



Catalyst 3750 Metro Switch System Message Guide

Cisco IOS Release 12.2(58)SE

January 2012

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-9651-06

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

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

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

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

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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

Catalyst 3750 Metro Switch System Message Guide
© 2006–2012 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface vii

Purpose vii

Conventions vii

Related Publications viii

Obtaining Documentation and Submitting a Service Request viii

CHAPTER 1

System Message Overview 1-1

How to Read System Messages 1-1

Error Message Traceback Reports 1-5

Output Interpreter 1-6

Bug Toolkit 1-6

Contacting TAC 1-6

CHAPTER 2

Message and Recovery Procedures 2-1

ACLMGR Messages 2-3

AUTHMGR Messages 2-6

BACKUP_INTERFACE Messages 2-9

BADTRANSCEIVER Messages 2-9

BSPATCH Messages 2-9

CMP Messages 2-10

DHCP_SNOOPING Messages 2-11

DOT1Q Tunneling Messages 2-14

DOT1X Messages 2-14

DOT1X_SWITCH Messages 2-20

DTP Messages 2-23

EC Messages 2-25

EPM Messages 2-29

ESF Messages 2-30

ETHCNTR Messages 2-30

EXPRESS_SETUP Messages 2-31

FRNTEND_CTRLR Messages 2-32

GBIC_SECURITY Messages 2-32

GBIC_SECURITY_CRYPT Messages	2-34
GBIC_SECURITY_UNIQUE Messages	2-35
HARDWARE Messages	2-35
HLFM Messages	2-37
IDBMAN Messages	2-38
IFMGR Messages	2-41
ILET Messages	2-42
MAC_LIMIT Messages	2-42
IP Messages	2-43
MAC_MOVE Messages	2-43
PAGP_DUAL_ACTIVE Messages	2-43
PHY Messages	2-44
PIMSN Messages	2-46
PLATFORM Messages	2-46
PLATFORM_CAT3750 Messages	2-47
PLATFORM_FBM Messages	2-47
PLATFORM_PBR Messages	2-48
PLATFORM_PM Messages	2-50
PLATFORM_SPAN Messages	2-51
PLATFORM_UCAST Messages	2-51
PLATFORM_VLAN Messages	2-53
PM Messages	2-54
PORT SECURITY Messages	2-62
QOSMGR Messages	2-63
REP Messages	2-68
RMON Messages	2-69
SCHED Messages	2-70
SPAN Messages	2-70
SPANTREE Messages	2-71
SPANTREE_FAST Messages	2-78
SPANTREE_VLAN_SW Messages	2-79
STORM_CONTROL Messages	2-80
SUPERVISOR Messages	2-80
SUPQ Messages	2-81
SW_DAI Messages	2-83

SW_VLAN Messages	2-85
SWITCH_QOS_TB Messages	2-91
TCAMMGR Messages	2-92
UDLD Messages	2-93
VQPCIENT Messages	2-94

INDEX



Preface

Purpose

This guide describes the Catalyst 3750 Metro switch-specific messages that you might encounter. For a complete list of Cisco IOS system error messages, see the *Cisco IOS System Error Messages, Cisco IOS Release 12.2*.

This guide does not describe how to install your switch or how to configure software features on your switch. It also does not provide detailed information about commands that have been created or changed for use by the switch. For hardware installation information, see the hardware installation guide that shipped with your switch. For software information, see the software configuration guide and the command reference for this release.

For documentation updates, see the release notes for this release.

Conventions

This publication uses these conventions to convey instructions and information:

Command descriptions use these conventions:

- Commands and keywords are in **boldface** text.
- Arguments for which you supply values are in *italic*.
- Square brackets ([]) mean optional elements.
- Braces ({ }) group required choices, and vertical bars (|) separate the alternative elements.
- Braces and vertical bars within square brackets ([{ | }]) mean a required choice within an optional element.

Interactive examples use these conventions:

- Terminal sessions and system displays are in `screen` font.
- Information you enter is in **boldface screen** font.
- Nonprinting characters, such as passwords or tabs, are in angle brackets (< >).

Notes use this convention and symbol:



Note

Means *reader take note*. Notes contain helpful suggestions or references to materials not in this manual.

Related Publications

These documents provide complete information about the switch and are available from this Cisco.com site:

http://www.cisco.com/en/US/products/hw/switches/ps5532/tsd_products_support_series_home.html

See these documents for other information about the switch:

- *Release Notes for the Catalyst 3750 Metro Switch*
- *Catalyst 3750 Metro Switch Software Configuration Guide*
- *Catalyst 3750 Metro Switch Command Reference*
- *Catalyst 3750 Metro Switch Hardware Installation Guide*
- *Cisco Small Form-Factor Pluggable Modules Installation Notes*
- Compatibility matrix documents
http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html
 - *Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix*
 - *Cisco 100-Megabit Ethernet SFP Modules Compatibility Matrix*
 - *Cisco Small Form-Factor Pluggable Modules Compatibility Matrix*
 - *Compatibility Matrix for 1000BASE-T Small Form-Factor Pluggable Modules*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation:

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

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.



CHAPTER 1

System Message Overview

This guide describes the Catalyst 3750 Metro-specific system messages. During operation, the system software sends these messages to the console (and, optionally, to a logging server on another system). Not all system messages mean problems with your system. Some messages are informational, and others can help diagnose problems with communications lines, internal hardware, or the system software.



Note

For information about system messages that are not Catalyst 3750 Metro-specific, see the *Cisco IOS System Error Messages, Cisco IOS Release 12.2*.

- [How to Read System Messages, page 1-1](#)
- [Error Message Traceback Reports, page 1-5](#)

How to Read System Messages

System log messages can contain up to 80 characters and a percent sign (%), which follows the optional sequence number or time-stamp information, if configured. Messages appear in this format:

seq no:timestamp: %facility-severity-MNEMONIC:description (hostname-n)

By default, a switch sends the output from system messages to a logging process.

Each system message begins with a percent sign (%) and is structured as follows:

%FACILITY-SEVERITY-MNEMONIC: Message-text

- FACILITY is a two or more uppercase letters that show the facility to which the message refers. A facility can be a hardware device, a protocol, or a module of the system software. [Table 1-1](#) lists Catalyst 3750-specific facility codes.

These messages are described in [Chapter 2, “Message and Recovery Procedures,”](#) in alphabetical order by facility code with the most severe (lowest number) errors described first.

Table 1-1 Facility Codes

Facility Code	Description	Location
ACLMGR	ACL manager	“ACLMGR Messages” section on page 2-3
AUTHMGR	Authorization Manager	“AUTHMGR Messages” section on page 2-6

Table 1-1 Facility Codes (continued)

Facility Code	Description	Location
BACKUP_INTERFACE	Backup Interface	“BACKUP_INTERFACE Messages” section on page 2-9
BADTRANSCEIVER	Bad Transceiver	“BADTRANSCEIVER Messages” section on page 2-9
BSPATCH	Boot loader patch	“BSPATCH Messages” section on page 2-9
CMP	Cluster Membership Protocol	“CMP Messages” section on page 2-10
DHCP_SNOOPING	DHCP snooping	“DHCP_SNOOPING Messages” section on page 2-11
DOT1Q_TUNNELLING	802.1Q tunneling	“DOT1Q Tunneling Messages” section on page 2-14
DOT1X	802.1x	“DOT1X Messages” section on page 2-14
DOT1X_SWITCH	802.1x for switches	“DOT1X_SWITCH Messages” section on page 2-20
DTP	Dynamic Trunking Protocol	“DTP Messages” section on page 2-23
EC	EtherChannel	“EC Messages” section on page 2-25
EPM	EPM	“EPM Messages” section on page 2-29
ESF	Enhanced services forwarding (ESF)	“ESF Messages” section on page 2-30
ETHCNTR	Ethernet Controller	“ETHCNTR Messages” section on page 2-30
EXPRESS_SETUP	Express Setup	“EXPRESS_SETUP Messages” section on page 2-31
FRNTEND_CTRLR	Front-end controller	“FRNTEND_CTRLR Messages” section on page 2-32
GBIC_SECURITY	Gigabit Interface Converter (GBIC) module and small form-factor pluggable (SFP) module security	“GBIC_SECURITY Messages” section on page 2-32
GBIC_SECURITY_CRYPT	GBIC and SFP module security	“GBIC_SECURITY_CRYPT Messages” section on page 2-34
GBIC_SECURITY_UNIQUE	GBIC and SFP module security	“GBIC_SECURITY_UNIQUE Messages” section on page 2-35
HARDWARE	Hardware	“HARDWARE Messages” section on page 2-35
HLFM	Local forwarding manager	“HLFM Messages” section on page 2-37
IDBMAN	Interface database manager process	“IDBMAN Messages” section on page 2-38

Table 1-1 Facility Codes (continued)

Facility Code	Description	Location
IF MGR	Interface manager	“IFMGR Messages” section on page 2-41
ILET	ILET	“ILET Messages” section on page 2-42
IP	Internet Protocol	“IP Messages” section on page 2-43
MAC_LIMIT	MAC address table entries	“Recommended Action Contact your Cisco sales representative for assistance” section on page 2-42
MAC_MOVE	Host activity	“MAC_MOVE Messages” section on page 2-43
PAGP_DUAL_ACTIVE	Port Aggregation Protocol (PAgP) dual-active detection	“PAGP_DUAL_ACTIVE Messages” section on page 2-43
PHY	PHY	“PHY Messages” section on page 2-44
PIMSN	Protocol Independent Multicast (PIM) snooping	“PIMSN Messages” section on page 2-46
PLATFORM	Low-level platform-specific	“PLATFORM Messages” section on page 2-46
PLATFORM_CAT3750	Catalyst 3750 internal	“PLATFORM_CAT3750 Messages” section on page 2-47
PLATFORM_FBM	Fallback bridging manager	“PLATFORM_FBM Messages” section on page 2-47
PLATFORM_PBR	Policy-based routing	“PLATFORM_PBR Messages” section on page 2-48
PLATFORM_PM	Port manager	“PLATFORM_PM Messages” section on page 2-50
PLATFORM_SPAN	Switched Port Analyzer (SPAN)	“PLATFORM_SPAN Messages” section on page 2-51
PLATFORM_UCAST	Platform unicast routing	“PLATFORM_UCAST Messages” section on page 2-51
PLATFORM_VLAN	VLAN	“PLATFORM_VLAN Messages” section on page 2-53
PM	Port manager	“PM Messages” section on page 2-54
PORT SECURITY	Port security	“PORT SECURITY Messages” section on page 2-62
QOSMGR	QoS manager	“QOSMGR Messages” section on page 2-63
REP	Resilient Ethernet Protocol	“REP Messages” section on page 2-68
RMON	Remote network monitoring	“RMON Messages” section on page 2-69
SCHED	SCHED	“SCHED Messages” section on page 2-70

Table 1-1 Facility Codes (continued)

Facility Code	Description	Location
SPAN	Switched Port Analyzer (SPAN)	“SPAN Messages” section on page 2-70
SPANTREE	Spanning tree	“SPANTREE Messages” section on page 2-71
SPANTREE_FAST	Spanning-tree fast convergence	“SPANTREE_FAST Messages” section on page 2-78
SPANTREE_VLAN_SW	Spanning-tree VLAN switch	“SPANTREE_VLAN_SW Messages” section on page 2-79
STORM_CONTROL	Storm control	“STORM_CONTROL Messages” section on page 2-80
SUPERVISOR	Supervisor ASIC	“SUPERVISOR Messages” section on page 2-80
SUPQ	Supervisor queue	“SUPQ Messages” section on page 2-81
SW_DAI	Dynamic ARP inspection	“SW_DAI Messages” section on page 2-83
SW_VLAN	VLAN manager	“SW_VLAN Messages” section on page 2-85
SWITCH_QOS_TB	QoS trusted boundary	“SWITCH_QOS_TB Messages” section on page 2-91
TCAMMGR	Ternary content addressable memory manager	“TCAMMGR Messages” section on page 2-92
UDLD	UniDirectional Link Detection (UDLD)	“UDLD Messages” section on page 2-93
VQPCLIENT	VLAN Query Protocol (VQP) client	“VQPCLIENT Messages” section on page 2-94

- SEVERITY is a single-digit code from 0 to 7 that reflects the severity of the condition. The lower the number, the more serious the situation. [Table 1-2](#) lists the message severity levels.

Table 1-2 Message Severity Levels

Severity Level	Description
0 – emergency	System is unusable.
1 – alert	Immediate action required.
2 – critical	Critical condition.
3 – error	Error condition.
4 – warning	Warning condition.
5 – notification	Normal but significant condition.
6 – informational	Informational message only.
7 – debugging	Message that appears during debugging only.

- MNEMONIC is a code that uniquely identifies the message.
- Message-text is a text string describing the condition. This portion of the message sometimes contains detailed information about the event, including terminal port numbers, network addresses, or addresses that correspond to locations in the system memory address space. Because the information in these variable fields changes from message to message, it is represented here by short strings enclosed in square brackets ([]). A decimal number, for example, is represented as [dec]. Table 1-3 lists the variable fields in messages.

