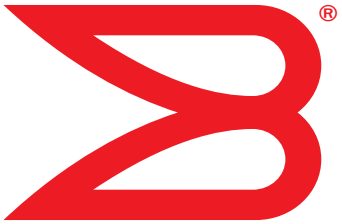
53-1002082-01
07 December 2010



Network OS

Message Reference

Supporting Network OS v2.0.0

BROCADE

Brocade Communications Systems, Incorporated

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

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

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

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

Document History

Title	Publication number	Summary of changes	Date
Network OS Message Reference	*53-1002082-01*	New document	December 2010

Contents

About This Document

In this chapter

How this document is organized

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

The document contains the following components:

- Chapter 1, “Introduction To System Messages” provides basic information on system messages.
- Chapters 2 through 31 provides 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 5.3.0, documenting all possible configurations and scenarios is beyond the scope of this document.

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

- Brocade VDX 6720-24
- Brocade VDX 6720-60

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. Otherwise, this manual specifically notes those cases in which a command is case sensitive.

Command syntax conventions

Command syntax in this manual follows these conventions:

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

Notes, cautions, and warnings

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

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

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

CAUTION

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

DANGER

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

Key terms

For definitions specific to Brocade and Fibre Channel, see the *Brocade Glossary*.

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, Windows NT, Internet Explorer
Red Hat, Inc.	Red Hat, Red Hat Network, Maximum RPM, Linux Undercover

Additional information

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

Brocade resources

To get up-to-the-minute information, go to http://my.brocade.com 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

Release notes are available on the MyBrocade website and are also bundled with the Network OS firmware.

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 ftp** 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 is located as follows:

- Brocade 300, 4100, 4900, 5100, 5300, 7500, 7800, 8000, and Brocade Encryption Switch—On the switch ID pull-out tab located inside the chassis on the port side on the left
- Brocade 5000—On the switch ID pull-out tab located on the bottom of the port side of the switch
- Brocade 7600—On the bottom of the chassis
- Brocade 48000—Inside the chassis next to the power supply bays
- Brocade DCX—On the bottom right on the port side of the chassis
- Brocade DCX-4S—On the bottom right on the port side of the chassis, directly above the cable management comb.
- World Wide Name (WWN)
- Use the **show license id** command to display the WWN of the chassis.
- If you cannot use the **show license id** command because the switch is inoperable, you can get the WWN from the same place as the serial number, except for the Brocade DCX. For the Brocade DCX, access the numbers on the WWN cards by removing the Brocade logo plate at the top of the nonport side of the chassis.

Document feedback

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

documentation@brocade.com

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

Chapter

1

Introduction To System Messages

In this chapter

Overview of System Messages

This guide supports Brocade Network OS v2.0.0 and documents system messages that can help you diagnose and fix problems with a switch or network. The messages are organized first by event type, reliability, availability, and serviceability log (RASLog) or AUDIT, and then 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, or configuration changes. Network OS supports a different methodology for storing and accessing each type of message.

System Error Message Logging

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

- All RASLog error messages are saved to nonvolatile storage by default.
- The system error message log can save a maximum of 1024 messages in random access memory (RAM).
- The system message log is implemented as a circular buffer. When more than maximum entries are added to the log file, old entries are overwritten by new entries.
- Messages are numbered sequentially from 1 to 2,147,483,647 (0x7fffffff). The sequence number will continue to increase beyond the storage limit of 1024 messages. The sequence number can be reset to 1 using the **errClear** command. The sequence number is persistent across power cycles and switch reboots.

- By default, the **show logging raslog** command display all of the system error messages.
- Trace dump, first-time failure detection capture (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 particularly important for dual-domain switches because the **syslogd** facility saves messages from two logical switches as a single file and in sequential order. See "System Logging Daemon (syslogd)" on page 3 for more information.

Event Auditing

Event auditing is designed to support post-event audits and problem determination based on high-frequency events of certain types such as security violations, zoning configuration changes, firmware downloads, and certain types of network events. In Network OS v2.0.0 and later, messages flagged as AUDIT are no longer saved in the switch's error logs. Instead, the switch can be configured to stream Audit messages to the switch console and to forward the messages to specified syslog servers. There is no limit to the number of audit events.

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 five event classes described in the following table can be audited.

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

Network OS v2.0.0 generates component-specific Audit messages see "Audit Log Messages".

Event auditing is a configurable feature, set to off by default. You must enable event auditing by configuring the syslog daemon to send the events to a configured remote host using the **syslogIpAdd** command. You can set up filters to screen out particular classes of events using the **auditCfg** command (the classes include zone, security, configuration, firmware, and network). 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 might occur in the network. For details on how to configure event auditing, see "Viewing and Configuring System Message Logs" on page 4.

System Logging Daemon (syslogd)

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. Configuring for **syslogd** involves configuring the host, enabling **syslogd** on the Brocade model, and, optionally, setting the facility level.

For the *Brocade DCX, 24000 and 48000*, each CP has a unique error log, depending on which CP was active when that message was reported. To fully understand message logging on the *Brocade 24000 and 48000* you should enable the system logging daemon, because the logs on the host computer are maintained in a single merged file for both CPs and are in sequential order. Otherwise, you must examine the error logs in both CPs, particularly for events such as **firmwareDownload** or **haFailover**, for which the active CP changes.

For the *Brocade DCX, 24000 and 48000*, any security violations that occur through Telnet, HTTP, or serial connections are not propagated between CPs. Security violations on the active CP are not propagated to the standby CP counters in the event of a failover, nor do security violations on the standby CP get propagated to the active CP counters.

For information on configuring **syslogd** functionality, refer to the *Fabric OS Administrator's Guide*.

System Console

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

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.

