator IP: <Coordinator's Public IP>, VCS ID: <VCS Id>, Status: DB operation stuck longer than expected on rbridgeId <RBridge-id of switch that is stuck>.`

Message Type LOG | VCS

Severity INFO

Probable Cause Indicates that DB commit operation is taking longer time than expected.

Recommended Action If you had issued the **reload** command, no action is required. Node might need to be isolated if it cannot be recovered following a reboot.

VCS-1011

Message `Event: VCS configuration backup, Coordinator IP: <Coordinator's Public IP>, VCS ID: <VCS Id>, Status: VCS configuration backup completed successfully.`

Message Type LOG | VCS

Severity INFO

Probable Cause Indicates that a VCS configuration backup has been saved successfully across all nodes in the VCS cluster.

Recommended Action No action is required.

VCS-1012

Message `Event: VCS configuration backup, Coordinator IP: <Coordinator's Public IP>, VCS ID: <VCS Id>, Status: VCS configuration backup failed, Reason <Error Reason>.`

Message Type LOG | VCS

Severity ERROR

Probable Cause Indicates that a VCS configuration backup could not be saved.

Recommended Action Refer to reason code for possible action.

VRRP Messages

VRRP-1001

Message `<message>: <message>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the system has failed to allocate memory.

Recommended Action Check the memory usage on the switch using the **show process memory** command.
Reload or power cycle the switch.

VRRP-1002

Message `<msg>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the Virtual Router Redundancy Protocol (VRRP) session state has changed.

Recommended Action No action is required.

VRRP-1003

Message `<msg>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the Virtual Router Redundancy Protocol (VRRP) session is enabled.

Recommended Action No action is required.

VRRP-1004

Message `<msg>.`

Message Type DCE

Severity INFO

Probable Cause Indicates that the Virtual Router Redundancy Protocol (VRRP) session is disabled.

Recommended Action No action is required.

VRRP-1501

Message `<message>: <message>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates that the system has failed to initialize.

Recommended Action Reload or power cycle the switch.

VRRP-2001

Message `<message>: <message>.`

Message Type DCE

Severity ERROR

Probable Cause Indicates a connection, transfer, or receiving error in the socket.

Recommended Action If this is a modular switch, execute the **ha failover** command. If the problem persists or if this is a compact switch, download a new firmware version using the **firmware download** command.

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 SSL certificate file is either invalid or absent.

Recommended Action Install a valid key 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 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 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 HTTP logfile 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 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 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, where the built-in recovery process has failed to restore http services. The problem often results from invalid configuration of SSL certificates, but therecan be more than one reason for such a failure.

Recommended Action Verify the certification file as there may be a mismatch involved.

WEBD-1009

Message `<Message>`

Message Type LOG

Severity INFO

Probable Cause Indicates that the HTTP or HTTPS server configuration has changed.

Recommended Action No action is required.

WLV Messages

WLV-1001

Message `Port <port number> port fault. Change the SFP transceiver 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.

WLV-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 interface module or switch will be disrupted.

Recommended Action For a modular switch, execute the **power-off** and **power-on** commands to power cycle the interface module.

For a compact switch, reload or power cycle the switch.

WLV-1003

Message `PORT:<port number> Slot:<Slot num> faulted due to excessive link flapping. Check the SFP transceiver/cable and issue shutdown/no shutdown commands to recover.`

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 cable is not faulty. Replace the SFP transceivers or the cable, if necessary. Execute the **shutdown** and **no shutdown** commands to restart the link up process.

WLV-1004

Message `Port <port number> faulted due to excessive Symbol Errors. Check the SFP/QSFP transceiver/cable and issue shutdown/no shutdown commands to recover.`

Message Type LOG

Severity WARNING

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

Recommended Action Verify that compatible SFP or QSFP transceivers are used on the peer ports, the SFP or QSFP transceivers have not deteriorated, and the cable is not faulty. Replace the SFP or QSFP transceivers or the cable, if necessary. Execute the **shutdown** and **no shutdown** commands to restart the link-up process.