Table 1-3 Variable Fields

Representation	Type of Information
[dec]	Decimal integer
[char]	Single character
[chars]	Character string
[enet]	Ethernet address (for example, 0000.FEED.00C0)
[hex]	Hexadecimal integer
[inet]	Internet address

This example shows a partial switch system message:

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/2, changed state to up
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed
state to down 2
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
18:47:02: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
*Mar  1 18:48:50.483 UTC: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)

00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up (Switch-2)
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet2/0/1, changed state to up (Switch-2)
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet2/0/2, changed state to up (Switch-2)
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
(Switch-2)
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/0/1, changed
state to down 2 (Switch-2)
```

Error Message Traceback Reports

Some messages describe internal errors and contain traceback information. Include this information when you report a problem to your technical support representative.

This message example includes traceback information:

```
-Process= "Exec", level= 0, pid= 17
-Traceback= 1A82 1AB4 6378 A072 1054 1860
```

Some system messages ask you to copy the error messages and take further action. These online tools also provide more information about system error messages.

Output Interpreter

The Output Interpreter provides additional information and suggested resolutions based on the output of many CLI commands, such as the **show tech-support** privileged EXEC command.

<https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl>

Bug Toolkit

The Bug Toolkit provides information on open and closed caveats and allows you to search for all known bugs in a specific Cisco IOS Release.

<http://tools.cisco.com/Support/BugToolKit/>

Contacting TAC

If you cannot determine the nature of the error, see the “[Obtaining Documentation and Submitting a Service Request](#)” section on page viii for further information.



CHAPTER 2

Message and Recovery Procedures

This chapter describes messages specific to the Catalyst 3750 Metro switch in alphabetical order by facility. Within each facility, the messages are listed by severity levels 0 to 7: 0 is the highest severity level, and 7 is the lowest severity level. Each message is followed by an explanation and a recommended action.



Note

The messages listed in this chapter do not include the hostname or the date/time-stamp designation that appears only if the software is configured for system log messaging.

- [ACLMGR Messages, page 2-3](#)
- [AUTHMGR Messages, page 2-6](#)
- [BACKUP_INTERFACE Messages, page 2-9](#)
- [BADTRANSCEIVER Messages, page 2-9](#)
- [BSPATCH Messages, page 2-9](#)
- [CMP Messages, page 2-10](#)
- [DHCP_SNOOPING Messages, page 2-11](#)
- [DOT1Q Tunneling Messages, page 2-14](#)
- [DOT1X Messages, page 2-14](#)
- [DOT1X_SWITCH Messages, page 2-20](#)
- [DTP Messages, page 2-23](#)
- [EC Messages, page 2-25](#)
- [EPM Messages, page 2-29](#)
- [ESF Messages, page 2-30](#)
- [ETHCNTR Messages, page 2-30](#)
- [EXPRESS_SETUP Messages, page 2-31](#)
- [FRNTEND_CTRLR Messages, page 2-32](#)
- [GBIC_SECURITY Messages, page 2-32](#)
- [GBIC_SECURITY_CRYPT Messages, page 2-34](#)
- [GBIC_SECURITY_UNIQUE Messages, page 2-35](#)
- [HARDWARE Messages, page 2-35](#)

- HLFM Messages, page 2-37
- IDBMAN Messages, page 2-38
- IFMGR Messages, page 2-41
- ILET Messages, page 2-42
- IP Messages, page 2-43
- MAC_MOVE Messages, page 2-43
- PAGP_DUAL_ACTIVE Messages, page 2-43
- PHY Messages, page 2-44
- PIMSN Messages, page 2-46
- PLATFORM Messages, page 2-46
- PLATFORM _CAT3750 Messages, page 2-47
- PLATFORM_FBM Messages, page 2-47
- PLATFORM_PBR Messages, page 2-48
- PLATFORM_PM Messages, page 2-50
- PLATFORM_SPAN Messages, page 2-51
- PLATFORM_UCAST Messages, page 2-51
- PLATFORM_VLAN Messages, page 2-53
- PM Messages, page 2-54
- PORT SECURITY Messages, page 2-62
- QOSMGR Messages, page 2-63
- REP Messages, page 2-68
- RMON Messages, page 2-69
- SCHED Messages, page 2-70
- SPAN Messages, page 2-70
- SPANTREE Messages, page 2-71
- SPANTREE_FAST Messages, page 2-78
- SPANTREE_VLAN_SW Messages, page 2-79
- STORM_CONTROL Messages, page 2-80
- SUPERVISOR Messages, page 2-80
- SUPQ Messages, page 2-81
- SW_DAI Messages, page 2-83
- SW_VLAN Messages, page 2-85
- SWITCH_QOS_TB Messages, page 2-91
- TCAMMGR Messages, page 2-92
- UDLD Messages, page 2-93
- VQPCCLIENT Messages, page 2-94

ACLMGR Messages

Error Message ACLMGR-2-NOMAP: Cannot create ACL Manager data structures for VLAN Map [chars].

Explanation The ACL manager could not allocate the data structures needed to describe a VLAN map into a form that can be loaded into hardware. This error is most likely caused by lack of free memory. [chars] is the VLAN map name.

Recommended Action Reduce other system activity to ease memory demands.

Error Message ACLMGR-2-NOVLB: Cannot create memory block for VLAN [dec].

Explanation The ACL manager could not save per-VLAN information needed for its correct operation. Some per-interface features, such as access groups or VLAN maps, will not be configured correctly. [dec] is the VLAN number.

Recommended Action Use a less complicated configuration that requires less memory.

Error Message ACLMGR-2-NOVMR: Cannot generate hardware representation of access list [chars]

Explanation Available resources are not sufficient to create a hardware representation of the ACL. A lack of available logical operation units or specialized hardware resources can cause this problem. Logical operation units are needed for a TCP flag match or a test other than **eq** (**ne**, **gt**, **lt**, or **range**) on TCP, UDP, or SCTP port numbers.

Recommended Action Modify the ACL configuration to use fewer resources, or rename the ACL with a name or number that alphanumerically precedes the other ACL names or numbers.

Error Message ACLMGR-3-ACLTCAMFULL: Acl Tcam Full. Drop packets on Output Acl label [dec] on [chars] [chars].

Explanation The platform-specific ACL TCAM cannot support the number of configured ACLs. [dec] is the label number, and [chars] is the layer. The first [chars] is Layer 3, and the second [chars] is Layer 2. If only one layer of TCAM is full, only one string is displayed, and the other string is NULL.

Recommended Action Reduce the number of IP or MAC access lists to be applied to interfaces.

Error Message ACLMGR-3-AUGMENTFAIL: Augmenting of access-map [chars] on [chars] label [dec] failed.

Explanation The system ran out of CPU DRAM when trying to merge internally required elements with the configured access maps. The first [chars] is the access-map name, the second [chars] is the direction in which the map was applied (*input* or *output*), and [dec] is the label number.

Recommended Action Reduce other system activity to ease memory demands.

Error Message ACLMGR-3-IECPORTLABELERROR: ACL labels are out-of-sync on interface [chars], label [dec] is not available on asic [dec].

Explanation An internal software error has occurred. [chars] is the interface name. The first [dec] is the label associated with the ACL, and the second [dec] is the ASIC number.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message ACLMGR-3-INSERTFAIL: Insert of access-map [chars] #[dec] into [chars] label [dec] failed.

Explanation The system ran out of CPU memory when trying to merge sections of an access map. The first [chars] is the map name, and the second [chars] is the direction in which the map was applied. The first [dec] is the entry number, and the second [dec] is the label number.

Recommended Action Reduce other system activity to ease memory demands. For example, remove any ACLs that have been defined but not used. Use simpler ACLs with fewer access control entries (ACEs). Use fewer VLANs, and remove any unneeded VLANs from the VLAN database.

Error Message ACLMGR-3-INTTABLE: Not in truth table: VLMAP [dec] RACL [dec] Mcb [dec] Feat [dec].

Explanation An unrecoverable software error occurred while trying to merge the configured input features. [dec] are internal action codes.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message ACLMGR-3-MAXRECURSION: Too many ([dec]) levels of recursion while merging ACLs (code [dec]).

Explanation The configuration is too complicated for the platform-specific ACL merge code to support. The most likely cause is too many separate access lists in a single VLAN map or policy map. The first [dec] is the number of levels of recursion. The second [dec] is an internal code number of the merge stage that encountered the problem.

Recommended Action Reduce the number of IP or MAC access lists (considered separately) in any one VLAN or policy map to fewer than the number of levels reported by this log message.

Error Message ACLMGR-3-MERGEFAIL: [chars] ACL merge error [dec] ([chars]) on [chars] label [dec].

Explanation The ACL manager could not complete the merge of the configured features into a form suitable for loading into the hardware. Packets potentially affected by this feature will be sent to the CPU for processing. The most likely cause is specifying an ACL that is too large or too complex for the system. The first [chars] is the ACL-type error (*ip* or *mac*), the first [dec] is the error code, the second [chars] is the message string for the preceding error code, the second [dec] is the label number, and the third [chars] is either *input* or *output*.

Recommended Action Specify a smaller and less complicated configuration.

Error Message ACLMGR-3-NOLABEL: Cannot allocate [chars] label for interface [chars].

Explanation The ACL manager could not allocate a label for the features on this interface. This means that the hardware cannot be programmed to implement the features, and packets for this interface will be filtered in software. There is a limit of 256 labels per direction. The first [chars] is the direction (*input* or *output*), and the second [chars] is the interface name.

Recommended Action Use a simpler configuration. Use the same ACLs on multiple interfaces, if possible.

Error Message ACLMGR-3-OUTTTABLE: Not in truth table: RACL [dec] VLMAP [dec].

Explanation An unrecoverable software error occurred while trying to merge the configured output features. [dec] are internal action codes.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message ACLMGR-3-PACLTTABLE: Not in truth table: IPSrcGrd [dec] PACL [dec].

Explanation An unrecoverable software error occurred while trying to merge the configured port ACL features. The first [dec] is the action specified by IP source guard, and the second [dec] is the action specified by the port ACL.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message ACLMGR-3-QOSTTABLE: Not in truth table: ACL [dec] in map, action [dec].

Explanation A software error occurred while trying to merge a quality of service (QoS) policy map. The first [dec] is the ACL number, and the second [dec] is the action corresponding to the specified ACL number.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message ACLMGR-3-RELOADED: Reloading [chars] label [dec] feature.

Explanation The ACL manager can now load more of the configured features on this label into the hardware. One or more features had previously been unloaded because of lack of space. [chars] is the direction (*input* or *output*), and [dec] is the label number.

Recommended Action No action is required.

Error Message ACLMGR-3-UNLOADING: Unloading [chars] label [dec] feature.

Explanation The ACL manager could not load the complete configuration into the hardware, so some features will be applied in the software. Some or all of the packets in a VLAN are forwarded by the CPU. Multicast packets might be dropped entirely instead of being forwarded. [chars] is the direction (*input* or *output*), and [dec] is the label number.

Recommended Action Use a simpler configuration. Use the same ACLs on multiple interfaces, if possible.

AUTHMGR Messages

Error Message AUTHMGR-7-STOPPING: Stopping '[chars]' for client [enet] on Interface [chars] AuditSessionID [chars]

Explanation The authentication process has been stopped. The first [chars] is the authentication method, [enet] is the Ethernet address of the host, the second [chars] is the interface for the host, and the third [chars] is the session ID.

Recommended Action No action is required.

Error Message AUTHMGR-5-MACMOVE: MAC address ([enet]) moved from Interface [chars] to Interface [chars]

Explanation The client moved to a new interface but did not log off from the first interface. [enet] is the MAC address of the client, the first [chars] is the earlier interface, and the second [chars] is the newer interface.

Recommended Action No action is required.

Error Message AUTHMGR-5-MACREPLACE: MAC address ([enet]) on Interface [chars] is replaced by MAC ([enet])

Explanation A new client has triggered a violation that caused an existing client to be replaced. The first [enet] is the first client, [chars] is the interface, the second [enet] is the new client.

Recommended Action No action is required.

Error Message AUTHMGR-5-SECURITY_VIOLATION: Security violation on the interface [chars], new MAC address ([enet]) is seen. AuditSessionID [chars]

Explanation Interface host mode limits the number of hosts that can be attached to an interface. The limit was exceeded and caused a security violation. The interface is error disabled.. The first [chars] is the interface, [enet] is the host MAC address, and the second [chars] is the session ID.

Recommended Action Reconfigure the interface to support the number of attached hosts. Enter the **shutdown** interface configuration command and then the **no shutdown** interface configuration command to re-enable the interface.

Error Message AUTHMGR-5-VLANASSIGN: VLAN [dec] assigned to Interface [chars] AuditSessionID [chars]

Explanation A VLAN was assigned. [dec] is the VLAN ID, the first [chars] is the interface, and the second [chars] is the session ID.

Recommended Action No action is required.

Error Message AUTHMGR-7-FAILOVER: Failing over from [chars] for client ([chars]) on Interface [chars] AuditSessionID [chars]

Explanation The authorization manager is failing over from the current authentication method to another method. The first [chars] is the current authentication method, the second [chars] is the client ID, the third [chars] is the interface, and the fourth [chars] is the session ID.

Recommended Action No action is required.