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

Port Logs

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

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

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

Refer to the *Fabric OS Administrator's Guide* for information on interpreting results of the **portLogDump** command.

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

Viewing and Configuring System Message Logs

This section provides information on viewing and configuring system message logs, including.

- Viewing System Messages from Web Tools
- Dumping System Messages
- Viewing System Messages One Message at a Time
- Clearing the System Message Log
- Configuring Event Auditing

The procedures are valid for the Brocade VDX 6720-24 and 6720-60.

For detailed information on required access levels and commands, refer to the *Fabric OS Command Reference*.

Viewing System Messages from Web Tools

To view the system message log for a switch from Web Tools:

1. Launch Web Tools.
2. Select the desired switch from the Fabric Tree. The Switch View displays.
3. Click the **Switch Events** button. A Switch Events Report displays.
4. View the switch events and messages.

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

Dumping System Messages

To display the system message log, with no page breaks:

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

```
switch:admin> show logging raslog
Version: 5.0.1
2004/07/28-17:04:59, [FSSM-1002], 1,, INFO, switch, HA State is in sync

2004/07/28-17:04:59, [FSSM-1003], 2,, WARNING, switch, HA State out of sync

2004/07/28-17:04:51, [EM-1055], 3,, WARNING, switch, Media 27: Port media
incompatible. Reason: Configured port speed.

2004/07/28-17:04:54, [FABR-1001], 4,, WARNING, switch, port 4, ELP rejected by
the other switch
```

```
2004/07/28-17:05:06, [FW-1050], 5,, WARNING, switch, Sfp Supply Voltage 0, is
below low boundary(High=3600, Low=3150). Current value is 0 mV.

switch:admin>
```

Viewing System Messages One Message at a Time

To display the system message log one message at a time:

1. Log in to the switch as admin.
2. At the command line, enter the **show logging raslog** command:

```
switch:admin> show logging raslog
Version: 5.0.1
2004/07/28-17:04:59, [FSSM-1002], 1,, INFO, switch, HA State is in sync

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

2004/07/28-17:04:59, [FSSM-1003], 2,, WARNING, switch, HA State out of sync

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

2004/07/28-17:04:51, [EM-1055], 3,, WARNING, switch, Media 27: Port media
incompatible
e. Reason: Configured port speed.

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

Clearing the System Message Log

To clear the system message log for a particular switch instance:

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

NOTE

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

Configuring Event Auditing

To configure event auditing:

1. Configure the event classes you wish to audit:

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

2. Verify the configuration:

```
switch:admin> auditcfg --show
Audit filter is enabled.
1-ZONE
2-SECURITY
```

```
3-CONFIGURATION
4-FIRMWARE
5-FABRIC
```

3. Enable the audit feature:

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

4. Configure up to six syslog servers to receive the audit events that will be generated through syslog (procedure will vary depending on server type).
5. Configure syslog on the switch to point to the configured servers' IP addresses.

```
switch:admin> syslogdipadd 10.128.128.160
```

6. Verify the switch's syslog configuration:

```
switch:admin> syslogdipshow
syslog.1        192.168.163.234
syslog.2        10.128.128.160
```

Reading a RAS System Message

This section provides information about reading 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 a sample message from the error log:

```
2009/02/10-14:18:04, [SS-1000], 88, SLOT 6 | FFDC | CHASSIS, INFO, ESNSVT_DCX,
copy support ftp has uploaded support information to the host with IP address
168.159.16.128

2009/02/10-14:13:34, [SS-1001], 87, SLOT 6/1 | FFDC | CHASSIS, WARNING,
ESNSVT_DCX, copy support ftp's upload operation to host IP address aborted

2009/02/10-15:44:51, [SEC-1203], 89, SLOT 6 | FFDC | FID 128, INFO, ESNSVT_DCX,
Login information: Login successful via TELNET/SSH/RSH. IP Addr:168.159.16.128
```

The fields in the error message are described in Table 1.:

TABLE 1 System Message Field Description

Example	Variable Name	Description
2004/07/22-10:12:33	Date and Time Stamp	The system time (UTC) when the message was generated on the switch. The RASLog subsystem supports an internationalized timestamp format base on the "LOCAL" setting.
[EM-1031]	Message Module and Message Number	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.

TABLE 1 System Message Field Description (Continued)

Example	Variable Name	Description
4	Sequence Number	The error message position in the log. When a new message is added to the log, this number is incremented by 1. When this message reaches the last position in the error log and becomes the oldest message in the log, it is deleted when a new message is added. The message sequence number starts at 1 after a **firmwareDownload** and will increase up to a value of 2,147,483,647 (0x7fffffff). The sequence number will continue to increase beyond the storage limit of 1024 messages. The sequence number can be reset to 1 using the **errClear** command. The sequence number is persistent across power cycles and switch reboots.
<NULL> (blank)	Audit and/or FFDC/SLOT/CHASSIS/FID Flags	For most messages, this field contains a space character (null value) indicating that the message is neither an AUDIT or FFDC message. Messages may contain the following values: AUDIT indicates that this message is for a security issue. FFDC indicates that additional first failure data capture information has also been generated for this event. FID is the Network ID that can range from 0 to 128. FID 128 means the message was generated by the default switch instance. CHASSIS is the message that was generated by the chassis instance. SLOT number indicates the message was generated from slot # blade main CPU. SLOT #/1 indicates the message was generated from slot # blade Co-CPU. AUDIT:FFDC indicates that the message is for a security issue and additional FFDC information has been generated.
ERROR	Severity Level	The severity of the error: 1 = Critical 2 = Error 3 = Warning 4 = Info
switchname	Switch name or chassis name, depending on the action; for example, high-availability (HA) messages typically show the chassis name, and login failures show the logical switch name.	The defined switch name or the chassis name of the switch. This value is truncated if it exceeds 16 characters in length. Run either the **chassisName** command to name the chassis or the **switchName** command to rename the logical switch.
Slot 7 ejector not closed	Error Description	A text string explaining the error encountered and providing 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.

Audit event message format:

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

The following is a sample audit event message:

