53-1002489-01
15 December 2011

Network OS

Message Reference

Supporting Network OS v2.1.1

BROCADE

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. shall have no liability or responsibility to any person or entity with respect to any loss, cost, liability, or damages arising from the information contained in this book 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, and TS. • Added new messages: L2SS, PORT, SEC, and SSMD. • Modified messages: L2SS, SEC, and ZONE.	December 2011

Contents

About This Document

Chapter 1 Introduction to System Messages

Chapter 5 DOT1 System Messages

Chapter 9 FABR System Messages

Chapter 10 FCOE System Messages

Chapter 11 **FVCS System Messages**

Chapter 12 **FW System Messages**

Chapter 22 **NSM System Messages**

Section II Audit Log Messages

Chapter 42 AUDIT DCM System Messages

Chapter 43 AUDIT RAS System Messages

Chapter 44 AUDIT SEC System Messages

About This Document

In this chapter

How this document is organized

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

The document contains the following components:

- Chapter 1, "Introduction to System Messages" provides basic information on system messages.
- Chapters 2 through 46 provide message syntax, probable cause, recommended action, and severity for each of the system messages.

Supported hardware and software

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

Although many different software and hardware configurations are tested and supported by Brocade Communications Systems, Inc. for Network OS v2.1.1, 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 6710
- Brocade VDX 6720-24
- Brocade VDX 6720-60

- Brocade VDX 6730-32
- Brocade VDX 6730-76

NOTE
The information on the bladed system, active CP, and standby CP in the system messages is not applicable to Network OS v2.1.1.

What's new in this document

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

- Information that was added:
  - AUTH System Messages
  - C2 System Messages
  - ELD System Messages
  - L2SS System Messages
  - PORT System Messages
  - RCS System Messages
  - SEC System Messages
  - SSMD System Messages
  - TS System Messages
- Information that was changed:
  - L2SS System Messages
  - SEC System Messages
  - ZONE System Messages
  - AUDIT SEC System Messages
- Information that was deleted:
  - FW System Messages
  - ZONE System Messages

Document conventions

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

Text formatting

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

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

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

Command syntax conventions

Command syntax in this manual follows these conventions:

command	Commands are printed in bold.
variable	Variables are printed in italics.
[ ]	Keywords or arguments that appear within square brackets are optional.
{ x | y | z }	A choice of required keywords appears in braces separated by vertical bars. You must select one.
`screen font`	Examples of information displayed on the screen.
< >	Non-printing characters, for example, passwords, appear in angle brackets.

Notes, cautions, and warnings

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

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

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

Key terms

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

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

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

Notice to the reader

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

These references are made for informational purposes only.

Corporation	Referenced trademarks and products
Microsoft Corporation	Windows
Red Hat, Inc.	Red Hat package manager (RPM)

Additional information

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

Brocade resources

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

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

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

For additional Brocade documentation, visit the Brocade website:

http://www.brocade.com

Other industry resources

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

http://www.t11.org

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

http://www.fibrechannel.org

Getting technical help

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

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

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

   The serial number label for the Brocade VDX 6710, Brocade VDX 6720, and Brocade VDX 6730 is located on the switch ID pull-out tab located on the bottom of the port side of the switch.

Document feedback

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

documentation@brocade.com

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

Chapter

Introduction to System Messages

1

In this chapter

Overview of system messages

This guide supports Brocade Network OS v2.1.1 and documents system messages that can help you diagnose and fix problems with a switch or network. The guide is organized alphabetically by module name. A *module* is a subsystem in the Network OS. Each module generates a set of numbered messages. For each message, this guide provides message text, probable cause, recommended action, and severity level. There may be more than one cause and more than one recommended action for any given message. This guide discusses the most probable cause and typical action recommended.

This chapter provides an introduction to system messages. The Network OS maintains an internal system message log of all messages. All messages are tagged by type as either RASLog system error messages, Audit messages, or both. RASLog error messages are primarily designed to indicate and log abnormal, error-related events, whereas Audit messages record events such as login failures, zone changes, or configuration changes. Network OS supports a different methodology for storing and accessing each type of message.

System message types

Network OS supports four types of system messages. A system message can be of one or more of the following types.

RASLog messages

RASLog messages report significant events or information and are also used to show the status of the high-level user-initiated actions. RASLog messages are forwarded to the console, to the configured syslog servers, and through the SNMP traps or informs.

The following is an example of a RASLog 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 Log messages, refer to "Viewing and clearing RASLog messages" on page 9.

VCS RASLog messages

VCS RASLog messages are supported in the management cluster. A VCS message is generated from any VCS node and is distributed to all the nodes in the management cluster. The VCS RASLog messages are used to broadcast fabric-wide events such as node removal and node join from the cluster.

When a node generates a VCS RASLog message, it is forwarded to the system console, remote syslog, SNMP, and is distributed to the other nodes in the cluster. The node that receives the VCS message displays the message in the system console and the message is not forwarded to the remote syslog and SNMP.

The following is an example of the 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.
```

For information on displaying and clearing the VCS RASLog messages, refer to "Viewing and clearing RASLog messages" on page 9.

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. In Network OS v2.1.1, the 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 1 can be audited.

TABLE 1 Event classes of the Audit messages

Event class	Operand	Description
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.
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.

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 10.

FFDC messages

First Failure Data Capture (FFDC) is used to capture failure-specific data when a problem or failure is first noted before the switch reboots, or trace and log buffer get wrapped. 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 or analyzing the problem.

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 the 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.
```

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. For all cases, you must look at each specific error message description thoroughly before taking action. System messages have the severity levels as listed in Table 2.

TABLE 2 Severity levels of the system 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.

TABLE 2 Severity levels of the system messages (Continued)

Severity level	Description
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 relay 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.

System error message logging

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

- All RASLog error messages are saved to nonvolatile storage by default.
- The system error message log can save a maximum of 4096 messages.
- The system 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 (0x7ffffff). The sequence number continues to increase after the message log wraps around. The sequence number can be reset to 1 using the **clear logging raslog** command. The sequence number is persistent across power cycles and switch reboots.
- By default, the **show logging raslog** command displays all the system error messages.
- Trace dump, FFDC, and core dump files can be uploaded to the FTP server using the **copy support ftp** command.
- It is recommended to configure the syslogd facility as a management tool for error logs. This is important for dual-domain switches because the syslogd facility saves messages from two logical switches as a single file and in sequential order. For more information, refer to “System logging daemon” on page 4.

Configuring the syslog message destinations

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

System logging daemon

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

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 system error messages and Audit 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 system events and error 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.

   ```
   switch# configure terminal
   Entering configuration mode terminal
   ```

2. Execute the **logging syslog-server** *IPv4 address* command to add a server to which system messages are forwarded.

   ```
   switch(config)# logging syslog-server 172.26.3.83
   ```

   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.

   ```
   switch# show running-config logging syslog-server
   logging syslog-server 172.26.3.83
   ```

You can remove a configured syslog server using the **no logging syslog-server** *IPv4 address* command.

System console

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

The system console displays messages only through the serial port. If you log into 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 and syslog (if enabled).

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 filtered up to and include the configured severity level. 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.

   ```
   switch# 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: 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.

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

3. Execute the **copy running-config startup-config** command to save the configuration changes.

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 v2.1.1 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 7.

SNMP informs

An SNMP inform is similar to the 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 inform request can be sent again. An SNMP inform request is saved in the switch memory until a response is received or the request times out. The informs are more reliable and they consume more resources in the device and in the network. Use SNMP informs only if it is important that the management station receives all event notifications. Otherwise, use the SNMP traps.

Brocade devices support SNMPv3 informs. For more information, refer to "Configuring the SNMPv3 server" on page 8.

Port logs

The Network OS maintains an internal log of all port activity. Each switch or logical switch maintain a log file for each port. Port logs are circular buffers that can save up to 8,000 entries per logical switch. When the log is full, the newest log entries overwrite the oldest log entries. Port logs capture switch-to-device, device-to-switch, switch-to-switch, some device A-to-device B, and control information. Port logs are not persistent and are lost over power cycles and reboots.

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 v2.1.1 supports SNMP version 1, version 2c, and version 3. Use the commands listed in Table 3 to configure the SNMPv1, SNMPv2c, and SNMPv3 hosts and their configurations.

TABLE 3 Commands for configuring SNMP server hosts

Command	Description
[no] **snmp-server host** *ipv4 host* **community-string** [**version** [**1** | **2c**]] [**udp-port** *port*] [**severity-level** [**None** | **Debug** | **Info** | **Warning** | **Error** | **Critical**]]	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 added 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** *host-addr username* [**notifytype** {**traps** | **informs**}] **engineid** *engine-id* **udp-port** *port_number* **severity-level** [**None** |**Debug** | **Info** | **Warning** | **Error** | **Critical**]	This command specifies the recipient of the SNMP version 3 notification option. The **severity-level** option is added 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.

```
switch# configure terminal
Entering configuration mode terminal
```

2. Execute the following command to set the trap recipient with IP address 172.26.1.93, which receives all traps with the severity levels of Critical, Error, Info, and Warning.

```
switch(config)# snmp-server host 172.26.1.93 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.

```
switch(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 172.26.1.93 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: trap or inform. 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.

```
switch# configure terminal
Entering configuration mode terminal
```

2. Execute the following command to set the inform recipient with IP address 172.26.1.93, which receives all traps with the severity levels of Critical, Error, Info, and Warning.

```
switch(config)# snmp-server v3host 172.26.1.93 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, 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.

```
switch# 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 groupname snmpadmin auth md5 auth-password * priv
DES priv-password *
snmp-server user snmpadmin2 groupname snmpadmin auth-password * priv-password
*
snmp-server user snmpadmin3 groupname snmpadmin auth-password * priv-password
*
snmp-server user snmpuser1 auth-password * priv-password *
snmp-server user snmpuser2 auth-password * priv-password *
snmp-server user snmpuser3 auth-password * priv-password *
snmp-server v3host 172.26.1.93 snmpadmin1
 udp-port 4425
 notifytype informs
 engineid 80:00:05:23:01:AC:1A:01:79
 severity-level Info
!
```

Viewing and clearing RASLog messages

This section provides information on viewing and clearing the system message logs.

Displaying the RASLog messages

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

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

```
switch# show logging raslog
NOS: v2.1.1

2011/09/14-04:52:05, [LOG-1003], 1,, INFO, VDX6720-60, The 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.

2011/09/14-04:58:25, [SULB-1001], 3,, WARNING, VDX6720-60, firmware download
command has started.

2011/09/14-05:05:21, [SULB-1002], 4,, INFO, VDX6720-60, firmware download
command has completed successfully.

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

2011/09/14-05:10:14, [HAM-1004], 6,, INFO, VDX6720-60, Processor rebooted -
FirmwareDownload.
```

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.

NOTE

The **clear logging raslog** command clears all the VCS RASLog messages on the local switch and does not affect the other nodes in the cluster.

Viewing, clearing, and configuring Audit 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.

   ```
   switch# show logging auditlog

   0 AUDIT,2011/08/26-07:50:42 (GMT), [SEC-3034], INFO, SECURITY,
   NONE/root/NONE/None/CLI,, VDX6720-24, Event: AAA Authentication Login Mode
   Configuration, Status: success, Info: Authentication configuration changed
   from Local Only to Local Only.

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

   2 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,.

   3 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.

   4 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.

   5 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.

   ```
   switch# 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.

```
switch# logging auditlog class
Possible completions:
  CONFIGURATION  FIRMWARE  SECURITY
switch# logging auditlog class CONFIGURATION
```

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

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

Reading the system messages

This section provides information about reading the system messages.

RAS system messages

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

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.
```

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

TABLE 4 System 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 (0x7ffffff). The sequence number continues to increase after the message log wraps around, i.e. the oldest message in the log is deleted when a new message is added. The sequence number can be reset to 1 using the **clear logging raslog** command. The sequence number is persistent across power cycles and switch reboots.

TABLE 4 System message field description (Continued)

Variable name	Description
Flags	For most messages, this field contains a space character (null value) indicating that the message is neither an FFDC or VCS message. Messages may contain the following values: • FFDC–Indicates that additional first failure data capture information has also been generated for this event. • VCS–Indicates a VCS message generated by a node in the management cluster.
Severity	The severity level of the notification: • 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 RASLog 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 5.

TABLE 5 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 error: • CRITICAL • ERROR • WARNING • INFO

TABLE 5 Audit message field description (Continued)

Variable name	Description
Event Class	The event class: • SECURITY • DCMCFG • FIRMWARE • SYSTEM
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 system message

This section provides procedures on gathering information on system messages.

Looking up a system message

Error messages in this manual are arranged alphabetically. To look up an error message, copy down the module (see Table 6 on page 15) and the error code and compare this with the Table of Contents to determine the location of the information for that error message.

The following information is provided for each message:

- Module and code name for the error
- Message text
- Probable cause
- Recommended action
- Message severity

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 level?
- What is the switch hardware version?
- Is the switch operational?

- Assess impact and urgency:
  - Is the switch down?
  - Is it a standalone switch?
  - How large is the fabric?
  - Is the fabric redundant?
- Execute the **show logging raslog** command on each logical 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 security enabled?
- Was 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 system messages (RASLog), the trace files, and the output of the **copy support** command to an off-switch storage location through FTP or SCP. 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 6 provides a summary of the system modules for which messages are documented in this reference guide; the system modules are listed alphabetically by name.

TABLE 6 System module descriptions

System module	Description
AUTH	Authentication error messages indicate problems with the authentication module of the Network OS.
C2	Condor2 error messages indicate problems with the Condor2 ASIC driver module of the Network OS.
DCM	Distributed Configuration Manager (DCM) messages indicate major switch bootup events, user login or logout, and the configuration operations.
DOT1	DOT1 error messages indicate problems with the 802.1x authentication module of the Network OS.
EANV	EANV module messages indicate any issues associated with eAnvil ASIC operation and eAnvil ASIC driver operations.
ELD	End Loop Detection (ELD) messages indicate a loop in the Layer 2 network and the status of the port on which the loop is detected.
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.
FABR	The FABR (network of Fibre Channel switches) error messages come from the fabric daemon. The fabric daemon follows the FC-SW-3 standard for the fabric initialization process, such as determining the E_Ports, assigning unique domain IDs to switches, creating a spanning tree, throttling the trunking process, and distributing the domain and alias lists to all switches in the fabric.
FCOE	FCoE error messages indicate problems with the Fibre Channel over Ethernet (FCoE) module of the Network OS.
FVCS	The Fabric Services VCS (FVCS) daemon provides fabric distribution services for Virtual Cluster Switch (VCS) and Virtual Link Aggregation Group (vLAG).

TABLE 6 System module descriptions (Continued)

System module	Description
FW	The Fabric Watch (FW) module monitors thresholds for many switch subsystems; for example, temperature, voltage, fan speed, and switch status. Any changes that cross a specified threshold are reported to the system message log.
HAM	HAM is a user-space daemon responsible for the high availability management.
HIL	The HIL module messages indicate any issues associated with the Hardware Independent Layer (HIL) for general platform components, such as Environmental Monitoring (EM), FAN and PSU subsystems, and other platform FRUs.
HSL	HSL error messages indicate problems with the Hardware Subsystem Layer (HSL) of the Network OS.
IGMP	IGMP module messages indicate any issue associated with the Internet Group Management Protocol (IGMP) snooping feature.
IPAD	System messages generated by the IP admin demon.
L2SS	L2SS error messages indicate problems with the Layer 2 system manager that controls the Layer 2 forwarding engine and controls the learning, aging, and forwarding functionality.
L3SS	The L3SS module messages indicate any issues associated with IP forwarding, ARP, and IP routes.
LOG	The LOG module messages describe events and problems associated with the RASLog and Audit log facilities.
MSTP	MSTP error messages indicate problems with Multiple Spanning Tree Protocol (MSTP) modules of the Network OS.
NSM	NSM error messages indicate problems with the Interface management and VLAN management module of the Network OS.
ONMD	ONMD error messages indicate problems with the Operation, Administration and Maintenance module of the Network OS.
PHP	PHP module messages indicate any important information associated with the discovery and creation, deletion, and updating of the port profiles.
PLAT	PLAT messages indicate hardware problems.
PORT	PORT error messages refer to the front-end user ports on the switch. Front-end user ports are directly accessible by users to connect end devices or connect to other switches.
RAS	Informational messages 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.
RTWR	The reliable transport write 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.
SEC	The security daemon generates 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 6 System module descriptions (Continued)

System module	Description
SFLO	sFlow is a standard-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 error or information related to sflowd daemon.
SNMP	Simple Network Management Protocol (SNMP) is an universally supported low-level protocol that allows simple get, get next, and set requests to go to the switch (acting as an SNMP agent). It also allows the switch to send traps to the defined and configured management station. Brocade switches support six management entities that can be configured to receive these traps.
SS	The **copy support** command generates these error messages if problems are encountered.
SSMD	SSMD error 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. These messages may display if there are any problems during the **firmware download** procedure. Most messages are informational only and are generated even during successful firmware download.
TOAM	TRILL OAM (TOAM) module messages indicate problems with the **l2traceroute** family of commands that help in VCS cluster data path troubleshooting.
TRCE	The TRCE module messages describe events and problems associated with the tracedump facility.
TS	Time Service provides switch time-synchronization by synchronizing all clocks in the network.
VC	VC module messages indicates 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.
ZONE	The zone module messages indicate any problems associated with the zoning features, including commands associated with aliases, zones, and configurations.

Section

I

RASLog Messages

This section provides the RASLog messages, including:

Chapter

AUTH System Messages 2

AUTH-1001

Message

```
<timestamp>, [AUTH-1001], <sequence-number>,, INFO, <system-name>, <Operation
type> has been successfully completed.
```

Probable Cause

Indicates that the secret database operation 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.

Severity

INFO

AUTH-1002

Message

```
<timestamp>, [AUTH-1002], <sequence-number>,, ERROR, <system-name>, <Operation
type> has failed.
```

Probable Cause

Indicates that the specified action has failed to update the secret database using the **fcsp auth-secret** or **no fcsp auth-secret** command. The values for *Operation type* can be “set” or “remove”.

Recommended Action

Retry the **fcsp auth-secret** command.

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

Severity

ERROR

AUTH-1010

Message

```
<timestamp>, [AUTH-1010], <sequence-number>,, ERROR, <system-name>, Failed to
initialize security policy: switch <switch number>, error <error code>.
```

Probable Cause

Indicates an internal problem with the Secure Network OS.

Recommended Action

Reboot or power cycle the switch.

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

Severity

ERROR

AUTH-1031

Message

```
<timestamp>, [AUTH-1031], <sequence-number>,, ERROR, <system-name>, Failed to
retrieve secret value: port <port number>.
```

Probable Cause

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

Recommended Action

Reset the secret value using the **no fcsp auth-secret** command.

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

Severity

ERROR

AUTH-1032

Message

```
<timestamp>, [AUTH-1032], <sequence-number>,, ERROR, <system-name>, Failed to
generate <data type> for <message payload> payload: length <data length>, error
code <error code>, port <port number>.
```

Probable Cause

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

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

Recommended Action

Usually this problem is transient. The authentication may fail.

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.

Severity

ERROR

AUTH-1041

Message

```
<timestamp>, [AUTH-1041], <sequence-number>,, ERROR, <system-name>, Port <port
number> has been disabled, because an authentication-reject was received with code
'<Reason String>' and explanation '<Explanation String>'.
```

Probable Cause

Indicates that the specified port had been disabled, because it received an authentication-reject response from the connected switch or device. 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 **fcsp auth-secret** command and reinitialize authentication using the **shutdown** and **no shutdown** commands.

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

Severity ERROR

AUTH-1042

Message

```
<timestamp>, [AUTH-1042], <sequence-number>,, ERROR, <system-name>, Port <port
number> has been disabled, because authentication failed with code '<Reason
String>' and explanation '<Explanation String>'.
```

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 **fcsp auth-secret** command and reinitialize authentication using the **shutdown** and **no shutdown** commands.

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

Severity ERROR

Chapter

C2 System Messages

3

C2-1011

Message

```
<timestamp>, [C2-1011], <sequence-number>,, WARNING, <switch-name>, S<slot
number>,P<port number>(<blade port number>): Primitive received with Encoding
errors, do AL_RESET.
```

Probable Cause

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

Recommended Action

If the error is observed continuously, power cycle the faulted blade. If the problem persists, check the backplane or replace the blade.

Severity

WARNING

Chapter

DCM System Messages 4

DCM-1001

Message
```
<timestamp>, [DCM-1001], <sequence-number>,, INFO, <switch-name>, VCS ID is
changed from <Previous Vcs Id> to <New Vcs Id>.
```

Probable Cause Indicates that the Virtual Clustered Switch (VCS) ID has been changed.

Recommended Action No action is required.

Severity INFO

DCM-1002

Message
```
<timestamp>, [DCM-1002], <sequence-number>,, INFO, <switch-name>, PostBoot
processing has started.
```

Probable Cause Indicates that the PostBoot processing has started.

Recommended Action No action is required.

Severity INFO

DCM-1003

Message
```
<timestamp>, [DCM-1003], <sequence-number>,, INFO, <switch-name>, PostBoot
processing is complete.
```

Probable Cause Indicates that the PostBoot processing has been completed.

Recommended Action No action is required.

Severity INFO

DCM-1004

Message
```
<timestamp>, [DCM-1004], <sequence-number>,, INFO, <switch-name>, Configuration
Replay has started.
```

Probable Cause Indicates that the configuration replay has started.

Recommended Action No action is required.

Severity INFO

DCM-1005

Message `<timestamp>, [DCM-1005], <sequence-number>,, INFO, <switch-name>, Configuration Replay is complete.`

Probable Cause Indicates that the configuration replay has been completed.

Recommended Action No action is required.

Severity INFO

DCM-1008

Message `<timestamp>, [DCM-1008], <sequence-number>,, INFO, <switch-name>, Configuration has been reset to default due to changes in configuration metadata.`

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

Recommended Action Replay the saved configuration manually.

Severity INFO

DCM-1009

Message `<timestamp>, [DCM-1009], <sequence-number>,, INFO, <switch-name>, rBridge ID is set to <Rbridge-id>.`

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

Recommended Action No action is required.

Severity INFO

DCM-1010

Message `<timestamp>, [DCM-1010], <sequence-number>,, INFO, <switch-name>, Operation of setting rBridge ID to <Rbridge-id> failed.`

Probable Cause Indicates a failure while changing the rBridge ID.

Recommended Action No action is required.

Severity INFO

DCM-1011

Message
```
<timestamp>, [DCM-1011], <sequence-number>,, INFO, <switch-name>, VCS enabled:
VCS ID is set to <New Vcs Id>.
```

Probable Cause Indicates that the VCS mode has been enabled.

Recommended Action No action is required.

Severity INFO

DCM-1012

Message
```
<timestamp>, [DCM-1012], <sequence-number>,, INFO, <switch-name>, VCS disabled:
VCS ID is set to <New Vcs Id>.
```

Probable Cause Indicates that the VCS mode has been disabled.

Recommended Action No action is required.

Severity INFO

DCM-1101

Message
```
<timestamp>, [DCM-1101], <sequence-number>,, INFO, <switch-name>, Copy
running-config to startup-config operation successful on this node.
```

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

Recommended Action No action is required.

Severity INFO

DCM-1102

Message
```
<timestamp>, [DCM-1102], <sequence-number>,, INFO, <switch-name>, Copy
running-config to startup-config operation failed on this node.
```

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

Recommended Action No action is required.

Severity INFO

DCM-1103

Message

```
<timestamp>, [DCM-1103], <sequence-number>,, INFO, <switch-name>, Copy
default-config to startup-config operation successful on this node.
```

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

Recommended Action No action is required.

Severity INFO

DCM-1104

Message

```
<timestamp>, [DCM-1104], <sequence-number>,, INFO, <switch-name>, Copy
default-config to startup-config operation failed on this node.
```

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

Recommended Action No action is required.

Severity INFO

DCM-1105

Message

```
<timestamp>, [DCM-1105], <sequence-number>,, INFO, <switch-name>, Copy of the
downloaded config file to the current running-config has completed successfully on
this node.
```

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

Recommended Action No action is required.

Severity INFO

DCM-1106

Message
```
<timestamp>, [DCM-1106], <sequence-number>,, INFO, <switch-name>, Copy of the
downloaded config file to the current startup-config has completed successfully on
this node.
```

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

Recommended Action
No action is required.

Severity
INFO

DCM-1107

Message
```
<timestamp>, [DCM-1107], <sequence-number>,, INFO, <switch-name>, Startup
configuration file has been uploaded successfully to the remote location.
```

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

Recommended Action
No action is required.

Severity
INFO

DCM-1108

Message
```
<timestamp>, [DCM-1108], <sequence-number>,, INFO, <switch-name>, Running
configuration file has been uploaded successfully to the remote location.
```

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

Recommended Action
No action is required.

Severity
INFO

DCM-1201

Message
```
<timestamp>, [DCM-1201], <sequence-number>,, INFO, <switch-name>, FIPS Zeroize
operation request received.
```

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

Recommended Action
No action is required.

Severity
INFO

DCM-1202

Message

```
<timestamp>, [DCM-1202], <sequence-number>,, ERROR, <switch-name>, FIPS Zeroize
operation: failed as VCS is enabled for this node.
```

Probable Cause
Indicates that the 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.

Severity
ERROR

DCM-1203

Message

```
<timestamp>, [DCM-1203], <sequence-number>,, INFO, <switch-name>, FIPS Zeroize
operation: confirmed that VCS is not enabled for this node.
```

Probable Cause
Indicates that VCS is not enabled on the node and therefore the FIPS Zeroize operation will proceed.

Recommended Action
No action is required.

Severity
INFO

DCM-1204

Message

```
<timestamp>, [DCM-1204], <sequence-number>,, INFO, <switch-name>, FIPS Zeroize
operation: all client sessions are notified that Zeroize in progress.
```

Probable Cause
Indicates that all the client sessions are notified about the Zeroize operation in progress and the commands cannot be executed.

Recommended Action
No action is required.

Severity
INFO

DCM-1205

Message

```
<timestamp>, [DCM-1205], <sequence-number>,, INFO, <switch-name>, FIPS Zeroize
operation: starting with cleanup for Zeroize.
```

Probable Cause
Indicates that the configuration files cleanup for Zeroize has started.

Recommended Action
No action is required.

Severity
INFO

DCM-1206

Message

```
<timestamp>, [DCM-1206], <sequence-number>,, INFO, <switch-name>, FIPS Zeroize
operation: starting prepare phase for Zeroize.
```

Probable Cause

Indicates that the prepare phase for Zeroize has started, during which all the services will be shut down.

Recommended Action

No action is required.

Severity

INFO

DCM-1207

Message

```
<timestamp>, [DCM-1207], <sequence-number>,, INFO, <switch-name>, FIPS Zeroize
operation: failed in prepare phase step for Zeroize.
```

Probable Cause

Indicates that the Zeroize operation has failed during the prepare phase.

Recommended Action

No action is required.

Severity

INFO

DCM-1208

Message

```
<timestamp>, [DCM-1208], <sequence-number>,, INFO, <switch-name>, FIPS Zeroize
operation: Running Zeroize for secure deletion of the user configuration data.
```

Probable Cause

Indicates that the Zeroize operation is running for secure deletion of the user configuration data.

Recommended Action

No action is required.

Severity

INFO

DCM-1209

Message