Error Message AUTHMGR-7-NOMOREMETHODS: Exhausted all authentication methods for client ([chars]) on Interface [chars] AuditSessionID [chars]

Explanation All available authentication methods have been tried. The first [chars] is the client identifier, the second [chars]s is the interface for the client, and the third [chars] is the session ID.

Recommended Action No action is required.

Error Message AUTHMGR-7-RESULT: Authentication result [chars] from [chars] for client [chars] on Interface [chars] AuditSessionID [chars]

Explanation Authentication results: the first [chars] is the authentication status, the second [chars] is the authentication method, the third [chars] is the client ID, the fourth [chars] is the interface, and the fifth [chars] is the session ID.

Recommended Action No action is required.

BACKUP_INTERFACE Messages

Error Message BACKUP_INTERFACE-5-VLB_NON_TRUNK: Warning: Flexlink VLB is not allowed on non-trunk ports. Please configure [chars] to be a trunk port.

Explanation Flex Link VLAN load-balancing (VLB) detected a nontrunk port. [chars] is the interface name.

Recommended Action Change the interface to trunking mode.

BADTRANSCEIVER Messages

Error Message BADTRANSCEIVER, PHY, LOG_WARNING: An inappropriate transceiver has been inserted in interface [chars].

Explanation A defective module is installed in the specified interface. [chars] is the interface.

Recommended Action Remove the transceiver. If it was purchased from Cisco, contact your Cisco representative to have the transceiver replaced.

BSPATCH Messages

Error Message BSPATCH-1-RELOAD: System will reboot to activate newly patched Boot Loader.

Explanation The switch automatically reboots after the boot loader is patched.

Recommended Action If this message recurs, copy it exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message BSPATCH-1-PATCHED: Boot Loader patch ([chars]) installed.

Explanation A boot loader patch installed successfully. [chars] is the SDRAM refresh timer register setting.

Recommended Action If this message recurs, copy it exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message BSPATCH-3-FAILED: Failed to install Boot Loader patch ([chars]).

Explanation The switch did not apply a boot loader patch. [chars] is the SDRAM refresh timer register setting.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

CMP Messages

Error Message CMP-4-MEM_CMPIP_ADDR_CONFLICT: Conflict with CMP IP address [IP_address], Reissuing a new CMP IP address to member [dec]

Explanation The cluster commander found a conflict with the assigned CMP IP address of the member. A new unique CMP IP address is assigned to the member. [dec] is the member number.

Recommended Action This is only a warning message. The commander has already assigned the cluster member a new unique address. Clear any open TCP connections on the member by using **clear tcp** privileged EXEC command.

Error Message CMP-5-ADD: The Device is added to the cluster (Cluster Name: [chars], CMDR IP Address [IP_address]).

Explanation The device is added to the cluster. [chars] is the cluster name, and [IP_address] is the Internet address of the command switch.

Recommended Action No action is required.

Error Message CMP-5-MEMBER_CONFIG_UPDATE: Received member configuration from member [dec].

Explanation The active or standby command switch received a member configuration. [dec] is the member number of the sender.

Recommended Action No action is required.

Error Message CMP-5-MGMT_VLAN_CHNG: The management vlan has been changed to [dec].

Explanation The management VLAN has changed. [dec] is the new management VLAN number.

Recommended Action No action is required.

Error Message CMP-5-NBR_UPD_SIZE_TOO_BIG: Number of neighbors in neighbor update is [int], maximum number of neighbors allowed in neighbor update is [int].

Explanation The number of cluster neighbors in the clustering neighbor update packet exceeds the number of neighbors supported by the clustering module. The first [int] is the new number of neighbors, and the second [int] the maximum number of neighbors.

Recommended Action No action is required.

Error Message CMP-5-REMOVE: The Device is removed from the cluster (Cluster Name: [chars]).

Explanation The device is removed from the cluster. [chars] is the cluster name.

Recommended Action No action is required.

DHCP_SNOOPING Messages

This section contains the DHCP snooping messages.

Error Message DHCP_SNOOPING-3-DHCP_SNOOPING_INTERNAL_ERROR: DHCP Snooping internal error, [chars].

Explanation A software sanity check failed in the DHCP snooping process. [chars] is the error.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message DHCP_SNOOPING-4-AGENT_OPERATION_FAILED: DHCP snooping binding transfer failed. [chars].

Explanation The DHCP snooping binding transfer process failed. [chars] is the reason the process failed.

Recommended Action No action is required.

Error Message DHCP_SNOOPING-4-AGENT_OPERATION_FAILED_N: DHCP snooping binding transfer failed ([dec]). [chars].

Explanation The DHCP snooping binding transfer process failed. [dec] is the number of times the process failed, and [chars] is the reason the process failed. This message is rate-limited.

Recommended Action No action is required.

Error Message DHCP_SNOOPING-4-DHCP_SNOOPING_ERRDISABLE_WARNING: DHCP Snooping received [dec] DHCP packets on interface [chars].

Explanation The switch detected a DHCP packet rate-limit violation on the specified interface and put the interface in the error-disabled state. [dec] is the number of DHCP packets, and [chars] is the interface.

Recommended Action No action is required.

Error Message DHCP_SNOOPING-4-DHCP_SNOOPING_PVLAN_WARNING: DHCP Snooping configuration may not take effect on secondary vlan [dec]. [chars]

Explanation If private VLANs are configured, the DHCP Snooping configuration on the primary VLAN automatically propagates to all the secondary VLANs. [dec] is the VLAN IDs of the secondary VLANs, and [chars] is the warning.

Recommended Action No action is required.

Error Message DHCP_SNOOPING-4-IP_SOURCE_BINDING_PVLAN_WARNING: IP source filter may not take effect on secondary vlan [dec] where IP source binding is configured. [chars].

Explanation If private VLANs are configured, the IP-source-guard filter on the primary VLAN automatically propagates to all secondary VLANs. [dec] is the secondary VLAN, and [chars] is the warning.

Recommended Action No action is required.

Error Message DHCP_SNOOPING-4-IP_SOURCE_BINDING_NON_EXISTING_VLAN_WARNING: IP source binding is configured on non existing vlan [dec].

Explanation An IP source binding was configured on a VLAN that has not been configured yet. [dec] is the VLAN.

Recommended Action No action is required.

Error Message DHCP_SNOOPING-4-NTP_NOT_RUNNING: NTP is not running; reloaded binding lease expiration times are incorrect.

Explanation If the DHCP snooping database agent loads the DHCP snooping bindings and Network Time Protocol (NTP) is not running, the calculated lease duration for the bindings is incorrect.

Recommended Action Configure NTP on the switch to provide an accurate time and date for the system clock. Then disable and re-enable DHCP snooping to clear the DHCP snooping binding database.

Error Message DHCP_SNOOPING-4-QUEUE_FULL: Fail to enqueue DHCP packet into processing queue: [chars], the queue is most likely full and the packet will be dropped.

Explanation The CPU is receiving DHCP packets at a higher rate than the DHCP snooping process can handle. These DHCP packets are dropped to prevent a denial of service attack. [chars] is the warning.

Recommended Action No action is required.

Error Message DHCP_SNOOPING-4-STANDBY_AGENT_OPERATION_FAILED: DHCP snooping binding transfer failed on the Standby Supervisor. [chars].

Explanation The DHCP snooping binding transfer process failed on a standby supervisor engine. [chars] is the standby supervisor engine.

Recommended Action No action is required.

Error Message DHCP_SNOOPING-6-AGENT_OPERATION_SUCCEEDED: DHCP snooping database [chars] succeeded.

Explanation The DHCP binding transfer process succeeded. [chars] is the DHCP snooping database.

Recommended Action No action is required.

Error Message DHCP_SNOOPING-6-BINDING_COLLISION: Binding collision. [dec] bindings ignored.

Explanation The specified number of bindings were ignored when the switch read the database file. The bindings from the database file have MAC address and VLAN information that a configured DHCP snooping binding already uses.

Recommended Action No action is required.

Error Message DHCP_SNOOPING-6-INTERFACE_NOT_VALID: Interface not valid. [dec] bindings ignored.

Explanation The specified number of bindings were ignored when the switch read the database file because the interface in binding database is not available, the interface is a routed port, or the interface is a DHCP snooping-trusted Layer 2 interface. [dec] is the number of bindings that the switch ignores.

Recommended Action No action is required.

Error Message DHCP_SNOOPING-6-LEASE_EXPIRED: Lease Expired. [dec] bindings ignored.

Explanation The specified number of bindings were ignored when the switch read the database file because the DHCP lease expired. [dec] is the number of bindings.

Recommended Action No action is required.

Error Message DHCP_SNOOPING-6-PARSE_FAILURE: Parsing failed for [dec] bindings.

Explanation The specified number of bindings were ignored when the switch read the database file because the database read operation failed. [dec] is the number of bindings.

Recommended Action No action is required.

Error Message DHCP_SNOOPING-6-VLAN_NOT_SUPPORTED: Vlan not supported. [dec] bindings ignored.

Explanation The specified number of bindings were ignored when the switch read the database file because VLAN is no longer configured on the switch. [dec] is the number of bindings that the switch ignores.

Recommended Action No action is required.

DOT1Q Tunneling Messages

Error Message DOT1Q_TUNNELING-4-MTU_WARNING: System MTU of [dec] might be insufficient for 802.1Q tunnelling. 802.1Q tunnelling requires system MTU size of [dec] to handle maximum size ethernet frames.

Explanation The switch MTU setting might not be sufficient for 802.1Q tunneling. The MTU needs to include the 4-byte overhead associated with the additional 802.1Q tag. The first [dec] is the current system MTU setting in bytes, and the second [dec] is the required MTU size in bytes.

Recommended Action Adjust the system MTU for the additional 802.1Q tag by using the **system mtu** global configuration command, and reload the switch by using the **reload** privileged EXEC command.

DOT1X Messages

Error Message DOT1X-5-FAIL: Authentication failed for client ([chars]) on Interface [chars] AuditSessionID [chars]

Explanation Authentication was not successful. The first [chars] is the client ID, the second [chars] is the interface, and the third [chars] is the session ID.

Recommended Action No action is required.

Error Message DOT1X-5-RESULT_OVERRIDE: Authentication result overridden for client ([chars]) on Interface [chars] AuditSessionID [chars]

Explanation The authentication result was overridden. The first [chars] is the client ID, the second [chars] is the interface, and the third [chars] is the session ID.

Recommended Action No action is required.

Error Message DOT1X-5-SUCCESS: Authentication successful for client ([chars]) on Interface [chars] AuditSessionID [chars]

Explanation Authentication was successful. The first [chars] is the client ID, the second [chars] is the interface, and the third [chars] is the session ID.

Recommended Action No action is required.

Error Message DOT1X-4-MEM_UNAVAIL: Memory was not available to perform the 802.1X action. AuditSessionID [chars]

Explanation The switch does not have enough memory to run 802.1x authentication. [chars] is the session ID.

Recommended Action Reconfigure the switch to reduce memory usage.

Error Message DOT1X-4-MSG_ERR: Unknown message event received.

Explanation The 802.1x process received an unknown message event.

Recommended Action Enter the **dot1x system-auth-control** global configuration command, and restart the 802.1x process. If this message recurs, reload the device.

Error Message DOT1X-4-PROC_START_ERR: Dot1x unable to start.

Explanation The system did not create the 802.1x process.

Recommended Action Enter the **dot1x system-auth-control** global configuration command to restart 802.1x. Then reload the device.

Error Message DOT1X-4-UNKN_ERR: An unknown operational error occurred.

Explanation The 802.1x process cannot operate because of an internal system error.

Recommended Action No action is required.

Error Message DOT1X-5-ERR_CHANNELLING: Dot1x can not be enabled on Channelling ports.

Explanation 802.1x could not be enabled on the channeling port. An attempt was made to set 802.1x port-control to auto or force-unauthorized mode on a channeling port, which is not allowed.

Recommended Action Disable channeling on the interface, and then enable 802.1x.

Error Message DOT1X-5-ERR_DYNAMIC: Dot1x can not be enabled on Dynamic ports.

Explanation 802.1x could not be enabled on the dynamic mode port. An attempt to set 802.1x port-control to auto or force-unauthorized mode on a dynamic mode port, which is not allowed.

Recommended Action Disable dynamic mode on the interface, and then enable 802.1x.

Error Message DOT1X-5-ERR_DYNAMIC_VLAN: Dot1x can not be enabled on Dynamic VLAN ports.

Explanation 802.1x could not be enabled on the dynamic VLAN port. An attempt to set 802.1x port-control to auto or force-unauthorized mode on a dynamic VLAN port, which is not allowed, causes this condition.

Recommended Action Disable dynamic VLAN configuration on the interface, and enable 802.1x.

Error Message DOT1X-5-ERR_INVALID_TUNNEL_MEDIUM_TYPE: Got an invalid value [chars] for TUNNEL_MEDIUM_TYPE [chars].

Explanation The provided tunnel medium is either unsupported or invalid. [chars] is the text received from the RADIUS server.

Recommended Action Change the value to a valid tunnel medium.

Error Message DOT1X-5-ERR_INVALID_TUNNEL_TYPE: Got an invalid value of [chars] for TUNNEL_TYPE [chars].

Explanation The provided tunnel type is either unsupported or invalid. [chars] is the text received from the RADIUS server.

Recommended Action Change the value to a valid tunnel type.

Error Message DOT1X-5-ERR_MULTI_ACCESS: Dot1x can not be enabled on voice vlan configured ports.

Explanation 802.1x could not be enabled on a voice VLAN-configured port. An attempt to set 802.1x port-control to auto or force-unauthorized mode on a voice VLAN-configured port, which is not allowed, causes this condition.