```
AUDIT, 2005/12/10-09:54:03, [SEC-1000], WARNING, SECURITY,
JohnSmith/root/192.168.132.10/Telnet/CLI, Domain A/JohnsSwitch, , Incorrect
password during login attempt.
```

The fields in the error message are described in Table 2.

TABLE 2 Audit Message Field Description

Example	Variable Name	Description
AUDIT	Audit flag	Identifies the message as an Audit message.
2005/12/10-09:54:03	Date and Time Stamp	The system time (UTC) when the message was generated on the switch. The RASLog subsystem will support an internationalized timestamp format base on the “LOCAL” setting.
[SEC-1000]	Message Module and Message Number	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.
WARNING	Severity Level	The severity of the error: 1 = Critical 2 = Error 3 = Warning 4 = Info
SECURITY	Event Class	The event class: Zone Security Configuration Firmware Fabric
JohnSmith	User ID	The user ID.
root	Role	The role of the user ID.
192.168.132.10	IP Address	The IP address.
Telnet	Interface	The interface being used.
CLI	Application Name	The application name being used on the interface.
Domain A	Admin Domain	The Admin Domain, if there is one.
switchname	Switch name or chassis name, depending on the action; for example, HA messages typically show the chassis name and login failures show the logical 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. Run either the **chassisName** command to name the chassis or the **switchName** command to rename the logical switch.

TABLE 2 Audit Message Field Description (Continued)

Example	Variable Name	Description
, ,	Null	Reserved for future use.
`Slot 7 ejector not closed`	Error Description	A text string explaining the error encountered and providing parameters supplied by the software at runtime.

Message Severity Levels

There are four levels of severity for messages, ranging from Critical (1) to Info (4). In general, the definitions are wide ranging and are to be used as general guidelines for troubleshooting. For all cases, you should look at each specific error message description thoroughly before taking action. System messages have the following severity levels.

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

Responding to a System Message

This section provides procedures on gathering information on system messages, including:

- Looking Up a System Message
- Gathering Information About the Problem
- Support
- Panic Dump and Core Dump Files
- Trace Dumps
- copy support ftp Command

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 3 on page 12) 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

Common steps and questions to ask yourself when troubleshooting a system message are as follows:

1. What is the current Network OS level?
2. What is the switch hardware version?
3. Is the switch operational?
4. Assess impact and urgency:
   - Is the switch down?
   - Is it a standalone switch?
   - How large is the fabric?
   - Is the fabric redundant?
5. Run the **show logging raslog** command on each logical switch.
6. Run the **supportFtp** command (as needed) to set up automatic FTP transfers, and then run the **copy support ftp** command.
7. Document the sequence of events by answering the following questions:
   - What happened just prior to the problem?
   - Is the problem repeatable?
   - If so, what are the steps to produce the problem?
   - What configuration was in place when the problem occurred?
8. Did a failover occur?
9. Was security enabled?
10. Was POST enabled?
11. Are serial port (console) logs available?
12. Which CP was master? (only applicable to the Brocade DCX, 12000, 24000, or 48000)
13. What and when were the last actions or changes made to the system?

Support

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

Panic Dump and Core Dump Files

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

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

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.

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

Trace Dumps

The 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 ftp** or **supportFTP** commands to collect trace dump files to a specified remote location to provide to support when requested.

copy support ftp Command

The **copy support ftp** command can be used to send the output of the system messages (RASLog), the trace files, and the output of the **supportShow** command to an off-switch storage location through FTP. Prior to running the **copy support ftp** command, you can optionally set up the FTP parameters using the **supportFtp** command. The **supportShow** command runs a large number of dump and show commands to provide a global output of the status of the switch. Refer to the *Fabric OS Command Reference* for more information on these commands.

System Module Descriptions

NOTE

Any reference seen in a system message to slot 0 is a reference to the blade within the switch platform, for example: Brocade DCC contains FC8-48, FC9-32, and FC8-16 blades.

Table 3 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 3 System Module Descriptions

System Module	Description
CEE CONFIG	CEEConfig error messages indicate problems with the Converged Enhanced Ethernet Configuration module of the Network OS.
EANV	?
EM	The environmental monitor (EM) manages and monitors the various field replaceable units (FRUs), including the port cards, control processor (CP) blades, blower assemblies, power supplies, and world wide name (WWN) cards. EM controls the state of the FRUs during system startup, hot-plug sequences, and fault recovery. EM provides access to and monitors the sensor and status data from the FRUs and maintains the integrity of the system using the environmental and power policies. EM reflects system status by way of CLI commands, system light emitting diodes (LEDs), and status and alarm messages. EM also manages some component-related data.
FABR	Network refers to a network of Fibre Channel switches. The Network 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.
FAB_VCS	Fabric Services VCS (FAB_VCS) daemon provides fabric distribution services for VCS and vLAG.
FCOE	FCoE error messages indicate problems with the FCoE module of the Network OS.
HAM	HAM is a user space daemon responsible for high availability management.
HIL	Hardware independent layer.
HSL	HSL error messages indicate problems with the Hardware Subsystem Layer of the Network OS.
IPAD	System messages generated by the IP admin demon.
LACP	LACP error messages indicate problems with the Link Aggregation Control Protocol module of the Network OS.
LOG	RASLog subsystem.
MFIC	MS-FICON messages relate to Fibre Connection (FICON) installations. Fibre Connection control unit port (FICON-CUP) messages are displayed under the FICU module.
MSTP	MSTP error messages indicate problems with Multiple Spanning Tree Protocol modules of the Network OS.
NSM	NSM error messages indicate problems with the Interface Management and VLAN Management module of the Network OS.
ONM	ONM error messages indicate problems with the Operation, Administration and Maintenance module of the Network OS.
PDTR	These messages indicate panic dump trace files have been created.
RAS	First failure data capture (FFDC), informational message when FFDC events are logged to the FFDC log and size/roll over warning.