```
<timestamp>, [DCM-1209], <sequence-number>,, ERROR, <switch-name>, FIPS Zeroize
operation: failed during secure deletion of the user configuration data.
```

Probable Cause

Indicates that the 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.

Severity

ERROR

DCM-1210

Message
```
<timestamp>, [DCM-1210], <sequence-number>,, INFO, <switch-name>, FIPS Zeroize
operation failed.
```

Probable Cause Indicates that the FIPS Zeroize operation has failed.

Recommended Action No action is required.

Severity INFO

DCM-1211

Message
```
<timestamp>, [DCM-1211], <sequence-number>,, INFO, <switch-name>, FIPS Zeroize
operation executed successfully.
```

Probable Cause Indicates that the FIPS Zeroize operation has been executed successfully.

Recommended Action No action is required.

Severity INFO

DCM-1212

Message
```
<timestamp>, [DCM-1212], <sequence-number>,, INFO, <switch-name>, FIPS Zeroize
operation failed. Node zeroizing or already zeroized.
```

Probable Cause Indicates that the FIPS Zeroize operation has failed because the node is zeroizing or it was already zeroized.

Recommended Action No action is required.

Severity INFO

Chapter

DOT1 System Messages 5

DOT1-1001

Message

```
<timestamp>, [DOT1-1001], <sequence-number>,, INFO, <switch-name>, 802.1X is
enabled globally.
```

Probable Cause

Indicates that 802.1X is enabled globally.

Recommended Action

No action is required.

Severity

INFO

DOT1-1002

Message

```
<timestamp>, [DOT1-1002], <sequence-number>,, INFO, <switch-name>, 802.1X is
disabled globally.
```

Probable Cause

Indicates that 802.1X is disabled globally.

Recommended Action

No action is required.

Severity

INFO

DOT1-1003

Message

```
<timestamp>, [DOT1-1003], <sequence-number>,, INFO, <switch-name>, 802.1X is
enabled for port <port_name>.
```

Probable Cause

Indicates that 802.1X is enabled for the specified port.

Recommended Action

No action is required.

Severity

INFO

DOT1-1004

Message

```
<timestamp>, [DOT1-1004], <sequence-number>,, INFO, <switch-name>, Port
<port_name> is forcefully unauthorized.
```

Probable Cause

Indicates that the specified port is unauthorized forcefully.

Recommended Action
No action is required.

Severity
INFO

DOT1-1005

Message
```
<timestamp>, [DOT1-1005], <sequence-number>,, INFO, <switch-name>, 802.1X
authentication is successful on port <port_name>.
```

Probable Cause
Indicates that the authentication has succeeded on the specified port.

Recommended Action
No action is required.

Severity
INFO

DOT1-1006

Message
```
<timestamp>, [DOT1-1006], <sequence-number>,, WARNING, <switch-name>, 802.1X
authentication has failed on port <port_name>.
```

Probable Cause
Indicates that the authentication has failed on the specified port.

Recommended Action
Check the credentials configured with the Supplicant and the RADIUS server.

Severity
WARNING

DOT1-1007

Message
```
<timestamp>, [DOT1-1007], <sequence-number>,, CRITICAL, <switch-name>, No RADIUS
server available for authentication.
```

Probable Cause
Indicates that there is no RADIUS server available for authentication.

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

Severity
CRITICAL

DOT1-1008

Message
```
<timestamp>, [DOT1-1008], <sequence-number>,, INFO, <switch-name>, Port
<port_name> is forcefully authorized.
```

Probable Cause
Indicates that the port is authorized forcefully.

Recommended Action
No action is required.

Severity
INFO

DOT1-1009

Message

```
<timestamp>, [DOT1-1009], <sequence-number>,, INFO, <switch-name>, 802.1X is
disabled for port <port_name>.
```

Probable Cause
Indicates that 802.1X is disabled for the specified port.

Recommended Action
No action is required.

Severity
INFO

DOT1-1010

Message

```
<timestamp>, [DOT1-1010], <sequence-number>,, INFO, <switch-name>, Port
<port_name> is set in auto mode.
```

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

Recommended Action
No action is required.

Severity
INFO

DOT1-1011

Message

```
<timestamp>, [DOT1-1011], <sequence-number>,, INFO, <switch-name>,
DOT1X_PORT_EAPOL_CAPABLE: Peer with MAC <mac1><mac2>.<mac3><mac4>.<mac5><mac6>
connected to port <port_name> is EAPOL Capable.
```

Probable Cause
Indicates that the peer's DOT1X capability connected to the specified port.

Recommended Action
No action is required.

Severity
INFO

DOT1-1012

Message

```
<timestamp>, [DOT1-1012], <sequence-number>,, INFO, <switch-name>,
DOT1X_PORT_EAPOL_CAPABLE: Peer connected to port <port_name> is NOT EAPOL capable.
```

Probable Cause
Indicates that the peer's DOT1X capability connected to a particular port.

Recommended Action
: No action is required.

Severity
: INFO

DOT1-1013

Message

```
<timestamp>, [DOT1-1013], <sequence-number>,, INFO, <switch-name>, DOT1X test
timeout has updated from <Previous test timeout value> to <Updated  test timeout
value>.
```

Probable Cause
: Indicates that the DOT1X test timeout value has changed.

Recommended Action
: No action is required.

Severity
: INFO

Chapter

EANV System Messages 6

EANV-1001

Message	`<timestamp>, [EANV-1001], <sequence-number>,, ERROR, <switch-name>, Port <port number> port fault. Change the SFP or check the cable.`
Probable Cause	Indicates a deteriorated small form-factor pluggable (SFP), an incompatible SFP pair, or a faulty cable between the peer ports.
Recommended Action	Verify that compatible SFPs are used on the peer ports, the SFPs have not deteriorated, and the Fibre Channel cable is not faulty. Replace the SFPs or the cable if necessary.
Severity	ERROR

EANV-1002

Message	`<timestamp>, [EANV-1002], <sequence-number>, FFDC, ERROR, <switch-name>, Port <port number> chip faulted due to an internal error.`
Probable Cause	Indicates an internal error. All the ports on this chip will be disrupted.
Recommended Action	Reboot the system at the next maintenance window.
Severity	ERROR

EANV-1003

Message	`<timestamp>, [EANV-1003], <sequence-number>,, CRITICAL, <switch-name>, S<slot number>,C<chip index>: HW ASIC Chip error. Type = 0x<chip error type>, Error = <chip error string>.`
Probable Cause	Indicates an internal error in the application-specific integrated circuit (ASIC) hardware that may degrade data traffic.
Recommended Action	When this error occurs, reboot the system at the next maintenance window.
Severity	CRITICAL

EANV-1004

Message
```
<timestamp>, [EANV-1004], <sequence-number>,, ERROR, <switch-name>, S<slot
number>,C<chip index>: Invalid DMA ch pointer, chan: <Channel number>,
good_addr:0x<Good address> bad_addr:0x<Bad address>.
```

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

Recommended Action When this error occurs, reboot the system at the next maintenance window.

Severity ERROR

EANV-1005

Message
```
<timestamp>, [EANV-1005], <sequence-number>,, ERROR, <switch-name>, S<slot
number>,C<chip index>, A<eanvil id>: Memory allocation failed.
```

Probable Cause Indicates memory allocation failure in the software.

Recommended Action When this error occurs, reboot the system at the next maintenance window. If the problem persists, replace the switch or contact your switch service provider.

Severity ERROR

EANV-1006

Message
```
<timestamp>, [EANV-1006], <sequence-number>,, CRITICAL, <switch-name>, S<slot
number>,C<chip index>: HW ASIC Chip fault. Type = 0x<chip error type>, Error =
<chip error string>.
```

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

Recommended Action When this error occurs, reboot the system at the next maintenance window. If the problem persists, replace the switch or contact your switch service provider.

Severity CRITICAL

Chapter

ELD System Messages 7

ELD-1001

Message

```
<timestamp>, [ELD-1001], <sequence-number>,, INFO, <switch-name>, Interface
<InterfaceName> is shut down by Edge Loop Detection (ELD) for loop in VLAN <VLAN
ID>.
```

Probable Cause Indicates that a loop has been detected by Edge Loop Detection (ELD) protocol on the specified interface. The interface is shut down.

Recommended Action Action needs to be taken to fix the loop.

Severity INFO

ELD-1002

Message

```
<timestamp>, [ELD-1002], <sequence-number>,, INFO, <switch-name>, Interface
<InterfaceName> is auto enabled by Edge Loop Detection (ELD).
```

Probable Cause Indicates that the specified interface on which a loop was detected is auto enabled after the configured shutdown time.

Recommended Action No action is required.

Severity INFO

Chapter

EM System Messages

8

EM-1001

Message

```
<timestamp>, [EM-1001], <sequence-number>, FFDC, CRITICAL, <switch-name>, <FRU
ID> is over heating: Shutting down.
```

Probable Cause

Indicates that a field-replaceable unit (FRU) is shutting down due to overheating. The 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 the fans if they are missing or not performing at high enough speed.

Severity

CRITICAL

EM-1002

Message

```
<timestamp>, [EM-1002], <sequence-number>, FFDC, INFO, <switch-name>, System
fan(s) status <fan FRU>.
```

Probable Cause

Indicates that a nonbladed system has overheated and may shut down. All 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 the fans if they are missing or not performing at high enough speed.

Severity

INFO

EM-1003

Message

```
<timestamp>, [EM-1003], <sequence-number>, FFDC, CRITICAL, <switch-name>, <FRU
ID> has unknown hardware identifier: FRU faulted.
```

Probable Cause

Indicates that a FRU header cannot be read or is invalid. The FRU is faulted.

Recommended Action

Reboot or power cycle the switch.

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

Severity

CRITICAL

EM-1004

Message

```
<timestamp>, [EM-1004], <sequence-number>, FFDC, CRITICAL, <switch-name>, <FRU
ID> failed to power on.
```

Probable Cause

Indicates that the 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

Try reseating the FRU. If the message persists, replace the FRU.

Severity

CRITICAL

EM-1012

Message

```
<timestamp>, [EM-1012], <sequence-number>, FFDC, CRITICAL, <switch-name>, <FRU
Id> failed <state> state transition, unit faulted.
```

Probable Cause

Indicates that a switch blade or nonbladed 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

Reboot or power cycle the switch.

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

If the message persists, replace the FRU.

Severity

CRITICAL

EM-1013

Message

```
<timestamp>, [EM-1013], <sequence-number>,, ERROR, <switch-name>, Failed to
update FRU information for <FRU Id>.
```

Probable Cause

Indicates that the environmental monitor (EM) was unable to update the time alive or the original equipment manufacturer (OEM) data in the memory of a FRU.

Recommended Action

The update is automatically attempted again. If it continues to fail, try reseating the FRU.

If the message persists, replace the FRU.

Severity

ERROR

EM-1014

Message
```
<timestamp>, [EM-1014], <sequence-number>,, ERROR, <switch-name>, Unable to read
sensor on <FRU Id> (<Return code>).
```

Probable Cause
Indicates that the environmental monitor (EM) was unable to access the sensors on the specified FRU.

Recommended Action
Try reseating the FRU. If the message persists, replace the FRU.

Severity
ERROR

EM-1015

Message
```
<timestamp>, [EM-1015], <sequence-number>,, WARNING, <switch-name>, Warm recovery
failed (<Return code>).
```

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, reboot or power cycle the switch.

Severity
WARNING

EM-1016

Message
```
<timestamp>, [EM-1016], <sequence-number>,, WARNING, <switch-name>, Cold recovery
failed (<Return code>).
```

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 ftp** command and contact your switch service provider.

Severity
WARNING

EM-1028

Message
```
<timestamp>, [EM-1028], <sequence-number>, FFDC, WARNING, <switch-name>, HIL
Error: <function> failed to access history log for FRU: <FRU Id> (rc=<return
code>).
```

Probable Cause
Indicates a problem accessing the data on the World Wide Name (WWN) card field-replaceable unit (FRU) or the WWN card storage area on the main logic board.

The problems were encountered when the software attempted to write to the history log storage to record an event for the specified FRU. This can indicate a significant hardware problem.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port. The return code is for internal use only.

Recommended Action

If the message persists, reboot or power cycle the switch.

If the message still persists, replace the WWN card or the switch (for nonbladed switches).

Severity

WARNING

EM-1029

Message

```
<timestamp>, [EM-1029], <sequence-number>,, WARNING, <switch-name>, <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.
```

Probable Cause

Indicates that the 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 FRU. Replace the FRU if it continues to fail.

Severity

WARNING

EM-1034

Message

```
<timestamp>, [EM-1034], <sequence-number>,, ERROR, <switch-name>, <FRU Id> set to
faulty, rc=<return code>.
```

Probable Cause

Indicates that the specified FRU has been marked as faulty for the specified reason.

Recommended Action

Try reseating the FRU.

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

If the message persists, replace the FRU.

Severity

ERROR

EM-1036

Message

```
<timestamp>, [EM-1036], <sequence-number>,, WARNING, <switch-name>, <FRU Id> is
not accessible.
```

Probable Cause

Indicates that the specified FRU is not present on the switch.

If the FRU is a WWN card, then default WWN and IP addresses are used for the switch.

Recommended Action

Reseat the FRU card.

If the message persists, reboot or power cycle the switch.

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

If the message persists, replace the FRU.

Severity WARNING

EM-1037

Message
```
<timestamp>, [EM-1037], <sequence-number>,, INFO, <switch-name>, <FRU Id> is no
longer faulted.
```

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.

Severity INFO

EM-1041

Message
```
<timestamp>, [EM-1041], <sequence-number>,, WARNING, <switch-name>, Sensor values
for <FRU Id>: <Sensor Value> <Sensor Value> <Sensor Value> <Sensor Value> <Sensor
Value> <Sensor Value> <Sensor Value>.
```

Probable Cause Indicates that the sensors detected a warning condition. All the significant sensors for the FRU are displayed; each contains a header.

This message can display:

- Voltages in volts
- Temperature in Celsius
- Fan speeds in RPM

Recommended Action If the message is isolated, monitor the error messages on the switch. If the message is associated with other messages, follow the recommended actions for those messages.

Severity WARNING

EM-1042

Message
```
<timestamp>, [EM-1042], <sequence-number>, , WARNING, <switch-name>, Important
FRU header data for <FRU Id> is invalid.
```

Probable Cause Indicates that the specified 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
Try reseating the FRU. If the message persists, replace the FRU.

Severity
WARNING

EM-1048

Message

```
<timestamp>, [EM-1048], <sequence-number>,, INFO, <switch-name>, <FRU Id> I2C
access recovered: state <current state>.
```

Probable Cause
Indicates that the I2C bus problems have been resolved and the FRU is accessible on the I2C bus.

Recommended Action
No action is required. The EM-1048 message is displayed when the EM-1029 error is resolved.

Severity
INFO

EM-1049

Message

```
<timestamp>, [EM-1049], <sequence-number>,, INFO, <switch-name>, FRU <FRU Id>
insertion detected.
```

Probable Cause
Indicates that a FRU of the type and location specified by the *FRU ID* was inserted into the chassis.

Recommended Action
No action is required.

Severity
INFO

EM-1050

Message

```
<timestamp>, [EM-1050], <sequence-number>,, INFO, <switch-name>, FRU <FRU Id>
removal detected.
```

Probable Cause
Indicates that a 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.

Severity
INFO

EM-1068

Message

```
<timestamp>, [EM-1068], <sequence-number>, FFDC, ERROR, <switch-name>, High
Availability Service Management subsystem failed to respond.  A required component
is not operating.
```

Probable Cause

Indicates that the High Availability (HA) subsystem has not returned a response within 4 minutes of the request from the environmental monitor (EM). It usually indicates that some component has not started properly or has terminated. The specific component that has failed may be indicated in other messages or debug data. There are serious internal Network OS configuration or hardware problems on the switch.

Recommended Action

Reboot or power cycle the switch.

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

Severity

ERROR

EM-2003

Message

```
<timestamp>, [EM-2003], <sequence-number>,, ERROR, <switch-name>, <Slot Id or
Switch for pizza boxes> has failed the POST tests. FRU is being faulted.
```

Probable Cause

Indicates that the FRU has failed the Power-On Self-Test. Refer to the */tmp/post[1/2].slot#.log* file for more information on faults. To view this log file you must be logged in at the root level.The login ID is Switch for non-bladed systems.

Recommended Action

On bladed systems, try reseating the specified FRU.

On nonbladed switches, reboot 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 bladed systems, replace the specified FRU; otherwise replace the switch.

Severity

ERROR

Chapter

FABR System Messages

9

FABR-1001

Message

```
<timestamp>, [FABR-1001], <sequence-number>,, WARNING, <switch-name>, port <port
number>, <segmentation reason>.
```

Probable Cause

Indicates that the specified switch port is isolated because of a segmentation resulting from mismatched configuration parameters.

Recommended Action

Based on the segmentation reason displayed in the message, look for a possible mismatch of relevant parameters in the switches at both ends of the link.

Severity

WARNING

FABR-1003

Message

```
<timestamp>, [FABR-1003], <sequence-number>,, WARNING, <switch-name>, port <port
number>: ILS <command> bad size <payload size>, wanted <expected payload size>.
```

Probable Cause

Indicates that an internal link service (ILS) information unit of invalid size has been received. The neighbor switch has sent a payload with an invalid size.

Recommended Action

Investigate the neighbor switch for problems. Run the **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). Replace the cable or SFP if necessary.

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

Severity

WARNING

FABR-1004

Message

```
<timestamp>, [FABR-1004], <sequence-number>,, WARNING, <switch-name>, port: <port
number>, req iu: 0x<address of IU request sent>, state: 0x<command sent>, resp iu:
0x<address of response IU received>, state 0x<response IU state>, <additional
description>.
```

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, run the **copy support** command and contact your switch service provider.

Severity WARNING

FABR-1005

Message

```
<timestamp>, [FABR-1005], <sequence-number>,, WARNING, <switch-name>, <command
sent>: port <port number>: status 0x<reason for failure> (<description of failure
reason>) xid = 0x<exchange ID of command>.
```

Probable Cause Indicates that the application failed to send an async command for the specified port. The message provides additional details regarding the reason for the failure and the exchange ID of the command. This can happen if a port is about to go down.

Recommended Action This message is often transitory. No action is required.

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

Severity WARNING

FABR-1006

Message

```
<timestamp>, [FABR-1006], <sequence-number>,, WARNING, <switch-name>, Node free
error, caller: <error description>.
```

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, run the **copy support** command and contact your switch service provider.

Severity WARNING

FABR-1007

Message

```
<timestamp>, [FABR-1007], <sequence-number>,, WARNING, <switch-name>, IU free
error, caller: <function attempting to de-allocate IU>.
```

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, run the **copy support** command and contact your switch service provider.

Severity WARNING

FABR-1008

Message `<timestamp>, [FABR-1008], <sequence-number>,, WARNING, <switch-name>, <error description>.`

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, run the **copy support** command and contact your switch service provider.

Severity WARNING

FABR-1009

Message `<timestamp>, [FABR-1009], <sequence-number>,, WARNING, <switch-name>, <error description>.`

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, run the **copy support** command and contact your switch service provider.

Severity WARNING

FABR-1010

Message `<timestamp>, [FABR-1010], <sequence-number>,, WARNING, <switch-name>, <error description>.`

Probable Cause Indicates that errors occurred while cleaning up the RDI (request rBridge ID). 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, run the **copy support** command and contact your switch service provider.

Severity WARNING

FABR-1012

Message

```
<timestamp>, [FABR-1012], <sequence-number>,, WARNING, <switch-name>, <function
stream>: no such type, <invalid type>.
```

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, run the **copy support** command and contact your switch service provider.

Severity

WARNING

FABR-1013

Message

```
<timestamp>, [FABR-1013], <sequence-number>, FFDC, CRITICAL, <switch-name>, No
Memory: pid=<fabric process id> file=<source file name> line=<line number within
the source file>.
```

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 CP.

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

Severity

CRITICAL

FABR-1014

Message

```
<timestamp>, [FABR-1014], <sequence-number>,, ERROR, <switch-name>, Port <port
number> Disabled: rBridge IDs overlap. Insistent rBridge ID <RBridge ID> could not
be obtained. Principal is trying to assign rBridge ID <RBridge ID>.
```

Probable Cause

Indicates that the switch received an rBridge ID other than the one it requested. The port 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.

Severity

ERROR

FABR-1019

Message
```
<timestamp>, [FABR-1019], <sequence-number>, FFDC, CRITICAL, <switch-name>,
Critical fabric size (<current rBridges>) exceeds supported configuration
(<supported rBridges>).
```

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.

Severity CRITICAL

FABR-1029

Message
```
<timestamp>, [FABR-1029], <sequence-number>,, INFO, <switch-name>, Port <port
number> negotiated <flow control mode description> (mode = <received flow control
mode>).
```

Probable Cause Indicates that a different flow control mode, as described in the message, is negotiated with the port at the other end of the link. The flow control is a mechanism of throttling the transmitter port to avoid buffer overrun at the receiving port.

There are three types of flow control modes:

- VC_RDY mode: Virtual-channel flow control mode. This is a proprietary protocol.
- R_RDY mode: Receiver-ready flow control mode. This is the Fibre Channel standard protocol, that uses R_RDY primitive for flow control.
- DUAL_CR mode: Dual-credit flow control mode. In both of the previous modes, the buffer credits are fixed, based on the port configuration information. In this mode, the buffer credits are negotiated as part of exchange link parameter (ELP) exchange. This mode also uses the R_RDY primitive for flow control.

Recommended Action No action is required.

Severity INFO

FABR-1030

Message
```
<timestamp>, [FABR-1030], <sequence-number>,, INFO, <switch-name>, fabric:
rBridge <new rBridge ID> (was <old rBridge ID>).
```

Probable Cause Indicates that the rBridge ID has changed.

Recommended Action: No action is required.

Severity: INFO

FABR-1039

Message

```
<timestamp>, [FABR-1039], <sequence-number>,, WARNING, <switch-name>, Invalid
rBridge ID zero received from principal switch (rBridge ID=<Principal rBridge
id>).
```

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.

Severity: WARNING

FABR-1041

Message

```
<timestamp>, [FABR-1041], <sequence-number>,, ERROR, <switch-name>, Port <Port
that is being disabled> is disabled due to trunk protocol error.
```

Probable Cause: Indicates 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, run the **copy support** command and contact your switch service provider.

Severity: ERROR

Chapter

FCOE System Messages 10

FCOE-1001

Message

```
<timestamp>, [FCOE-1001], <sequence-number>,, ERROR, <switch-name>, calloc failed
for <object>.
```

Probable Cause Indicates a memory failure.

Recommended Action Check the switch memory status.

Severity ERROR

FCOE-1019

Message

```
<timestamp>, [FCOE-1019], <sequence-number>,, WARNING, <switch-name>, FLOGI
ignored as FC-MAP not configured on FCOE VLAN.
```

Probable Cause Indicates that the FC-MAP is not configured on the FCoE VLAN.

Recommended Action Configure the FC-MAP.

Severity WARNING

FCOE-1020

Message

```
<timestamp>, [FCOE-1020], <sequence-number>,, INFO, <switch-name>, Login rejected
by FC stack.
```

Probable Cause Indicates that the login was rejected by the FC stack.

Recommended Action No action is required. The device will try to re-login.

Severity INFO

FCOE-1022

Message

```
<timestamp>, [FCOE-1022], <sequence-number>,, WARNING, <switch-name>, Max FCoE
device login limit reached.
```

Probable Cause Indicates that the maximum allowed FCoE device limit has been reached for the switch.

Recommended Action

Do not add more FCoE devices to the switch.

Severity

WARNING

FCOE-1023

Message

```
<timestamp>, [FCOE-1023], <sequence-number>,, WARNING, <switch-name>, Too many
logins on FCoE controller, max allowed = <MAX_DEVS_PER_CTLR>.
```

Probable Cause

Indicates that the maximum allowed FCoE login limit has reached for the controller.

Recommended Action

Firstly, logout a device that was already logged in and then try to log in the new device.

Severity

WARNING

FCOE-1024

Message

```
<timestamp>, [FCOE-1024], <sequence-number>,, WARNING, <switch-name>, FDISC
received from Enode without prior FLOGI.
```

Probable Cause

Indicates that the end node sent an FDISC that has not logged in. The end node must send an FLOGI before it can send an FDISC.

Recommended Action

No action is required.

Severity

WARNING

FCOE-1026

Message

```
<timestamp>, [FCOE-1026], <sequence-number>,, WARNING, <switch-name>, FDISC/FLOGI
mismatch. FDISC addressed to different FCF than base FLOGI.
```

Probable Cause

Indicates that the received FDISC has a DA other than the FCoE Forwarder's (FCF) MAC address.

Recommended Action

Make sure that the device that is trying to log in conforms to the FC-BB-5 standard.

Severity

WARNING

FCOE-1027

Message

```
<timestamp>, [FCOE-1027], <sequence-number>,, ERROR, <switch-name>, <msg> :
<mac1>:<mac2>:<mac3>:<mac4>:<mac5>:<mac6>.
```

Probable Cause

Indicates that the FCF controller is not found for the DA. The end node may be sending the FLOGI with a wrong DA MAC address.

Recommended Action Some parameters are not getting exchanged correctly between the switch and the end device. Reconfigure the port.

Severity ERROR

FCOE-1029

Message

```
<timestamp>, [FCOE-1029], <sequence-number>,, WARNING, <switch-name>, Version
mismatch between FIP FDISC and root VN port.
```

Probable Cause Indicates that the FCoE Initialization Protocol (FIP) version does not match between the FLOGI and FDISC.

Recommended Action Make sure that the device that is trying to log in conforms to the FC-BB-5 standard.

Severity WARNING

FCOE-1030

Message

```
<timestamp>, [FCOE-1030], <sequence-number>,, WARNING, <switch-name>, Version
mismatch between FIP LOGO and root VN port.
```

Probable Cause Indicates that the switch received an FIP LOGO 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.

Severity WARNING

FCOE-1031

Message

```
<timestamp>, [FCOE-1031], <sequence-number>,, WARNING, <switch-name>, FCoE port
deleted port <prt> slot <slt>.
```

Probable Cause Indicates that the user port has been removed from the system.

Recommended Action If the message is displayed while the switch is booting up or powering down, no action is required. However, if the message is displayed during normal operation, reboot the switch. If the problem persists, contact your switch service provider.

Severity WARNING

FCOE-1032

Message
```
<timestamp>, [FCOE-1032], <sequence-number>,, INFO, <switch-name>, We are in WARM
RECOVERING state.
```

Probable Cause Indicates that the chassis is in a warm recovering state and therefore cannot perform the specific actions.

Recommended Action Wait until the chassis is up.

Severity INFO

FCOE-1033

Message
```
<timestamp>, [FCOE-1033], <sequence-number>,, WARNING, <switch-name>, FIP v1
FLOGI received - VF port in use.
```

Probable Cause Indicates that the port that received FLOGI has another device logged in already.

Recommended Action Currently, only the direct attached model is supported. Therefore, each port can have only one FLOGI. The subsequent devices can log in as FDISCs.

Severity WARNING

FCOE-1034

Message
```
<timestamp>, [FCOE-1034], <sequence-number>,, WARNING, <switch-name>, FIP/FCoE
frame received on priority <pkt_ctrlp->pri_in>. Discarding it because PFC/FCoE is
not enabled on this priority.
```

Probable Cause Indicates that the priority is not PFC or FCoE enabled.

Recommended Action Configure as required.

Severity WARNING

FCOE-1035

Message
```
<timestamp>, [FCOE-1035], <sequence-number>,, INFO, <switch-name>, Virtual FCoE
port <port number> (<port wwn>) is online.
```

Probable Cause Indicates an administrative action on the FCoE port.

Recommended Action No action is required.

Severity INFO

FCOE-1036

Message