Recommended Action Disable the voice VLAN on the interface, and enable 802.1x.

Error Message DOT1X-5-ERR_PROTO_TUNNELLING: Dot1x can not be enabled on protocol tunnelling enabled ports.

Explanation 802.1x could not be enabled on the protocol-tunneling-enabled port. An attempt to set 802.1x port-control to auto or force-unauthorized mode on a protocol-tunneling-enabled port, which is not allowed, causes this condition.

Recommended Action Change the voice VLAN or the access VLAN on the interface, and then enable 802.1x.

Error Message DOT1X-5-ERR_PVLAN_EQ_VVLAN: Dot1x can not be enabled on a port with Access VLAN equal to Voice VLAN.

Explanation 802.1x could not be enabled on a port because the configured data VLAN on the port is the same as the voice VLAN. An attempt to set 802.1x port-control to auto or force-unauthorized mode on a voice VLAN port that is the same as the data VLAN port, which is not allowed, causes this condition.

Recommended Action Change the voice VLAN or access VLAN on the interface, and try again to enable 802.1x on the port.

Error Message DOT1X-5-ERR_PVLAN_TRUNK: Dot1x can not be enabled on private VLAN trunk ports.

Explanation 802.1x could not be enabled on private VLAN ports on which trunking is enabled.

Recommended Action No action is required.

Error Message DOT1X-5-ERR_RADIUSVLAN_EQ_VVLAN: RADIUS attempted to assign a VLAN to Dot1x port [chars] whose Voice VLAN is same as AccessVlan.

Explanation The RADIUS server attempted to assign a VLAN to a supplicant on a port with a voice VLAN that is equal to the access VLAN. [chars] is the port number.

Recommended Action Either update the RADIUS configuration to not assign the VLAN equal to the voice VLAN, or change the voice VLAN on this port.

Error Message DOT1X-5-ERR_RSPAN_VLAN: Dot1x can not be enabled on ports configured in Remote SPAN vlan.

Explanation 802.1x could not be enabled on the remote Switched Port Analyzer (SPAN) VLAN port. An attempt to set 802.1x port-control to auto or force-unauthorized mode on a port that is in a remote SPAN VLAN, which is not allowed, causes this condition.

Recommended Action Disable the remote SPAN on the VLAN, and enable 802.1x.

Error Message DOT1X-5-ERR_SPANDST: Dot1x can not be enabled on [chars]. It is configured as a SPAN Best port.

Explanation 802.1x cannot be enabled on a port that is a SPAN destination port because these features are mutually exclusive. [chars] is the port.

Recommended Action Remove the SPAN destination port from the SPAN session before reconfiguring 802.1x on the port.

Error Message DOT1X-5-ERR_TRUNK: Dot1x can not be enabled on Trunk port.

Explanation 802.1x could not be enabled on the trunk port. An attempt to set 802.1x port-control to auto or force-unauthorized mode on a trunk port, which is not allowed, causes this condition.

Recommended Action Disable trunking on the interface, and then enable 802.1x.

Error Message DOT1X-5-ERR_TUNNEL: Dot1x can not be enabled on 802.1q tunnelling enabled ports.

Explanation 802.1x could not be enabled on the 802.1Q tunneling-enabled port. An attempt to set 802.1x port-control to auto or force-unauthorized mode on a 802.1Q tunneling-enabled port, which is not allowed, causes this condition.

Recommended Action Disable 802.1Q tunneling on the interface, and enable 802.1x.

Error Message DOT1X-5-ERR_VLAN_INTERNAL: The VLAN [dec] is being used internally and cannot be assigned for use on the Dot1x port [chars] Vlan.

Explanation The VLAN is used internally and cannot be assigned again for use on this port. [dec] is the VLAN ID, and [chars] is the port number.

Recommended Action Assign a different VLAN.

Error Message DOT1X-5-ERR_VLAN_INVALID: The VLAN [dec] is invalid and cannot be assigned for use on the 802.1x port [chars] Vlan.

Explanation The specified VLAN is out of range and cannot be assigned for use on this port. [dec] is the VLAN ID, and [chars] is the port number.

Recommended Action Use a valid VLAN.

Error Message DOT1X-5-ERR_VLAN_NOT_ASSIGNABLE: RADIUS tried to assign a VLAN to dot1x port [chars] whose VLAN cannot be assigned.

Explanation The RADIUS server tried to assign a VLAN to a supplicant on a port whose VLAN cannot be changed, such as a routed port. [chars] is the port number.

Recommended Action There is no recommended action.

Error Message DOT1X-5-ERR_VLAN_NOT_FOUND: Attempt to assign non-existent [chars] VLAN [chars] to dot1x port [chars].

Explanation An attempt to assign a VLAN to a supplicant on a port failed because the VLAN was not found in the VLAN Trunking Protocol (VTP) database. [chars] is the port number.

Recommended Action Make sure that the VLAN exists, or use another VLAN.

Error Message DOT1X-5-ERR_VLAN_RESERVED: The VLAN [dec] is a reserved vlan and cannot be assigned for use on the Dot1x port [chars] Vlan.

Explanation The VLAN specified is a reserved VLAN and cannot be assigned for use on this port. [dec] is the VLAN ID, and [chars] is the port number.

Recommended Action Assign a different VLAN.

Error Message DOT1X-5-ERR_VLAN_RSPAN_CONFIGURED: VLAN [dec] is configured as a Remote SPAN VLAN, which has Dot1x enabled interface(s) configured. Please disable Dot1x on all ports in this VLAN or do not enable RSPAN on this VLAN.

Explanation Remote SPAN should not be enabled on a VLAN with 802.1x-enabled interfaces. [dec] is the VLAN ID.

Recommended Action Either disable the RSPAN configuration on the VLAN, or disable 802.1x on all interfaces in this VLAN.

Error Message DOT1X-5-ERR_VVID_NOT_SUPPORTED: Dot1x can not be enabled on this port with Voice VLAN configured.

Explanation 802.1x and voice VLAN cannot be configured on the same port.

Recommended Action Remove the voice VLAN configuration on the port, and retry the 802.1x authentication process.

Error Message DOT1X-5-INVALID_MAC: Invalid MAC address (zero, broadcast or multicast mac address [chars] is trying to authenticate).

Explanation An authentication was attempted for a zero, broadcast, or multicast MAC address using 802.1x. 802.1x authentication is allowed only for a valid nonzero, nonbroadcast, or nonmulticast source MAC address. [chars] is the MAC address.

Recommended Action Connect a 802.1x-supported host to the 802.1x-enabled port.

Error Message DOT1X-5-NO_UNIDIR_EDGE: Unidirectional port-control is configured on interface [chars], but will not be activated. Port is not configured for portfast.

Explanation The unidirectional port-control feature is configured but will not be activated because the specified port is not configured as a PortFast port. [chars] is the name of the specified port.

Recommended Action To activate the unidirectional port-control feature, enter the **spanning-tree portfast** interface configuration command.

Error Message DOT1X-5-NO_UNIDIR_MULTIAUTH: Unidirectional port-control is configured on interface [chars], but will not be activated. Port is in multi-auth mode.

Explanation The unidirectional port-control feature is configured but will not be activated because the specified port is configured in multi-auth mode. [chars] is the interface number.

Recommended Action To activate the unidirectional port-control feature, enter the **dot1x host-mode** interface configuration command to change the mode.

Error Message DOT1X-5-NOT_DOT1X_CAPABLE: Dot1x disabled on interface [chars] because it is not an Ethernet interface.

Explanation 802.1x authentication is disabled on the interface because it is not an Ethernet interface. [chars] is the interface.

Recommended Action Enable 802.1x authentication only on Ethernet interfaces.

DOT1X_SWITCH Messages

Error Message DOT1X_SWITCH-5-ERR_ADDING_ADDRESS: Unable to add address [enet] on [chars] AuditSessionID [chars]

Explanation The client MAC address could not be added to the MAC address table because the hardware memory is full or because the address is a secure address on another port. This message might appear if 802.1x is enabled. [enet] is the client MAC address, the first [chars] is the interface, and the second [chars] is the session ID.

Recommended Action If hardware memory is full, remove some of the dynamic MAC addresses. If the client address is on another port, remove it from that port.

Error Message DOT1X_SWITCH-5-ERR_INVALID_PRIMARY_VLAN: Attempt to assign primary VLAN [dec] to 802.1x port [chars] AuditSessionID [chars]

Explanation An attempt was made to assign a primary VLAN to an 802.1x port. This is not allowed. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Assign a different VLAN.

Error Message DOT1X_SWITCH-5-ERR_INVALID_SEC_VLAN: Attempt to assign invalid secondary VLAN [dec] to PVLAN host 802.1x port [chars] AuditSessionID [chars]

Explanation An attempt was made to assign a nonsecondary VLAN to a private VLAN host 802.1x port. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Change the port mode so that it is no longer a private VLAN host port, or use a valid secondary VLAN.

Error Message DOT1X_SWITCH-5-ERR_PRIMARY_VLAN_NOT_FOUND: Attempt to assign VLAN [dec], whose primary VLAN does not exist or is shutdown, to 802.1x port [chars] AuditSessionID [chars]

Explanation An attempt was made to assign a private VLAN whose primary VLAN does not exist or is shut down. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Check that the primary VLAN exists and is not shut down. Check that the private VLAN is associated with a primary VLAN.

Error Message DOT1X_SWITCH-5-ERR_RADIUS_VLAN_NOT_FOUND: Attempt to assign non-existent VLAN [chars] to dot1x port [chars]

Explanation RADIUS attempted to assign a VLAN with a particular name or ID to a supplicant on a port but the name or ID could not be found on the switch. [dec] is the VLAN, and [chars] is the port.

Recommended Action Check that a VLAN with the specified name or ID exists on the switch.

Error Message DOT1X_SWITCH-5-ERR_SEC_VLAN_INVALID: Attempt to assign secondary VLAN [dec] to non-PVLAN host 802.1x port [chars] AuditSessionID [chars]

Explanation An attempt was made to assign a secondary VLAN to a port that is not a private VLAN host port. This is not allowed. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Change the port mode so that it is configured as a private VLAN host port, or use a different VLAN that is not configured as a secondary VLAN..

Error Message DOT1X_SWITCH-5-ERR_SPAN_DST_PORT: Attempt to assign VLAN [dec] to 802.1x port [chars], which is configured as a SPAN destination AuditSessionID [chars]

Explanation An attempt was made to assign a VLAN to an 802.1x port that is configured as a Switched Port Analyzer (SPAN) destination port. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Change the SPAN configuration so that the port is no longer a SPAN destination port, or change the configuration so that no VLAN is assigned.

Error Message DOT1X_SWITCH-5-ERR_VLAN_EQ_MDA_INACTIVE: Multi-Domain Authentication cannot activate because Data and Voice VLANs are the same on port AuditSessionID [chars]

Explanation Multi-Domain Authentication (MDA) host mode cannot start when the configured data VLAN on a port is the same as the voice VLAN. [chars] is the port session ID.

Recommended Action Change either the voice VLAN or the access VLAN on the interface so that they are not the same. MDA then starts.

Error Message DOT1X_SWITCH-5-ERR_VLAN_EQ_VVLAN: Data VLAN [dec] on port [chars] cannot be equivalent to the Voice VLAN AuditSessionID [chars]

Explanation An attempt was made to assign a data VLAN to an 802.1x port that is the same as the voice VLAN. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Change either the voice VLAN or the 802.1x-assigned VLAN on the interface so that they are not the same.

Error Message DOT1X_SWITCH-5-ERR_VLAN_INTERNAL: Attempt to assign internal VLAN [dec] to 802.1x port [chars] AuditSessionID [chars]

Explanation An attempt was made to assign an invalid VLAN to an 802.1x port. The VLAN specified is used internally and cannot be assigned to this port. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Assign a different VLAN.

Error Message DOT1X_SWITCH-5-ERR_VLAN_INVALID: Attempt to assign invalid VLAN [dec] to 802.1x port [chars] AuditSessionID [chars]

Explanation An attempt was made to assign an invalid VLAN to an 802.1x port. The VLAN specified is out of range. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Change the configuration to use a valid VLAN.

Error Message DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND: Attempt to assign non-existent or shutdown VLAN [chars] to 802.1x port [chars] AuditSessionID [chars]

Explanation An attempt was made to assign a VLAN to an 802.1x port, but the VLAN was not found in the VLAN Trunking Protocol (VTP) database. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Check that the VLAN exists and is not shut down, or use another VLAN.

Error Message DOT1X_SWITCH-5-ERR_VLAN_ON_ROUTED_PORT: Attempt to assign VLAN [dec] to routed 802.1x port [chars] AuditSessionID [chars]

Explanation An attempt was made to assign a VLAN to a supplicant on a routed port. This is not allowed. [dec] is the VLAN ID, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Either disable the VLAN assignment or change the port type to a nonrouted port.

Error Message DOT1X_SWITCH-5-ERR_VLAN_PROMISC_PORT: Attempt to assign VLAN [dec] to promiscuous 802.1x port [chars] AuditSessionID [chars]

Explanation An attempt was made to assign a VLAN to a promiscuous 802.1x port. This is not allowed. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Change the port mode so that it is no longer a promiscuous port or change the configuration so that no VLAN is assigned.

Error Message DOT1X_SWITCH-5-ERR_VLAN_RESERVED: Attempt to assign reserved VLAN [dec] to 802.1x port [chars] AuditSessionID [chars]

Explanation An attempt was made to assign an invalid VLAN to an 802.1x port. The VLAN specified is a reserved VLAN and cannot be assigned to this port. [dec] is the VLAN, the first [chars] is the port, and the seconds [chars] is the session ID.

Recommended Action Assign a different VLAN.

Error Message DOT1X_SWITCH-5-ERR_VLAN_RSPAN: Attempt to assign RSPAN VLAN [dec] to 802.1x port [chars]. 802.1x is incompatible with RSPAN AuditSessionID [chars]

Explanation Remote SPAN should not be enabled on a VLAN with 802.1x-enabled. [dec] is the VLAN, the first [chars] is the port, and the second [chars] is the session ID.

Recommended Action Either disable remote SPAN configuration on the VLAN or disable 802.1x on all the ports in this VLAN.

DTP Messages

Error Message DTP-4-MEM_UNAVAIL: Memory was not available to perform the trunk negotiation action.

Explanation The system is unable to negotiate trunks because of a lack of memory.

Recommended Action Reduce other system activity to ease memory demands.