RTWR	The reliable transport write and read daemon helps deliver data messages either to specific switches in the fabric or to all of the switches in the fabric. For example, if some of the switches are not reachable or are offline, RTWR returns an “unreachable” message to the caller, allowing the caller to take the appropriate action. If a switch is not responding, RTWR retries 100 times.

TABLE 3 System Module Descriptions (Continued)

System Module	Description
SEC	The security daemon generates security errors, warnings, or information during security-related data management or fabric merge operations. Administrators should watch for these messages, to distinguish between internal switch and fabric operation errors, and external attack.
SFLOW	?
SNMP	Simple Network Management Protocol is a universally supported low-level protocol that allows simple get, get next, and set requests to go to the switch (acting as an SNMP agent). It also allows the switch to send traps to the defined and configured management station. Brocade switches support six management entities that can be configured to receive these traps.
SSM	SSM error messages indicate problems with the System Services Module of the Network OS.
SULB	The software upgrade library provides the **firmwareDownload** command capability, which enables firmware upgrades to both CP blades with a single command, as well as nondisruptive code load to all 4.x switches. These messages might display if there are any problems during the **firmwareDownload** procedure. Most messages are informational only and are generated even during successful firmware download. For additional information, refer to the *Fabric OS Administrator's Guide*.
TRCE	RAS TRACE error messages.
TOAM	?
ZONE	The zone module messages indicate any problems associated with the zoning features, including commands associated with aliases, zones, and configurations.

1 System Module Descriptions

Section

I

RASLog Messages

This section provides the RASLog messages, including:

Chapter

CEE CONFIG System Messages

2

CCFG-1002

Message `<timestamp>, [CCFG-1002], <sequence-number>,, INFO, <system-name>, Started loading CEE system configuration.`

Probable Cause Indicates that the Converged Enhanced Ethernet (CEE) system configuration has started loading.

Recommended Action No action is required.

Severity INFO

CCFG-1003

Message `<timestamp>, [CCFG-1003], <sequence-number>,, INFO, <system-name>, System is ready to accept CEE user commands.`

Probable Cause Indicates that the Converged Enhanced Ethernet (CEE) shell is ready to accept configuration commands from the user.

Recommended Action No action is required.

Severity INFO

Chapter

EANV System Messages

3

EANV-1001

Message `<timestamp>, [EANV-1001], <sequence-number>,, ERROR, <system-name>, Port <port number> port fault. Please change the SFP or check cable.`

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

Recommended Action Verify that you are using compatible SFPs on the peer ports.

Verify that the SFPs have not deteriorated and that the Fibre Channel cable is not faulty. Replace the SFPs or cable if necessary.

Severity ERROR

EANV-1002

Message `<timestamp>, [EANV-1002], <sequence-number>,, ERROR, <system-name>, Port <port number> chip faulted due to internal error.`

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

Recommended Action For a bladed system, execute the **slotPowerOff** and **slotPowerOn** commands on the blade to recover the system. For a non-bladed system, perform **reload** on the switch to recover the system.

Severity ERROR

EANV-1003

Message `<timestamp>, [EANV-1003], <sequence-number>,, CRITICAL, <system-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 Whenever this error occurs, reboot the system at the next maintenance window. If the problem persists, replace the blade.

Severity CRITICAL

EANV-1004

Message `<timestamp>, [EANV-1004], <sequence-number>,, ERROR, <system-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 Whenever this error occurs, reboot the system at the next maintenance window. If the problem persists, replace the blade.

Severity ERROR

EANV-1005

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

Probable Cause Indicates the memory allocation failure in the software.

Recommended Action Whenever this error occurs, reboot the system at the next maintenance window. If the problem persists, replace the CP blade.

Severity ERROR

EANV-1006

Message `<timestamp>, [EANV-1006], <sequence-number>,, CRITICAL, <system-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 Whenever this error occurs, reboot the system at the next maintenance window. If the problem persists, replace the blade.

Severity CRITICAL

Chapter

4

EM System Messages

EM-1034

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

Probable Cause Indicates that the specified field-replaceable unit (FRU) has been marked as faulty for the specified reason.

Recommended Action Try reseating the FRU.

Run the **systemVerification** command to verify that the switch does not have hardware problems. To run this command root access is required. Refer to the *Fabric OS Command Reference* for more information on this command.

If the message persists, replace the FRU.

Severity ERROR

Chapter

FABR System Messages

5

FABR-1001

Message `<timestamp>, [FABR-1001], <sequence-number>,, WARNING, <system-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 within the message, look for a possible mismatch of relevant configuration parameters in the switches at both ends of the link.

Run the **configure** command to modify the appropriate switch parameters on both the local and remote switch.

Severity WARNING

FABR-1047

Message `<timestamp>, [FABR-1047], <sequence-number>, WARNING, <system-name>, Switch will be taken offline and back online for RBridge Id auto configuration to take effect.`

Probable Cause Indicates that the specified switch has been bounced in order to effect rBridgedId auto configuration on unconfigured vcs switch.

Recommended Action No action is required.

Severity WARNING

5 FABR-1047

Chapter

FVCS System Messages

6

FVCS-1002

Message `<timestamp>, [FVCS-1002], <sequence-number>,, WARNING, <system-name>, Test FAB_VCS RAS RBridge ID (<port number>)`

Probable Cause Indicates that the rBridge is valid.

Recommended Action If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **copy support ftp** command and contact your switch service provider.

Severity WARNING

FVCS-1003

Message `<timestamp>, [FVCS-1003], <sequence-number>,, WARNING, <system-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 its status.

Severity WARNING

FVCS-1004

Message `<timestamp>, [FVCS-1004], <sequence-number>,, WARNING, <system-name>, Configure vLAG exceed 2 RBridge Limit vLAG ifindex (<vLAG ifindex>) cfg RBridge ID1(<Configured RBridge ID-1>) cfg RBridge ID2 (<Configured RBridge ID-2>)`

Probable Cause Indicates attempting to configure more than the allowed number of 2 RBridges for vLAG.

Recommended Action Check the vLAG configuration and delete one of the vLAG configurations.

Severity WARNING

FVCS-1005

Message `<timestamp>, [FVCS-1005], <sequence-number>,, WARNING, <system-name>, Joining RBridge with overlapping vLAG exceedes 2 RBridge Limit vLAG ifindex (<vLAG ifindex>) joining RBridge ID(<Joining rBridge id>) cfg RBridge ID1(<Configured RBridge ID-1>) cfg RBridge ID2 (<Configured RBridge ID-2>)`