```
<timestamp>, [FCOE-1036], <sequence-number>,, INFO, <switch-name>, Virtual FCoE
port <port number> (<port wwn>) is offline.
```

Probable Cause

Indicates an administrative action on the FCoE port.

Recommended Action

No action is required.

Severity

INFO

Chapter

FVCS System Messages 11

FVCS-1002

Message

```
<timestamp>, [FVCS-1002], <sequence-number>,, WARNING, <switch-name>, Test
FAB_VCS RAS rBridge ID (<port number>).
```

Probable Cause

Indicates that the rBridge is valid.

Recommended Action

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

Severity

WARNING

FVCS-1003

Message

```
<timestamp>, [FVCS-1003], <sequence-number>,, WARNING, <switch-name>, Possible
vLAG Split Detected vLAG - ifindex (<vLAG ifindex>) split rBridge(<split
rBridge>).
```

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.

Severity

WARNING

FVCS-2001

Message

```
<timestamp>, [FVCS-2001], <sequence-number>,, WARNING, <switch-name>, FCS Primary
Update Send attempt Failed - reason (<Failure Reason>).
```

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 ftp** command and contact your switch service provider.

Severity

WARNING

FVCS-2002

Message

```
<timestamp>, [FVCS-2002], <sequence-number>,, WARNING, <switch-name>, Link State
Update send to Remote rBridge Failed - reason (<Failure Reason Code>).
```

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 ftp** command and contact your switch service provider.

Severity

WARNING

FVCS-2003

Message

```
<timestamp>, [FVCS-2003], <sequence-number>,, WARNING, <switch-name>, Lag
Configuration Update send to Remote rBridge Failed - reason (<Failure Reason
Code>).
```

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 ftp** command on this rBridge and the remote rBridge specified in the domain field and contact your switch service provider.

Severity

WARNING

FVCS-2004

Message

```
<timestamp>, [FVCS-2004], <sequence-number>,, WARNING, <switch-name>, FCS Commit
stage Failed - cfg type <Configuration Type>, cfg tag <Configuration Tag>, domain
<Source Domain>, reason (<Failure Reason Code>).
```

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 ftp** command on this rBridge and the remote rBridge specified in the domain field and contact your switch service provider.

Severity

WARNING

FVCS-2005

Message

```
<timestamp>, [FVCS-2005], <sequence-number>,, WARNING, <switch-name>, FCS Cancel
stage Failed - cfg type <Configuration Type>, cfg tag <Configuration Tag>, domain
<Source Domain>, reason (<Failure Reason Code>).
```

Probable Cause

Indicates that the 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 vLAG identified by the configuration tag.

If the message persists, execute the **copy support ftp** command on this rBridge and the remote rBridge specified in the domain field and contact your switch service provider.

Severity

WARNING

FVCS-2006

Message

```
<timestamp>, [FVCS-2006], <sequence-number>,, WARNING, <switch-name>, FCS
Transaction Hung - cfg type <Configuration Type>, cfg tag <Configuration Tag>,
trans state<Trans State>.
```

Probable Cause

Indicates that the update cannot be completed for an unknown reason.

Recommended Action

Check the status of the vLAG identified by the configuration tag.

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

Severity

WARNING

FVCS-3001

Message

```
<timestamp>, [FVCS-3001], <sequence-number>,, WARNING, <switch-name>, Eth_ns
Message Queue Overflow. Failed to send update. MAC or MCAST Database may be out of
sync. Drop count = (<Drop Count>).
```

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.

Severity

WARNING

FVCS-3002

Message

```
<timestamp>, [FVCS-3002], <sequence-number>,, WARNING, <switch-name>, Eth_ns
Message Queue Overflow. Failed to add Received update. MAC or MCAST database may
be out of sync. Drop count = (<Drop Count>).
```

Probable Cause

Indicates that the Eth_ns (component of FVCS), that kept the 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 L2 and MCAST databases will synchronize with the fabric after the local congestion issue is resolved.

Severity

WARNING

Chapter

FW System Messages 12

FW-1001

Message

```
<timestamp>, [FW-1001], <sequence-number>,, INFO, <switch-name>, <label>, value
has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause

Indicates that the internal temperature of the switch has changed.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. To prevent recurring messages, disable the changed alarm for this threshold. If you receive a temperature-related message, check for an accompanying fan-related message and check fan performance. If all fans are functioning normally, check the climate control in your lab.

Severity

INFO

FW-1002

Message

```
<timestamp>, [FW-1002], <sequence-number>,, WARNING, <switch-name>, <Label>, is
below low boundary (High=<High value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable Cause

Indicates that the internal temperature of the switch has fallen below the low boundary.

Recommended Action

No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Typically, low temperatures 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.

Severity

WARNING

FW-1003

Message

```
<timestamp>, [FW-1003], <sequence-number>,, WARNING, <switch-name>, <Label>, is
above high boundary(High=<High value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable Cause

Indicates that the internal temperature of the switch has risen above the high boundary to a value that could 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.

Severity
WARNING

FW-1004

Message

```
<timestamp>, [FW-1004], <sequence-number>,, INFO, <switch-name>, <Label>, is
between high and low boundaries(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Probable Cause
Indicates that the internal temperature of the switch has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action
No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. If you receive a temperature-related message, check for an accompanying fan-related message and check fan performance. If all fans are functioning normally, check the climate control in your lab.

Severity
INFO

FW-1005

Message

```
<timestamp>, [FW-1005], <sequence-number>,, INFO, <switch-name>, <Label>, value
has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.
```

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.

Severity
INFO

FW-1006

Message

```
<timestamp>, [FW-1006], <sequence-number>,, WARNING, <switch-name>, <Label>, is
below low boundary(High=<High value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable Cause
Indicates that the speed of the fan has fallen below the low boundary. Fan problems typically contribute to temperature problems.

Recommended Action
Consistently abnormal fan speeds generally indicate that the fan is failing. Replace the fan field-replaceable unit (FRU).

Severity
WARNING

FW-1007

Message `<timestamp>, [FW-1007], <sequence-number>,, WARNING, <switch-name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the speed of the fan has risen above the high boundary. Fan problems typically contribute to temperature problems.

Recommended Action Consistently abnormal fan speeds generally indicate that the fan is failing. Replace the fan field-replaceable unit (FRU).

Severity WARNING

FW-1008

Message `<timestamp>, [FW-1008], <sequence-number>,, INFO, <switch-name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the speed of the fan has changed from a value outside of the acceptable range to a value within the acceptable range. Fan problems typically contribute to temperature problems.

Recommended Action No action is required. Consistently abnormal fan speeds generally indicate that the fan is failing. If this message occurs repeatedly, replace the fan field-replaceable unit (FRU).

Severity INFO

FW-1009

Message `<timestamp>, [FW-1009], <sequence-number>,, INFO, <switch-name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the state of the power supply has changed from faulty to functional, or from functional to faulty.

Recommended Action If the power supply is functioning correctly, no action is required.

If the power supply is functioning below the acceptable boundary, verify that it is seated correctly in the chassis. Run the **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.

Severity INFO

FW-1010

Message `<timestamp>, [FW-1010], <sequence-number>,, WARNING, <switch-name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the power supply is faulty. The power supply is not producing enough power.

Recommended Action
: Verify that you have installed the power supply correctly and that it is correctly seated in the chassis. If the problem persists, replace the faulty power supply.

Severity
: WARNING

FW-1011

Message
: `<timestamp>, [FW-1011], <sequence-number>,, INFO, <switch-name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause
: Indicates that the power supply is functioning properly.

Recommended Action
: Set the high boundary above the normal operation range.

Severity
: INFO

FW-1012

Message
: `<timestamp>, [FW-1012], <sequence-number>,, INFO, <switch-name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

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.

Severity
: INFO

FW-1401

Message
: `<timestamp>, [FW-1401], <sequence-number>,, INFO, <switch-name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause
: Indicates that the flash usage percentage has fallen below the low boundary. Flash increases and decreases slightly with normal operation of the switch. Excessive permanent increases can lead to future problems.

Recommended Action
: No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity
: INFO

FW-1402

Message `<timestamp>, [FW-1402], <sequence-number>,, WARNING, <switch-name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the flash usage percentage has risen above the high boundary. Flash increases and decreases slightly with normal operation of the switch. Excessive permanent increases can lead to future problems.

Recommended Action You may have to remove some unwanted files to create some flash space. Run the **clear support** command to remove files from the kernel space.

Severity WARNING

FW-1403

Message `<timestamp>, [FW-1403], <sequence-number>,, INFO, <switch-name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the CPU or memory usage is between the boundary limits.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1404

Message `<timestamp>, [FW-1404], <sequence-number>,, INFO, <switch-name>, <Label>,is above high boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the CPU or memory usage is above its threshold. If this message is pertaining to memory usage, then the usage is above middle memory threshold.

Recommended Action No action is required.

Severity INFO

FW-1405

Message `<timestamp>, [FW-1405], <sequence-number>,, INFO, <switch-name>, <Label>,is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that memory usage below low threshold.

Recommended Action No action is required.

Severity INFO

FW-1406

Message `<timestamp>, [FW-1406], <sequence-number>,, CRITICAL, <switch-name>, <Label>,is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the memory usage is above high memory threshold.

Recommended Action No action is required.

Severity CRITICAL

FW-1407

Message `<timestamp>, [FW-1407], <sequence-number>,, INFO, <switch-name>, <Label>,is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the memory usage is between high and middle thresholds.

Recommended Action No action is required.

Severity INFO

FW-1408

Message `<timestamp>, [FW-1408], <sequence-number>,, INFO, <switch-name>, <Label>,is between high boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the memory usage is between low and high or middle thresholds.

Recommended Action No action is required.

Severity INFO

FW-1424

Message `<timestamp>, [FW-1424], <sequence-number>,, WARNING, <switch-name>, Switch status changed from <Previous state> to <Current state>.`

Probable Cause Indicates that the switch is not in a healthy state. This occurred because of a policy violation.

Recommended Action: Run the **show system monitor** command to determine the policy violation.

Severity: WARNING

FW-1425

Message:

```
<timestamp>, [FW-1425], <sequence-number>,, INFO, <switch-name>, Switch status
changed from <Bad state> to HEALTHY.
```

Probable Cause: Indicates that the switch status has changed to a healthy state. This occurred because a policy is no longer violated.

Recommended Action: No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity: INFO

FW-1426

Message:

```
<timestamp>, [FW-1426], <sequence-number>,, WARNING, <switch-name>, Switch status
change contributing factor Power supply: <Number Bad> bad, <Number Missing>
absent.
```

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 supply.

Severity: WARNING

FW-1427

Message:

```
<timestamp>, [FW-1427], <sequence-number>,, WARNING, <switch-name>, Switch status
change contributing factor Power supply: <Number Bad> bad.
```

Probable Cause: Indicates that the switch status 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 supply.

Severity: WARNING

FW-1428

Message

```
<timestamp>, [FW-1428], <sequence-number>,, WARNING, <switch-name>, Switch status
change contributing factor Power supply: <Number Missing> absent.
```

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 supply.

Severity

WARNING

FW-1429

Message

```
<timestamp>, [FW-1429], <sequence-number>,, WARNING, <switch-name>, Switch status
change contributing factor: Power supplies are not redundant.
```

Probable Cause

Indicates that the switch status 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 other in an even slot to make them redundant.

Severity

WARNING

FW-1430

Message

```
<timestamp>, [FW-1430], <sequence-number>,, WARNING, <switch-name>, Switch status
change contributing factor <string>.
```

Probable Cause

Indicates that the switch status 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.

Severity

WARNING

FW-1431

Message

```
<timestamp>, [FW-1431], <sequence-number>,, WARNING, <switch-name>, Switch status
change contributing factor Fan: <Number Bad> bad.
```

Probable Cause

Indicates that the switch status 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 fan field-replaceable units (FRUs).

Severity
WARNING

FW-1435

Message

```
<timestamp>, [FW-1435], <sequence-number>,, WARNING, <switch-name>, Switch status
change contributing factor Flash: usage out of range.
```

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
Run the **clear support** command to clear the kernel flash.

Severity
WARNING

FW-1439

Message

```
<timestamp>, [FW-1439], <sequence-number>,, WARNING, <switch-name>, Switch status
change contributing factor Switch offline.
```

Probable Cause
Indicates that the switch is not in a healthy state. This occurred because the switch is offline.

Recommended Action
Run the **chassis enable** command.

Severity
WARNING

FW-1440

Message

```
<timestamp>, [FW-1440], <sequence-number>,, INFO, <switch-name>, <FRU label>
state has changed to <FRU state>.
```

Probable Cause
Indicates that the state of the specified field-replaceable unit (FRU) has changed to absent.

Recommended Action
Verify that the event was planned.

Severity
INFO

FW-1441

Message

```
<timestamp>, [FW-1441], <sequence-number>,, INFO, <switch-name>, <FRU label>
state has changed to <FRU state>.
```

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 that the event was planned.

Severity
INFO

FW-1442

Message
```
<timestamp>, [FW-1442], <sequence-number>,, INFO, <switch-name>, <FRU label>
state has changed to <FRU state>.
```

Probable Cause
Indicates that the state of the specified field-replaceable unit (FRU) has changed to on.

Recommended Action
Verify that the event was planned.

Severity
INFO

FW-1443

Message
```
<timestamp>, [FW-1443], <sequence-number>,, INFO, <switch-name>, <FRU label>
state has changed to <FRU state>.
```

Probable Cause
Indicates that the state of the specified field-replaceable unit (FRU) has changed to off.

Recommended Action
Verify that the event was planned.

Severity
INFO

FW-1444

Message
```
<timestamp>, [FW-1444], <sequence-number>,, WARNING, <switch-name>, <FRU label>
state has changed to <FRU state>.
```

Probable Cause
Indicates that the state of the specified field-replaceable unit (FRU) has changed to faulty.

Recommended Action
Replace the FRU.

Severity
WARNING

FW-1445

Message

```
<timestamp>, [FW-1445], <sequence-number>,, INFO, <switch-name>, Four power
supplies are now required for 2X redundancy, Switch Status Policy values changed.
```

Probable Cause

Indicates that the switch now requires 4 power supplies and previous Switch Status Policy parameters will be overwritten to reflect this. The presence of an AP blade means that more than one power supply may be required to provide adequate power. So (even if the AP blade is powered down or removed) the Switch Status Policy values will now reflect the need for 4 power supplies to maintain full (2X) redundancy.

Recommended Action

No action required, unless there are fewer than 4 power supplies active in the chassis. If there are fewer than 4, insert additional power supplies so that there are 4 active.

Severity

INFO

FW-1446

Message

```
<timestamp>, [FW-1446], <sequence-number>,, WARNING, <switch-name>, Four power
supplies now required for 2X redundancy, not enforced by Fabric Watch due to
Switch Status Policy overridden by User.
```

Probable Cause

Indicates that the switch now requires four power supplies for full (2X) redundancy, but the user has previously overridden the Switch Status Policy values pertaining to number of power supplies. So those values will not be automatically changed. The default values with no AP blades are: 3 out of service indicates switch status is DOWN, 0 indicates no checking for switch status MARGINAL. The default values when an AP blade is or has been present are: 2 out of service indicates switch status is DOWN, 1 out of service indicates switch status is MARGINAL.

Recommended Action

To maintain full (2X) redundancy and proper monitoring by Fabric Watch, 4 active power supplies should be supplied and the default values associated with the presence of an AP blade should be entered with **system-monitor** command.

Severity

WARNING

FW-1500

Message

```
<timestamp>, [FW-1500], <sequence-number>,, WARNING, <switch-name>, Mail overflow
- Alerts being discarded.
```

Probable Cause

Indicates that the mail alert overflow condition has occurred.

Recommended Action

Resolve or disable the mail alert using the **system-monitor-mail fru** command.

Severity

WARNING

FW-1501

Message

```
<timestamp>, [FW-1501], <sequence-number>,, INFO, <switch-name>, Mail overflow
cleared - <Mails discarded> alerts discarded.
```

Probable Cause

Indicates that the mail overflow condition has cleared.

Recommended Action

No action is required.

Severity

INFO

Chapter

HAM System Messages 13

HAM-1004

Message

```
<timestamp>, [HAM-1004], <sequence-number>,, INFO, <switch-name>, Processor
rebooted - <Reboot Reason>.
```

Probable Cause

Indicates the system has been rebooted either because of a user action or an error. The switch reboots can be initiated by the **firmware download**, **fastboot**, and **reload** commands. Some examples of errors that may initiate this message are hardware errors, software errors, compact flash errors, or memory errors. The reason for reboot 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
- Reboot:API
- Reboot:HAM
- EMFault:EM

Recommended Action

Check the error log on both CPs for additional messages that may indicate the reason for the reboot.

Severity

INFO

HAM-1007

Message
```
<timestamp>, [HAM-1007], <sequence-number>, FFDC, CRITICAL, <switch-name>, Need
to reboot the system for recovery, reason: <reason name>.
```

Probable Cause Indicates that the system in the current condition must be rebooted to achieve a reliable recovery. The reason can be that the system failed when timeout occurred at a certain stage. If auto-reboot is enabled, the system reboots automatically. Otherwise, you must manually reboot the system.

Recommended Action If auto-reboot recovery is disabled, reboot the system manually for a reliable recovery.

Severity CRITICAL

HAM-1008

Message
```
<timestamp>, [HAM-1008], <sequence-number>, FFDC, CRITICAL, <switch-name>,
Rebooting the system for recovery; auto-reboot is enabled.
```

Probable Cause Indicates that the recovery by reboot is enabled, therefore the system reboots automatically. If the event logged in HAM-1007 occurs, auto-reboot is enabled.

Recommended Action No action is required.

Severity CRITICAL

HAM-1009

Message
```
<timestamp>, [HAM-1009], <sequence-number>, FFDC, CRITICAL, <switch-name>, Need
to MANUALLY REBOOT the system for recovery; auto-reboot is disabled.
```

Probable Cause Indicates that the recovery by reboot is disabled, therefore the system needs to be manually rebooted for recovery. If the event logged in HAM-1007 occurs, auto-reboot is disabled.

Recommended Action Reboot the whole system manually.

Severity CRITICAL

Chapter

HIL System Messages 14

HIL-1404

Message
```
<timestamp>, [HIL-1404], <sequence-number>,, WARNING, <switch-name>, <count> fan
FRUs missing. Install fan FRUs immediately.
```

Probable Cause Indicates that one or more fan field-replaceable units (FRUs) have been removed.

Recommended Action Install the missing fan FRUs immediately.

Severity WARNING

HIL-1511

Message
```
<timestamp>, [HIL-1511], <sequence-number>,, WARNING, <switch-name>, MISMATCH in
Fan Airflow direction. Replace FRU with fan airflow in same direction.
```

Probable Cause Indicates that the airflow of the fan is in reverse direction. This can heat up the system.

Recommended Action Replace the fan FRUs with airflow in the same direction.

Severity WARNING

HIL-1512

Message
```
<timestamp>, [HIL-1512], <sequence-number>,, WARNING, <switch-name>, MISMATCH in
PSU-Fan FRUs Airflow direction. Replace PSU with fan airflow in same direction.
```

Probable Cause Indicates that the airflow of the power supply unit (PSU) fan is in reverse direction. This can heat up the system.

Recommended Action Replace the PSU fan FRU with airflow in the same direction.

Severity WARNING

Chapter

HSL System Messages 15

HSL-1000

Message
```
<timestamp>, [HSL-1000], <sequence-number>,, CRITICAL, <switch-name>, HSL
initialization failed.
```

Probable Cause Indicates a Hardware Subsystem Layer (HSL) initialization failure. This error is caused by other system errors.

Recommended Action Check if other system errors are present.

Severity CRITICAL

HSL-1001

Message
```
<timestamp>, [HSL-1001], <sequence-number>,, CRITICAL, <switch-name>, Failed to
acquire the system MAC address pool.
```

Probable Cause Indicates the failure to acquire system address. This error is caused by other system errors.

Recommended Action Check if other system errors are present.

Severity CRITICAL

HSL-1005

Message
```
<timestamp>, [HSL-1005], <sequence-number>,, CRITICAL, <switch-name>, Failed to
initialize with FSS.
```

Probable Cause Indicates a failure to initialize the FSS. This error is caused by other system errors.

Recommended Action Check if other system errors are present.

Severity CRITICAL

HSL-1006

Message
```
<timestamp>, [HSL-1006], <sequence-number>,, CRITICAL, <switch-name>, Failed to
get the kernel page size <PageSize> bytes for the Memory Map (MMap).
```

Probable Cause Indicates that there is not enough contiguous kernel memory.

Recommended Action Install more memory on the board.

Severity CRITICAL

HSL-1008

Message
```
<timestamp>, [HSL-1008], <sequence-number>,, INFO, <switch-name>, ARP CACHE TABLE
HAS REACHED MAX LIMIT.
```

Probable Cause Indicates that the Address Resolution Protocol (ARP) cache table has reached its maximum limit.

Recommended Action No action is required.

Severity INFO

HSL-1009

Message
```
<timestamp>, [HSL-1009], <sequence-number>,, ERROR, <switch-name>, Failed to
create Brocade trunk interface <InterfaceName>.
```

Probable Cause Indicates failure to create Brocade trunk because the hardware resources have exhausted.

Recommended Action Do not exceed the maximum trunk configuration allowed by the system.

Severity ERROR

Chapter

IGMP System Messages 16

IGMP-1001

Message

```
<timestamp>, [IGMP-1001], <sequence-number>,, ERROR, <switch-name>, MsgQ enqueue
failed (rc: <rc>).
```

Probable Cause

Indicates an internal inter-process communication (IPC) failure due to the scalability scenario.

Recommended Action

Reduce the protocol traffic load.

Severity

ERROR

IGMP-1002

Message

```
<timestamp>, [IGMP-1002], <sequence-number>,, ERROR, <switch-name>, IPC with
McastSS failed (message-id: <message-id>, rc: <rc>).
```

Probable Cause

Indicates an internal IPC failure due to the scalability scenario.

Recommended Action

Reduce the protocol traffic load.

Severity

ERROR

IGMP-1003

Message

```
<timestamp>, [IGMP-1003], <sequence-number>,, ERROR, <switch-name>, MRouter eNS
update from a VCS rBridge (ID:<rbid>) running lower firmware version.
```

Probable Cause

Indicates an unsupported message update.

Recommended Action

Upgrade the Virtual Clustered Switch (VCS) rBridge firmware to the latest build.

Severity

ERROR

Chapter

IPAD System Messages 17

IPAD-1000

Message
```
<timestamp>, [IPAD-1000], <sequence-number>,, INFO, <switch-name> <Type of
managed entity> <Instance number of managed entity> <Type of network interface>
<Instance number of network interface> <Protocol address family> <Source of
address change> <Value of address and prefix> <DHCP enabled or not>.
```

Probable Cause
Indicates that the local IP address has been changed. If the source of the address change is manual, this means that the address change was initiated by a user. If the source of the address change is the Dynamic Host Configuration Protocol (DHCP), this means that the address change resulted from interaction with a DHCP server.

Recommended Action
No action is required.

Severity
INFO

IPAD-1001

Message
```
<timestamp>, [IPAD-1001], <sequence-number>,, INFO, <switch-name> <Type of
managed entity> <Instance number of managed entity> <Protocol address family>
<Source of address change> <Value of addres> <DHCP enabled or not>.
```

Probable Cause
Indicates that the gateway IP address has been changed. If the source of the address change is manual, this means that the address change was initiated by a user. If the source of the address change is the Dynamic Host Configuration Protocol (DHCP), this means that the address change resulted from interaction with a DHCP server.

Recommended Action
No action is required.

Severity
INFO

IPAD-1002

Message
```
<timestamp>, [IPAD-1002], <sequence-number>,, INFO, <switch-name>, Switch name
has been successfully changed to <switch name>.
```

Probable Cause
Indicates that the switch name has been changed.

Recommended Action
No action is required.

Severity
INFO

IPAD-1003

Message
```
<timestamp>, [IPAD-1003], <sequence-number>, FFDC, ERROR, <switch-name>,
libipadm: <error message> <error message specific code>.
```

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.

Severity
ERROR

Chapter

L2SS System Messages 18

L2SS-1001

Message

```
<timestamp>, [L2SS-1001], <sequence-number>,, ERROR, <switch-name>, Linux socket
error - error reason: <reason>, socket name: <sockname>, error name <errorname>.
```

Probable Cause

Indicates that an error has occurred in the Linux socket.

Recommended Action

Restart or power cycle the switch.

Severity

ERROR

L2SS-1002

Message

```
<timestamp>, [L2SS-1002], <sequence-number>,, ERROR, <switch-name>,
Initialization error: <reason>.
```

Probable Cause

Indicates that the Layer 2 system (l2sys) has encountered an error during initialization.

Recommended Action

Restart or power cycle the switch.

Severity

ERROR

L2SS-1003

Message

```
<timestamp>, [L2SS-1003], <sequence-number>,, ERROR, <switch-name>, Message Queue
Error: Failed to create a Message Queue.
```

Probable Cause

Indicates that the l2sys has encountered System Service Manager (SSM) message queue errors.

Recommended Action

Restart or power cycle the switch.

Severity

ERROR

L2SS-1004

Message

```
<timestamp>, [L2SS-1004], <sequence-number>,, ERROR, <switch-name>, FDB error:
Error in creating the AVL tree.
```

Probable Cause

Indicates that the l2sys has encountered an error while initializing the AVL tree.

Recommended Action
Restart or power cycle the switch.

Severity
ERROR

L2SS-1005

Message
```
<timestamp>, [L2SS-1005], <sequence-number>,, ERROR, <switch-name>,
MAC-address-table hash failed even after two attempts for slot <slot> chip <chip>.
```

Probable Cause
Indicates that the Media Access Control (MAC) address table hash failed even after two hash changes on the specified chip.

Recommended Action
Restart or power cycle the switch.

Severity
ERROR

L2SS-1006

Message
```
<timestamp>, [L2SS-1006], <sequence-number>,, INFO, <switch-name>,
MAC-address-table is 95 percent full.
```

Probable Cause
Indicates that the MAC address table on the chip is 95 percent (%) full.

Recommended Action
Clear some of the entries using the **no mac-address-table static** *MAC address* command or wait until the old entries age out.

Severity
INFO

L2SS-1007

Message
```
<timestamp>, [L2SS-1007], <sequence-number>,, INFO, <switch-name>,
MAC-address-table on slot <Slot_id> chip <Chip_id> is less than 90 percent full.
```

Probable Cause
Indicates that the MAC address table on the specified chip is less than 90 percent (%) full.

Recommended Action
No action is required. The l2sys starts learning the entries.