Error Message DTP-4-TMRERR: An internal timer error occurred when trunking on interface [chars].

Explanation A timer used by the trunking protocol unexpectedly expired. [chars] is the trunked interface.

Recommended Action This problem is corrected internally and has no long-term ramifications. However, if more problems with trunking occur, reload the switch by using the **reload** privileged EXEC command.

Error Message DTP-4-UNKN_ERR: An unknown operational error occurred.

Explanation The system is unable to negotiate trunks because an internal operation generated an unexpected error.

Recommended Action Reload the switch by using the **reload** privileged EXEC command.

Error Message DTP-5-DOMAINMISMATCH: Unable to perform trunk negotiation on port [chars] because of VTP domain mismatch.

Explanation The two ports in the trunk negotiation belong to different VTP domains. Trunking can be configured only when the ports belong to the same VTP domain. [chars] is the port number.

Recommended Action Ensure that the ports in the trunk negotiation belong to the same VTP domain.

Error Message DTP-5-ILGLCFG: Illegal config (on, isl--on,dot1q) on [chars].

Explanation One end of the trunk link is configured as *on* with Inter-Switch Link (ISL) encapsulation and that the other end is configured as *on* with 802.1Q encapsulation. [chars] is the interface.

Recommended Action This configuration is illegal and will not establish a trunk between two switches. You must change the encapsulation type so that both ends of the trunk match.

Error Message DTP-5-NONTRUNKPORTON: Port [chars] has become non-trunk.

Explanation The interface changed from a trunk port to an access port. [chars] is the interface that changed.

Recommended Action No action is required.

Error Message DTP-5-TRUNKPORTCHG: Port [chars] has changed from [chars] trunk to [chars] trunk.

Explanation The encapsulation type of the trunk port has changed. The first [chars] is the interface, the second [chars] is the original encapsulation type, and the third [chars] is the new encapsulation type.

Recommended Action No action is required.

Error Message DTP-5-TRUNKPORTON: Port [chars] has become [chars] trunk.

Explanation The interface has changed from an access port to a trunk port. The first [chars] is the interface, and the second [chars] is the encapsulation type.

Recommended Action No action is required.

EC Messages

Error Message EC-4-NOMEM: Not enough memory available for [chars].

Explanation The LACP or the PAgP EtherChannel could not obtain the memory it needed to initialize the required data structures. [chars] is the data structure name.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message EC-4-NOMEMORINCOMPAT: Allocation of the [chars] failed.

Explanation The system could not obtain the required memory, or the operation was not allowed by the system. [chars] is the name of the data structure that cannot be allocated.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message EC-4-SSOINCOMPAT: Routed port channels cannot be created while the switch is configured in the SSO redundancy mode.

Explanation Routed-Port Channels are not supported when the switch is configured in stateful switchover (SSO) redundancy mode.

Recommended Action Switch to route processor redundancy (RPR) mode, or use a switch virtual interface (SVI) in a VLAN where a Layer 2 PortChannel is the only member.

Error Message EC-5-BUNDLE: Interface [chars] joined port-channel [chars].

Explanation The listed interface joined the specified EtherChannel. The first [chars] is the physical interface, and the second [chars] is the EtherChannel interface.

Recommended Action No action is required.

Error Message EC-5-DONTBNL: [chars] suspended: incompatible remote port with [chars]

Explanation The configuration of the remote port is different from the configuration of other remote ports in the bundle. A port can only join the bundle when the configuration of the local port and the configuration of the remote port are the same as other ports already in the bundle. The first [chars] is the name of the local interface that is being suspended, and the second [chars] is the name of the local interface that is already bundled.

Recommended Action Make sure that the configuration of the remote ports is the same for all ports in the bundle.

Error Message EC-5-CANNOT_ALLOCATE_AGGREGATOR: Aggregator limit reached, cannot allocate aggregator for group [dec].

Explanation A new aggregator cannot be allocated in the group. [dec] is the affected group.

Recommended Action Change the port attributes of the ports in the group so that they match and join the same aggregator.

Error Message EC-5-CANNOT_BUNDLE1: Port-channel [chars] is down, port [chars] will remain stand-alone.

Explanation The aggregation port is down. The port remains standalone until the aggregation port is up. The first [chars] is the EtherChannel, and the second [chars] is the port number.

Recommended Action Ensure that the other ports in the bundle have the same configuration.

Error Message EC-5-CANNOT_BUNDLE2: [chars] is not compatible with [chars] and will be suspended ([chars]).

Explanation The interface has different interface attributes than other ports in the EtherChannel. For the interface to join the bundle (EtherChannel), change the interface attributes to match the EtherChannel attributes. The first [chars] is the interface to be bundled, the second [chars] is the physical interface (a switch port or a routed port) that is already in the bundle, and the third [chars] is the reason for the incompatibility.

Recommended Action Change the interface attributes to match the EtherChannel attributes.

Error Message EC-5-CANNOT_BUNDLE_LACP: [chars] is not compatible with aggregators in channel [dec] and cannot attach to them ([chars]).

Explanation The port has different port attributes than the port channel or ports within the port channel. [chars] is the incompatible port, [dec] is the channel group number, and the last [chars] is the reason.

Recommended Action For the port to join the bundle, change the port attributes so that they match the port.

Error Message EC-5-COMPATIBLE: [chars] is compatible with port-channel members.

Explanation A port was not operational because its attributes were different from those of the port channel or ports within the port channel. The system has detected that the attributes of the port now match the port-channel attributes. [chars] is the affected port.

Recommended Action No action is required.

Error Message EC-5-DONTBNDL: [chars] suspended: incompatible partner port with [chars].

Explanation Configuration of the remote port differs from the configuration of other remote ports in the bundle. A port can only join the bundle when its global configuration and the configuration of the remote port are the same as other ports in the bundle. The first [chars] is the suspended local interface, and the second [chars] is the local interface that is already bundled.

Recommended Action Verify that the configuration of the partner ports is the same for all ports in the bundle.

Error Message EC-5-ERRPROT: Channel protocol mismatch for interface [chars] in group [dec]: the interface can not be added to the channel group.

Explanation The interface cannot be added to the channel-group with the specified mode. [chars] is the interface, and [dec] is the channel-group.

Recommended Action Change the channel-group or the mode for the interface.

Error Message EC-5-ERRPROT2: Command rejected: the interface [chars] is already part of a channel with a different type of protocol enabled.

Explanation The interface cannot be selected for the specified protocol because it is already part of a channel with a different protocol. [chars] is the interface.

Recommended Action Remove the interface from the channel group.

Error Message EC-5-ERRPROT3: Command rejected: the interface [chars] is already part of a channel.

Explanation The interface cannot be unselected for the specified protocol because it is already part of a channel group. [chars] is the interface.

Recommended Action Remove the interface from the channel group.

Error Message EC-5-L3DONTBNL1: [chars] suspended: PAgP not enabled on the remote port.

Explanation PAgP is enabled on the Layer 3 interface but the partner port is not enabled for PAgP. In this mode, the port is placed in a suspended state. [chars] is the Layer 3 interface.

Recommended Action Enable PAgP on the remote side by using the **channel-group** interface configuration command.

Error Message EC-5-L3DONTBNL2: [chars] suspended: LACP currently not enabled on the remote port.

Explanation LACP is enabled on a Layer 3 interface but is not enabled on the partner port. In this mode, the port is put in a suspended state. [chars] is the interface name.

Recommended Action Enable LACP on the remote side.

Error Message EC-5-NOLACP: Invalid EC mode, LACP not enabled.

Explanation The EtherChannel mode cannot be set because LACP is not included in the software image.

Recommended Action Install a software image that includes LACP, and set the EC mode to *on*.

Error Message EC-5-NOPAGP: Invalid EC mode, PAgP not enabled.

Explanation PAgP is not included in the Cisco IOS image and the EtherChannel mode cannot be set to **desirable** or **auto**.

Recommended Action Obtain an image with PAgP included, or set the mode to *on* by using the **channel-group** *channel-group-number* **mode on** interface configuration command.

Error Message EC-5-PORTDOWN: Shutting down [chars] as its port-channel is admin-down.

Explanation The administrative state of the port is controlled by the administrative state of its aggregate port. If the administrative state of the aggregate port is down, the administrative state of the port is also forced to be down. [chars] is the physical interface.

Recommended Action Enter the **no shutdown** interface configuration command on the aggregate port to activate the aggregation port.

Error Message EC-5-STAYDOWN: [chars] will remain down as its port-channel [chars] is admin-down.

Explanation The administrative state of the aggregation port overrides that of the affected port. If the aggregation port is administratively down, all ports in the aggregation port are forced to be administratively down. The first [chars] is the physical interface, and the second [chars] is the EtherChannel.

Recommended Action Enter the **no shutdown** interface configuration command on the aggregation port to activate (unshut) the aggregation port.

Error Message EC-5-STAYDOWN: no-shut not allowed on [chars]. Module [dec] not online.

Explanation An interface with an EtherChannel configuration cannot be enabled by using the **no shutdown** interface configuration command because it is a member of an EtherChannel group and that EtherChannel group has been administratively shut down. The interface has an EtherChannel configuration but no information is available yet about its port channel. [chars] is the interface, and [dec] is the module.

Recommended Action No action is required. Wait until the module is online to find out the port-channel setting of the EtherChannel.

Error Message EC-5-UNBUNDLE: Interface [chars] left the port-channel [chars].

Explanation The listed interface left the specified EtherChannel. The first [chars] is the physical interface, which can be a switch port or a routed port, and the second [chars] is the EtherChannel.

Recommended Action No action is required.

Error Message EC-5-UNSUITABLE: [chars] will not join any port-channel, [chars].

Explanation The interfaces cannot join the EtherChannel because it is configured for PortFast, as a VLAN Membership Policy Server (VMPS), for 802.1x, as a voice VLAN, or as a SPAN destination port. All of these are illegal configurations for EtherChannels. The first [chars] is the interface name, and the second [chars] describes the details of the unsuitable configuration.

Recommended Action Reconfigure the port, removing the illegal configuration.

EPM Messages

Error Message EPM-6-AUTH_ACL: POLICY [chars] | EVENT [chars]

Explanation The switch has sent or received a download request for a downloadable ACL (dACL). The first [chars] is the dACL policy, and the second [chars] is the event.

Recommended Action No action is required.

ESF Messages

Error Message ESF_API-3-MTU_SET_FAILED: MTU size of [dec] failed on port [dec]

Explanation An internal error prevents the switch from configuring the jumbo maximum transmission unit (MTU) setting on the enhanced-services ports. The first [dec] is the MTU size, and the second [dec] is the port number.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still need assistance, open a case with the TAC, or provide your Cisco technical support representative with your information.

ETHCNTR Messages

Error Message ETHCNTR-3-HALF_DUX_COLLISION_EXCEED_THRESHOLD: Collision at [chars] exceed threshold. Consider as loop-back.

Explanation The collisions on a half-duplex port exceeded the threshold, and the port is treated as a loopback. [chars] is the port where the threshold was exceeded.

Recommended Action No action is required. The port is error disabled until the problem is resolved.

Error Message ETHCNTR-3-LOOP_BACK_DETECTED: , Loop-back detected on [chars]. The port is forced to linkdown.

Explanation A keepalive packet was looped back to the port that sent the keepalive. The loopback condition might be caused by a balun cable being accidentally connected to the port, or there might be a loop in the network. [chars] is the port.

Recommended Action Examine the cables. If a balun cable is connected, and the loopback condition is desired, no action is required. Otherwise, connect the correct cable, and bring the port up by entering the **no shutdown** interface configuration command. We do not recommend using the **no keepalive** interface command to disable keepalives. The cause of this network loop must be found and corrected. Although disabling keepalives prevents the port from being error disabled, it does not resolve the cause of the problem and can affect network stability. See CSCe46385 for more information.

Error Message ETHCNTR-3-NO_HARDWARE_RESOURCES: Not enough hardware resources. Shutting down [chars].

Explanation Too many VLANs and routed ports are configured. [chars] is the short interface name, such as Gi1/0/1, or the VLAN name, such as VLAN0002.

Recommended Action Reduce the total number of VLANs and routed ports to less than 1023. To preserve configuration and connections across reboots, save the configuration.

EXPRESS_SETUP Messages

Error Message EXPRESS_SETUP-3-UNABLE_TO_RESET_CONFIG: [chars].