Probable Cause Indicates the joining RBridge with overlapping vLAG.

Recommended Action Check the vLAG configuration and delete one of the vLAG configurations.

Severity WARNING

FVCS-2001

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

Probable Cause Indicates that the RCS primary attempt has failed.

Recommended Action Check Cluster Connection Status.

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

Severity WARNING

FVCS-2002

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

Probable Cause Indicates that the link state update has failed.

Recommended Action Check Cluster Connection Status.

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

Severity WARNING

FVCS-2003

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

Probable Cause Indicates that the lag configuration update has failed.

Recommended Action Check Cluster Connection Status.

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

Severity WARNING

FVCS-3001

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

Probable Cause Indicates a failure to send update.

Recommended Action Resynchronize MAC and MCSAT Database.

Severity WARNING

FVCS-3002

Message `<timestamp>, [FVCS-3002], <sequence-number>,, WARNING, <system-name>, Eth_ns Message Queue Overflow. Failed to add Received update. MAC or MCSAT Database may be out of sync. Droup count=<Drop Count>`

Probable Cause Indicates a failure to add the received update.

Recommended Action Resynchronize MAC and MCSAT Database.

Severity WARNING

Chapter

FCOE System Messages

7

FCOE-1035

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

Probable Cause Indicates an administrative action on FCoE port.

Recommended Action No action is required.

Severity INFO

FCOE-1036

Message `<timestamp>, [FCOE-1036], <sequence-number>,, INFO, <system-name>, Virtual FCoE port <port number> (<port wwn>) disabled.`

Probable Cause Indicates an administrative action on FCoE port.

Recommended Action No action is required.

Severity INFO

Chapter

HAM System Messages

8

HAM-1004

Message `<timestamp>, [HAM-1004], <sequence-number>, SLOT cp-slot-number | CHASSIS, INFO, <system-name>, Processor rebooted - <Reboot Reason>.`

Probable Cause Indicates the system has been rebooted either because of a user action or an error. The switch reboot can be initiated by the **firmwareDownload, reload, haFailover,** and **reboot** commands. Some examples of errors that might initiate this message are hardware errors, software errors, compact flash errors, or memory errors. The *reboot reasons* can be any of the following:

- Hafailover
- Reset
- Reload
- Giveup Master:SYSM
- CP Faulty:SYSM
- FirmwareDownload
- ConfigDownload:MS
- ChangeWWN:EM
- Reboot:WebTool
- Reload:WebTool
- Software Fault:Software Watchdog
- Software Fault:Kernel Panic
- Software Fault:ASSERT
- Reboot:SNMP
- Reload:SNMP
- Reboot
- Chassis Config
- Reboot:API
- Reboot:HAM
- EMFault:EM

Recommended Action Check the error log on both CPs for additional messages that might indicate the reason for the reboot.

Severity INFO

Chapter

HIL System Messages

9

HIL-1404

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

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

Recommended Action Install the missing fan FRUs immediately.

Severity WARNING

HIL-1511

Message `<timestamp>, [HIL-1511], <sequence-number>,, WARNING, <system-name>, MISMATCH in FAN Air Flow direction. Replace FRU with fan air flows in same direction.`

Probable Cause Indicates that FAN Air Flows are in reverse direction. Could heat up the system.

Recommended Action Replace FRU with fan air flows in same direction.

Severity WARNING

HIL-1512

Message `<timestamp>, [HIL-1512], <sequence-number>,, WARNING, <system-name>, MISMATCH in PSU-FAN FRUS Air Flow direction. Replace PSU  with fan air flows in same direction.`

Probable Cause Indicates that PSU FAN Air Flows are in reverse direction. Could heat up the system.

Recommended Action Replace PSU with fan air flows in same direction.

Severity WARNING

Chapter

HSL System Messages

10

HSL-1002

Message `<timestamp>, [HSL-1002], <sequence-number>,, INFO, <system-name>, SFP for interface <Interface Name> is inserted.`

Probable Cause Indicates an SFP is inserted.

Recommended Action No action is required.

Severity INFO

HSL-1003

Message `<timestamp>, [HSL-1003], <sequence-number>,, INFO, <system-name>, SFP for interface <Interface Name> is removed.`

Probable Cause Indicates an SFP is removed.

Recommended Action No action is required.

Severity INFO

HSL-1008

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

Probable Cause Indicates that the 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, <system-name>, Failed to create Brocade trunk interface <InterfaceName>.`

Probable Cause Indicates failure to create Brocade trunk because hw resources are exhausted.

Recommended Action No action is required.

Severity ERROR

Chapter

IPAD System Messages

11

IPAD-1000

Message `<timestamp>, [IPAD-1000], <sequence-number>,, INFO, <system-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 a change in the local IP address has occurred. 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, <system-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 a change in the gateway IP address has occurred. 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, <system-name>, Switch name has been successfully changed to <switch name>.`

Probable Cause Indicates that a change with the switch name has occurred.

Recommended Action No action is required.

11 IPAD-1002

Severity INFO

Chapter

LACP System Messages

12

LACP-1002

Message `<timestamp>, [LACP-1002], <sequence-number>,, ERROR, <system-name>, <msg> <msg>.`

Probable Cause Indicates the error occured in LACP daemon.

Recommended Action Take action specific to the error message.

Severity ERROR

Chapter

LOG System Messages

13

LOG-1000

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

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

Recommended Action No action is required.

Severity INFO

LOG-1003

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

Probable Cause Indicates the persistent error log has been cleared.

Recommended Action No action is required.

Severity INFO

13 LOG-1003

Chapter

MFIC System Messages

14

MFIC-1002

Message `<timestamp>, [MFIC-1002], <sequence-number>,, INFO, <system-name>, Chassis FRU header not programmed for switch NID, using defaults (applies only to FICON environments).`

Probable Cause Indicates that custom switch node descriptor (NID) fields have not been programmed in nonvolatile storage. The default values are used. The Switch NID is used only in the following SB ELS frames: Request Node Identification Data (RNID) and Registered Link Incident Record (RLIR).

The use of SB-3 link incident registration and reporting is typically limited to FICON environments.

Recommended Action No action is required if SB-3 link incident registration and reporting is not used by the host or if default values are desired for the switch node descriptor fields.

Severity INFO

MFIC-1003

Message `<timestamp>, [MFIC-1003], <sequence-number>,, WARNING, <system-name>, Effective Insistent domain ID for the fabric changed from <state> to <state>`