Severity
INFO

L2SS-1008

Message
```
<timestamp>, [L2SS-1008], <sequence-number>,, INFO, <switch-name>, Fabric-wide
Layer 2 flush command issued.
```

Probable Cause
Indicates that the **clear fabric-mac vlan** command is executed. The entire Layer 2 forwarding table will be cleared.

Recommended Action
No action is required.

Severity
INFO

L2SS-1009

Message

```
<timestamp>, [L2SS-1009], <sequence-number>,, INFO, <switch-name>, Fabric-wide l2
flush completed, status - <command status>.
```

Probable Cause
Indicates that the **clear fabric-mac vlan** command has completed and the entire Layer 2 forwarding table is cleared.

Recommended Action
No action is required.

Severity
INFO

Chapter

L3SS System Messages 19

L3SS-1004

Message
```
<timestamp>, [L3SS-1004], <sequence-number>,, ERROR, <switch-name>, <Function
Name>, <Line No>: HW/Driver Error (possibly the CAM/LPM/EXM is full): <HW Error
Message>, rc=<Error Code>.
```

Probable Cause: Indicates an error in the hardware or the driver of the Layer 3 subsystem (L3SS). The hardware content-addressable memory (CAM), longest prefix match (LPM), or exact match (EXM) may be full.

Recommended Action: Retry or clear the CAM.

Severity: ERROR

L3SS-1005

Message
```
<timestamp>, [L3SS-1005], <sequence-number>,, ERROR, <switch-name>, Exceeded the
maximum allowed ECMPs (64) for the system.
```

Probable Cause: Indicates that the equal-cost multi-path (ECMP) table is full and no more ECMPs can be programmed in the hardware.

Recommended Action: Retry or clear the CAM.

Severity: ERROR

Chapter

LOG System Messages 20

LOG-1000

Message

```
<timestamp>, [LOG-1000], <sequence-number>,, INFO, <switch-name>, Previous
message has repeated <repeat count> times.
```

Probable Cause Indicates that the previous message was repeated the specified number of times.

Recommended Action No action is required.

Severity INFO

LOG-1001

Message

```
<timestamp>, [LOG-1001], <sequence-number>,, WARNING, <switch-name>, A log
message was dropped.
```

Probable Cause Indicates that a log message was dropped. A trace dump file is created.

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

Severity WARNING

LOG-1002

Message

```
<timestamp>, [LOG-1002], <sequence-number>,, WARNING, <switch-name>, A log
message was not recorded.
```

Probable Cause Indicates that a log message was not recorded by the error logging system. A trace dump file is created. The message may still be visible through SNMP or other management tools.

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

Severity WARNING

LOG-1003

Message
```
<timestamp>, [LOG-1003], <sequence-number>,, INFO, <switch-name>, The log has
been cleared.
```

Probable Cause Indicates that the persistent error log has been cleared.

Recommended Action No action is required.

Severity INFO

Chapter

MSTP System Messages 21

MSTP-1001

Message `<timestamp>, [MSTP-1001], <sequence-number>,, ERROR, <switch-name>, <msg>: <msg>.`

Probable Cause Indicates that the system has failed to allocate memory.

Recommended Action Check the memory usage on the switch using the **show processes memory** command.

Restart or power cycle the switch.

Severity ERROR

MSTP-1002

Message `<timestamp>, [MSTP-1002], <sequence-number>,, ERROR, <switch-name>, <msg>: <msg>.`

Probable Cause Indicates that the system has failed to initialize.

Recommended Action Restart or power cycle the switch.

Severity ERROR

MSTP-1003

Message `<timestamp>, [MSTP-1003], <sequence-number>,, ERROR, <switch-name>, <msg>: <msg>.`

Probable Cause Indicates a socket connection or socket transferring or receiving error.

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

Severity ERROR

MSTP-2001

Message `<timestamp>, [MSTP-2001], <sequence-number>,, INFO, <switch-name>, <msg>.`

Probable Cause Indicates that the Multiple Spanning Tree Protocol (MSTP) bridge mode has changed.

Recommended Action No action is required.

Severity INFO

MSTP-2002

Message `<timestamp>, [MSTP-2002], <sequence-number>,, INFO, <switch-name>, <Bridge mode information>. My Bridge ID: <Bridge ID> Old Root: <Old Root id> New Root: <New Root ID>.`

Probable Cause Indicates that the MSTP bridge or bridge instance root has changed.

Recommended Action No action is required.

Severity INFO

MSTP-2003

Message `<timestamp>, [MSTP-2003], <sequence-number>,, INFO, <switch-name>, MSTP instance <instance> is created.`

Probable Cause Indicates that the MSTP instance has been created.

Recommended Action No action is required.

Severity INFO

MSTP-2004

Message `<timestamp>, [MSTP-2004], <sequence-number>,, INFO, <switch-name>, MSTP instance <instance> is deleted.`

Probable Cause Indicates that the MSTP instance has been deleted.

Recommended Action No action is required.

Severity INFO

MSTP-2005

Message `<timestamp>, [MSTP-2005], <sequence-number>,, INFO, <switch-name>, VLAN <vlan_ids> is <action> on MSTP instance <instance>.`

Probable Cause Indicates that the MSTP instance has been modified.

Recommended Action No action is required.

Severity INFO

MSTP-2006

Message

```
<timestamp>, [MSTP-2006], <sequence-number>,, INFO, <switch-name>, MSTP instance
<instance> brigde priority is changed from <priority_old> to <priority_new>.
```

Probable Cause Indicates that the MSTP instance priority has been modified.

Recommended Action No action is required.

Severity INFO

Chapter

NSM System Messages 22

NSM-1001

Message

```
<timestamp>, [NSM-1001], <sequence-number>,, INFO, <switch-name>, Interface
<Interface Name> is online.
```

Probable Cause Indicates that the interface is online after the protocol dependencies are resolved.

Recommended Action No action is required.

Severity INFO

NSM-1002

Message

```
<timestamp>, [NSM-1002], <sequence-number>,, INFO, <switch-name>, Interface
<Interface Name> is protocol down.
```

Probable Cause Indicates that the interface is offline as one of the protocol dependency is unresolved.

Recommended Action Check for the reason codes using the **show interface** command and resolve the protocol dependencies.

Severity INFO

NSM-1003

Message

```
<timestamp>, [NSM-1003], <sequence-number>,, INFO, <switch-name>, Interface
<Interface Name> is link down.
```

Probable Cause Indicates that the interface is offline as the link is down.

Recommended Action Check whether the connectivity is proper and the remote link is up.

Severity INFO

NSM-1004

Message

```
<timestamp>, [NSM-1004], <sequence-number>,, INFO, <switch-name>, Interface
<interface name> is created.
```

Probable Cause Indicates that a new logical interface has been created.

Recommended Action: No action is required.

Severity: INFO

NSM-1007

Message
```
<timestamp>, [NSM-1007], <sequence-number>,, INFO, <switch-name>, Chassis is
<status>.
```

Probable Cause: Indicates that the chassis is enabled or disabled.

Recommended Action: No action is required.

Severity: INFO

NSM-1009

Message
```
<timestamp>, [NSM-1009], <sequence-number>,, INFO, <switch-name>, Interface
<InterfaceName> is deleted.
```

Probable Cause: Indicates that the logical interface has been deleted.

Recommended Action: No action is required.

Severity: INFO

NSM-1010

Message
```
<timestamp>, [NSM-1010], <sequence-number>,, INFO, <switch-name>, InterfaceMode
changed from <Mode_old> to <Mode_new> for interface <InterfaceName>.
```

Probable Cause: Indicates that the interface mode has been changed.

Recommended Action: No action is required.

Severity: INFO

NSM-1011

Message
```
<timestamp>, [NSM-1011], <sequence-number>,, INFO, <switch-name>,
OperationalEndpointMode changed from <Mode_old> to <Mode_new> for interface
<InterfaceName>.
```

Probable Cause: Indicates that the interface OperationalEndpoint mode has been changed.

Recommended Action No action is required.

Severity INFO

NSM-1012

Message

```
<timestamp>, [NSM-1012], <sequence-number>,, INFO, <switch-name>, VLAN classifier
group <group_id> is created.
```

Probable Cause Indicates that the VLAN classifier group has been created.

Recommended Action No action is required.

Severity INFO

NSM-1013

Message

```
<timestamp>, [NSM-1013], <sequence-number>,, INFO, <switch-name>, VLAN classifier
group <group_id> is deleted.
```

Probable Cause Indicates that the VLAN classifier group has been deleted.

Recommended Action No action is required.

Severity INFO

NSM-1014

Message

```
<timestamp>, [NSM-1014], <sequence-number>,, INFO, <switch-name>, VLAN classifier
rule <rule_id> is created.
```

Probable Cause Indicates that the VLAN classifier rule has been created.

Recommended Action No action is required.

Severity INFO

NSM-1015

Message

```
<timestamp>, [NSM-1015], <sequence-number>,, INFO, <switch-name>, VLAN classifier
rule <rule_id> is deleted.
```

Probable Cause Indicates that the VLAN classifier rule has been deleted.

Recommended Action No action is required.

Severity INFO

NSM-1016

Message `<timestamp>, [NSM-1016], <sequence-number>,, INFO, <switch-name>, VLAN classifier rule <rule_id> is <action> on VLAN classifier group <grouip_id>.`

Probable Cause Indicates that the VLAN classifier group has been modified.

Recommended Action No action is required.

Severity INFO

NSM-1017

Message `<timestamp>, [NSM-1017], <sequence-number>,, INFO, <switch-name>, Interface <InterfaceName> is <action> on interface <Logical_InterfaceName>.`

Probable Cause Indicates that the logical interface member list has been changed.

Recommended Action No action is required.

Severity INFO

NSM-1018

Message `<timestamp>, [NSM-1018], <sequence-number>,, INFO, <switch-name>, <count> VLANs <except> will be allowed on interface <Logical_InterfaceName>.`

Probable Cause Indicates that the VLAN membership has been changed.

Recommended Action No action is required.

Severity INFO

NSM-1019

Message `<timestamp>, [NSM-1019], <sequence-number>,, INFO, <switch-name>, Interface <InterfaceName> is administratively up.`

Probable Cause Indicates that the interface administrative status has changed to up.

Recommended Action
No action is required.

Severity
INFO

NSM-1020

Message

```
<timestamp>, [NSM-1020], <sequence-number>,, INFO, <switch-name>, Interface
<InterfaceName> is administratively down.
```

Probable Cause
Indicates that the interface administrative status has changed to down.

Recommended Action
No action is required.

Severity
INFO

NSM-1021

Message

```
<timestamp>, [NSM-1021], <sequence-number>,, ERROR, <switch-name>, Interface IP
overlap with management IP <ipAddr> ifname:<ifname>.
```

Probable Cause
Indicates that the IP address configured on the interface overlaps with the management IP address.

Recommended Action
Change the interface IP address.

Severity
ERROR

NSM-1022

Message

```
<timestamp>, [NSM-1022], <sequence-number>,, INFO, <switch-name>, FCoE
configuration has been <Option> on interface <InterfaceName>.
```

Probable Cause
Indicates that the FCoE configuration has been enabled or disabled on the interface.

Recommended Action
No action is required.

Severity
INFO

NSM-1023

Message

```
<timestamp>, [NSM-1023], <sequence-number>,, INFO, <switch-name>, rBridge ID
<DomainId> has joined Port-channel <PortChannelKey>. Port-channel is a vLAG with
rBridge IDs <RbridgeList>.
```

Probable Cause
Indicates that an rBridge has joined the Virtual Link Aggregation Group (vLAG).

Recommended Action
No action is required.

Severity
INFO

NSM-1024

Message

```
<timestamp>, [NSM-1024], <sequence-number>,, INFO, <switch-name>, rBridge ID
<DomainId> has left Port-channel <PortChannelKey>. Port-channel is a vLAG with
rBridge IDs<RbridgeList>.
```

Probable Cause
Indicates that an rBridge has left the vLAG.

Recommended Action
No action is required.

Severity
INFO

NSM-1025

Message

```
<timestamp>, [NSM-1025], <sequence-number>,, INFO, <switch-name>, rBridge ID
<DomainId> has left Port-channel <PortChannelKey>. Port-channel has only rBridge
ID <RbridgeList> and is no longer a vLAG.
```

Probable Cause
Indicates that the vLAG no longer exists.

Recommended Action
No action is required.

Severity
INFO

NSM-1026

Message

```
<timestamp>, [NSM-1026], <sequence-number>,, INFO, <switch-name>, SFP for
interface <InterfaceName> is inserted.
```

Probable Cause
Indicates that a small form-factor pluggable (SFP) has been inserted in an interface.

Recommended Action
No action is required.

Severity
INFO

NSM-1027

Message

```
<timestamp>, [NSM-1027], <sequence-number>,, INFO, <switch-name>, SFP for
interface <InterfaceName> is removed.
```

Probable Cause
Indicates that an SFP has been removed from an interface.

Recommended Action No action is required.

Severity INFO

NSM-1028

Message

```
<timestamp>, [NSM-1028], <sequence-number>,, ERROR, <switch-name>, Incompatible
SFP for interface <InterfaceName> is detected.
```

Probable Cause Indicates that an incompatible SFP for the interface has been inserted.

Recommended Action Use the compatible SFP for the interface.

Severity ERROR

NSM-1029

Message

```
<timestamp>, [NSM-1029], <sequence-number>,, ERROR, <switch-name>, Failed to read
SFP for interface <InterfaceName>.
```

Probable Cause Indicates failure to read the SFP.

Recommended Action No action is required.

Severity ERROR

NSM-1030

Message

```
<timestamp>, [NSM-1030], <sequence-number>,, INFO, <switch-name>, Interface
<InterfaceName> is administratively down due to speed mismatch in portchannel.
```

Probable Cause Indicates that the interface is administratively down due to a speed mismatch in the port channel.

Recommended Action Set the correct speed for the interface.

Severity INFO

NSM-1031

Message

```
<timestamp>, [NSM-1031], <sequence-number>,, INFO, <switch-name>, Session
<SessionNumber> is created.
```

Probable Cause Indicates that a session has been created.

Recommended Action
No action is required.

Severity
INFO

NSM-1032

Message

```
<timestamp>, [NSM-1032], <sequence-number>,, INFO, <switch-name>, Session
<SessionNumber> is deleted.
```

Probable Cause
Indicates that a session has been deleted.

Recommended Action
No action is required.

Severity
INFO

NSM-1033

Message

```
<timestamp>, [NSM-1033], <sequence-number>,, INFO, <switch-name>, Session
<SessionNumber> configuration is deleted.
```

Probable Cause
Indicates that the session configuration has been deleted.

Recommended Action
No action is required.

Severity
INFO

NSM-1034

Message

```
<timestamp>, [NSM-1034], <sequence-number>,, INFO, <switch-name>, Session
<SessionNumber> configuration is added.
```

Probable Cause
Indicates that the session configuration has been added.

Recommended Action
No action is required.

Severity
INFO

NSM-1035

Message

```
<timestamp>, [NSM-1035], <sequence-number>,, INFO, <switch-name>, Description for
Session <SessionNumber> is added.
```

Probable Cause
Indicates that the session description has been added.

Recommended Action No action is required.

Severity INFO

NSM-1036

Message `<timestamp>, [NSM-1036], <sequence-number>,, INFO, <switch-name>, Description for Session <SessionNumber> is deleted.`

Probable Cause Indicates that the session description has been deleted.

Recommended Action No action is required.

Severity INFO

NSM-2000

Message `<timestamp>, [NSM-2000], <sequence-number>,, INFO, <switch-name>, Port-profile <ProfileName> activation succeeded.`

Probable Cause Indicates that the profile activation was successful.

Recommended Action No action is required.

Severity INFO

NSM-2001

Message `<timestamp>, [NSM-2001], <sequence-number>,, ERROR, <switch-name>, Port-profile <ProfileName> activation failed, reason <Reason>.`

Probable Cause Indicates that the profile activation was unsuccessful.

Recommended Action Check the configuration and port-profile status. For further guidance, contact your switch service provider.

Severity ERROR

NSM-2002

Message `<timestamp>, [NSM-2002], <sequence-number>,, INFO, <switch-name>, Port-profile <ProfileName> deactivation succeeded.`

Probable Cause Indicates that the profile deactivation was successful.

Recommended Action: No action is required.

Severity: INFO

NSM-2003

Message
```
<timestamp>, [NSM-2003], <sequence-number>,, ERROR, <switch-name>, Port-profile
<ProfileName> deactivation failed, reason <Reason>.
```

Probable Cause: Indicates that the profile deactivation was unsuccessful.

Recommended Action: Check the configuration and port-profile status. For further guidance, contact your switch service provider.

Severity: ERROR

NSM-2004

Message
```
<timestamp>, [NSM-2004], <sequence-number>,, INFO, <switch-name>, Port-profile
<ProfileName> application succeeded on <InterfaceName>.
```

Probable Cause: Indicates that the profile application was successful.

Recommended Action: No action is required.

Severity: INFO

NSM-2005

Message
```
<timestamp>, [NSM-2005], <sequence-number>,, ERROR, <switch-name>, Port-profile
<ProfileName> application failed on <InterfaceName>, reason <Reason>, removing
any applied configuration.
```

Probable Cause: Indicates that the profile application was unsuccessful.

Recommended Action: Check the configuration and port-profile status. For further guidance, contact your switch service provider.

Severity: ERROR

NSM-2006

Message
```
<timestamp>, [NSM-2006], <sequence-number>,, INFO, <switch-name>, Port-profile
<ProfileName> removed successfully on <InterfaceName>.
```

Probable Cause: Indicates that the profile de-application was successful.

Recommended Action No action is required.

Severity INFO

NSM-2007

Message
```
<timestamp>, [NSM-2007], <sequence-number>,, INFO, <switch-name>, Interface
<InterfaceName> became port-profile-port.
```

Probable Cause Indicates that the **port-profile-port** operation was successful.

Recommended Action No action is required.

Severity INFO

NSM-2008

Message
```
<timestamp>, [NSM-2008], <sequence-number>,, INFO, <switch-name>, Interface
<InterfaceName> became non-port-profile-port.
```

Probable Cause Indicates that the **no port-profile-port** operation was successful.

Recommended Action No action is required.

Severity INFO

NSM-2010

Message
```
<timestamp>, [NSM-2010], <sequence-number>,, ERROR, <switch-name>, Interface
<InterfaceName> could not become non-port-profile-port.
```

Probable Cause Indicates that the **no port-profile-port** operation was unsuccessful.

Recommended Action Check the configuration and port-profile status. For further guidance contact your switch service provider.

Severity ERROR

NSM-2011

Message
```
<timestamp>, [NSM-2011], <sequence-number>,, INFO, <switch-name>, Port-profile
<ProfileName> removed failed on <InterfaceName>.
```

Probable Cause Indicates that the profile removal was unsuccessful.

Recommended Action No action is required.

Severity INFO

NSM-2012

Message
```
<timestamp>, [NSM-2012], <sequence-number>,, INFO, <switch-name>, MAC
<ProfileMac> is associated to port-profile <ProfileName>.
```

Probable Cause Indicates that the profile to MAC association was successful.

Recommended Action No action is required.

Severity INFO

NSM-2013

Message
```
<timestamp>, [NSM-2013], <sequence-number>,, INFO, <switch-name>, MAC
<ProfileMac> is disassociated from port-profile <ProfileName>.
```

Probable Cause Indicates that the profile MAC disassociation was successful.

Recommended Action No action is required.

Severity INFO

NSM-2014

Message
```
<timestamp>, [NSM-2014], <sequence-number>,, INFO, <switch-name>, VLAN
sub-profile for port-profile <ProfileName> is created.
```

Probable Cause Indicates that the VLAN sub-profile has been created successfully.

Recommended Action No action is required.

Severity INFO

NSM-2015

Message
```
<timestamp>, [NSM-2015], <sequence-number>,, INFO, <switch-name>, Access VLAN
<VlanId> is configured for port-profile <ProfileName>.
```

Probable Cause Indicates that the untagged VLAN has been configured to the port-profile successfully.

Recommended Action No action is required.

Severity INFO

NSM-2016

Message `<timestamp>, [NSM-2016], <sequence-number>,, INFO, <switch-name>, Access VLAN is deleted from port-profile <ProfileName>.`

Probable Cause Indicates that the untagged VLAN has been removed from the port-profile successfully.

Recommended Action No action is required.

Severity INFO

NSM-2017

Message `<timestamp>, [NSM-2017], <sequence-number>,, INFO, <switch-name>, Port-profile <ProfileName> is configured for switching properties.`

Probable Cause Indicates that the switchport has been configured on the port-profile.

Recommended Action No action is required.

Severity INFO

NSM-2018

Message `<timestamp>, [NSM-2018], <sequence-number>,, INFO, <switch-name>, Switching properties are removed for port-profile <ProfileName>.`

Probable Cause Indicates that the no switchport has been configured on the port-profile.

Recommended Action No action is required.

Severity INFO

NSM-2019

Message `<timestamp>, [NSM-2019], <sequence-number>,, INFO, <switch-name>, The <ModeName> mode is configured for port-profile <ProfileName>.`

Probable Cause Indicates that the switchport mode has been configured for the port-profile.

Recommended Action No action is required.

Severity INFO

NSM-2020

Message
```
<timestamp>, [NSM-2020], <sequence-number>,, INFO, <switch-name>, The <ModeName>
mode is de-configured for port-profile <ProfileName>.
```

Probable Cause Indicates that the switchport mode has been modified for the port-profile.

Recommended Action No action is required.

Severity INFO

NSM-2021

Message
```
<timestamp>, [NSM-2021], <sequence-number>,, INFO, <switch-name>, The tagged
VLANs <TaggedVlanStr> are configured for port-profile <ProfileName>.
```

Probable Cause Indicates that the tagged VLANs are configured from the VLAN sub-profile.

Recommended Action No action is required.

Severity INFO

NSM-2022

Message
```
<timestamp>, [NSM-2022], <sequence-number>,, INFO, <switch-name>, The tagged
VLANs <TaggedVlanStr> are removed for port-profile <ProfileName>.
```

Probable Cause Indicates that the tagged VLANs are removed in the VLAN sub-profile.

Recommended Action No action is required.

Severity INFO

NSM-2023

Message
```
<timestamp>, [NSM-2023], <sequence-number>,, INFO, <switch-name>, The tagged
VLANs except <TaggedVlanStr> are configured for port-profile <ProfileName>.
```

Probable Cause Indicates that the tagged VLANs are configured in the VLAN sub-profile.

Recommended Action No action is required.

Severity INFO

NSM-2024

Message `<timestamp>, [NSM-2024], <sequence-number>,, INFO, <switch-name>, All VLANs are configured as tagged VLANs for port-profile <ProfileName>.`

Probable Cause Indicates that all the available tagged VLANs are configured in the VLAN sub-profile.

Recommended Action No action is required.

Severity INFO

NSM-2025

Message `<timestamp>, [NSM-2025], <sequence-number>,, INFO, <switch-name>, All tagged VLANs are removed for port-profile <ProfileName>.`

Probable Cause Indicates that all the available tagged VLANs are removed from the VLAN sub-profile.

Recommended Action No action is required.

Severity INFO

NSM-2026

Message `<timestamp>, [NSM-2026], <sequence-number>,, INFO, <switch-name>, Native VLAN <VlanId> is configured to port-profile <ProfileName>.`

Probable Cause Indicates that the native VLAN has been configured to the port-profile.

Recommended Action No action is required.

Severity INFO

NSM-2027

Message `<timestamp>, [NSM-2027], <sequence-number>,, INFO, <switch-name>, Native VLAN is deleted from port-profile <ProfileName>.`

Probable Cause Indicates that the native VLAN has been removed from the port-profile.

Recommended Action No action is required.

Severity INFO

NSM-2028

Message

```
<timestamp>, [NSM-2028], <sequence-number>,, INFO, <switch-name>, FCoE
sub-profile for port-profile <ProfileName> is created.
```

Probable Cause Indicates that the FCoE sub-profile has been created successfully.

Recommended Action No action is required.

Severity INFO

NSM-2029

Message

```
<timestamp>, [NSM-2029], <sequence-number>,, INFO, <switch-name>, Fcoeport is
configured successfully for port-profile <ProfileName>.
```

Probable Cause Indicates that the FCoE port is configured in the FCoE sub-profile.

Recommended Action No action is required.

Severity INFO

NSM-2030

Message

```
<timestamp>, [NSM-2030], <sequence-number>,, INFO, <switch-name>, Fcoeport is
removed successfully for port-profile <ProfileName>.
```

Probable Cause Indicates that the FCoE port has been removed for the port-profile.

Recommended Action No action is required.

Severity INFO

NSM-2031

Message

```
<timestamp>, [NSM-2031], <sequence-number>,, INFO, <switch-name>, Port-profile
<ProfileName> is created.
```

Probable Cause Indicates that the port-profile has been created successfully.

Recommended Action No action is required.

Severity INFO

NSM-2032

Message
```
<timestamp>, [NSM-2032], <sequence-number>,, INFO, <switch-name>, Port-profile
<ProfileName> is removed.
```

Probable Cause Indicates that the port-profile has been removed successfully.

Recommended Action No action is required.

Severity INFO

NSM-2033

Message
```
<timestamp>, [NSM-2033], <sequence-number>,, INFO, <switch-name>, VLAN
sub-profile for port-profile <ProfileName> is deleted.
```

Probable Cause Indicates that the VLAN sub-profile has been deleted successfully.

Recommended Action No action is required.

Severity INFO

NSM-2034

Message
```
<timestamp>, [NSM-2034], <sequence-number>,, INFO, <switch-name>, FCoE
sub-profile for port-profile <ProfileName> is deleted.
```

Probable Cause Indicates that the FCoE sub-profile has been deleted successfully.

Recommended Action No action is required.

Severity INFO

Chapter

ONMD System Messages

23

ONMD-1000

Message

```
<timestamp>, [ONMD-1000], <sequence-number>,, INFO, <switch-name>, LLDP is
enabled.
```

Probable Cause Indicates that the Link Layer Discovery Protocol (LLDP) is enabled globally.

Recommended Action No action is required.

Severity INFO

ONMD-1001

Message

```
<timestamp>, [ONMD-1001], <sequence-number>,, INFO, <switch-name>, LLDP is
disabled.
```

Probable Cause Indicates that LLDP is disabled globally.

Recommended Action No action is required.

Severity INFO

ONMD-1002

Message

```
<timestamp>, [ONMD-1002], <sequence-number>,, INFO, <switch-name>, LLDP global
configuration is changed.
```

Probable Cause Indicates that the LLDP global configuration has been changed.

Recommended Action No action is required.

Severity INFO

ONMD-1003

Message

```
<timestamp>, [ONMD-1003], <sequence-number>,, INFO, <switch-name>, LLDP is
enabled on interface <InterfaceName>.
```

Probable Cause Indicates that LLDP is enabled on the interface.

Recommended Action
No action is required.

Severity
INFO

ONMD-1004

Message
```
<timestamp>, [ONMD-1004], <sequence-number>,, INFO, <switch-name>, LLDP is
disabled on interface <InterfaceName>.
```

Probable Cause
Indicates that LLDP is disabled on the interface.

Recommended Action
No action is required.

Severity
INFO

Chapter

24

PHP System Messages

PHP-1001

Message `<timestamp>, [PHP-1001], <sequence-number>,, INFO, <switch-name>, <PHP Script message>.`

Probable Cause Indicates a user defined informative message.