Explanation The system cannot reset the configuration. [chars] is a text string that explains why the reset failed. For example, error renaming config file, error removing config file, or error removing private config file.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message EXPRESS_SETUP-6-CONFIG_IS_RESET: [chars].

Explanation The configuration is reset. [chars] is a text message that clarifies the reset event, such as The configuration is reset and the system will now reboot.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message EXPRESS_SETUP-6-MODE_ENTERED.

Explanation The Express Setup mode is active.

Recommended Action No action is required.

Error Message EXPRESS_SETUP-6-MODE_EXITED.

Explanation The Express Setup mode is no longer active.

Recommended Action No action is required.

FRNTEND_CTRLR Messages

Error Message FRNTEND_CTRLR-1-MGR_TXQ_FULL: The front end controller Tx queue reached watermark level

Explanation There are too many messages in the queue between the front-end controller and the switch software.

Recommended Action Try reloading the switch. If this does not resolve the issue, this might be a hardware problem. Contact the Cisco technical support representative.

GBIC_SECURITY Messages



Note

The Catalyst 3750 Metro switch supports SFP modules and does not support GBIC modules. Although the error message text refers to GBIC interfaces and modules, on the Catalyst 3750 Metro switch, the messages actually refer to the SFP interfaces and modules.

Error Message GBIC_SECURITY-4-EEPROM_CRC_ERR: EEPROM checksum error for GBIC in [chars].

Explanation The GBIC in the specified port has invalid EEPROM data. [chars] is the port in which the GBIC is inserted.

Recommended Action Remove the GBIC from the port.

Error Message GBIC_SECURITY-4-EEPROM_READ_ERR: Error in reading GBIC serial ID in [chars].

Explanation An error occurred while the switch was reading the GBIC type from the EEPROM. [chars] is the port in which the GBIC is inserted.

Recommended Action Remove the GBIC from the port.

Error Message GBIC_SECURITY-4-EEPROM_SECURITY_ERR: GBIC in [chars] failed security check.

Explanation The GBIC in the specified port has invalid EEPROM data. [chars] is the port in which the GBIC is inserted.

Recommended Action Remove the GBIC from the port.

Error Message GBIC_SECURITY-4-GBIC_INTERR: Internal error occurred in setup for GBIC interface [chars].

Explanation The system could not allocate resources or had some other problem during the setup for the specified GBIC interface. [chars] is the interface in which the GBIC module is installed.

Recommended Action Reload the switch by using the reload privileged EXEC command. If the problem persists, find out more about the error by using the **show tech-support** privileged EXEC command. Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5 for more information.

Error Message GBIC_SECURITY-6-SFP_INSERTED: Transceiver SFP [chars] module inserted in [chars]

Explanation The online insertion and removal (OIR) facility detected a newly inserted transceiver module for the interface specified in the message. The first [chars] is the module, and the second [chars] is the interface.

Recommended Action No action is required.

Error Message GBIC_SECURITY-6-SFP_REMOVED: Transceiver SFP [chars] module removed from [chars]

Explanation The OIR facility detected the removal of a transceiver module from the interface specified in the message. The first [chars] is the module, and the second [chars] is the interface.

Recommended Action No action is required.

GBIC_SECURITY_CRYPT Messages

**Note**

The switch supports SFP modules and does not support GBIC modules. Although the error message text refers to GBIC interfaces and modules, the messages from the switch actually refer to the SFP interfaces and modules.

Error Message GBIC_SECURITY_CRYPT-4-ID_MISMATCH: Identification check failed for GBIC in port [chars]

Explanation The SFP module was identified as a Cisco SFP module but the system could not verify its identity. [chars] is the port.

Recommended Action Ensure that the Cisco IOS software running on the switch supports the SFP module. You might need to upgrade your software. Otherwise, verify that the SFP module was obtained from Cisco or from a supported vendor.

Error Message GBIC_SECURITY_CRYPT-4-UNRECOGNIZED_VENDOR: GBIC in port [chars] manufactured by an unrecognized vendor

Explanation The SFP module was identified as a Cisco SFP module but the switch could not match its manufacturer with one on the known list of Cisco SFP module vendors. [chars] is the port.

Recommended Action Ensure that the Cisco IOS software running on the switch supports the SFP module. You might need to upgrade your software.

Error Message GBIC_SECURITY_CRYPT-4-VN_DATA_CRC_ERROR: GBIC in port [chars] has bad crc

Explanation The SFP module was identified as a Cisco SFP module but it does not have valid CRC in the EEPROM data. [chars] is the port.

Recommended Action Ensure that the Cisco IOS software running on the switch supports the SFP module. You might need to upgrade your software. Even if the SFP module is unrecognized by the switch, the SFP module might still operate properly but have limited functionality.

GBIC_SECURITY_UNIQUE Messages

This section contains the Cisco GBIC module and SFP module security messages that identify whether the module is unique.

**Note**

The switch supports SFP modules and does not support GBIC modules. Although the error message text refers to GBIC interfaces and modules, the messages from the switch actually refer to the SFP interfaces and modules.

Error Message GBIC_SECURITY_UNIQUE-3-DUPLICATE_GBIC: GBIC interface [dec]/[dec] is a duplicate of GBIC interface [dec]/[dec].

Explanation The SFP module was identified as a Cisco SFP module but its vendor ID and serial number match that of another interface on the system. The first [dec]/[dec] is the interface of the duplicate SFP module, and the second [dec]/[dec] is the interface of the existing module.

Recommended Action Cisco SFP modules are assigned unique serial numbers. Verify that the module was obtained from Cisco or a supported vendor.

Error Message GBIC_SECURITY_UNIQUE-4-DUPLICATE_SN: GBIC interface [dec]/[dec] has the same serial number as another GBIC interface.

Explanation The SFP module was identified as a Cisco SFP module but its serial number matches that of another interface on the system. [dec]/[dec] is the interface in which the duplicate module is installed.

Recommended Action Cisco SFP modules are assigned unique serial numbers. Verify that the module was obtained from Cisco or a supported vendor.

HARDWARE Messages

Error Message HARDWARE-2-FAN_ERROR: Fan [chars] Failure

Explanation The switch fan is not working. [chars] is the fan name.

Recommended Action This is a hardware failure. The fan might recover automatically. If the fan fails persistently, copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about the online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message `HARDWARE-3-ASICNUM_ERROR: [traceback] Port-ASIC number [dec] is invalid`

Explanation The port ASIC number is invalid. [dec] is the port ASIC number.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still need assistance, open a case with the TAC, or provide your Cisco technical support representative with your information.

Error Message `HARDWARE-3-INDEX_ERROR: Index value [dec] is invalid.`

Explanation The index in the hardware table is out-of-range. [dec] is the index value.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message `HARDWARE-3-INTRNUM_ERROR: Port-ASIC Interrupt number [dec] is invalid.`

Explanation The interrupt ID used in a port ASIC is invalid. [dec] is the interrupt number.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message `HARDWARE-3-PORTNUM_ERROR: [traceback] port number [dec] is invalid`

Explanation The port number is out of range. [dec] is the port number.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still need assistance, open a case with the TAC, or provide your Cisco technical support representative with your information.

Error Message `HARDWARE-3-STATS_ERROR: Statistics ID [dec] is invalid.`

Explanation The statistics ID used is out of range. The statistics supported by the port ASIC are identified by an ID. [dec] is the statistics ID.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

HLFM Messages

Error Message `HLFM-3-MACFREE_ERROR: MAC address [enet], vlan [dec] is still referenced; cannot free.`

Explanation An attempt was made to free a MAC address before releasing all references to it. [enet] is the MAC address, and [dec] is the VLAN ID.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message `HLFM-3-MAP_ERROR: IP address [IP_address] not in mac tables, mac-address [enet], vlan [dec].`

Explanation The IP address and MAC address tables are out of sync. [IP_address] is the IP address, [enet] is the MAC address, and [dec] is the VLAN ID.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message HLFM-3-MOD_SD: Failed to modify Station Descriptor with index [dec], vlan [dec], di [dec], error [dec], mad [dec], ref-count [dec].

Explanation The forwarding manager attempted to modify a station descriptor that is no longer in use or is invalid. The first [dec] is the station index, the second [dec] is the VLAN ID, the third [dec] is the destination index, the fourth [dec] is the error code, the fifth [dec] is the MAC address descriptor, and the sixth [dec] is the ref-count for this MAC address descriptor.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message HLFM-3-SEND_FAIL: Failed to send RPC message, req [dec], [chars].

Explanation A local resource error occurred, or too many outgoing messages are queued for the message class. [dec] is the RPC request number, and [chars] is an optional comment.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

IDBMAN Messages

Error Message IDBMAN-3-AGGPORTMISMATCH: [chars]: [chars]([dec] / [dec]) does not match internal slot/port state [chars]([dec] / [dec]).

Explanation An internal error caused the software to use an invalid aggregate port. The first [chars] is the name of the function where the error occurred. The second and third [chars] are the port-channel names, and the ([dec] / [dec]) are the slot and port numbers (slot/port).

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message IDBMAN-3-DELETEDAGGPORT: [chars]([dec] / [dec]) Group [dec] has been deleted, but is being reused.

Explanation An internal error caused an interface that has been deleted to be reused for a new aggregate port. [chars] is the port-channel name, and the ([dec] / [dec]) are the slot and port numbers (slot/port). The last [dec] is the channel-group number.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message IDBMAN-3-INVALIDAGGPORTBANDWIDTH: [chars]([dec] / [dec]) has an invalid bandwidth value of [dec].

Explanation An internal error caused an invalid bandwidth to be used for an aggregate port. [chars] is the port-channel name, the ([dec] / [dec]) are the slot and port numbers (slot/port), and the last [dec] is the bandwidth.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message IDBMAN-3-INVALIDPORT: [chars]: trying to use invalid port number [dec] (Max [dec]).

Explanation An internal error caused an invalid port number to be used by the software. [chars] is the interface name, the first [dec] is the port number that is invalid, and the second [dec] is the maximum allowed value for a port number.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message IDBMAN-3-INVALIDVLAN: [chars]: trying to use invalid Vlan [dec].

Explanation An internal error caused an invalid VLAN to be used by the software. [chars] is the interface name, and [dec] is the VLAN number that is invalid.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message IDBMAN-3-NOTANAGGPORT: [chars] ([dec] / [dec]) is not an aggregate port.

Explanation An internal error caused an interface that is not an aggregate port to be used for aggregate port operations. [chars] is the interface name, and ([dec] / [dec]) are the slot and port number (slot/port).

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message IDBMAN-3-PORTNOTINAGGPORT: [chars] ([dec] / [dec]) is not present in Aggport [chars] ([dec] / [dec]).

Explanation Internal error detected. A port that was supposed to be in an aggregate port was found not to be. The first [chars] is the interface name, and the second [chars] is the port-channel name. The ([dec] / [dec]) are the slot and port numbers (slot/port).

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message IDBMAN-3-VLANINUSE: [chars]: Vlan [dec] is in use by [chars].

Explanation Each Layer 3 interface is associated with a VLAN. Another Layer 3 interface is using the associated VLAN. The first [chars] is the interface name, [dec] is the VLAN number, and the second [chars] is the interface using the VLAN.

Recommended Action No action is required.

Error Message IDBMAN-3-VLANNOTSET: [chars]: Vlan [dec] not set since it already has Vlan [dec].

Explanation An interface VLAN was not set to the requested value because of an internal error. [chars] is the interface name, the first [dec] is the new VLAN number, and the second [dec] is the currently assigned VLAN number.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message IDBMAN-6-VLANMAPPED: Vlan [dec] is mapped to [chars].

Explanation The VLAN is mapped to this interface.

Recommended Action No action is required.

Error Message IDBMAN-4-ACTIVEPORTSINAGGPORT: [chars]([dec] / [dec]) has [dec] active ports, but is being removed.

Explanation An internal error removed an aggregate port with active ports. [chars] is the port-channel name, and the ([dec] / [dec]) are the slot and port number (slot/port). The last [dec] is the number of currently active ports.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

IFMGR Messages

Error Message IFMGR-3-IFINDEX_PERSIST_ENTRY_CORRUPT: [chars] seems to be corrupted. Trying to read [dec] size

Explanation The ifIndex table is corrupted. [chars] is the path to the IfIndex file, and [dec] is the number of bytes being read from the ifIndex table when the corruption was detected.

Recommended Action Use the **delete nvram:ifindex-table** privileged EXEC command to delete the ifindex table.

Error Message IFMGR-3-INVALID_PERSISTENT_DATA: Invalid persistent data

Explanation The interface manager attempted to write invalid persistent data.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still need assistance, open a case with the TAC, or provide your Cisco technical support representative with your information.

ILET Messages