Probable Cause Indicates that one or more switches joined the fabric with an insistent domain ID (IDID) mode setting that is different from the current effective IDID mode for the fabric. This message also occurs when the IDID for the fabric has been turned on or off. The possible values for the state are "On" and "Off".

Recommended Action IDID mode is a fabric-wide mode; make sure that any switches added to the fabric are configured with the same IDID mode as the fabric. If you are enabling or disabling IDID mode, this message is for information purposes only, and no action is required.

IDID mode can be set using the **configure** command in the CLI or checking the Advanced Web Tools **Switch Admin > Configure Tab > Fabric Subtab > Insistent Domain ID Mode** check box. The switch must be disabled to change the IDID mode.

Severity WARNING

14 MFIC-1003

Chapter

MSTP System Messages

15

MSTP-2001

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

Probable Cause Indicates that the MSTP bridge mode has changed.

Recommended Action No action is required

Severity INFO

MSTP-2002

Message `<timestamp>, [MSTP-2002], <sequence-number>,, INFO, <system-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

Chapter

NSM System Messages

16

NSM-1001

Message `<timestamp>, [NSM-1001], <sequence-number>,, INFO, <system-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, <system-name>, Interface <Interface Name> is protocol down.`

Probable Cause Indicates that the interface is offline as one of the protocol dependencies 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, <system-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, <system-name>, Interface <interface name> is created.`

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

Recommended Action No action is required.

Severity INFO

NSM-1010

Message `<timestamp>, [NSM-1010], <sequence-number>,, INFO, <system-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, <system-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-1017

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

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

Recommended Action No action is required.

Severity INFO

NSM-1018

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

Probable Cause Indicates that vlan membership has been changed.

Recommended Action No action is required.

Severity INFO

NSM-1019

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

Probable Cause Indicates that interface admin status has changed to up.

Recommended Action No action is required.

Severity INFO

NSM-1020

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

Probable Cause Indicates that interface admin status has changed to down.

Recommended Action No action is required.

Severity INFO

NSM-1023

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

Probable Cause Indicates that a RBridge has joined the vLAG.

Recommended Action No action is required.

Severity INFO

NSM-1024

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

Probable Cause Indicates that a RBridge has left the vLAG.

Recommended Action No action is required.

Severity INFO

NSM-1025

Message `<timestamp>, [NSM-1025], <sequence-number>,, INFO, <system-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 a RBridge has left the vLAG.

Recommended Action No action is required.

Severity INFO

NSM-1026

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

Probable Cause Indicates an SFP is inserted.

Recommended Action No action is required.

Severity INFO

NSM-1027

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

Probable Cause Indicates an SFP is removed.

Recommended Action No action is required.

Severity INFO

NSM-1028

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

Probable Cause Indicates an incompatible SFP for the interface inserted.

Recommended Action Use the correct SFP for this interface.

Severity ERROR

NSM-1029

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

Probable Cause Indicates failure to read SFP.

Recommended Action No action is required.

Severity ERROR

NSM-2000

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

Probable Cause Indicates that Profile Activation was successful.

Recommended Action No action is required.

Severity INFO

NSM-2001

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

Probable Cause Indicates that 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, <system-name>, Port-profile <ProfileName> deactivation succeeded.`

Probable Cause Indicates that Profile Deactivation was unsuccessful.

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

Severity INFO

NSM-2003

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

Probable Cause Indicates that 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, <system-name>, Port-profile <ProfileName> application succeeded on <InterfaceName>.`

Probable Cause Indicates that Profile Application was successful.

Recommended Action No action is required.

Severity ERROR

NSM-2005

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

Probable Cause Indicates that 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, <system-name>, Port-profile <ProfileName> removed successfully on <InterfaceName>.`

Probable Cause Indicates that Profile De-Application was unsuccessful.

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

Severity INFO

NSM-2007

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

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

Recommended Action No action is required.

Severity INFO

NSM-2008

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

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

Recommended Action No action is required.

Severity INFO

NSM-2009

Message `<timestamp>, [NSM-2009], <sequence-number>,, ERROR, <system-name>, Interface <InterfaceName> could not become Port-profile-port, reason <Reason>.`

Probable Cause Indicates that 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-2010

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

Probable Cause Indicates that 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, <system-name>, Port-profile <ProfileName> removed failed on <InterfaceName>.`

Probable Cause Indicates that Profile removal was unsuccessful.

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

Severity INFO

Chapter

ONM System Messages

17

ONMD-1002

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

Probable Cause Indicates that LLDP Global configuration has been changed.

Recommended Action No action is required.

Severity INFO

Chapter

PORT System Messages

18

PORT-1006

Message `<timestamp>, [PORT-1006], <sequence-number>,, INFO, <system-name>, Configuration changed for port (ID: <port number>) in No_Module or No_Light state.`

Probable Cause Indicates the configuration changes were made to an offline port in No_Module or No_Light state.

Recommended Action No action is required.

Severity INFO

Chapter

RAS System Messages

19

RAS-1005

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

Probable Cause Indicates an internal software error.

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

Severity WARNING

Chapter

RTWR System Messages

20

RTWR-1003

Message