Recommended Action No action is required.

Severity INFO

PHP-1002

Message `<timestamp>, [PHP-1002], <sequence-number>,, WARNING, <switch-name>, <PHP Script message>.`

Probable Cause Indicates a user defined warning message.

Recommended Action No action is required.

Severity WARNING

PHP-1003

Message `<timestamp>, [PHP-1003], <sequence-number>,, ERROR, <switch-name>, <PHP Script message>.`

Probable Cause Indicates a user defined error message.

Recommended Action No action is required.

Severity ERROR

PHP-1004

Message `<timestamp>, [PHP-1004], <sequence-number>,, CRITICAL, <switch-name>, <PHP Script message>.`

Probable Cause Indicates a user defined critical message.

Recommended Action No action is required.

Severity CRITICAL

Chapter

PLAT System Messages 25

PLAT-1004

Message
```
<timestamp>, [PLAT-1004], <sequence-number>, FFDC, CRITICAL, <switch-name>,
Turning off Fan <Fan Number> because of airflow direction mismatch.
```

Probable Cause Indicates that the fan field-replaceable unit (FRU) is turned off because of wrong airflow direction.

Recommended Action Replace the fan FRU.

Severity CRITICAL

PLAT-1005

Message
```
<timestamp>, [PLAT-1005], <sequence-number>, FFDC, CRITICAL, <switch-name>,
Unable to read EEPROM for Global airflow direction. Setting to default Port side
intake.
```

Probable Cause Indicates a failure to read the EEPROM.

Recommended Action Inform the factory about the error.

Severity CRITICAL

PLAT-1006

Message
```
<timestamp>, [PLAT-1006], <sequence-number>,, CRITICAL, <switch-name>, Unable to
read EEPROM for Global airflow direction. Shutting off Fans now.
```

Probable Cause Indicates a failure to read the EEPROM. The fans will be shut down.

Recommended Action Inform the factory about the error.

Severity CRITICAL

PLAT-1007

Message
```
<timestamp>, [PLAT-1007], <sequence-number>,, ERROR, <switch-name>, Turning off
Fan <Fan Number> because of airflow direction <Global airflow direction>.
```

Probable Cause Indicates that the fan is turned off because of the wrong airflow direction.

Recommended Action Replace the fan FRUs with airflow in the same direction.

Severity ERROR

PLAT-1008

Message
```
<timestamp>, [PLAT-1008], <sequence-number>,, ERROR, <switch-name>, Unable to
read EEPROM for Global airflow direction.
```

Probable Cause Indicates a failure to read the EEPROM.

Recommended Action Inform the factory about the error.

Severity ERROR

PLAT-1009

Message
```
<timestamp>, [PLAT-1009], <sequence-number>,, ERROR, <switch-name>, Unable to
read EEPROM Valid Signature for Global airflow direction.
```

Probable Cause Indicates a failure to read the EEPROM.

Recommended Action Inform the factory about the error.

Severity ERROR

Chapter

PORT System Messages 26

PORT-1003

Message
```
<timestamp>, [PORT-1003], <sequence-number>,, WARNING, <switch-name>, Port <port
number> Faulted because of many Link Failures.
```

Probable Cause
Indicates that the specified port is disabled because of multiple link failures on the port that has 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.

Severity
WARNING

PORT-1004

Message
```
<timestamp>, [PORT-1004], <sequence-number>,, INFO, <switch-name>, Port <port
number> (0x<port number (hex)>) could not be enabled because it is disabled due to
long distance.
```

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.

Severity
INFO

PORT-1011

Message
```
<timestamp>, [PORT-1011], <sequence-number>,, INFO, <switch-name>, An SFP for
interface Fibre Channel <rbridge-id number>/<slot number>/<port number> is
removed.
```

Probable Cause
Indicates that an SFP has been removed from the specified port.

Recommended Action
No action is required.

Severity
INFO

PORT-1012

Message

```
<timestamp>, [PORT-1012], <sequence-number>,, INFO, <switch-name>, An SFP for
interface Fibre Channel <rbridge-id number>/<slot number>/<port number> is
inserted.
```

Probable Cause
Indicates that an SFP has been inserted into the specified port.

Recommended Action
No action is required.

Severity
INFO

Chapter

RAS System Messages

27

RAS-1001

Message
```
<timestamp>, [RAS-1001], <sequence-number>,, INFO, <switch-name>, First failure
data capture (FFDC) event occurred.
```

Probable Cause Indicates that a failure occurred and the failure data was captured.

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

Severity INFO

RAS-1002

Message
```
<timestamp>, [RAS-1002], <sequence-number>,, WARNING, <switch-name>, First
failure data capture (FFDC) reached maximum storage size (<log size limit> MB).
```

Probable Cause Indicates that the storage size for first failure data capture (FFDC) has reached the maximum.

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

Severity WARNING

RAS-1004

Message
```
<timestamp>, [RAS-1004], <sequence-number>, FFDC, WARNING, <switch-name>,
Software 'verify' error detected.
```

Probable Cause Indicates an internal software error.

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

Severity WARNING

RAS-1005

Message
```
<timestamp>, [RAS-1005], <sequence-number>, FFDC, WARNING, <switch-name>,
Software 'assert' error detected.
```

Probable Cause Indicates an internal software error.

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

Severity WARNING

RAS-1007

Message
```
<timestamp>, [RAS-1007], <sequence-number>,, INFO, <switch-name>, System is about
to reboot.
```

Probable Cause Indicates that the system reboot was initiated.

Recommended Action No action is required.

Severity INFO

RAS-2001

Message
```
<timestamp>, [RAS-2001], <sequence-number>,, INFO, <switch-name>, Audit message
log is enabled.
```

Probable Cause Indicates that a user has enabled the audit message log.

Recommended Action No action is required.

Severity INFO

RAS-2002

Message
```
<timestamp>, [RAS-2002], <sequence-number>,, INFO, <switch-name>, Audit message
log is disabled.
```

Probable Cause Indicates that a user has disabled the audit message log.

Recommended Action No action is required.

Severity INFO

RAS-2003

Message
```
<timestamp>, [RAS-2003], <sequence-number>,, INFO, <switch-name>, Audit message
class configuration has been changed to <New audit class configuration>.
```

Probable Cause Indicates that a user has changed the configured classes of the audit feature.

Recommended Action No action is required.

Severity INFO

RAS-3001

Message
```
<timestamp>, [RAS-3001], <sequence-number>,, INFO, <switch-name>, USB storage
device plug-in detected.
```

Probable Cause Indicates that the USB storage device plug-in is being detected.

Recommended Action No action is required.

Severity INFO

RAS-3002

Message
```
<timestamp>, [RAS-3002], <sequence-number>,, INFO, <switch-name>, USB storage
device enabled.
```

Probable Cause Indicates that the USB storage device is enabled.

Recommended Action No action is required.

Severity INFO

RAS-3003

Message
```
<timestamp>, [RAS-3003], <sequence-number>,, WARNING, <switch-name>, USB storage
device was unplugged before it was disabled.
```

Probable Cause Indicates that the USB storage device was unplugged before it was disabled.

Recommended Action No action is required.

Severity WARNING

RAS-3004

Message
```
<timestamp>, [RAS-3004], <sequence-number>,, INFO, <switch-name>, USB storage
device disabled.
```

Probable Cause Indicates that the USB storage device is disabled.

Recommended Action No action is required.

Severity INFO

Chapter

RCS System Messages 28

RCS-1003

Message

```
<timestamp>, [RCS-1003], <sequence-number>,, ERROR, <system-name>, Failed to
allocate memory: (<function name>).
```

Probable Cause

Indicates that the specified Reliable Commit Service (RCS) function failed to allocate memory.

Recommended Action

This message is usually transitory. Wait for a few minutes and retry the command.

Check the memory usage on the switch using the **show process memory** command.

Restart or power cycle the switch.

Severity

ERROR

RCS-1005

Message

```
<timestamp>, [RCS-1005], <sequence-number>,, INFO, <system-name>, Phase <RCS
phase>, <Application Name> Application returned <Reject reason>, 0x<Reject code>.
```

Probable Cause

Indicates that a receiving switch is rejecting an RCS phase.

Recommended Action

If the reject is in acquire change authorization (ACA) phase, wait for a few minutes and then retry the operation from the sender switch.

If the reject is in the stage fabric configuration (SFC) phase, check if the application license exists for the local rBridge and if the application data is compatible.

Severity

INFO

RCS-1006

Message

```
<timestamp>, [RCS-1006], <sequence-number>,, INFO, <system-name>, 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>.
```

Probable Cause

Indicates that a remote rBridge rejected an RCS phase initiated by an application on the local switch.

If the reject phase is ACA, the remote rBridge may be busy and could not process the new request.

If the reject phase is SFC, the data sent by the application may not be compatible or the rBridge does not have the license to support that application.

Recommended Action
If the reject is in ACA phase, wait for a few minutes and then retry the operation.

If the reject is in the SFC phase, check if the application license exists for the remote domain and if the application data is compatible.

Severity
INFO

RCS-1007

Message

```
<timestamp>, [RCS-1007], <sequence-number>,, ERROR, <system-name>, Zone DB size
and propogation overhead exceeds rBridge <domain number>'s maximum supported Zone
DB size <max zone db size>. Retry after reducing the Zone DB size.
```

Probable Cause
Indicates that the specified rBridge cannot handle the zone database being committed.

Recommended Action
Reduce the zone database size.

Severity
ERROR

RCS-1008

Message

```
<timestamp>, [RCS-1008], <sequence-number>,, ERROR, <system-name>, Domain <domain
number> Lowest Max Zone DB size.
```

Probable Cause
Indicates that the rBridge has the lowest maximum zone database size.

Recommended Action
Reduce the zone database size.

Severity
ERROR

Chapter

RTWR System Messages 29

RTWR-1001

Message

```
<timestamp>, [RTWR-1001], <sequence-number>,, ERROR, <switch-name>, RTWR
<routine: error message> 0x<detail 1>, 0x<detail 2>, 0x<detail 3>, 0x<detail 4>,
0x<detail 5>.
```

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.

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 reboot the switch.

Severity

ERROR

RTWR-1002

Message

```
<timestamp>, [RTWR-1002], <sequence-number>,, WARNING, <switch-name>, RTWR <error
message> 0x<detail 1>, 0x<detail 2>, 0x<detail 3>, 0x<detail 4>, 0x<detail 5>.
```

Probable Cause

Indicates that RTWR has exhausted the maximum number of retries for sending data to the specified rBridge. The message details are as follows:

- error message: Maximum number of retries exhausted
- detail1: Port
- detail2: rBridge
- detail3: Retry Count
- detail4: Status
- detail5: Process ID

Recommended Action

Execute the **show fabric all** command to verify that the specified rBridge ID is online.

Enable the switch with the specified rBridge ID.

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

Severity WARNING

RTWR-1003

Message

```
<timestamp>, [RTWR-1003], <sequence-number>,, INFO, <switch-name>, <module name>:
RTWR retry <number of times retried> to domain <domain ID>, iu_data <first word of
iu_data>.
```

Probable Cause Indicates the number of times 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 ftp** command and then contact your switch service provider.

Severity INFO

Chapter

SEC System Messages 30

SEC-1180

Message
```
<timestamp>, [SEC-1180], <sequence-number>,, INFO, <switch-name>, Added account
<user name> with <role name> authorization.
```

Probable Cause Indicates that the specified new account has been created.

Recommended Action No action is required.

Severity INFO

SEC-1181

Message
```
<timestamp>, [SEC-1181], <sequence-number>,, INFO, <switch-name>, Deleted account
<user name>.
```

Probable Cause Indicates the specified account has been deleted.

Recommended Action No action is required.

Severity INFO

SEC-1182

Message
```
<timestamp>, [SEC-1182], <sequence-number>,, INFO, <switch-name>, Recovered
<number of> accounts.
```

Probable Cause Indicates that the specified number of accounts has been recovered from backup.

Recommended Action No action is required.

Severity INFO

SEC-1184

Message
```
<timestamp>, [SEC-1184], <sequence-number>,, INFO, <switch-name>, <configuration>
configuration change, action <action>, server ID <server>.
```

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.

Severity
INFO

SEC-1185

Message
```
<timestamp>, [SEC-1185], <sequence-number>,, INFO, <switch-name>, <action> switch
DB.
```

Probable Cause
Indicates that the switch database was enabled or disabled as the secondary authentication, accounting, and authorization (AAA) mechanism when the remote authentication dial-in user service (RADIUS)/LDAP is the primary AAA mechanism.

Recommended Action
No action is required.

Severity
INFO

SEC-1187

Message
```
<timestamp>, [SEC-1187], <sequence-number>,, INFO, <switch-name>, Security
violation: Unauthorized switch <switch WWN> tries to join fabric.
```

Probable Cause
Indicates a switch connection control (SCC) security violation was reported. The specified unauthorized switch attempts to join the fabric.

Recommended Action
Check the switch connection control policy (SCC) policy to verify the switches allowed in the fabric. If the switch should be allowed in the fabric but it is not included in the SCC policy, add the switch to the policy. If the switch is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity
INFO

SEC-1189

Message

```
<timestamp>, [SEC-1189], <sequence-number>,, INFO, <switch-name>, Security
violation: Unauthorized host with IP address <IP address> tries to do SNMP write
operation.
```

Probable Cause

Indicates that an SNMP security violation was reported. The specified unauthorized host attempted to perform a write SNMP operation.

Recommended Action

Check the WSNMP policy and verify which hosts are allowed access to the fabric through SNMP. If the host is allowed access to the fabric but is not included in the policy, add the host to the policy. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity

INFO

SEC-1190

Message

```
<timestamp>, [SEC-1190], <sequence-number>,, INFO, <switch-name>, Security
violation: Unauthorized host with IP address <IP address> tries to do SNMP read
operation.
```

Probable Cause

Indicates that an SNMP security violation was reported. The specified unauthorized host attempted to perform a read SNMP operation.

Recommended Action

Check the RSNMP policy to verify the hosts allowed access to the fabric through SNMP read operations are included in the RSNMP policy. If the host is allowed access but is not included in the RSNMP policy, add the host to the policy. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity

INFO

SEC-1191

Message

```
<timestamp>, [SEC-1191], <sequence-number>,, INFO, <switch-name>, Security
violation: Unauthorized host with IP address <Ip address> tries to establish HTTP
connection.
```

Probable Cause

Indicates that an HTTP security violation was reported. The specified unauthorized host attempted to establish an HTTP connection.

Recommended Action

Determine whether the host IP address specified in the message can be used to manage the fabric through an HTTP connection. If so, add the host IP address to the HTTP policy of the fabric. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity

INFO

SEC-1192

Message

```
<timestamp>, [SEC-1192], <sequence-number>,, INFO, <switch-name>, Security
violation: Login failure attempt via <connection method>.
```

Probable Cause

Indicates a serial or modem login security violation was reported. The wrong password was used while trying to log in through a serial or modem connection; the login failed.

Recommended Action

Use the correct password.

Severity

INFO

SEC-1193

Message

```
<timestamp>, [SEC-1193], <sequence-number>,, INFO, <switch-name>, Security
violation: Login failure attempt via <connection method>. IP Addr: <IP address>.
```

Probable Cause

Indicates a specified login security violation was reported. The wrong password was used while trying to log in through the specified connection method; the login failed.

Recommended Action

The error message lists the violating IP address. Verify that this IP address is being used by a valid switch admin. Use the correct password.

Severity

INFO

SEC-1197

Message

```
<timestamp>, [SEC-1197], <sequence-number>,, INFO, <switch-name>, Changed account
<user name>.
```

Probable Cause

Indicates that the specified account has changed.

Recommended Action

No action is required.

Severity

INFO

SEC-1199

Message

```
<timestamp>, [SEC-1199], <sequence-number>,, INFO, <switch-name>, Security
violation: Unauthorized access to serial port of switch <switch instance>.
```

Probable Cause

Indicates a serial connection policy security violation was reported. An attempt was made to access the serial console on the specified switch instance when it is disabled.

Recommended Action Check to see if an authorized access attempt is being made on the console. If so, add the switch World Wide Name (WWN) to the serial policy. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity INFO

SEC-1203

Message

```
<timestamp>, [SEC-1203], <sequence-number>,, INFO, <switch-name>, Login
information: Login successful via TELNET/SSH/RSH. IP Addr: <IP address>.
```

Probable Cause Indicates the IP address of the remote station logging in.

Recommended Action No action is required.

Severity INFO

SEC-1307

Message

```
<timestamp>, [SEC-1307], <sequence-number>,, INFO, <switch-name>, Got response
from <Radius/LDAP server identity> server <server>.
```

Probable Cause Indicates that after some servers timed out, the specified AAA (RADIUS/LDAP) server responded to a switch request.

Recommended Action If the message appears frequently, reconfigure the list of servers such that the responding server is the first server on the list.

Severity INFO

SEC-1308

Message

```
<timestamp>, [SEC-1308], <sequence-number>,, INFO, <switch-name>, All
<Radius/Tacacs+ server identity> servers have failed to respond.
```

Probable Cause Indicates that all servers in the remote AAA (RADIUS) configuration have failed to respond to a switch request within the specified timeout.

Recommended Action Verify the switch has proper network connectivity to the specified AAA (RADIUS/TACACS+) servers, and the servers are correctly configured.

Severity INFO

SEC-1312

Message `<timestamp>, [SEC-1312], <sequence-number>,, INFO, <switch-name>, <MESG Message>.`

Probable Cause Indicates the password attributes 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.

Severity INFO

SEC-1313

Message `<timestamp>, [SEC-1313], <sequence-number>,, INFO, <switch-name>, The password attributes parameters were set to default values.`

Probable Cause Indicates 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.

Severity INFO

SEC-1325

Message `<timestamp>, [SEC-1325], <sequence-number>,, ERROR, <switch-name>, Security enforcement: Switch <switch WWN> connecting to port <Port number> is not authorized to stay in fabric.`

Probable Cause Indicates that because of a switch connection control (SCC) policy violation, the switch is being disabled on the specified port.

Recommended Action No action is required unless the switch must remain in the fabric. If the switch must remain in the fabric, add the switch world wide name (WWN) to the SCC policy, then attempt to join the switch with the fabric.

Severity ERROR

SEC-1329

Message `<timestamp>, [SEC-1329], <sequence-number>,, ERROR, <switch-name>, IPFilter enforcement: Failed to enforce ipfilter policy of <policy Type> type because of <Error code>.`

Probable Cause Indicates the IP filter policy enforcement failed because of an internal system failure.

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

Severity ERROR

SEC-1334

Message
```
<timestamp>, [SEC-1334], <sequence-number>,, INFO, <switch-name>, local security
policy <Event name>.
```

Probable Cause Indicates 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.

Severity INFO

SEC-1335

Message
```
<timestamp>, [SEC-1335], <sequence-number>,, INFO, <switch-name>, local security
policy <Event name> WWN <Member WWN>.
```

Probable Cause Indicates the specified event has occurred.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3035

Message
```
<timestamp>, [SEC-3035], <sequence-number>,, INFO, <switch-name>, Event:
ipfilter, Status: success, Info: <IP Filter Policy> ipfilter policy(ies) saved.
```

Probable Cause Indicates that the specified IP filter policy has 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.

Severity INFO

SEC-3036

Message
```
<timestamp>, [SEC-3036], <sequence-number>,, INFO, <switch-name>, Event:
ipfilter, Status: failed, Info: Failed to save changes for <IP Filter Policy>
ipfilter policie(s).
```

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.

Severity INFO

SEC-3037

Message

```
<timestamp>, [SEC-3037], <sequence-number>,, INFO, <switch-name>, Event:
ipfilter, Status: success, Info: <IP Filter Policy> ipfilter policy activated.
```

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.

Severity INFO

SEC-3038

Message

```
<timestamp>, [SEC-3038], <sequence-number>,, INFO, <switch-name>, Event:
ipfilter, Status: failed, Info: Failed to activate <IP Filter Policy> ipfilter
policy.
```

Probable Cause Indicates that the specified IP filter policy failed to activate.

Recommended Action Verify that the security event was planned. If the event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3039

Message

```
<timestamp>, [SEC-3039], <sequence-number>,, INFO, <switch-name>, Event:Securty
Violation , Status: failed, Info: Unauthorized host with IP address <IP address of
the violating host> tries to establish connection using <Protocol Connection
Type>.
```

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.

Severity INFO

SEC-3051

Message `<timestamp>, [SEC-3051], <sequence-number>,, INFO, <switch-name>, The license key <key> is <Action>.`

Probable Cause Indicates that a license key is added or removed.

Recommended Action No action is required.

Severity INFO

SEC-3061

Message `<timestamp>, [SEC-3061], <sequence-number>,, INFO, <switch-name>, Role '<role name>' is created.`

Probable Cause Indicates a role is created.

Recommended Action No action is required.

Severity INFO

SEC-3062

Message `<timestamp>, [SEC-3062], <sequence-number>,, INFO, <switch-name>, Role '<role name>' is deleted.`

Probable Cause Indicates a role is deleted.

Recommended Action No action is required.

Severity INFO

SEC-3501

Message `<timestamp>, [SEC-3501], <sequence-number>,, INFO, <switch-name>, Role '<Role Name>' is changed.`

Probable Cause Indicates the attributes of a role are changed.

Recommended Action No action is required.

Severity INFO

Chapter

SFLO System Messages 31

SFLO-1001

Message `<timestamp>, [SFLO-1001], <sequence-number>,, INFO, <switch-name>, sFlow is <state> globally.`

Probable Cause Indicates that sFlow is enabled or disabled globally.

Recommended Action No action is required.

Severity INFO

SFLO-1002

Message `<timestamp>, [SFLO-1002], <sequence-number>,, INFO, <switch-name>, sFlow is <state> for port <name>.`

Probable Cause Indicates that sFlow is enabled or disabled for the specified port.

Recommended Action No action is required.

Severity INFO

SFLO-1003

Message `<timestamp>, [SFLO-1003], <sequence-number>,, INFO, <switch-name>, Global sFlow sampling rate is changed to <sample_rate>.`

Probable Cause Indicates that the global sampling rate has changed.

Recommended Action No action is required.

Severity INFO

SFLO-1004

Message `<timestamp>, [SFLO-1004], <sequence-number>,, INFO, <switch-name>, Global sFlow polling interval is changed to <polling_intvl>.`

Probable Cause Indicates that the global counter sampling interval has changed.

Recommended Action No action is required.

Severity INFO

SFLO-1005

Message `<timestamp>, [SFLO-1005], <sequence-number>,, INFO, <switch-name>, sFlow sampling rate on port <name> is changed to <sample_rate>.`

Probable Cause Indicates that the sampling rate has changed on the specified port.

Recommended Action No action is required.

Severity INFO

SFLO-1006

Message `<timestamp>, [SFLO-1006], <sequence-number>,, INFO, <switch-name>, sFlow polling interval on port <name> is changed to <poling_intvl>.`

Probable Cause Indicates that the polling interval has changed on the specified port.

Recommended Action No action is required.

Severity INFO

SFLO-1007

Message `<timestamp>, [SFLO-1007], <sequence-number>,, INFO, <switch-name>, <name> is <state> as sFlow collector.`

Probable Cause Indicates that the sFlow collector is either configured or not configured.

Recommended Action No action is required.

Severity INFO

SFLO-1008

Message `<timestamp>, [SFLO-1008], <sequence-number>,, INFO, <switch-name>, All the sFlow collectors are not configured.`

Probable Cause Indicates that all the sFlow collectors are not configured.

Recommended Action No action is required.

Severity INFO

SFLO-1009

Message

```
<timestamp>, [SFLO-1009], <sequence-number>,, INFO, <switch-name>, Socket
Operation Failed while connecting with the collector address.
```

Probable Cause Indicates that the connect to the collector server failed.

Recommended Action No action is required.

Severity INFO

Chapter

SNMP System Messages 32

SNMP-1001

Message `<timestamp>, [SNMP-1001], <sequence-number>,, ERROR, <switch-name>, SNMP service is not available <Reason>.`

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. If the specified *Reason* is an initialization failure, the switch requires a reboot.

Severity ERROR

SNMP-1002

Message `<timestamp>, [SNMP-1002], <sequence-number>,, ERROR, <switch-name>, SNMP <Error Details> initialization failed.`

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 Reboot or power cycle the switch. This will automatically initialize SNMP.

Severity ERROR

SNMP-1003

Message `<timestamp>, [SNMP-1003], <sequence-number>,, ERROR, <switch-name>, Distribution of Community Strings to Secure Fabric failed.`

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 from the primary switch.

Severity ERROR

SNMP-1004

Message

```
<timestamp>, [SNMP-1004], <sequence-number>, FFDC, ERROR, <switch-name>,
Incorrect SNMP configuration.
```

Probable Cause

Indicates the simple network management protocol (SNMP) configuration is incorrect and the SNMP service will not work correctly.

Recommended Action

Change the SNMP configuration back to the default.

Severity

ERROR

SNMP-1005

Message

```
<timestamp>, [SNMP-1005], <sequence-number>,, INFO, <switch-name>, SNMP
configuration attribute, <Changed attribute>, has changed from <Old Value> to <New
Value>.
```

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 for that parameter.

Recommended Action

Execute the **show running-config snmp-server** command to display the new SNMP configuration.

Severity

INFO

SNMP-1006

Message

```
<timestamp>, [SNMP-1006], <sequence-number>,, INFO, <switch-name>, <SNMP
Configuration group> configuration was reset to default.
```

Probable Cause

Indicates that the simple network management protocol (SNMP) configuration group was reset to the factory default.

Recommended Action

Execute the **show running-config snmp-server** command for the group to display the new SNMP configuration.

Severity

INFO

SNMP-1007

Message

```
<timestamp>, [SNMP-1007], <sequence-number>,, INFO, <switch-name>, The last
fabric change happened at: <string>.
```

Probable Cause

Indicates the time when the last fabric change occurred.

Recommended Action: Execute the **show fabric all** command to view the current fabric status.

Severity: INFO

SNMP-1008

Message:

```
<timestamp>, [SNMP-1008], <sequence-number>,, INFO, <switch-name>, The last
device change happened at: <string>.
```

Probable Cause: Indicates the time when the last device change occurred.

Recommended Action: Execute the **show name-server** command to view the current device status.

Severity: INFO

Chapter

SS System Messages

33

SS-1000

Message

```
<timestamp>, [SS-1000], <sequence-number>,, INFO, <switch-name>, copy support has
uploaded support information to the host with IP address <host ip>.
```

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.

Severity

INFO

SS-1001

Message

```
<timestamp>, [SS-1001], <sequence-number>,, WARNING, <switch-name>, copy support
upload operation to host IP address <host ip> aborted.
```

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.

Recommended Action

Check the remote server settings. After the problem is corrected, rerun the **copy support** command.

Severity

WARNING

SS-1002

Message

```
<timestamp>, [SS-1002], <sequence-number>,, INFO, <switch-name>, copy support has
stored support information to the USB storage device.
```

Probable Cause

Indicates that the **copy support** command was used to transfer support information to an attached USB (Universal Serial Bus) storage device.

Recommended Action

No action is required.

Severity

INFO

SS-1003

Message
```
<timestamp>, [SS-1003], <sequence-number>,, WARNING, <switch-name>, copy support
operation to USB storage device aborted.
```

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

Ensure that the attached USB device is enabled.