Error Message ILET-1-AUTHENTICATION_FAIL: This Switch may not have been manufactured by Cisco or with Cisco's authorization. This product may contain software that was copied in violation of Cisco's license terms. If your use of this product is the cause of a support issue, Cisco may deny operation of the product, support under your warranty or under a Cisco technical support program such as Smartnet. Please contact Cisco's Technical Assistance Center for more information.

Explanation A license authentication failure occurred for the switch.

Recommended Action Contact your Cisco sales representative for assistance.

Error Message ILET-1-DEVICE_AUTHENTICATION_FAIL: The [chars] inserted in this switch may not have been manufactured by Cisco or with Cisco's authorization. If your use of this product is the cause of a support issue, Cisco may deny operation of the product, support under your warranty or under a Cisco technical support program such as Smartnet. Please contact Cisco's Technical Assistance Center for more information.

Explanation A license authentication failure occurred for a component installed in the switch. [chars] is the component.

Recommended Action Contact your Cisco sales representative for assistance

MAC_LIMIT Messages

Error Message MAC_LIMIT-4-DROP: Vlan [dec] with Configured limit = [dec] has currently [dec] Entries.

Explanation The number of MAC address table entries for a VLAN is less than or equal to the maximum number allowed. The first [dec] is the VLAN ID, the second [dec] is the maximum number of MAC address entries, and the third [dec] is the number of entries in the MAC address table.

Recommended Action Contact your network administrator to configure this action.

Error Message MAC_LIMIT-4-ENFORCE: Enforcing limit on Vlan [dec] with Configured limit = [dec].

Explanation The number of MAC address entries for the VLAN exceeds the maximum number allowed. The configured action is to limit the number of entries to the maximum allowed. The first [dec] is the VLAN ID, and the second [dec] is the maximum number of MAC address entries.

Recommended Action Contact your network administrator to configure this action.

Error Message MAC_LIMIT-4-EXCEED: Vlan [dec] with Configured limit = [dec] has currently [dec] Entries.

Explanation The number of MAC address entries for a VLAN exceeds the maximum number allowed. The first [dec] is the VLAN ID, the second [dec] is the maximum number of MAC address entries, and the third [dec] is the number of entries in the MAC address table.

Recommended Action Contact your network administrator to configure this action.

IP Messages

Error Message IP-3-SBINIT: Error initializing [chars] subblock data structure. [chars]

Explanation The subblock data structure was not initialized. [chars] is the structure identifier.

Recommended Action No action is required.

MAC_MOVE Messages

Error Message MAC_MOVE-4-NOTIF: Host [enet] in vlan [dec] is flapping between port [chars] and port [chars].

Explanation The host is moving between the specified ports. [enet] is the Ethernet address of the host, [dec] is the VLAN ID, the first [chars] is the first port, and the second [chars] is the second port.

Recommended Action Check your network for loops.

PAGP_DUAL_ACTIVE Messages

Error Message PAGP_DUAL_ACTIVE-3-OBJECT_CREATE_FAILED: Unable to create [chars]

Explanation The switch cannot create the specified managed object. [chars] is the object name.

Recommended Action No action is required.

Error Message PAGP_DUAL_ACTIVE-3-RECOVERY_TRIGGER: PAGP running on [chars] informing virtual switches of dual-active: new active id [enet], old id [enet]

Explanation PAGP received a new active ID on the specified interface, which means that all virtual switches are in a dual-active scenario. The interface is informing virtual switches of this, which causes one switch to go into recovery mode. [chars] is the interface, the first [enet] is the new active ID, and the second [enet] is the ID that it replaces.

Recommended Action No action is required.

Error Message PAGP_DUAL_ACTIVE-3-REGISTRY_ADD_ERR: Failure in adding to [chars] registry

Explanation The switch could not add a function to the registry. [chars] is the registry name.

Recommended Action No action is required.

PHY Messages

Error Message PHY-4-BADTRANSCEIVER: An inappropriate transceiver has been inserted in interface [chars].

Explanation A transceiver that should not be used is in the specified interface.

Recommended Action Remove the transceiver. If the transceiver is a Cisco device, contact your Cisco technical support representative.

Error Message PHY-4-CHECK_SUM_FAILED: SFP EEPROM data check sum failed for SFP interface [chars].

Explanation The SFP module was identified as a Cisco SFP module but the system cannot read the vendor data information to verify whether it is correct. [chars] is the interface in which the SFP module is installed.

Recommended Action Remove and then reinsert the SFP module. If it fails again with the same error message, the SFP module might be defective.

Error Message PHY-4-EXCESSIVE_ERRORS: Excessive FCS, data, or idle word errors found on interface [chars].

Explanation The system detected excessive frame check sequence (FCS), data word, or idle word errors on the specified interface. [chars] is the interface.

Recommended Action Enter the **show interface** privileged EXEC command on the specified interface, and check for cyclic redundancy check (CRC) and other input errors. If errors are excessive, enter the **shutdown** interface configuration command and then the **no shutdown** interface configuration command to reset the interface.

Error Message PHY-4-MODULE_DUP: SFPs in [chars] and in [chars] have duplicate vendor-id and serial numbers.

Explanation The SFP module was identified as a Cisco SFP module, but its vendor ID and serial number match that of another SFP module in the system. The first [chars] is the slot in which the SFP module is installed, and the second [chars] is the slot where the duplicate SFP module is installed.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message PHY-4-SFP_NOT_SUPPORTED: The SFP in [chars] is not supported.

Explanation The SFP module type is not supported on this switch. [chars] is the interface.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message PHY-4-UNSUPPORTED_SFP_CARRIER: Unsupported SFP carrier module found in [chars]

Explanation The SFP carrier module was identified as an unsupported, non-Cisco SFP carrier module. [chars] is the unsupported module.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message PHY-4-UNSUPPORTED_TRANSCEIVER: Unsupported transceiver found in [chars].

Explanation The SFP module was identified as an unsupported, non-Cisco SFP module. [chars] is the unsupported module.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

PIMSN Messages

Error Message PIMSN-6-IGMPSN_GLOBAL: PIM Snooping global runtime mode [chars] due to IGMP Snooping [chars].

Explanation When IGMP snooping is disabled, PIM snooping is disabled. When IGMP snooping is re-enabled, PIM snooping is re-enabled. The first [chars] is the PIM snooping mode, and the second [chars] is the IGMP snooping mode.

Recommended Action No action is required.

Error Message PIMSN-6-IGMPSN_VLAN: PIM Snooping runtime mode on vlan [dec] [chars] due to IGMP Snooping [chars].

Explanation When IGMP snooping is disabled, PIM snooping is disabled. When IGMP snooping is re-enabled, PIM snooping is re-enabled. [dec] is the VLAN ID, the first [chars] is the PIM snooping mode, and the second [chars] is the IGMP snooping mode.

Recommended Action No action is required.

PLATFORM Messages

Error Message PLATFORM-1-CRASHED: [chars].

Explanation The system is trying to display the error message that appeared when the switch failed in a previous instance. [chars] is the description of the error message.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message PLATFORM-3-NO_HARDWARE_RESOURCES: Not enough hardware resources. Shutting down [chars].

Explanation There are too many VLANs and routed ports. [chars] is the short interface name, such as Gi0/1, or the VLAN name, such as VLAN0002.

Recommended Action Reduce the total number of VLANs and routed ports to be less than 1023. To preserve configurations and connections across reboots, save the configuration.

PLATFORM_CAT3750 Messages

Error Message PLATFORM_CAT3750-3-ERROR: [chars].

Explanation An internal error occurred. [chars] is the description of the error.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#) for more information.

PLATFORM_FBM Messages

Error Message PLATFORM_FBM-4-REMOTE_ADD_VLAN: seeing problems while adding vlan [dec] to bridge [dec] on box [dec], will keep retrying.

Explanation The VLAN could not be added to the bridge-group on a remote switch. The TCAM-full condition on the remote switch might be set to stop all traffic. The first [dec] is the VLAN number, the second [dec] is the bridge-group, and the third [dec] is the remote switch.

Recommended Action Enter the **clear mac-address-table** privileged EXEC command to restore the normal operation of the switch.

Error Message PLATFORM_FBM-4-REMOTE_DEL_BG: seeing problems while deleting bridge [dec] on box [dec], will keep retrying.

Explanation The bridge-group could not be deleted on a remote switch. The first [dec] is the bridge group, and the second [dec] is the remote switch.

Recommended Action If the error message recurs, find out more about the error by using the **show tech-support** privileged EXEC command. Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#) for more information.

Error Message PLATFORM_FBM-4-REMOTE_DEL_VLAN: seeing problems while deleting vlan [dec] from bridge [dec] on box [dec], will keep retrying.

Explanation The VLAN could not be deleted from bridge-group on a remote switch. The first [dec] is the VLAN number, the second [dec] is the bridge-group, and the third [dec] is the remote switch.

Recommended Action If the error message recurs, find out more about the error by using the **show tech-support** privileged EXEC command. Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#) for more information.

Error Message PLATFORM_FBM-4-RECOVERED: Fallback bridging recovered from resource crunch.

Explanation Fallback bridging has recovered from an earlier lack of resources.

Recommended Action No action is required.

Error Message PLATFORM_FBM-4-RESOURCE_CRUNCH: Fallback bridging on bridge-group [dec] is experiencing a resource crunch. One or more bridge-groups may not be functional. It will recover automatically when system recovers from resource crunch. Delete the bridge-group to immediately recover.

Explanation Fallback bridging could not be configured properly. The most likely cause is a TCAM-full condition on at least one stack member. [dec] is the bridge-group.

Recommended Action The switch automatically recovers but this could take some time. For an immediate recovery, use the **shutdown** interface configuration command to disable the port and stop the traffic flow to the switch. Use the **clear mac-address-table dynamic** privileged EXEC command to remove all MAC addresses from the TCAM. Use the **no shutdown** interface configuration command to re-enable the port.

PLATFORM_PBR Messages

This section contains the policy-based routing (PBR) messages.

Error Message PLATFORM_PBR-2-NO_RMAP: Cannot create PBR data structures for route-map [chars].

Explanation The PBR manager could not allocate the internal data structures for this route map. A likely cause is lack of available memory. [chars] is the route map.

Recommended Action Simplify the configuration so that it requires less memory.

Error Message PLATFORM_PBR-3-INSTALL_FAIL: Policy route-map [chars] not installed in hardware.

Explanation The PBR manager could not install the complete route map in hardware, so the packets are forwarded to the CPU for processing. [chars] is the route map.

Recommended Action Simplify route-map configurations. For example, use the same route map on multiple interfaces.

Error Message PLATFORM_PBR-3-MERGE_FAIL: [chars] ACL merge error [dec] on route-map [chars].

Explanation The PBR manager could not merge the configured route map into a suitable form for installing into the hardware. This error was probably caused by specifying an ACL that is too large or too complex for the system. The first [chars] is the ACL, [dec] is the error number, and the second [chars] is the route map.

Recommended Action Specify a smaller and less complicated configuration.

Error Message PLATFORM_PBR-3-NO_LABEL: Cannot allocate label for route-map [chars].

Explanation The PBR manager could not allocate a label for this route map. As a result, the hardware cannot be programmed to implement policy routing. There is a limit of 247 labels for policy routing. [chars] is the route map.

Recommended Action Simplify the configuration with label sharing. Use the same route maps on multiple interfaces, if possible.

Error Message PLATFORM_PBR-3-UNSUPPORTED_RMAP: Route-map [chars] not supported for Policy-Based Routing.

Explanation The route map attached to an interface for policy routing contains an action that is not supported. This is a hardware limitation. [chars] is the route map.

Recommended Action Use the **route-map** map-tag **permit** global configuration command and the **set ip next-hop** ip-address route-map configuration command to reconfigure the route map to use only these supported actions.

Error Message PLATFORM_PBR-4-CPU_SUPPORTED_ACTION: Set action in sequence [dec] of route-map [chars] supported by forwarding to CPU.

Explanation The route map attached to an interface for policy-based routing contains an action that is not supported in hardware, so the packets are forwarded to the CPU for processing. The route-map actions that invoke this forwarding are **set interface**, **set ip default next-hop**, **set default interface**, or **set ip df**. [dec] is the action number, and [chars] is the route map.

Recommended Action Use the **set ip next-hop** ip-address route-map configuration command to reconfigure the route map action to route the packet to the specified next hop.

Error Message PLATFORM_PBR-4-RETRY_INSTALL: Route-map [chars] installed in hardware upon retry.

Explanation The PBR manager was able to fit the complete configuration into the hardware. One or more route maps previously did not load because of lack of resources. [chars] is the route map.

Recommended Action No action is required.

Error Message PLATFORM_PBR-4-SDM_MISMATCH: [chars] requires sdm template routing.

Explanation The routing template is not enabled. [chars] is the text string PBR.