```
<timestamp>, [RTWR-1003], <sequence-number>,, INFO, <system-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 the RTWR has failed to get a response.

Recommended Action

Run the **dom** command to verify that the specified domain ID is reachable.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers and run the **copy support ftp** command then contact your switch service provider.

Severity

INFO

Chapter

SEC System Messages

21

SEC-1203

Message `<timestamp>, [SEC-1203], <sequence-number>,, INFO, <system-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-3051

Message `<timestamp>, [SEC-3051], <sequence-number>, AUDIT, INFO, <system-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-3501

Message `<timestamp>, [SEC-3501], <sequence-number>,, INFO, <system-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

SFLOW System Messages

22

SFLO-1009

Message `<timestamp>, [SFLO-1009], <sequence-number>,, INFO, <system-name>, Socket Operation Failed while connecting with collector address.`

Probable Cause Indicates that connect to collector server failed.

Recommended Action No action is required.

Severity INFO

Chapter

SNMP System Messages

23

SNMP-1007

Message `<timestamp>, [SNMP-1007], <sequence-number>,, INFO, <system-name>, The last fabric change happened at: <string>.`

Probable Cause Indicates the last fabric change time.

Recommended Action Execute the **fabricshow** command to view the current fabric status.

Severity INFO

SNMP-1008

Message `<timestamp>, [SNMP-1008], <sequence-number>,, INFO, <system-name>, The last device change happened at: <string>.`

Probable Cause Indicates the last device change time.

Recommended Action Execute the **nsshow** command to view the current device status.

Severity INFO

Chapter

SSM System Messages

24

SSMD-1300

Message `<timestamp>, [SSMD-1300], <sequence-number>,, INFO, <system-name>,CEEMap <ceemap> is created with precedence <precedence>.`

Probable Cause Indicates that CEEMap is created.

Recommended Action No action is required.

Severity INFO

SSMD-1302

Message `<timestamp>, [SSMD-1302], <sequence-number>,, INFO, <system-name>,CEEMap <ceemap> priority table <pg_ids> is <action>.`

Probable Cause Indicates that PGs added to or removed from existing ceemap.

Recommended Action No action is required.

Severity INFO

SSMD-1303

Message `<timestamp>, [SSMD-1303], <sequence-number>,, INFO, <system-name>,CEEMap <ceemap> priority group <pg_id> with weight <PGID> is created with pfc <pfc>.`

Probable Cause Indicates that priority Group has been created.

Recommended Action No action is required.

Severity INFO

SSMD-1304

Message `<timestamp>, [SSMD-1304], <sequence-number>,, INFO, <system-name>,CEEMap <ceemap> priority group <pg_id> is deleted.`

Probable Cause Indicates that priority Group has been deleted.

Recommended Action No action is required.

Severity INFO

SSMD-1305

Message `<timestamp>, [SSMD-1305], <sequence-number>,, INFO, <system-name>,CEEMap <ceemap> priority group <pg_id> weight is changed from <PGID_weight_new> to <PGID_weight_old>.`

Probable Cause Indicates that priority Group weight has been changed.

Recommended Action No action is required.

Severity INFO

SSMD-1306

Message `<timestamp>, [SSMD-1306], <sequence-number>,, INFO, <system-name>,CEEMap <ceemap> priority group <pg_id> is pfc <pfc_status>.`

Probable Cause Indicates that priority Group pfc status has been changed.

Recommended Action No action is required.

Severity INFO

SSMD-1312

Message `<timestamp>, [SSMD-1312], <sequence-number>,, INFO, <system-name>, <map_type> <map_name> is assigned to interface <InterfaceName>.`

Probable Cause Indicates that user profile Map is assigned to an interface.

Recommended Action No action is required.

Severity INFO

SSMD-1313

Message `<timestamp>, [SSMD-1313], <sequence-number>,, INFO, <system-name>, <map_type> <map_name> is removed from interface <InterfaceName>.`

Probable Cause Indicates that user profile Map is removed from interface.

Recommended Action No action is required.

Severity INFO

SSMD-1218

Message `<timestamp>, [SSMD-1218], <sequence-number>,, WARNING, <system-name>,QoS failed programming interface 0x<Interface ID> Priority Tag.`

Probable Cause Indicates the DCE System Services Manager encountered an unexpected error in programming 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-1315

Message `<timestamp>, [SSMD-1315], <sequence-number>,, INFO, <system-name>, CEEMap <ceemap> remap <lossless or fabric priority> to priority <remapped value>.`

Probable Cause Indicates that CEEMap precedence CoS has changed.