Execute the **usb on** command to enable an attached USB device. After the USB problem is corrected, rerun the **copy support** command.

Severity

WARNING

SS-1004

Message
```
<timestamp>, [SS-1004], <sequence-number>,, WARNING, <switch-name>, One or more
modules timed out during copy support. Retry copy support with timeout option to
collect all modules.
```

Probable Cause

Indicates timeout in modules during execution of the **copy support** command.

Recommended Action

Rerun **copy support** command.

Severity

WARNING

Chapter

SSMD System Messages

34

SSMD-1001

Message

```
<timestamp>, [SSMD-1001], <sequence-number>,, ERROR, <switch-name>, Failed to
allocate memory: (<function name>).
```

Probable Cause

Indicates that the specified function has failed to allocate memory.

Recommended Action

Check the memory usage on the switch using the **show processes memory** command.

Restart or power cycle the switch.

Severity

ERROR

SSMD-1002

Message

```
<timestamp>, [SSMD-1002], <sequence-number>,, ERROR, <switch-name>, Failed to
initialize <module> rc = <error>.
```

Probable Cause

Indicates that initialization of a module within the System Services Manager (SSM) has failed.

Recommended Action

Download a new firmware version using the **firmware download** command.

Severity

ERROR

SSMD-1003

Message

```
<timestamp>, [SSMD-1003], <sequence-number>,, ERROR, <switch-name>, Failed to
lock semaphore mutex: (<function name>).
```

Probable Cause

Indicates that the specified function has failed to lock the mutex (semaphore).

Recommended Action

Restart or power cycle the switch.

Severity

ERROR

SSMD-1004

Message

```
<timestamp>, [SSMD-1004], <sequence-number>,, ERROR, <switch-name>, Failed to
unlock semaphore mutex: (<function name>).
```

Probable Cause

Indicates that the specified function failed to unlock the mutex (semaphore).

Recommended Action Restart or power cycle the switch.

Severity ERROR

SSMD-1005

Message
```
<timestamp>, [SSMD-1005], <sequence-number>,, ERROR, <switch-name>, SSM startup
failed.
```

Probable Cause Indicates that the Data Center Ethernet (DCE) SSM encountered an unexpected, severe error during basic startup and initialization.

Recommended Action Restart or power cycle the switch.

If condition persists then download a new firmware version using the **firmware download** command.

Severity ERROR

SSMD-1200

Message
```
<timestamp>, [SSMD-1200], <sequence-number>,, WARNING, <switch-name>, QoS failed
programming ASIC <ASIC slot number>/<ASIC chip number> Multicast Rate Limit.
```

Probable Cause Indicates that the DCE System Services Manager (SSM) encountered an unexpected error in the programming dataplane ASIC for enforcing Multicast Rate Limit feature.

Recommended Action Delete and reapply QoS Multicast Rate Limit policy.

Restart or power cycle the switch.

Severity WARNING

SSMD-1201

Message
```
<timestamp>, [SSMD-1201], <sequence-number>,, WARNING, <switch-name>, QoS failed
programming ASIC <ASIC slot number>/<ASIC chip number> Multicast Tail Drop.
```

Probable Cause Indicates that the DCE System Services Manager (SSM) encountered an unexpected error in the programming dataplane ASIC for enforcing Multicast Tail Drop feature.

Recommended Action Delete and reapply QoS Multicast Tail Drop policy.

Restart or power cycle the switch.

Severity WARNING

SSMD-1202

Message
```
<timestamp>, [SSMD-1202], <sequence-number>,, WARNING, <switch-name>, QoS failed
programming interface 0x<Interface ID> 802.3x Pause flow control.
```

Probable Cause
Indicates that the DCE System Services Manager (SSM) encountered an unexpected error in the programming dataplane ASIC for enforcing interface 802.3x Pause flow control feature.

Recommended Action
Delete and reapply QoS 802.3x Pause flow control policy.

Restart or power cycle the switch.

Severity
WARNING

SSMD-1203

Message
```
<timestamp>, [SSMD-1203], <sequence-number>,, WARNING, <switch-name>, QoS failed
programming interface 0x<Interface ID> PFC flow control.
```

Probable Cause
Indicates that the DCE System Services Manager (SSM) encountered an unexpected error in the programming dataplane ASIC for enforcing interface PFC flow control feature.

Recommended Action
Delete and reapply QoS PFC flow control policy.

Restart or power cycle the switch.

Severity
WARNING

SSMD-1204

Message
```
<timestamp>, [SSMD-1204], <sequence-number>,, WARNING, <switch-name>, QoS failed
initializing ASIC <ASIC slot number>/<ASIC chip number>.
```

Probable Cause
Indicates that the DCE System Services Manager (SSM) encountered an unexpected error in initializing the dataplane ASIC QoS infrastructure.

Recommended Action
Restart or power cycle the switch.

Severity
WARNING

SSMD-1205

Message
```
<timestamp>, [SSMD-1205], <sequence-number>,, WARNING, <switch-name>, CEE failed
programming ETS policy for CEE Map <CEE Map name>.
```

Probable Cause
Indicates that the DCE System Services Manager (SSM) encountered an unexpected error in programming dataplane ASIC for enforcing CEE Map ETS feature.

Recommended Action

Delete and reapply CEE Map ETS policy.

Restart or power cycle the switch.

Severity

WARNING

SSMD-1206

Message

```
<timestamp>, [SSMD-1206], <sequence-number>,, WARNING, <switch-name>, CEE failed
programming CoS to PGID policy for CEE Map <CEE Map name>.
```

Probable Cause

Indicates that the DCE System Services Manager (SSM) encountered an unexpected error in programming the dataplane ASIC for enforcing CEE Map CoS to PGID mapping feature.

Recommended Action

Delete and reapply CEE Map CoS to PGID policy.

Restart or power cycle the switch.

Severity

WARNING

SSMD-1207

Message

```
<timestamp>, [SSMD-1207], <sequence-number>,, WARNING, <switch-name>, QoS failed
programming interface 0x<Interface ID> Default CoS.
```

Probable Cause

Indicates that the DCE System Services Manager (SSM) encountered an unexpected error in programming the dataplane ASIC for enforcing interface Default CoS feature.

Recommended Action

Delete and reapply QoS interface Default CoS policy.

Restart or power cycle the switch.

Severity

WARNING

SSMD-1208

Message

```
<timestamp>, [SSMD-1208], <sequence-number>,, WARNING, <switch-name>, QoS failed
programming interface 0x<Interface ID> Trust.
```

Probable Cause

Indicates that the DCE System Services Manager (SSM) encountered an unexpected error in programming the dataplane ASIC for enforcing interface Trust feature.

Recommended Action

Delete and reapply QoS interface Trust policy.

Restart or power cycle the switch.

Severity

WARNING

SSMD-1209

Message

```
<timestamp>, [SSMD-1209], <sequence-number>,, WARNING, <switch-name>, QoS failed
programming interface 0x<Interface ID> CoS Mutation map.
```

Probable Cause

Indicates that the DCE System Services Manager (SSM) encountered an unexpected error in programming the dataplane ASIC for enforcing CoS Mutation mapping feature.

Recommended Action

Delete and reapply QoS interface CoS Mutation policy.

Restart or power cycle the switch.

Severity

WARNING

SSMD-1210

Message

```
<timestamp>, [SSMD-1210], <sequence-number>,, WARNING, <switch-name>, QoS failed
programming interface 0x<Interface ID> CoS to Traffic Class map.
```

Probable Cause

Indicates that the DCE System Services Manager (SSM) encountered an unexpected error in programming the dataplane ASIC for enforcing CoS to Traffic Class mapping feature.

Recommended Action

Delete and reapply QoS interface CoS to Traffic Class policy.

Restart or power cycle the switch.

Severity

WARNING

SSMD-1211

Message

```
<timestamp>, [SSMD-1211], <sequence-number>,, WARNING, <switch-name>, QoS failed
programming ASIC <ASIC slot number>/<ASIC chip number> Scheduler Control.
```

Probable Cause

Indicates that the DCE System Services Manager (SSM) encountered an unexpected error in programming the dataplane ASIC for enforcing packet Scheduler Control feature.

Recommended Action

Delete and reapply QoS packet Scheduler Control policy.

Restart or power cycle the switch.

Severity

WARNING

SSMD-1212

Message

```
<timestamp>, [SSMD-1212], <sequence-number>,, WARNING, <switch-name>, QoS failed
programming ASIC <ASIC slot number>/<ASIC chip number> Multicast Scheduler
Control.
```

Probable Cause

Indicates that the DCE System Services Manager (SSM) encountered an unexpected error in programming the dataplane ASIC for enforcing multicast packet Scheduler Control feature.

Recommended Action

Delete and reapply QoS multicast packet Scheduler Control policy.

Restart or power cycle the switch.

Severity

WARNING

SSMD-1213

Message

```
<timestamp>, [SSMD-1213], <sequence-number>,, WARNING, <switch-name>, QoS failed
programming interface 0x<Interface ID> CoS Tail Drop Threshold.
```

Probable Cause

Indicates that the DCE System Services Manager (SSM) encountered an unexpected error in programming the dataplane ASIC for enforcing interface CoS Tail Drop Threshold feature.

Recommended Action

Delete and reapply QoS CoS Tail Drop Threshold policy.

Restart or power cycle the switch.

Severity

WARNING

SSMD-1214

Message

```
<timestamp>, [SSMD-1214], <sequence-number>,, WARNING, <switch-name>, QoS failed
programming interface 0x<Interface ID> CoS Tail Drop Threshold.
```

Probable Cause

Indicates that the DCE System Services Manager (SSM) encountered an unexpected error in programming the dataplane ASIC for enforcing interface CoS Tail Drop Threshold feature.

Recommended Action

Delete and reapply QoS CoS Tail Drop Threshold policy.

Restart or power cycle the switch.

Severity

WARNING

SSMD-1215

Message

```
<timestamp>, [SSMD-1215], <sequence-number>,, WARNING, <switch-name>, QoS failed
programming interface 0x<Interface ID> CoS Tail Drop Threshold.
```

Probable Cause

Indicates that the DCE System Services Manager (SSM) encountered an unexpected error in programming the dataplane ASIC for enforcing interface CoS Tail Drop Threshold feature.

Recommended Action

Delete and reapply QoS CoS Tail Drop Threshold policy.

Restart or power cycle the switch.

Severity

WARNING

SSMD-1216

Message

```
<timestamp>, [SSMD-1216], <sequence-number>,, WARNING, <switch-name>, QoS failed
programming interface 0x<Interface ID> Pause.
```

Probable Cause

Indicates that the DCE System Services Manager (SSM) encountered an unexpected error in programming the dataplane ASIC for enforcing interface Pause feature.

Recommended Action

Delete and reapply QoS Pause policy.

Restart or power cycle the switch.

Severity

WARNING

SSMD-1217

Message

```
<timestamp>, [SSMD-1217], <sequence-number>,, WARNING, <switch-name>, QoS CEE
could not comply with FCoE scheduler policy for CEE Map <CEE Map name>.
```

Probable Cause

Indicates that the DCE System Services Manager (SSM) was unable to translate CEE Map and FCoE configuration into an Enhanced Transmission Selection (ETS) scheduler policy implementable by the dataplane ASIC.

Recommended Action

Redefine CEE Map and FCoE into a configuration that translates into an ETS scheduler policy requiring 8 or fewer Traffic Class.

Severity

WARNING

SSMD-1218

Message

```
<timestamp>, [SSMD-1218], <sequence-number>,, WARNING, <switch-name>, QoS failed
programming interface 0x<Interface ID> Priority Tag.
```

Probable Cause

Indicates that the DCE System Services Manager (SSM) encountered an unexpected error in programming the dataplane ASIC for enforcing interface Priority Tag feature.

Recommended Action

Delete and reapply QoS interface Priority Tag policy.

Restart or power cycle the switch.

Severity

WARNING

SSMD-1219

Message

```
<timestamp>, [SSMD-1219], <sequence-number>,, WARNING, <switch-name>, QoS failed
programming interface 0x<Interface ID> CoS7 TCAM.
```

Probable Cause

Indicates that the DCE System Services Manager (SSM) encountered an unexpected error in programming the dataplane ASIC for enforcing interface CoS7 TCAM feature.

Recommended Action
Delete and reapply the CoS7 interface Priority Tag policy.

Restart or power cycle the switch.

Severity
WARNING

SSMD-1220

Message

```
<timestamp>, [SSMD-1220], <sequence-number>,, WARNING, <switch-name>, QoS failed
adding member port 0x<member port> to LAG 0x<LAG port>.
```

Probable Cause
Indicates conflicting QoS configurations on the member port.

Recommended Action
Delete CEE or FCoE configuration on the member port.

Severity
WARNING

SSMD-1221

Message

```
<timestamp>, [SSMD-1221], <sequence-number>,, WARNING, <switch-name>, QoS
configuration rejected due to Long Distance configuration restriction on port
<member port>.
```

Probable Cause
Indicates that the number of inter-switch links (ISLs) supported by the long distance configuration has reached the maximum.

Recommended Action
Disable the ISL port using the **no fabric isl enable** command.

Severity
WARNING

SSMD-1222

Message

```
<timestamp>, [SSMD-1222], <sequence-number>,, WARNING, <switch-name>, Long
distance configuration cannot be completed for Chip <ASIC slot number>/<ASIC chip
number> because ports are not shut down. Maximum retry count exceeded.
```

Probable Cause
Indicates that the Network Service Module (NSM) has failed to disable all the ports after maximum retry attempts.

Recommended Action
Delete and reconfigure long distance on the link using the **long-distance-port** command.

Severity
WARNING

SSMD-1300

Message
```
<timestamp>, [SSMD-1300], <sequence-number>,, INFO, <switch-name>, CEEMap
<ceemap> is created with precedence <precedence>.
```

Probable Cause Indicates that the CEE Map has been created.

Recommended Action No action is required.

Severity INFO

SSMD-1301

Message
```
<timestamp>, [SSMD-1301], <sequence-number>,, INFO, <switch-name>, CEEMap
<ceemap> is is deleted.
```

Probable Cause Indicates that the CEE Map has been deleted.

Recommended Action No action is required.

Severity INFO

SSMD-1302

Message
```
<timestamp>, [SSMD-1302], <sequence-number>,, INFO, <switch-name>, CEEMap
<ceemap> priority table <pg_ids> is <action>.
```

Probable Cause Indicates that the priority groups (PGs) are added to or removed from the existing CEE Map.

Recommended Action No action is required.

Severity INFO

SSMD-1303

Message
```
<timestamp>, [SSMD-1303], <sequence-number>,, INFO, <switch-name>, CEEMap
<ceemap> priority group <pg_id> with weight <PGID_weight> is created with PFC
<pfc>.
```

Probable Cause Indicates that the priority group has been created.

Recommended Action No action is required.

Severity INFO

SSMD-1304

Message
```
<timestamp>, [SSMD-1304], <sequence-number>,, INFO, <switch-name>, CEEMap
<ceemap> priority group <pg_id> is deleted.
```

Probable Cause Indicates that the priority group has been deleted.

Recommended Action No action is required.

Severity INFO

SSMD-1305

Message
```
<timestamp>, [SSMD-1305], <sequence-number>,, INFO, <switch-name>, CEEMap
<ceemap> priority group <pg_id> weight is changed from <PGID_weight_new> to
<PGID_weight_old>.
```

Probable Cause Indicates that the priority group weight has been changed.

Recommended Action No action is required.

Severity INFO

SSMD-1306

Message
```
<timestamp>, [SSMD-1306], <sequence-number>,, INFO, <switch-name>, CEEMap
<ceemap> priority group <pg_id> is PFC <pfc_status>.
```

Probable Cause Indicates that priority group Priority-based Flow Control (PFC) status has been changed.

Recommended Action No action is required.

Severity INFO

SSMD-1307

Message
```
<timestamp>, [SSMD-1307], <sequence-number>,, INFO, <switch-name>, <acl_type>
access list <acl_name> is created.
```

Probable Cause Indicates that the Access List has been created.

Recommended Action No action is required.

Severity INFO

SSMD-1308

Message

```
<timestamp>, [SSMD-1308], <sequence-number>,, INFO, <switch-name>, <acl_type>
access list <acl_name> is deleted.
```

Probable Cause
Indicates that the Access List has been deleted.

Recommended Action
No action is required.

Severity
INFO

SSMD-1309

Message

```
<timestamp>, [SSMD-1309], <sequence-number>,, INFO, <switch-name>, <acl_type>
access list <acl_name> rule sequence number <rule_sq_no> is <action>.
```

Probable Cause
Indicates that the Access List rules are added to or removed from the existing policy.

Recommended Action
No action is required.

Severity
INFO

SSMD-1310

Message

```
<timestamp>, [SSMD-1310], <sequence-number>,, INFO, <switch-name>, ACL <acl_name>
configured on interface <InterfaceName>.
```

Probable Cause
Indicates that the Access List has been configured on an interface.

Recommended Action
No action is required.

Severity
INFO

SSMD-1311

Message

```
<timestamp>, [SSMD-1311], <sequence-number>,, INFO, <switch-name>, ACL <acl_name>
is removed from interface <InterfaceName>.
```

Probable Cause
Indicates that the Access List has been removed from an interface.

Recommended Action
No action is required.

Severity
INFO

SSMD-1312

Message

```
<timestamp>, [SSMD-1312], <sequence-number>,, INFO, <switch-name>, <map_type>
<map_name> assigned to interface <InterfaceName>.
```

Probable Cause Indicates that the user profile map has been assigned to an interface.

Recommended Action No action is required.

Severity INFO

SSMD-1313

Message

```
<timestamp>, [SSMD-1313], <sequence-number>,, INFO, <switch-name>, <map_type>
<map_name> is removed from interface <InterfaceName>.
```

Probable Cause Indicates that an user profile Map has been removed from the interface.

Recommended Action No action is required.

Severity INFO

SSMD-1314

Message

```
<timestamp>, [SSMD-1314], <sequence-number>,, INFO, <switch-name>, CEEMap
<ceemap> precedence changed from <precedence_old> to <precedence_new>.
```

Probable Cause Indicates that the CEE Map precedence has been changed.

Recommended Action No action is required.

Severity INFO

SSMD-1315

Message

```
<timestamp>, [SSMD-1315], <sequence-number>,, INFO, <switch-name>, CEEMap
<ceemap> remap <lossless or fabric priority> to priority <remapped value>.
```

Probable Cause Indicates that the CEE Map remapped CoS has changed.

Recommended Action No action is required.

Severity INFO

SSMD-1900

Message

```
<timestamp>, [SSMD-1900], <sequence-number>,, INFO, <switch-name>, Security
sub-profile is created for port-profile <Profile name>.
```

Probable Cause

Indicates that a security sub-profile has been created.

Recommended Action

No action is required.

Severity

INFO

SSMD-1901

Message

```
<timestamp>, [SSMD-1901], <sequence-number>,, INFO, <switch-name>, ACL <ACL name>
is configured successfully for security sub-profile of port-profile <Profile
name>.
```

Probable Cause

Indicates that an ACL has been configured for security sub-profile.

Recommended Action

No action is required.

Severity

INFO

SSMD-1902

Message

```
<timestamp>, [SSMD-1902], <sequence-number>,, INFO, <switch-name>, ACL <ACL name>
is removed successfully for security sub-profile of port-profile <Profile name>.
```

Probable Cause

Indicates that an ACL has been removed for security sub-profile.

Recommended Action

No action is required.

Severity

INFO

SSMD-1903

Message

```
<timestamp>, [SSMD-1903], <sequence-number>,, INFO, <switch-name>, CoS <Cos
value> is configured successfully for QoS sub-profile of port-profile <Profile
name>.
```

Probable Cause

Indicates that the CoS has been configured for QoS sub-profile.

Recommended Action

No action is required.

Severity

INFO

SSMD-1904

Message

```
<timestamp>, [SSMD-1904], <sequence-number>,, INFO, <switch-name>, Trust is
configured successfully for QoS sub-profile of port-profile <Profile name>.
```

Probable Cause
Indicates that a trust has been configured for QoS sub-profile.

Recommended Action
No action is required.

Severity
INFO

SSMD-1905

Message

```
<timestamp>, [SSMD-1905], <sequence-number>,, INFO, <switch-name>, Trust is
removed successfully for QoS sub-profile of port-profile <Profile name>.
```

Probable Cause
Indicates that a trust has been removed for QoS sub-profile.

Recommended Action
No action is required.

Severity
INFO

SSMD-1906

Message

```
<timestamp>, [SSMD-1906], <sequence-number>,, INFO, <switch-name>, Flowcontrol Tx
<Tx flag> Rx <Rx flag> is configured successfully for QoS sub-profile of
port-profile <Profile name>.
```

Probable Cause
Indicates that flow control has been configured for QoS sub-profile.

Recommended Action
No action is required.

Severity
INFO

SSMD-1907

Message

```
<timestamp>, [SSMD-1907], <sequence-number>,, INFO, <switch-name>, CoS-mutation
<Map name> is configured successfully for QoS sub-profile of port-profile <Profile
name>.
```

Probable Cause
Indicates that CoS-mutation has been configured for QoS sub-profile.

Recommended Action
No action is required.

Severity
INFO

SSMD-1908

Message

```
<timestamp>, [SSMD-1908], <sequence-number>,, INFO, <switch-name>, CoS-mutation
is removed successfully for QoS sub-profile of port-profile <Profile name>.
```

Probable Cause Indicates that the CoS-mutation has been removed for QoS sub-profile.

Recommended Action No action is required.

Severity INFO

SSMD-1909

Message

```
<timestamp>, [SSMD-1909], <sequence-number>,, INFO, <switch-name>,
CoS-traffic-class <Map name> is configured successfully for QoS sub-profile of
port-profile <Profile name>.
```

Probable Cause Indicates that the CoS-traffic-class has been configured for QoS sub-profile.

Recommended Action No action is required.

Severity INFO

SSMD-1910

Message

```
<timestamp>, [SSMD-1910], <sequence-number>,, INFO, <switch-name>,
CoS-traffic-class is removed successfully for qos sub-profile of port-profile
<Profile name>.
```

Probable Cause Indicates that the CoS-traffic-class has been removed for QoS sub-profile.

Recommended Action No action is required.

Severity INFO

SSMD-1911

Message

```
<timestamp>, [SSMD-1911], <sequence-number>,, INFO, <switch-name>, CEE is removed
successfully for QoS sub-profile of port-profile <Profile name>.
```

Probable Cause Indicates that CEE has been removed for QoS sub-profile.

Recommended Action No action is required.

Severity INFO

SSMD-1912

Message

```
<timestamp>, [SSMD-1912], <sequence-number>,, INFO, <switch-name>, CEE <Map name>
is configured successfully for QoS sub-profile of port-profile <Profile name>.
```

Probable Cause Indicates that CEE has been configured for QoS sub-profile.

Recommended Action No action is required.

Severity INFO

SSMD-1913

Message

```
<timestamp>, [SSMD-1913], <sequence-number>,, INFO, <switch-name>, Flowcontrol
PFC-CoS <Pfc-Cos value> Tx <Tx flag> Rx <Rx flag> is configured successfully for
QoS sub-profile of port-profile <Profile name>.
```

Probable Cause Indicates that the flow control PFC has been configured for QoS sub-profile.

Recommended Action No action is required.

Severity INFO

SSMD-1914

Message

```
<timestamp>, [SSMD-1914], <sequence-number>,, INFO, <switch-name>, QoS
sub-profile is created for port-profile <Profile name>.
```

Probable Cause Indicates that the QoS sub-profile has been created.

Recommended Action No action is required.

Severity INFO

SSMD-1915

Message

```
<timestamp>, [SSMD-1915], <sequence-number>,, INFO, <switch-name>, Security
sub-profile is deleted for port-profile <Profile name>.
```

Probable Cause Indicates that the security sub-profile has been deleted.

Recommended Action No action is required.

Severity INFO

SSMD-1916

Message

```
<timestamp>, [SSMD-1916], <sequence-number>,, INFO, <switch-name>, QoS
sub-profile is deleted for port-profile <Profile name>.
```

Probable Cause

Indicates that the QoS sub-profile has been deleted.

Recommended Action

No action is required.

Severity

INFO

Chapter

SULB System Messages 35

SULB-1001

Message

```
<timestamp>, [SULB-1001], <sequence-number>,, WARNING, <switch-name>, firmware
download command has started.
```

Probable Cause

Indicates that the **firmware download** command has been executed. This process takes about 17 minutes to complete. The process is set to time out after 30 minutes.

Recommended Action

Do not fail over or power down the system during the firmware upgrade. Allow the **firmware download** command to continue without disruption. No action is required.

Execute the **show firmwaredownloadstatus** command for more information.

Severity

WARNING

SULB-1002

Message

```
<timestamp>, [SULB-1002],<sequence-number>, , INFO, <switch-name>, firmware
download command has completed successfully.
```

Probable Cause

Indicates that the **firmware download** command has completed successfully and the switch firmware has been updated.

Recommended Action

No action is required. The **firmware download** command has completed as expected.

Execute the **show firmwaredownloadstatus** command for more information. Execute the **show version** command to verify the firmware version.

Severity

INFO

SULB-1003

Message

```
<timestamp>, [SULB-1003], <sequence-number>,, INFO, <switch-name>, firmware
commit has started.
```

Probable Cause

Indicates that the **firmware commit** command has been executed.

Recommended Action

No action is required. Execute the **show firmwaredownloadstatus** command for more information.

Severity

INFO

SULB-1004

Message
```
<timestamp>, [SULB-1004], <sequence-number>,, INFO, <switch-name>, firmware
commit has completed.
```

Probable Cause Indicates that the **firmware commit** command has been completed.

Recommended Action No action is required. Execute the **show firmwaredownloadstatus** command for more information.

Severity INFO

SULB-1009

Message
```
AUDIT, <timestamp>, [SULB-1009], <sequence-number>,, INFO, <switch-name>,
firmware download command failed. status: 0x<status code>, error: 0x<error code>.
```

Probable Cause Indicates that the **firmware download** command failed. The additional *status code* and *error code* provide debugging information.

Table 7 lists **firmware download** status messages and status codes. Some of them will not be displayed in this RASLOG message and are listed for completeness.