ZONE Messages

ZONE-1010

Message `Duplicate entries in zone (<zone name>) specification.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that there are duplicate entries in a zone object. A zone object member is specified twice in a given zone object. This message occurs only when enabling a zone configuration.

Recommended Action Check the members of the zone and delete the duplicate member using the **no member-zone** command.

ZONE-1015

Message `Not owner of the current transaction <transaction ID>.`

Message Type LOG

Severity WARNING

Probable Cause Indicates that a zoning change operation was not allowed because the zoning transaction was 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-1019

Message `Transaction Commit failed. Reason code <reason code> (<Application reason>) - \"<reason string>\".`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the 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 **show zoning operation-info** command to know if there is any outstanding transaction running on the local switches.

If the message persists, execute the **copy support** command and contact your switch service provider.

ZONE-1022

Message `The effective configuration has changed to <Effective configuration name>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the effective zone configuration has changed to the specified configuration 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 interface (<interfaceName>) is busy. Retrying zone merge.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the switch is retrying the zone merge operation. This usually occurs if the switch on the other side of the port is busy.

Recommended Action If the message persists, execute the **copy support** command and contact your switch service provider.

ZONE-1024

Message `<Information message>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the **zoning enabled-configuration cfg-action cfg-save** command was executed successfully.

Recommended Action No action is required.

ZONE-1027

Message `Zoning transaction aborted <error reason>.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the zoning transaction was aborted because of 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 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 Edit the zone database to keep it within the allowable limit for the specific switches in your fabric. You can view the zone database size information using the **show zoning operation-info** command.

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 was faulty. This error will save the faulty zone configuration in the zoned core file directory.

Recommended Action If the message persists, execute the **copy support** 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 Network 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 by deleting some zones and retry the operation. Refer to the *Network OS Administrator's Guide* for instructions to delete a zone.

ZONE-1037

Message `Unable to examine <config file name>: error message <System Error Message>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that the Network 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 by deleting some zones and retry the operation. Refer to the *Network OS Administrator's Guide* for instructions to delete a zone.

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 Network 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 by deleting some zones and retry the operation. Refer to the *Network OS Administrator's Guide* for instructions to delete a zone.

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 Network 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 by deleting some zones and retry the operation. Refer to the *Network OS Administrator's Guide* for instructions to delete a zone.

ZONE-1040

Message `Merged zone database exceeds limit.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the Network 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 by deleting some zones and retry the operation. Refer to the *Network OS Administrator's Guide* for instructions to delete a zone.

ZONE-1041

Message `Unstable link detected during merge at interfaceName (<interfaceName>).`

Message Type LOG

Severity WARNING

Probable Cause Indicates a possible unstable link or a faulty cable.

Recommended Action Verify that the small form-factor pluggable (SFP) transceiver and cable at the specified port are not faulty. Replace the SFP transceiver and cable if necessary.

ZONE-1042

Message `The effective configuration has been disabled.`

Message Type LOG

Severity INFO

Probable Cause Indicates that the effective 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-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 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-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 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-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 acquire change authorization (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 management module using the **ha sync start** command.

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 **zoning enabled-configuration cfg-name** *cfgName* 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 high availability (HA) synchronization has failed using the **show ha** command. If HA synchronization has failed, execute the **ha sync start** command on active CP to resynchronize the HA state.

ZONE-1066

Message `Zoning operation failed to complete on the local switch - code <Error Code>.`

Message Type LOG

Severity ERROR

Probable Cause Indicates that an inter process communication (IPC) error occurred between the Name Server and the 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 the **zoning enabled-configuration cfg-action cfg-clear** command.

If there is an enabled-configuration, commit the **zoning enabled-configuration cfg-action cfg-clear** operation by issuing **no zoning enabled-configuration cfg-name**.

If there is no enabled-configuration, commit the **zoning enabled-configuration cfg-action cfg-clear** operation by issuing **zoning enabled-configuration cfg-action cfg-save**.