Recommended Action No action is required.

Severity INFO

Chapter

SULB System Messages

25

SULB-1001

Message `<timestamp>, [SULB-1001], <sequence-number>, AUDIT, WARNING, <system-name>, Firmwaredownload command has started.`

Probable Cause Indicates the **firmwareDownload** command has been started. This process should take approximately 17 minutes. The process is set to time out after 30 minutes.

Recommended Action Do not fail over or power down the system during firmware upgrade. Allow the **firmwareDownload** command to continue without disruption.

Run the **firmwareDownloadStatus** command for more information.

Severity WARNING

SULB-1002

Message `<timestamp>, [SULB-1002],<sequence-number>, AUDIT, INFO, <system-name>, Firmwaredownload command has completed successfully.`

Probable Cause Indicates the **firmwareDownload** command has completed successfully and switch firmware has been updated.

Recommended Action No action is required. The **firmwareDownload** command has completed as expected.

Run the **firmwareDownloadStatus** command for more information. Run the **firmwareShow** command to verify the firmware versions.

Severity INFO

SULB-1003

Message `<timestamp>, [SULB-1003], <sequence-number>, AUDIT, INFO, <system-name>, Firmwarecommit has started.`

Probable Cause Indicates that the **firmwareCommit** command has been started.

Recommended Action No action is required. Run the **firmwareDownloadStatus** command for more information.

Severity INFO

SULB-1004

Message `<timestamp>, [SULB-1004], INFO, FIRMWARE, <event-initiator-details>, <event-location>, , Firmwarecommit has completed.`

Probable Cause Indicates the **FirmwareCommit** command is executed.

Recommended Action No action is required. Run the **firmwareDownloadStatus** command for more information.

Severity INFO

SULB-1036

Message `<timestamp>, [SULB-1036], <sequence-number>,, INFO, <system-name>, <The Version being logged><Version String>.`

Probable Cause Indicates the firmware version is running in the system. This is generally logged before download and after download of the firmware to store version information.

Recommended Action No action is required.

Severity INFO

Chapter

TRCE System Messages

26

TRCE-1001

Message `<timestamp>, [TRCE-1001], <sequence-number>,, WARNING, <system-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
- MANUAL generated by the **tracedump -n** command
- TRIGGER when triggered by a specific Message ID generated by CRITICAL RASLog message or RASLog message trigger setup using the **traceTrig** command.

Recommended Action Run the **supportFtp** command to set up automatic FTP transfers; then run the **copy support ftp** command and contact your switch service provider.

Severity WARNING

TRCE-1004

Message `<timestamp>, [TRCE-1004], <sequence-number>,, WARNING, <system-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 **supportFtp** command to set up automatic FTP transfers; then run the **copy support ftp** command and contact your switch service provider.

Severity WARNING

Chapter

TOAM System Messages

27

TOAM-1000

Message `<timestamp>, [TOAM-1000], <sequence-number>,, INFO, <system-name>, Cannot run this command because VCS is disabled`

Probable Cause Indicates inability to run Trill OAM commands because of no VCS.

Recommended Action Enable VCS if this command is to be run.

Severity INFO

TOAM-1001

Message `<timestamp>, [TOAM-1001], <sequence-number>,, INFO, <system-name>, Cannot run this command since this switch is not on the network edge`

Probable Cause Indicates inability to run this command because this switch is not on the network edge.

Recommended Action Execute this command from edge switches.

Severity INFO

TOAM-1002

Message `<timestamp>, [TOAM-1002], <sequence-number>,, INFO, <system-name>, Source MAC address in not known/learned`

Probable Cause Indicates that the source MAC address is unknown.

Recommended Action Use only a correctly learned source MAC address.

Severity INFO

TOAM-1003

Message `<timestamp>, [TOAM-1003], <sequence-number>,, ERROR, <system-name>, Initilisation error: <reason>`

Probable Cause Indicates that toam encountered an error during initialization.

27 TOAM-1003

Recommended Action Restart the toam daemon.

Severity ERROR

Chapter

ZONE System Messages

28

ZONE-1034

Message `<timestamp>, [ZONE-1034], <sequence-number>,, INFO, <system-name>, A new zone database file is created.`

Probable Cause Indicates that a new zone database was created.

Recommended Action No action is required.

Severity INFO

Section

II

Audit Log Messages

This section provides the Audit messages, including:

Chapter

AUDIT CEE CONFIG System Messages

29

CCFG-1002

Message `AUDIT, <timestamp>, [CCFG-1002], <sequence-number>,, INFO, <system-name>, Started loading CEE system configuration.`

Probable Cause Indicates that the Converged Enhanced Ethernet (CEE) system configuration has started loading.

Recommended Action No action is required.

Severity INFO

CCFG-1003

Message `AUDIT, <timestamp>, [CCFG-1003], <sequence-number>,, INFO, <system-name>, System is ready to accept CEE user commands.`

Probable Cause Indicates that the Converged Enhanced Ethernet (CEE) shell is ready to accept configuration commands from the user.

Recommended Action No action is required.

Severity INFO

Chapter

AUDIT IPAD System Messages

30

IPAD-1002

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

Probable Cause Indicates that a change with the switch name has occurred.

Recommended Action No action is required.

Severity INFO

Chapter

AUDIT SEC System Messages

31

SEC-3051

Message `<timestamp>, [SEC-3051], <sequence-number>, AUDIT, INFO, <system-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-3501

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

Probable Cause Indicates the attributes of a role are changed.

Recommended Action No action is required.

Severity INFO