TABLE 7 Status messages and status codes

Status message	Status code
“**firmware download** sanity check failed.”	0x30
"Sanity check failed because system is non-redundant."	0x31
“Sanity check failed because **firmware download** is already in progress.”	0x32
"Sanity check failed because Network OS is disabled on the Active CP."	0x33
"Sanity check failed because the high availability management daemon (HAMD) is disabled on Active CP."	0x34
“Sanity check failed because **firmware download** is already in progress.”	0x35
"Sanity check failed because Network OS is disabled on Standby CP."	0x36
"Sanity check failed because HAMD is disabled on Standby CP."	0x37
“**firmware download** failed on the Standby CP.”	0x40
“**firmware download** failed on the Standby CP.”	0x41
“**firmware download** failed on the Standby CP.”	0x42
“**firmware commit** failed on the Standby CP.”	0x43
“**firmware download** failed.”	0x44
“**firmware download** failed due to inter-process communication (IPC) error.”	0x50
"Unable to check the firmware version on Standby CP due to IPC error."	0x51
“**firmware download** failed due to IPC error.”	0x52
“**firmware download** failed due to IPC error.”	0x53
"Standby CP failed to reboot due to IPC error."	0x54

TABLE 7 Status messages and status codes (Continued)

Status message	Status code
“**firmware commit** operation failed due to IPC error.”	0x55
"Unable to check the firmware version on Standby CP due to IPC error."	0x56
“Unable to restore the original firmware due to Standby CP timeout.”	0x57
"Standby CP failed to reboot and was not responding."	0x58
"Unable to check the firmware version on Standby CP due to IPC error."	0x59
“Sanity check failed because **firmware download** is already in progress.”	0x60
“Sanity check failed because **firmware download** is already in progress.”	0x61
NOT USED	0x62
"System error."	0x63
"Active CP forced failover succeeded. Now this CP becomes Active."	0x64
"Standby CP booted up."	0x65
"Active and Standby CP failed to gain HA synchronization within 10 minutes."	0x66
"Standby rebooted successfully."	0x67
"Standby failed to reboot."	0x68
“**firmware commit** has started to restore the secondary partition.”	0x69
"Local CP is restoring its secondary partition."	0x6a
“Unable to restore the secondary partition. Execute the **show firmwaredownloadstatus** command to display the firmware download event log. Execute the **show version** command to display the firmware version.”	0x6b
“**firmware download** has started on Standby CP. It might take up to 10 minutes.”	0x6c
“**firmware download** has completed successfully on Standby CP.”	0x6d
"Standby CP reboots."	0x6e
"Standby CP failed to boot up."	0x6f
"Standby CP booted up with new firmware."	0x70
"Standby CP failed to boot up with new firmware."	0x71
“**firmware download** has completed successfully on Standby CP.”	0x72
“**firmware download** has started on Standby CP. It might take up to 10 minutes.”	0x73
“**firmware download** has completed successfully on Standby CP.”	0x74
"Standby CP reboots."	0x75
"Standby CP failed to reboot."	0x76
“**firmware commit** has started on Standby CP.”	0x77
“**firmware commit** has completed successfully on Standby CP.”	0x78
"Standby CP booted up with new firmware."	0x79
"Standby CP failed to boot up with new firmware."	0x7a
“**firmware commit** has started on both Active and Standby CPs.”	0x7b
“**firmware commit** has completed successfully on both CPs.”	0x7c

TABLE 7 Status messages and status codes (Continued)

Status message	Status code
“**firmware commit** failed on Active CP.”	0x7d
"The original firmware has been restored successfully on Standby CP."	0x7e
"Unable to restore the original firmware on Standby CP."	0x7f
"Standby CP reboots."	0x80
"Standby CP failed to reboot."	0x81
"Standby CP booted up with new firmware."	0x82
"Standby CP failed to boot up with new firmware."	0x83
“There was an unexpected reboot during **firmware download**. The command is aborted.”	0x84
"Standby CP was not responding. The command is aborted."	0x85
“**firmware commit** has started on both CPs. Execute the **show firmwaredownloadstatus** command to display the firmware download event log. Execute the **show version** command to display the firmware version.”	0x86
“**firmware commit** has started on the local CP. Execute the **show firmwaredownloadstatus** command to display the firmware download event log. Execute the **show version** command to display the firmware version.”	0x87
“**firmware commit** has started on the remote CP. Execute the **show firmwaredownloadstatus** command to display the firmware download event log. Execute the **show version** command to display the firmware version.”	0x88
“Execute the **show firmwaredownloadstatus** command to display the firmware download event log. Execute the **show version** command to display the firmware version.”	0x89
“**firmware download** command has completed successfully.”	0x8a
"The original firmware has been restored successfully."	0x8b
"Remote CP is restoring its secondary partition."	0x8c
"Local CP is restoring its secondary partition."	0x8d
"Remote CP is restoring its secondary partition."	0x8e
“**firmware download** has started.”	0x8f
“**firmware commit** has started.”	0x90
“**firmware download** has completed successfully.”	0x91
“**firmware commit** has completed successfully.”	0x92
“**firmware commit** has started to restore the secondary partition.”	0x93
“**firmware commit** failed.”	0x94
"The secondary partition has been restored successfully."	0x95
"Firmware is being downloaded to the blade. This step may take up to 10 minutes."	0xa0
“**firmware download** timed out.”	0xa1
“Reboot occurred during **firmware download. firmware commit** will be started to recover the blade.”	0xa2
“Blade rebooted during **firmware commit**. The operation will be restarted.”	0xa3
"Firmware has been downloaded successfully. Blade is rebooting with the new firmware."	0xa4
"Blade has rebooted successfully."	0xa5

TABLE 7 Status messages and status codes (Continued)

Status message	Status code
“New firmware failed to boot up. Retry the **firmware download**.”	0xa6
“**firmware commit** has started on the blade. This may take up to 10 minutes.”	0xa7
“The **firmware restore** command is executed. System will reboot and a **firmware commit** operation will start upon bootup.”	0xa8
"Switch is relocating the AP image."	0xa9
"The AP image is relocated successfully."	0xaa
"Switch reboots during relocating the AP image. The operation will be restarted."	0xab
“Blade failed to reboot with the original image. The **firmware restore** command failed.”	0xac

Table 8 lists additional **firmware download** error messages and error codes. They provide more details on why **firmware download** failed.

TABLE 8 Error messages and error codes

Error message	Error code
"Image is up-to-date. No need to download the same version of firmware."	0xF
“Upgrade is inconsistent.”	0x10
“OSRootPartition is inconsistent.”	0x11
“Unable to access the required package list file. Check whether the switch is supported by the requested firmware. Also check **firmware download** help page for other possible failure reasons.”	0x12
"The RPM package database is inconsistent. Contact your service provider for recovery."	0x13
"Out of memory."	0x14
"Failed to download Red Hat package manager (RPM) package.”	0x15
"Unable to create firmware version file."	0x16
"Unexpected system error."	0x17
“Error in getting lock device for **firmware download**.”	0x18
“Error in releasing lock device for **firmware download**.”	0x19
“**firmware commit** failed.”	0x1a
"Firmware directory structure is not compatible. Check whether the firmware is supported on this platform."	0x1b
"Failed to load the Linux kernel image."	0x1c
“OSLoader is inconsistent.”	0x1d
“New image has not been committed. Execute the **firmware commit** or **firmware restore** command and then execute the **firmware download** command.”	0x1e
“**firmware restore** failed.”	0x1f
"Both images are mounted to the same device."	0x20
“Unable to unionist old packages.”	0x21
“**firmware download** is already in progress.”	0x22
“**firmware download** timed out.”	0x23

TABLE 8 Error messages and error codes (Continued)

Error message	Error code
“Out of disk space.”	0x24
“Primary filesystem is inconsistent. Execute the **firmware restore** command to restore the original firmware, or contact your service provider for recovery.”	0x25
"The post-install script failed."	0x26
"Unexpected reboot."	0x27
“Primary kernel partition is inconsistent. Contact your service provider for recovery.”	0x28
"The pre-install script failed."	0x29
“The platform option is not supported.”	0x2a
"Failed to install RPM package."	0x2b

The following section explains the causes of some common error messages:

0x15 - Failed to download Red Hat package manager (RPM) package. If this error occurs immediately after **firmware download** is started, the firmware on the switch may be two releases older than the requested firmware. The **firmware download** command supports firmware upgrades within two feature releases (a feature release is indicated by a major number and a minor number, for example, X.Y). In this case, you will need to upgrade to an intermediate version before downloading the desired version. If this error occurs in the middle of **firmware download**, the firmware in the file server may be corrupted or there may be a temporary network issue. In this case, retry the **firmware download** command. If the problem persists, contact your system administrator.

0x18 - Error in getting lock device for **firmware download**. This error can be due to another **firmware download** already in progress. Execute the **show firmwaredownloadstatus** command to verify that this is the case. Wait for the current session to finish before proceeding.

0x23 - **firmware download** timed out. This error may occur because the **firmware download** has not completed within the predefined timeout period. It is most often caused by network issues. If the problem persists, contact your system administrator.

0x24 - Out of disk space. This error may occur because some core dump files have not been removed from the filesystem and are using up disk space. Remove these core dump files by using the **copy support** command before proceeding.

0x29 - The pre-install script failed. This error may be caused by an unsupported blade type. Remove or power off the unsupported blades before proceeding.

Recommended Action

Execute the **show firmwaredownloadstatus** command for more information.

In a director-class switch, when **firmware download** fails, the command will synchronize the firmware on the two partitions of each CP by starting a firmware commit operation. Wait until this operation completes (about 10 minutes) before attempting another firmware download.

In a director-class switch, when **firmware download** fails, the two CPs may end up with different versions of firmware and they may not gain high-availability (HA) sync. In that case, upgrade the firmware on the standby CP to the same version as the active CP and then retry the **firmware download** command to download the desired version of firmware onto the CPs.

Severity

INFO

SULB-1010

Message `<timestamp>, [SULB-1010], <sequence-number>,, INFO, <switch-name>, firmware commit failed (status=0x<error code>).`

Probable Cause Indicates that the **firmware commit** command has failed. The error code provides debugging information. Refer to the Status messages and status codes table in the SULB-1009 message for more information.

Recommended Action If the failure is caused by an inconsistent filesystem, contact your switch service provider.

Severity INFO

SULB-1011

Message `<timestamp>, [SULB-1011], <sequence-number>,, INFO, <switch-name>, firmware download command failed. <error string>.`

Probable Cause Indicates that the **firmware download** command has failed. The additional *error string* indicates the reason for the failure.

Recommended Action Execute the **show firmwaredownloadstatus** command for more information.

Severity INFO

SULB-1036

Message `<timestamp>, [SULB-1036], <sequence-number>,, INFO, <switch-name>, <The Version being logged> <Version String>.`

Probable Cause Indicates the version running on the system. This is generally logged before download and after download of the firmware to store version information.

Recommended Action No action is required.

Severity INFO

SULB-1037

Message `<timestamp>, [SULB-1037], <sequence-number>, INFO, <switch-name>, Hot Code Load (HCL) failed.`

Probable Cause Indicates that the Hot Code Load (HCL) has failed. Many reasons, such as domain not confirmed, can cause this failure.

Recommended Action Execute the **reload** command to reboot the switch manually. However, it will disrupt the FC traffic.

Severity INFO

Chapter

TOAM System Messages 36

TOAM-1000

Message

```
<timestamp>, [TOAM-1000], <sequence-number>,, INFO, <switch-name>, Cannot run
this command because VCS is disabled.
```

Probable Cause

Indicates inability to run the TRILL OAM (TOAM) command because Virtual Cluster Switch (VCS) is disabled.

Recommended Action

To run the TOAM commands, enable VCS using the **vcs enable** command.

Severity

INFO

TOAM-1003

Message

```
<timestamp>, [TOAM-1003], <sequence-number>,, ERROR, <switch-name>, Initilization
error: <reason>.
```

Probable Cause

Indicates that TOAM has encountered an error during initialization.

Recommended Action

Restart the toam daemon.

Severity

ERROR

Chapter

TRCE System Messages 37

TRCE-1001

Message

```
<timestamp>, [TRCE-1001], <sequence-number>,, WARNING, <switch-name>, Trace dump
available <optional slot indicating on which slot the dump occurs>! (reason: <Text
explanation of what triggered the dump. (PANIC DUMP, WATCHDOG EXPIRED, MANUAL,
TRIGGER)>)
```

Probable Cause

Indicates that trace dump files have been generated on the switch or the indicated slot. The reason field indicates the cause for generating the dump as one of the following:

- PANICDUMP generated by panic dump
- WATCHDOG EXPIRED generated by hardware watchdog expiration

Recommended Action

Run the **copy support** command to collect supportsave and contact your switch service provider.

Severity

WARNING

TRCE-1004

Message

```
<timestamp>, [TRCE-1004], <sequence-number>,, WARNING, <switch-name>, Trace dump
<optional slot indicating on which slot the dump occurs> was not transferred
because trace auto-FTP disabled.
```

Probable Cause

Indicates that trace dump files have been created on the switch or the indicated slot but are not automatically transferred from the switch because auto-FTP is disabled.

Recommended Action

Run the **copy support** command to collect supportsave and contact your switch service provider.

Severity

WARNING

Chapter

TS System Messages 38

TS-1002

Message

```
<timestamp>, [TS-1002], <sequence-number>,, INFO, <system-name>, <Type of clock
server used> Clock Server used instead of <Type of clock server configured>: locl:
0x<code> remote: 0x<code>.
```

Probable Cause

Indicates the switch time synchronization was not sourced from the *Type of clock server configured*, instead, an alternate server was used, indicated by *Type of clock server used*. The type of clock server used or configured may be one of the following:

- LOCL
  Local switch clock
- External
  External NTP server address configured

This 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 should be ignored.

Recommended Action

Run the **show ntp status** command to verify that the switch has the clock server IP configured correctly. Verify this clock server is accessible to the switch and functional. If it is not accessible or functional, either configure a accessible and functional clock server or reset the clock server to LOCL.

Severity

INFO

TS-1008

Message

```
<timestamp>, [TS-1008], <sequence-number>,, WARNING, <system-name>, <New clock
server used> Clock Server used instead of <Old server configured>.
```

Probable Cause

Indicates there is a change in the source of switch time synchronization to the switch. Another clock server in the list of clock servers configured is being used. This happens when the network time protocol (NTP) query to the current active external clock server fails.

Recommended Action

No action is required. New clock server synchronization may adjust the clock time.

Severity

WARNING

Chapter

VC System Messages

39

VC-1000

Message
```
<timestamp>, [VC-1000], <sequence-number>,, INFO, <switch-name>, vCenter
<vCenterName> configuration is added.
```

Probable Cause Indicates that a new vCenter configuration was added.

Recommended Action No action is required.

Severity INFO

VC-1001

Message
```
<timestamp>, [VC-1001], <sequence-number>,, INFO, <switch-name>, vCenter
<vCenterName> configuration is changed.
```

Probable Cause Indicates that the vCenter configuration has been updated.

Recommended Action No action is required.

Severity INFO

VC-1002

Message
```
<timestamp>, [VC-1002], <sequence-number>,, INFO, <switch-name>, vCenter
<vCenterName> configuration is deleted.
```

Probable Cause Indicates that the vCenter configuration has been deleted.

Recommended Action No action is required.

Severity INFO

VC-1003

Message
```
<timestamp>, [VC-1003], <sequence-number>,, INFO, <switch-name>, vCenter
<vCenterName> configuration has been activated successfully.
```

Probable Cause Indicates that the vCenter configuration has been activated.

Recommended Action
No action is required.

Severity
INFO

VC-1004

Message
```
<timestamp>, [VC-1004], <sequence-number>,, INFO, <switch-name>, vCenter
<vCenterName> configuration has been deactivated successfully.
```

Probable Cause
Indicates that the vCenter configuration has been deactivated.

Recommended Action
No action is required.

Severity
INFO

VC-1005

Message
```
<timestamp>, [VC-1005], <sequence-number>,, WARNING, <switch-name>, Login to
vCenter <vCenterName> failed (attempt(s) <failedAttempts>) - check credentials
for user <userName>.
```

Probable Cause
Indicates that the vCenter login failed due to invalid credentials.

Recommended Action
Enter the correct username and password for the vCenter.

Severity
WARNING

VC-1006

Message
```
<timestamp>, [VC-1006], <sequence-number>,, INFO, <switch-name>, vCenter
<vCenterName> periodic discovery interval has been changed to <interval> minutes.
```

Probable Cause
Indicates that the vCenter periodic discovery timer interval has been changed.

Recommended Action
No action is required.

Severity
INFO

Chapter

VCS System Messages 40

VCS-1001

Message

```
<timestamp>, [VCS-1001], <sequence-number>, VCS, INFO, <switch-name>, Event: VCS
cluster create, Coordinator IP: <Co-ordinator's Public IP>, VCS ID: <VCS Id>,
Status: <Cluster status>.
```

Probable Cause

Indicates that the Virtual Cluster Switch (VCS) cluster is created in the following:

- Distributed Configuration Manager (DCM): The initial VCS enable and configuration distribute on two or more nodes where a VCS cluster of the same VCS ID did not exist before.
- Fabric Distribution Service (FDS): The initial VCS enable on two or more nodes with the same VCS ID where a VCS cluster of the same VCS ID did not exist before.

Recommended Action

No action is required.

Severity

INFO

VCS-1002

Message

```
<timestamp>, [VCS-1002], <sequence-number>, VCS, ERROR, <switch-name>, Event: VCS
cluster create, Coordinator IP: <Co-ordinator's Public IP>, VCS ID: <VCS Id>,
Status: VCS cluster failed to be created, Reason: <Error Reason>.
```

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.

Severity

ERROR

VCS-1003

Message

```
<timestamp>, [VCS-1003], <sequence-number>, VCS, INFO, <switch-name>, Event: VCS
node add, Coordinator IP: <Co-ordinator's Public IP>, VCS ID: <VCS Id>, Status:
rBridge ID <RBridge-id of Added Switch> (<IP of Added Switch>) added to VCS
cluster.
```

Probable Cause

Indicates that a node is added to the VCS cluster. The node is added when the following actions are performed:

- DCM: VCS is enabled on a node that was not a member of the VCS cluster.

- FDS: VCS is enabled on a node that was not a member of the VCS cluster, or the node rejoined the VCS cluster after the **reload** command was issued or the inter-switch link (ISL) toggled.

Recommended Action: No action is required.

Severity: INFO

VCS-1004

Message

```
<timestamp>, [VCS-1004], <sequence-number>, VCS, ERROR, <switch-name>, Event: VCS
node add, Coordinator IP: <Co-ordinator'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>.
```

Probable Cause: Indicates that a 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.

Severity: ERROR

VCS-1005

Message

```
<timestamp>, [VCS-1005], <sequence-number>, VCS, INFO, <switch-name>, Event: VCS
node rejoin, Coordinator IP: <Co-ordinator's Public IP>, VCS ID: <VCS Id>, Status:
rBridge ID <RBridge-id of Rejoined Switch> (<IP of Rejoined Switch>) rejoined VCS
cluster.
```

Probable Cause: Indicates that the DCM node has gone offline and returned online without any configuration changes.

Recommended Action: No action is required.

Severity: INFO

VCS-1006

Message

```
<timestamp>, [VCS-1006], <sequence-number>, VCS, ERROR, <switch-name>, Event: VCS
node rejoin, Coordinator IP: <Co-ordinator'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>.
```

Probable Cause: Indicates that the DCM 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.

Severity
ERROR

VCS-1007

Message
```
<timestamp>, [VCS-1007], <sequence-number>, VCS, INFO, <switch-name>, Event: VCS
node remove, Coordinator IP: <Co-ordinator's Public IP>, VCS ID: <VCS Id>, Status:
rBridge ID <RBridge-id of Removed Switch> (<IP of Removed Switch>) removed from
VCS cluster.
```

Probable Cause
Indicates that VCS is disabled on the node that was part of a VCS cluster.

Recommended Action
No action is required.

Severity
INFO

VCS-1008

Message
```
<timestamp>, [VCS-1008], <sequence-number>, VCS, ERROR, <switch-name>, Event: VCS
node remove, Coordinator IP: <Co-ordinator'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>.
```

Probable Cause
Indicates that a DCM 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.

Severity
ERROR

VCS-1009

Message
```
<timestamp>, [VCS-1009], <sequence-number>, VCS, INFO, <switch-name>, Event: VCS
node disconnect, Coordinator IP: <Co-ordinator'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.
```

Probable Cause
Indicates that the heartbeat loss to a secondary node occurred because the node was rebooted or all ISLs are down to the secondary node.

Recommended Action
If you had issued the **reload** command, no action is required. If any other reason, check the state of the disconnected node and the ISLs to the disconnected node.

Severity
INFO

Chapter

ZONE System Messages 41

ZONE-1002

Message

```
<timestamp>, [ZONE-1002], <sequence-number>,, WARNING, <switch-name>, WWN
zoneTypeCheck or zoneGroupCheck warning(<warning string>) at port(<port number>).
```

Probable Cause

Indicates that a zone filter or a zone group check failure occurred. The frame filter logic reported a failure when creating or adding the zone groups during port login (PLOGI) trap processing. This message usually indicates problems when adding the content-addressable memory (CAM) entries before the filter setup.

Recommended Action

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

Severity

WARNING

ZONE-1007

Message

```
<timestamp>, [ZONE-1007], <sequence-number>,, INFO, <switch-name>,
Ioctl(<function>) in (<error message>) at port (<port number>) returns code
(<error string>) and reason string (<reason string>).
```

Probable Cause

Indicates that the frame filter logic reported a failure during one of the IOCTL calls. The IOCTL call from which the failure is reported is listed as part of the error message. This is usually a programming error when adding the content-addressable memory (CAM) entries before the filter setup.

Recommended Action

There are two ways to avoid this problem:

- Avoid having too many hosts zoned with a set of target devices at a single port.
- Avoid having too many zones directed at a single port group on the switch.

Severity

INFO

ZONE-1010

Message

```
<timestamp>, [ZONE-1010], <sequence-number>,, WARNING, <switch-name>, Duplicate
entries in zone (<zone name>) specification.
```

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.

Severity
WARNING

ZONE-1012

Message
`<timestamp>, [ZONE-1012], <sequence-number>,, WARNING, <switch-name>, All ports are offline.`

Probable Cause
Indicates that all the ports in a zone are offline.

Recommended Action
Check the device connection.

Severity
WARNING

ZONE-1014

Message
`<timestamp>, [ZONE-1014], <sequence-number>,, ERROR, <switch-name>, Missing required license - <license name>.`

Probable Cause
Indicates that the required zoning license is missing.

Recommended Action
Install the zoning license using the **license add** command. Contact the switch supplier to obtain a zoning license, if you do not have one.

Severity
ERROR

ZONE-1015

Message
`<timestamp>, [ZONE-1015], <sequence-number>,, WARNING, <switch-name>, Not owner of the current transaction <transaction ID>.`

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.

Severity
WARNING

ZONE-1019

Message

```
<timestamp>, [ZONE-1019], <sequence-number>,, ERROR, <switch-name>, Transaction
Commit failed. Reason code <reason code> (<Application reason>) - \"<reason
string>\".
```

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 ftp** command and contact your switch service provider.

Severity

ERROR

ZONE-1022

Message

```
<timestamp>, [ZONE-1022], <sequence-number>,, INFO, <switch-name>, The effective
configuration has changed to <Effective configuration name>. <AD Id>.
```

Probable Cause

Indicates that the effective zone configuration has changed to the name displayed in the specified zone.

Recommended Action

Verify that the zone configuration change was done on purpose. If the new effective zone configuration is correct, no action is required.

Severity

INFO

ZONE-1023

Message

```
<timestamp>, [ZONE-1023], <sequence-number>,, INFO, <switch-name>, Switch
connected to port (<port number>) is busy. Retrying zone merge.
```

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 ftp** command and contact your switch service provider.

Severity

INFO

ZONE-1024

Message
```
<timestamp>, [ZONE-1024], <sequence-number>,, INFO, <switch-name>, <Information
message>.
```

Probable Cause
Indicates that the **zoning enabled-configuration cfg-action cfg-save** command was executed successfully.

Recommended Action
No action is required.

Severity
INFO

ZONE-1027

Message
```
<timestamp>, [ZONE-1027], <sequence-number>,, INFO, <switch-name>, Zoning
transaction aborted <error reason>. <AD Id>.
```

Probable Cause
Indicates that the zoning transaction was aborted due to a variety of potential errors. The *error reason* variable can be one of the following:

- 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 config 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.

Recommended Action
Many of the causes of this error message are transitory, for example, because two administrators are working with the zoning database concurrently. If you receive this error, wait for few minutes and try again. Verify that no one else is currently modifying the zone database.

Severity
INFO

ZONE-1028

Message
```
<timestamp>, [ZONE-1028], <sequence-number>,, WARNING, <switch-name>, Commit zone
DB larger than supported - <zone db size> greater than <max zone db size>.
```

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.

Severity
WARNING

ZONE-1029

Message `<timestamp>, [ZONE-1029], <sequence-number>,, WARNING, <switch-name>, Restoring zone cfg from flash failed - bad config saved to <config file name> [<return code>].`

Probable Cause Indicates that the zone configuration restored from the flash was faulty.

Recommended Action This error will save the faulty zone configuration in the zoned core file directory.

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

Severity WARNING

ZONE-1030

Message `<timestamp>, [ZONE-1030], <sequence-number>,, WARNING, <switch-name>, Converting the zone DB for PID format change failed.`

Probable Cause Indicates that the current zone database could not be converted to reflect the PID format change. Most likely this is caused due to the size of the zone database.

Recommended Action Change the PID format back to its original format. Reduce the size of the zone database. Then you can change the PID format to the requested format.

Severity WARNING

ZONE-1032

Message `<timestamp>, [ZONE-1032], <sequence-number>,, ERROR, <switch-name>, rBridge <rBridge number> Max Zone DB size <max zone db size>.`

Probable Cause Indicates that the specified rBridge does not have enough memory for the zone database being committed.

Recommended Action Reduce the size of the zone database and retry the operation.

Severity ERROR

ZONE-1033

Message `<timestamp>, [ZONE-1033], <sequence-number>,, ERROR, <switch-name>, rBridge <rBridge number> Lowest Max Zone DB size.`

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 size of the zone database and retry the operation.

Severity
ERROR

ZONE-1034

Message
```
<timestamp>, [ZONE-1034], <sequence-number>,, INFO, <switch-name>, A new zone
database file (<config file name>) is created.
```

Probable Cause
Indicates that a new zone database was created.

Recommended Action
No action is required.

Severity
INFO

ZONE-1035

Message
```
<timestamp>, [ZONE-1035], <sequence-number>,, ERROR, <switch-name>, Unable to
rename <Old config file name> to <New config file name>: error message <System
Error Message>.
```

Probable Cause
Indicates that the Network OS cannot rename the zone configuration file. Typically the zone configuration is too large for the memory available on the switch.

Recommended Action
Reduce the size of the zone database and retry the operation.

Severity
ERROR

ZONE-1036

Message
```
<timestamp>, [ZONE-1036], <sequence-number>,, ERROR, <switch-name>, Unable to
create <config file name>: error message <System Error Message>.
```

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 and retry the operation.

Severity
ERROR

ZONE-1037

Message
```
<timestamp>, [ZONE-1037], <sequence-number>,, ERROR, <switch-name>, Unable to
examine <config file name>: error message <System Error Message>.
```

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 and retry the operation.

Severity
ERROR

ZONE-1038

Message
```
<timestamp>, [ZONE-1038], <sequence-number>,, ERROR, <switch-name>, Unable to
allocate memory for <config file name>: error message <System Error Message>.
```

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 and retry the operation.

Severity
ERROR

ZONE-1039

Message
```
<timestamp>, [ZONE-1039], <sequence-number>,, ERROR, <switch-name>, Unable to
read contents of <config file name>: error message <System Error Message>.
```

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 and retry the operation.

Severity
ERROR

ZONE-1040

Message
```
<timestamp>, [ZONE-1040], <sequence-number>,, INFO, <switch-name>, Merged zone
database exceeds limit.
```

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 and retry the operation.

Severity INFO

ZONE-1041

Message
```
<timestamp>, [ZONE-1041], <sequence-number>,, WARNING, <switch-name>, Unstable
link detected during merge at port (<Port number>).
```

Probable Cause Indicates a possible unstable link or a faulty cable.

Recommended Action Verify that the small form-factor pluggable (SFP) and cable at the specified port are not faulty. Replace the SFP and cable if necessary.

Severity WARNING

ZONE-1042

Message
```
<timestamp>, [ZONE-1042], <sequence-number>,, INFO, <switch-name>, The effective
configuration has been disabled. <AD Id>.
```

Probable Cause Indicates that the effective zone configuration has been disabled.

Recommended Action Verify that the zone configuration change was done on purpose. If the effective zone configuration is not needed, no action is required.

Severity INFO

ZONE-1043

Message
```
<timestamp>, [ZONE-1043], <sequence-number>,, INFO, <switch-name>, The Default
Zone access mode is set to No Access.
```

Probable Cause Indicates that the Default Zone access mode is set to No Access.

Recommended Action Verify that this Default Zone access mode change was done on purpose.

Severity INFO

ZONE-1044

Message
```
<timestamp>, [ZONE-1044], <sequence-number>,, INFO, <switch-name>, The Default
Zone access mode is set to All Access.
```

Probable Cause Indicates that the Default Zone access mode is set to All Access.

Recommended Action Verify that this Default Zone access mode change was done on purpose.

Severity INFO

ZONE-1045

Message

```
<timestamp>, [ZONE-1045], <sequence-number>,, INFO, <switch-name>, The Default
Zone access mode is already set to No Access.
```

Probable Cause Indicates that the Default Zone access mode is already set to No Access.

Recommended Action No action is required.

Severity INFO

ZONE-1046

Message

```
<timestamp>, [ZONE-1046], <sequence-number>,, INFO, <switch-name>, The Default
Zone access mode is already set to All Access.
```

Probable Cause Indicates that the Default Zone access mode was already set to All Access.

Recommended Action No action is required.

Severity INFO

ZONE-1047

Message

```
<timestamp>, [ZONE-1047], <sequence-number>,, INFO, <switch-name>, Switch rBridge
(<rBridger>) does not support defined database.
```

Probable Cause Indicates that a remote Brocade switch is running a lower version of the Network OS that does not support the defined database.

Recommended Action It is recommended to upgrade all switches to the same release version.

Severity INFO

Section

II

Audit Log Messages

This section provides the Audit messages, including:

Chapter

AUDIT DCM System Messages 42

DCM-1006

Message

```
<sequence-number> AUDIT, <timestamp>, [DCM-1006], INFO, DCMCFG, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Event: <Event
Name>, Status: <Command status>, User command: <ConfD hpath string>.
```

Probable Cause

Indicates that the user command has been executed successfully.

Recommended Action

No action is required.

Severity

INFO

DCM-2001

Message

```
<sequence-number> AUDIT, <timestamp>, [DCM-2001], INFO, DCMCFG, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Event: <Event
Name>, Status: success, Info: Successful login attempt through <connection method
and IP Address>.
```

Probable Cause

Indicates a successful login. An IP address is displayed when the login occurs over a remote connection.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

DCM-2002

Message

```
<sequence-number> AUDIT, <timestamp>, [DCM-2002], INFO, DCMCFG, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Event: <Event
Name>, Status: success, Info: Successful logout by user [<User>].
```

Probable Cause

Indicates that the specified user has successfully logged out.

Recommended Action

No action is required.

Severity

INFO

Chapter

AUDIT RAS System Messages 43

RAS-2001

Message

```
<sequence-number> AUDIT, <timestamp>, [RAS-2001], INFO, SYSTEM, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Audit message log
is enabled.
```

Probable Cause
Indicates that a user has enabled the audit message log.

Recommended Action
No action is required.

Severity
INFO

RAS-2002

Message

```
<sequence-number> AUDIT, <timestamp>, [RAS-2002], INFO, SYSTEM, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Audit message log
is disabled.
```

Probable Cause
Indicates that a user has disabled the audit message log.

Recommended Action
No action is required.

Severity
INFO

RAS-2003

Message

```
<sequence-number> AUDIT, <timestamp>, [RAS-2003], INFO, SYSTEM, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Audit message
class configuration has been changed to <New audit class configuration>.
```

Probable Cause
Indicates that a user has changed the configured classes of the audit feature.

Recommended Action
No action is required.

Severity
INFO

Chapter

AUDIT SEC System Messages

44

SEC-3014

Message

```
<sequence-number> AUDIT, <timestamp>, [SEC-3014], INFO, SECURITY, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Event: <Event
Name>, Status: success, Info: <Event related info> <Event option> server <Server
Name> for AAA services.
```

Probable Cause

Indicates a user has changed the AAA server (RADIUS/TACACS+) configuration.

Recommended Action

Verify the RADIUS/TACACS+ configuration was changed intentionally. If the RADIUS/TACACS+ configuration was changed intentionally, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-3015

Message

```
<sequence-number> AUDIT, <timestamp>, [SEC-3015], INFO, SECURITY, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Event: <Event
Name>, Status: success, Info: Moved <Event option> server <Server name> to
position <New position>.
```

Probable Cause

Indicates a user has changed the position of the remote authentication dial-in user service (RADIUS)/LDAP server.

Recommended Action

Verify the RADIUS server position was intentionally changed. If the RADIUS server position was intentionally changed, no action is required. If the RADIUS server position was not intentionally changed, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-3016

Message

```
<sequence-number> AUDIT, <timestamp>, [SEC-3016], INFO, SECURITY, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Event: <Event
Name>, Status: success, Info: Attribute [<Attribute Name>] of <Attribute related
info> server <server ID> changed <Attribute related info, if any>.
```

Probable Cause

Indicates a user has changed the specified attribute of the remote AAA (RADIUS/TACACS+) server.

Recommended Action Verify the RADIUS attribute was intentionally changed. If the RADIUS attribute was intentionally changed, no action is required. If the RADIUS attribute was not intentionally changed, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3017

Message
```
<sequence-number> AUDIT, <timestamp>, [SEC-3017], INFO, SECURITY, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Event: <Event
Name>, Status: success, Info: <Event Related Info>.
```

Probable Cause Indicates a user has changed the remote authentication dial-in user service (RADIUS)/LDAP configuration.

Recommended Action Verify the RADIUS configuration was intentionally changed. If the RADIUS configuration was intentionally changed, no action is required. If the RADIUS configuration was not intentionally changed, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3018

Message
```
<sequence-number> AUDIT, <timestamp>, [SEC-3018], INFO, SECURITY, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Event: <Event
Name>, Status: success, Info: Parameter [<Parameter Name>] changed from [<Old
Value>] to [<New Value>].
```

Probable Cause Indicates the specified password attribute is changed.

Recommended Action Verify the password attribute was intentionally changed. If the password attribute was intentionally changed, no action is required. If the password attribute was not intentionally changed, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3019

Message
```
<sequence-number> AUDIT, <timestamp>, [SEC-3019], INFO, SECURITY, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Event: <Event
Name>, Status: success, Info: Password attributes set to default values.
```

Probable Cause Indicates the password attributes are set to default values.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3020

Message

```
<sequence-number> AUDIT, <timestamp>, [SEC-3020], INFO, SECURITY, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Event: <Event
Name>, Status: success, Info: Successful login attempt via <connection method and
IP Address>.
```

Probable Cause

Indicates a successful login occurred. An IP address is displayed when the login occurs over a remote connection.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-3021

Message

```
<sequence-number> AUDIT, <timestamp>, [SEC-3021], INFO, SECURITY, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Event: <Event
Name>, Status: failed, Info: Failed login attempt through <connection method and
IP Address>.
```

Probable Cause

Indicates a failed login attempt occurred.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-3022

Message

```
<sequence-number> AUDIT, <timestamp>, [SEC-3022], INFO, SECURITY, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Event: <Event
Name>, Status: success, Info: Successful logout by user [<User>].
```

Probable Cause

Indicates the specified user has successfully logged out.

Recommended Action

No action is required.

Severity

INFO

SEC-3023

Message

```
<sequence-number> AUDIT, <timestamp>, [SEC-3023], INFO, SECURITY, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Event: <Event
Name>, Status: failed, Info: Account [<User>] locked, failed password attempts
exceeded.
```

Probable Cause

Indicates that failed password attempts exceeded the allowed limit. The account has been locked as a result.

Recommended Action

The administrator may manually unlock the account.

Severity

INFO

SEC-3024

Message

```
<sequence-number> AUDIT, <timestamp>, [SEC-3024], INFO, SECURITY, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Event: <Event
Name>, Status: success, Info: User account [<User Name>], password changed.
```

Probable Cause

Indicates the user's password was changed.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-3025

Message

```
<sequence-number> AUDIT, <timestamp>, [SEC-3025], INFO, SECURITY, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, 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>].
```

Probable Cause

Indicates a new user account was created.

Recommended Action

Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity

INFO

SEC-3026

Message

```
<sequence-number> AUDIT, <timestamp>, [SEC-3026], INFO, SECURITY, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Event: <Event
Name>, Status: success, Info: User account [<User Name>], role changed from [<Old
Role Type>] to [<New Role Type>].
```

Probable Cause Indicates a user account role was changed.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3027

Message

```
<sequence-number> AUDIT, <timestamp>, [SEC-3027], INFO, SECURITY, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Event: <Event
Name>, Status: success, Info: User account [<User Name>] [<Changed Attributes>].
```

Probable Cause Indicates user account properties were changed.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3028

Message

```
<sequence-number> AUDIT, <timestamp>, [SEC-3028], INFO, SECURITY, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Event: <Event
Name>, Status: success, Info: User account [<User Name>] deleted.
```

Probable Cause Indicates the specified user account was deleted.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3030

Message

```
<sequence-number> AUDIT, <timestamp>, [SEC-3031], INFO, SECURITY, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Event: <Event
Name>, Status: success, Info:<Event Specific Info>.
```

Probable Cause Indicates the specified **certutil import ldapca** operation was performed.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3034

Message

```
<sequence-number> AUDIT, <timestamp>, [SEC-3034], INFO, SECURITY, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Event: AAA
Authentication Login Mode Configuration, Status: success, Info: Authentication
configuration changed from <Previous Mode> to <Current Mode>.
```

Probable Cause Indicates an authentication configuration has changed.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3035

Message

```
<sequence-number> AUDIT, <timestamp>, [SEC-3035], INFO, SECURITY, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Event: ipfilter,
Status: success, Info: <IP Filter Policy> ipfilter policy(ies) saved.
```

Probable Cause Indicates the specified IP filter policies have been saved.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3036

Message

```
<sequence-number> AUDIT, <timestamp>, [SEC-3036], INFO, SECURITY, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Event: ipfilter,
Status: failed, Info: Failed to save changes for <IP Filter Policy> ipfilter
policy(s).
```

Probable Cause Indicates the specified IP filter policies have not been saved.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3037

Message
```
<sequence-number> AUDIT, <timestamp>, [SEC-3037], INFO, SECURITY, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Event: ipfilter,
Status: success, Info: <IP Filter Policy> ipfilter policy activated.
```

Probable Cause Indicates that the specified IP filter policy has been activated.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3038

Message
```
<sequence-number> AUDIT, <timestamp>, [SEC-3038], INFO, SECURITY, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Event: ipfilter,
Status: failed, Info: Failed to activate <IP Filter Policy> ipfilter policy.
```

Probable Cause Indicates the specified IP filter policy failed to activate.

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.

Severity INFO

SEC-3039

Message
```
<sequence-number> AUDIT, <timestamp>, [SEC-3039], INFO, SECURITY, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Event: Securty
Violation, Status: failed, Info: Unauthorized host with IP address <IP address of
the violating host> tries to establish connection using <Protocol Connection
Type>.
```

Probable Cause Indicates a security violation was reported. The IP address of the unauthorized host is displayed in the message.

Recommended Action Check for unauthorized access to the switch through the specified protocol connection.

Severity INFO

SEC-3044

Message
```
<sequence-number> AUDIT, <timestamp>, [SEC-3044], INFO, SECURITY, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, The FIPS mode has
been changed to <Fips Mode>.
```

Probable Cause Indicates there was a change in the FIPS mode.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3045

Message
```
<sequence-number> AUDIT, <timestamp>, [SEC-3045], INFO, SECURITY, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Zeroization has
been executed on the system.
```

Probable Cause Indicates the system has been zeroized.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3046

Message
```
<sequence-number> AUDIT, <timestamp>, [SEC-3046], INFO, SECURITY, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, The FIPS Self
Tests mode has been set to <Self Test Mode>.
```

Probable Cause Indicates there was a change in the 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.

Severity INFO

SEC-3048

Message
```
<sequence-number> AUDIT, <timestamp>, [SEC-3048], INFO, SECURITY, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, FIPS mode has
been enabled in the system using force option.
```

Probable Cause Indicates the system has been forced to FIPS mode.

Recommended Action
Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy. Look for the status of the pre-requisites which did not conform to FIPS mode.

Severity
INFO

SEC-3049

Message
```
<sequence-number> AUDIT, <timestamp>, [SEC-3049], INFO, SECURITY, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Status of
bootprom access is changed using prom-access disable CLI: <Access Status>.
```

Probable Cause
Indicates the status of Boot PROM access has changed using the **prom-access disable** command. By default, the Boot PROM is accessible.

Recommended Action
No action is required.

Severity
INFO

SEC-3051

Message
```
<sequence-number> AUDIT, <timestamp>, [SEC-3051], INFO, SECURITY, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, The license key
<key> is <Action>.
```

Probable Cause
Indicates that a license key is added or removed.

Recommended Action
No action is required.

Severity
INFO

SEC-3061

Message
```
<sequence-number> AUDIT, <timestamp>, [SEC-3061], INFO, SECURITY, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Role ‘<Role
Name>’ is created.
```

Probable Cause
Indicates a role is created.

Recommended Action
No action is required.

Severity
INFO

SEC-3062

Message

```
<sequence-number> AUDIT, <timestamp>, [SEC-3062], INFO, SECURITY, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Role ‘<Role
Name>’ is deleted.
```

Probable Cause Indicates a role is deleted.

Recommended Action No action is required.

Severity INFO

SEC-3501

Message

```
<sequence-number> AUDIT, <timestamp>, [SEC-3501], INFO, SECURITY, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Role '<Role
Name>' is changed.
```

Probable Cause Indicates the attributes of a role are changed.

Recommended Action No action is required.

Severity INFO

Chapter

AUDIT SNMP System Messages 45

SNMP-1004

Message
```
<sequence-number> AUDIT, <timestamp>, [SNMP-1004], ERROR, SYSTEM, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Incorrect SNMP
configuration.
```

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 back to the default.

Severity ERROR

Chapter

AUDIT SULB System Messages 46

SULB-1001

Message
```
<sequence-number> AUDIT, <timestamp>, [SULB-1001], WARNING, FIRMWARE, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, firmware download
command has started.
```

Probable Cause
Indicates that the **firmware download** command has been executed. This process takes about 17 minutes to complete. The process is set to time out after 30 minutes.

Recommended Action
Do not fail over or power down the system during the firmware upgrade. Allow the **firmware download** command to continue without disruption. No action is required.

Execute the **show firmwaredownloadstatus** command for more information.

Severity
WARNING

SULB-1002

Message
```
<sequence-number> AUDIT, <timestamp>, [SULB-1002], INFO, FIRMWARE, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, firmware download
command has completed successfully.
```

Probable Cause
Indicates that the **firmware download** command has completed successfully and the switch firmware has been updated.

Recommended Action
No action is required. The **firmware download** command has completed as expected.

Execute the **show firmwaredownloadstatus** command for more information. Execute the **show version** command to verify the firmware version.

Severity
INFO

SULB-1003

Message
```
<sequence-number> AUDIT, <timestamp>, [SULB-1003], INFO, FIRMWARE, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, firmware commit
has started.
```

Probable Cause
Indicates that the **firmware commit** command has been executed.

Recommended Action
No action is required. Execute the **show firmwaredownloadstatus** command for more information.

Severity
INFO

SULB-1004

Message

```
<sequence-number> AUDIT, <timestamp>, [SULB-1004], INFO, FIRMWARE, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, firmware commit
has completed.
```

Probable Cause Indicates that the **firmware commit** command has been completed.

Recommended Action No action is required. Execute the **show firmwaredownloadstatus** command for more information.

Severity INFO

SULB-1009

Message

```
<sequence-number> AUDIT, <timestamp>, [SULB-1009], INFO, FIRMWARE, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, firmware download
command failed. status: 0x<status code>, error: 0x<error code>.
```

Probable Cause Indicates that the **firmware download** command failed. The additional *status code* and *error code* provide debugging information.

Table 9 lists **firmware download** status messages and status codes. Some of them will not be displayed in this RASLOG message and are listed for completeness.

TABLE 9 Status messages and status codes

Status message	Status code
"**firmware download** sanity check failed."	0x30
"Sanity check failed because system is non-redundant."	0x31
"Sanity check failed because **firmware download** is already in progress."	0x32
"Sanity check failed because Network OS is disabled on the Active CP."	0x33
"Sanity check failed because the high availability management daemon (HAMD) is disabled on Active CP."	0x34
"Sanity check failed because **firmware download** is already in progress."	0x35
"Sanity check failed because Network OS is disabled on Standby CP."	0x36
"Sanity check failed because HAMD is disabled on Standby CP."	0x37
"**firmware download** failed on the Standby CP."	0x40
"**firmware download** failed on the Standby CP."	0x41
"**firmware download** failed on the Standby CP."	0x42
"**firmware commit** failed on the Standby CP."	0x43
"**firmware download** failed."	0x44
"**firmware download** failed due to inter-process communication (IPC) error."	0x50
"Unable to check the firmware version on Standby CP due to IPC error."	0x51
"**firmware download** failed due to IPC error."	0x52
"**firmware download** failed due to IPC error."	0x53

TABLE 9 Status messages and status codes (Continued)

Status message	Status code
"Standby CP failed to reboot due to IPC error."	0x54
“**firmware commit** operation failed due to IPC error.”	0x55
"Unable to check the firmware version on Standby CP due to IPC error."	0x56
“Unable to restore the original firmware due to Standby CP timeout.”	0x57
"Standby CP failed to reboot and was not responding."	0x58
"Unable to check the firmware version on Standby CP due to IPC error."	0x59
“Sanity check failed because **firmware download** is already in progress.”	0x60
“Sanity check failed because **firmware download** is already in progress.”	0x61
NOT USED	0x62
"System error."	0x63
"Active CP forced failover succeeded. Now this CP becomes Active."	0x64
"Standby CP booted up."	0x65
"Active and Standby CP failed to gain HA synchronization within 10 minutes."	0x66
"Standby rebooted successfully."	0x67
"Standby failed to reboot."	0x68
“**firmware commit** has started to restore the secondary partition.”	0x69
"Local CP is restoring its secondary partition."	0x6a
“Unable to restore the secondary partition. Execute the **show firmwaredownloadstatus** command to display the firmware download event log. Execute the **show version** command to display the firmware version.”	0x6b
“**firmware download** has started on Standby CP. It might take up to 10 minutes.”	0x6c
“**firmware download** has completed successfully on Standby CP.”	0x6d
"Standby CP reboots."	0x6e
"Standby CP failed to boot up."	0x6f
"Standby CP booted up with new firmware."	0x70
"Standby CP failed to boot up with new firmware."	0x71
“**firmware download** has completed successfully on Standby CP.”	0x72
“**firmware download** has started on Standby CP. It might take up to 10 minutes.”	0x73
“**firmware download** has completed successfully on Standby CP.”	0x74
"Standby CP reboots."	0x75
"Standby CP failed to reboot."	0x76
“**firmware commit** has started on Standby CP.”	0x77
“**firmware commit** has completed successfully on Standby CP.”	0x78
"Standby CP booted up with new firmware."	0x79
"Standby CP failed to boot up with new firmware."	0x7a
“**firmware commit** has started on both Active and Standby Caps.”	0x7b

TABLE 9 Status messages and status codes (Continued)

Status message	Status code
“**firmware commit** has completed successfully on both Caps.”	0x7c
“**firmware commit** failed on Active CP.”	0x7d
"The original firmware has been restored successfully on Standby CP."	0x7e
"Unable to restore the original firmware on Standby CP."	0x7f
"Standby CP reboots."	0x80
"Standby CP failed to reboot."	0x81
"Standby CP booted up with new firmware."	0x82
"Standby CP failed to boot up with new firmware."	0x83
“There was an unexpected reboot during **firmware download**. The command is aborted.”	0x84
"Standby CP was not responding. The command is aborted."	0x85
“**firmware commit** has started on both CPs. Execute the **show firmwaredownloadstatus** command to display the firmware download event log. Execute the **show version** command to display the firmware version.”	0x86
“**firmware commit** has started on the local CP. Execute the **show firmwaredownloadstatus** command to display the firmware download event log. Execute the **show version** command to display the firmware version.”	0x87
“**firmware commit** has started on the remote CP. Execute the **show firmwaredownloadstatus** command to display the firmware download event log. Execute the **show version** command to display the firmware version.”	0x88
“Execute the **show firmwaredownloadstatus** command to display the firmware download event log. Execute the **show version** command to display the firmware version.”	0x89
“**firmware download** command has completed successfully.”	0x8a
"The original firmware has been restored successfully."	0x8b
"Remote CP is restoring its secondary partition."	0x8c
"Local CP is restoring its secondary partition."	0x8d
"Remote CP is restoring its secondary partition."	0x8e
“**firmware download** has started.”	0x8f
“**firmware commit** has started.”	0x90
“**firmware download** has completed successfully.”	0x91
“**firmware commit** has completed successfully.”	0x92
“**firmware commit** has started to restore the secondary partition.”	0x93
“**firmware commit** failed.”	0x94
"The secondary partition has been restored successfully."	0x95
"Firmware is being downloaded to the blade. This step may take up to 10 minutes."	0xa0
“**firmware download** timed out.”	0xa1
“Reboot occurred during **firmware download. firmware commit** will be started to recover the blade.”	0xa2
“Blade rebooted during **firmware commit**. The operation will be restarted.”	0xa3
"Firmware has been downloaded successfully. Blade is rebooting with the new firmware."	0xa4

TABLE 9 Status messages and status codes (Continued)

Status message	Status code
"Blade has rebooted successfully."	0xa5
“New firmware failed to boot up. Retry the **firmware download**.”	0xa6
“**firmware commit** has started on the blade. This may take up to 10 minutes.”	0xa7
“The **firmware restore** command is executed. System will reboot and a **firmware commit** operation will start upon bootup.”	0xa8
"Switch is relocating the AP image."	0xa9
"The AP image is relocated successfully."	0xaa
"Switch reboots during relocating the AP image. The operation will be restarted."	0xab
“Blade failed to reboot with the original image. The **firmware restore** command failed.”	0xac

Table 10 lists additional **firmware download** error messages and error codes. They provide more details on why **firmware download** failed.

TABLE 10 Error messages and error codes

Error message	Error code
"Image is up-to-date. No need to download the same version of firmware."	0xF
“Upgrade is inconsistent.”	0x10
“OSRootPartition is inconsistent.”	0x11
“Unable to access the required package list file. Check whether the switch is supported by the requested firmware. Also check **firmware download** help page for other possible failure reasons.”	0x12
"The RPM package database is inconsistent. Contact your service provider for recovery."	0x13
"Out of memory."	0x14
“Failed to download Red Hat package manager (RPM) package.”	0x15
"Unable to create firmware version file."	0x16
"Unexpected system error."	0x17
“Error in getting lock device for **firmware download**.”	0x18
“Error in releasing lock device for **firmware download**.”	0x19
“**firmware commit** failed.”	0x1a
"Firmware directory structure is not compatible. Check whether the firmware is supported on this platform."	0x1b
"Failed to load the Linux kernel image."	0x1c
“OSLo ad er is inconsistent.”	0x1d
“New image has not been committed. Execute the **firmware commit** or **firmware restore** command and then execute the **firmware download** command.”	0x1e
“**firmware restore** failed.”	0x1f
"Both images are mounted to the same device."	0x20
“Unable to unionist old packages.”	0x21
“**firmware download** is already in progress.”	0x22

TABLE 10 Error messages and error codes (Continued)

Error message	Error code
"**firmware download** timed out."	0x23
"Out of disk space."	0x24
"Primary filesystem is inconsistent. Execute the **firmware restore** command to restore the original firmware, or contact your service provider for recovery."	0x25
"The post-install script failed."	0x26
"Unexpected reboot."	0x27
"Primary kernel partition is inconsistent. Contact your service provider for recovery."	0x28
"The pre-install script failed."	0x29
"The platform option is not supported."	0x2a
"Failed to install RPM package."	0x2b

The following section explains the causes of some common error messages:

0x15 - Failed to download Red Hat package manager (RPM) package. If this error occurs immediately after **firmware download** is started, the firmware on the switch may be two releases older than the requested firmware. The **firmware download** command supports firmware upgrades within two feature releases (a feature release is indicated by a major number and a minor number, for example, X.Y). In this case, you will need to upgrade to an intermediate version before downloading the desired version. If this error occurs in the middle of **firmware download**, the firmware in the file server may be corrupted or there may be a temporary network issue. In this case, retry the **firmware download** command. If the problem persists, contact your system administrator.

0x18 - Error in getting lock device for **firmware download.** This error can be due to another **firmware download** already in progress. Execute the **show firmwaredownloadstatus** command to verify that this is the case. Wait for the current session to finish before proceeding.

0x23 - **firmware download** timed out. This error may occur because the **firmware download** has not completed within the predefined timeout period. It is most often caused by network issues. If the problem persists, contact your system administrator.

0x24 - Out of disk space. This error may occur because some core dump files have not been removed from the filesystem and are using up disk space. Remove these core dump files by using the **copy support** command before proceeding.

0x29 - The pre-install script failed. This error may be caused by an unsupported blade type. Remove or power off the unsupported blades before proceeding.

Recommended Action

Execute the **show firmwaredownloadstatus** command for more information.

In a director-class switch, when **firmware download** fails, the command will synchronize the firmware on the two partitions of each CP by starting a firmware commit operation. Wait untill this operation completes (about 10 minutes) before attempting another firmware download.

In a director-class switch, when **firmware download** fails, the two CPs may end up with different versions of firmware and they may not gain high-availability (HA) sync. In that case, upgrade the firmware on the standby CP to the same version as the active CP and then retry the **firmware download** to download the desired version of firmware onto the CPs.

Severity

INFO

SULB-1010

Message

```
<sequence-number> AUDIT, <timestamp>, [SULB-1010], INFO, FIRMWARE, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, firmware commit
failed (status=0x <error code>).
```

Probable Cause

Indicates that the **firmware commit** command has failed. The error code provides debugging information. Refer to the Status messages and status codes table in the SULB-1009 message for more information.

Recommended Action

If the failure is caused by an inconsistent filesystem, contact your switch service provider.

Severity

INFO

SULB-1037

Message

```
<sequence-number> AUDIT, <timestamp>, [SULB-1037], ERROR, FIRMWARE, <User
ID>/<Role>/<IP address>/<Interface>/<app name>,, <switch-name>, Hot Code Load
(HCL) failed.
```

Probable Cause

Indicates that the Hot Code Load (HCL) has failed. Many reasons, such as domain not confirmed, can cause this failure.

Recommended Action

Execute the **reboot** command to reboot the switch manually. However, it will disrupt the FC traffic.

Severity

ERROR