Recommended Action Modify the Switch Database Management (SDM) template to enable the routing template. Use the **sdm prefer** global configuration command, and then reload the switch by using the **reload** privileged EXEC command.

PLATFORM_PM Messages

Error Message PLATFORM_PM-3-IFCOUNTERERROR: Unit number [dec] of interface [chars] is more than max allowed value of [dec].

Explanation There are too many interfaces configured for the interface type. The first [dec] is the interface count, [chars] is the interface, and the second [dec] is the maximum number of interfaces.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message PLATFORM_PM-3-INTVLANINUSE: internal vlan-id [dec] allocated for interface [chars] is still in use.

Explanation An internal VLAN ID allocated for an interface is still in use. [dec] is the VLAN ID, and [chars] is the interface.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message PLATFORM_PM-3-NOINTVLAN: internal vlan of interface [chars] is not active for vlan-id [dec].

Explanation The internal vlan_data is not active for the given VLAN ID. [chars] is the interface, and [dec] is the VLAN ID.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

PLATFORM_SPAN Messages

Error Message PLATFORM_SPAN-3-PACKET_DROP: Decreases egress SPAN rate.

Explanation Egress SPAN rates are falling because SPAN is enabled with multicast routing or fallback bridging.

Recommended Action Find out more about the error by using the **show tech-support** privileged EXEC command. Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5 for more information.

PLATFORM_UCAST Messages

Error Message PLATFORM_UCAST-3-ADJ: [chars].

Explanation The adjacency module for unicast routing encountered an error. [chars] describes the error.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message PLATFORM_UCAST-3-ARP: [chars].

Explanation The ARP module for unicast routing encountered an error. [chars] describes the error.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message PLATFORM_UCAST-3-CEF: [chars].

Explanation The Cisco Express Forwarding (CEF) module for unicast routing encountered an error. [chars] describes the error.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message PLATFORM_UCAST-3-DYNAMIC: [chars].

Explanation The dynamic address tracking mechanism for unicast routing encountered an error. [chars] describes the error.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message PLATFORM_UCAST-3-ERROR: [chars].

Explanation An internal unicast routing error occurred. [chars] describes the error.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message PLATFORM_UCAST-3-HSRP: [chars].

Explanation The Hot Standby Router Protocol (HSRP) module for unicast routing encountered an error. [chars] describes the error.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message PLATFORM_UCAST-3-INTERFACE: [chars].

Explanation A unicast routing interface error occurred. [chars] describes the error.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message PLATFORM_UCAST-3-RPC: [chars].

Explanation The RPC module for unicast routing encountered an error. [chars] describes the error.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message PLATFORM_UCAST-6-PREFIX: One or more, more specific prefixes could not be programmed into TCAM and are being covered by a less specific prefix

Explanation A more specific prefix could not be programmed into TCAM and is covered by a less specific prefix. This could be a temporary condition. The output of the **show platform ip unicast failed route** privileged EXEC command lists the failed prefixes.

Recommended Action No action is required.

PLATFORM_VLAN Messages

Error Message PLATFORM_VLAN-3-LOCK_FAIL: Failed to lock vlan-id [dec], associated mapped vlan id value [dec].

Explanation The VLAN lock operation failed. This can occur if the VLAN is already active in the system or if the VLAN ID is not active. The first [dec] is the VLAN ID, and the second [dec] is the mapped-vlan-id (MVID).

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message PLATFORM_VLAN-3-MVID_ERROR: Mapped Vlan ID value [dec] associated with vlan-id [dec] is invalid.

Explanation An active VLAN is not correctly associated with a mapped-vlan-id (MVID). The first [dec] is the VLAN ID, and the second [dec] is the MVID.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message PLATFORM_VLAN-3-UNLOCK_FAIL: Failed to unlock vlan-id [dec], associated mapped vlan id value [dec].

Explanation The switch did not unlock a VLAN ID. The most likely cause is that the VLAN is already unlocked. The first [dec] is the VLAN ID, and the second [dec] is the MVID.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

PM Messages

Error Message PM-2-LOW_SP_MEM: Switch process available memory is less than [dec] bytes.

Explanation The available memory for the switch processor is low. This can occur when too many Layer 2 VLANs are configured. [dec] is the available memory.

Recommended Action Remove VLANs from the system to reduce memory usage.

Error Message PM-2-NOMEM: Not enough memory available for [chars].

Explanation The port manager subsystem could not obtain the memory it needed to initialize the specified operation. [chars] is the port manager operation.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message PM-2-VLAN_ADD: Failed to add VLAN [dec] - [chars].

Explanation The software did not add the VLAN to the VTP database. [dec] is the VLAN ID, and [chars] specifies the reason the software did not add the VLAN.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message PM-3-ERR_INCOMP_PORT: [dec]/[dec] is set to inactive because [dec]/[dec] is a [chars] port.

Explanation The private host port cannot be configured because trunk, private promiscuous, and a SPAN destination ports cannot be configured on the same coil. The first [dec]/[dec] is the private host port, the second [dec]/[dec] is the incompatible port, and [chars] is the incompatible port type.

Recommended Action Configure the incompatible ports on different coils.

Error Message PM-3-INTERNALERROR: Port Manager Internal Software Error ([chars]: [chars]: [dec]: [chars]).

Explanation An internal software error occurred in the Cisco IOS port manager. The parameters identify the problem for Cisco technical support. The first [chars] is the error message, and the second [chars] is the filename. [dec] is the line number, and the last [chars] is the function name.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message PM-4-BAD_APP_ID: an invalid application id ([dec]) was detected.

Explanation The port manager detected an invalid request. [dec] is the application ID.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message PM-4-BAD_APP_REQ: an invalid [chars] request by the '[chars]' application was detected.

Explanation The port manager detected an invalid request. The first [chars] is the invalid request, and the second [chars] is the application making the request.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message PM-4-BAD_CARD_COOKIE: an invalid card cookie was detected.

Explanation The port manager detected an invalid request.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message PM-4-BAD_CARD_SLOT: an invalid card slot ([dec]) was detected.

Explanation The port manager detected an invalid request. [dec] is the slot number.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message PM-4-BAD_COOKIE: [chars] was detected.

Explanation The port manager detected an invalid request. [chars] is the invalid request.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message PM-4-BAD_HA_ENTRY_EVENT: Invalid Host access entry event ([dec]) is received.

Explanation An invalid host access entry event was received. The host access table entry event should be an add, delete, or update event. [dec] is the event that is received.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message PM-4-BAD_PORT_COOKIE: an invalid port cookie was detected.

Explanation The port manager detected an invalid request.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message PM-4-BAD_PORT_NUMBER: an invalid port number ([dec]) was detected.

Explanation The port manager detected an invalid request. [dec] is the port number.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message PM-4-BAD_VLAN_COOKIE: an invalid vlan cookie was detected.

Explanation The port manager detected an invalid request.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message PM-4-BAD_VLAN_ID: an invalid vlan id ([dec]) was detected.

Explanation The port manager detected an invalid request. [dec] is the VLAN ID.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message PM-4-ERR_DISABLE: [chars] error detected on [chars], putting [chars] in err-disable state.

Explanation The port manager detected a misconfiguration or misbehavior and error-disabled the interface. A recovery is attempted after the configured retry time (the default is 5 minutes). The first [chars] is the error, and both the second and third [chars] are the affected interface.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message PM-4-ERR_DISABLE_VP: [chars] error detected on [chars], vlan [dec]. Putting in err-disable state.

Explanation The virtual port (that is, the port-VLAN pair) is error disabled when it detects a misconfiguration or misbehavior. If configured, a recovery will be attempted after the configured retry time (default time is 5 minutes). The first [chars] is the error, and the second [chars] is the port, and [dec] is the VLAN ID.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message PM-4-ERR_RECOVER: Attempting to recover from [chars] err-disable state on [chars].

Explanation The port manager is trying to restart an error-disabled interface. The first [chars] is the error, and the second [chars] is the interface.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message PM-4-ERR_RECOVER_VP: Attempting to recover from [chars] err-disable state on [chars], vlan [dec].

Explanation The port manager is trying to restart an error-disabled virtual port. The first [chars] is the error, the second [chars] is the virtual port, and [dec] is the VLAN ID.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message PM-4-EXT_VLAN_INUSE: VLAN [dec] currently in use by [chars].

Explanation The port manager did not allocate the VLAN for external use because the VLAN is being used by another feature. [dec] is the VLAN that is being used, and [chars] is the feature that is using it.

Recommended Action Reconfigure the feature (for example, the routed port) to use another internal VLAN or to request another available VLAN.

Error Message PM-4-EXT_VLAN_NOTAVAIL: VLAN [dec] not available in Port Manager.

Explanation The port manager did not allocate the requested VLAN. The VLAN is probably being used as an internal VLAN by other features. [dec] is the requested VLAN.

Recommended Action Configure a different VLAN on the device.

Error Message PM-4-INACTIVE: putting [chars] in inactive state because [chars].

Explanation The port is inactive because the port manager could not create a virtual port for the switch port and VLAN. The reason for this condition is specified in the error message. The first [chars] is the interface name, and the second [chars] is the reason.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message PM-4-INT_FAILUP: [chars] failed to come up. No internal VLAN available.

Explanation The port manager did not allocate an internal VLAN. The interface cannot be enabled. [chars] is the interface name.

Recommended Action Remove the extended-range VLAN by using the **no vlan** *vlan-id* global configuration command to free up resources.

Error Message PM-4-INT_VLAN_NOTAVAIL: Failed to allocate internal VLAN in Port Manager.

Explanation The port manager did not find any available internal VLAN.

Recommended Action Delete some extended-range VLANs created by users or remove some features (such as routed ports) that require internal VLAN allocation. To delete extended-range VLANs, use the **no vlan *vlan-id*** global configuration command. To delete a routed port, use the **no switchport** interface configuration command.

Error Message PM-4-INVALID_HOST_ACCESS_ENTRY: Invalid Host access entry type ([dec]) is received.

Explanation An invalid host access entry type was received. The host access entry should be a configured or dynamic type. [dec] is the entry type that is received.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message PM-4-LIMITS: The number of vlan-port instances on [chars] exceeded the recommended limit of [dec].

Explanation The total number of individual VLAN ports on the module or the switch has exceeded the recommended limit. VLANs can be counted more than once. If VLAN 1 is carried on ten interfaces, it counts as ten VLAN ports. On some platforms, bundling is also ignored for purposes of this count. If eight interfaces on the same module are in one bundle, and the port channel is carrying VLAN 1, it counts as eight VLAN ports. [chars] is the module name (for example, switch or the module number), and [dec] is the recommended limit.

Recommended Action Reduce the number of trunks and VLANs configured in the module or switch as recommended in [dec]. Enter the **show interfaces trunk** privileged EXEC command to see the total number of trunks and VLANs.

Error Message PM-4-NO_SUBBLOCK: No PM subblock found for [chars].

Explanation The port manager did not find the subblock for this interface. [chars] is the interface name.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message PM-4-PORT_BOUNCED: Port [chars] was bounced by [chars].

Explanation During a change-over when the port was in the link-down state, the port manager restarted the port. A port can be restarted only when the port data structures are not consistent in the active and standby supervisors. Active ports in the link-down state return to the link-up state when the port is restarted. The first [chars] is the port number, and the second [chars] is the re-activation event.

Recommended Action No action is required.

Error Message PM-4-PORT_CONSISTENT: Port [chars] consistency has been restored, IDB state: [chars].

Explanation The port manager on standby discovered that the port state became consistent again. The first [chars] is the interface name, and the second [chars] describes the state of the interface.

Recommended Action No action is required.

Error Message PM-4-PORT_INCONSISTENT: Port [chars] is inconsistent: IDB state [chars] (set [time-stamp] ago), link: [chars] ([time-stamp] ago), admin: [chars] ([time-stamp] ago).

Explanation The standby port manager identified a port state that has been inconsistent for more than 1 second. Inconsistent ports are reactivated on change-over and the `PORT_BOUNCED` message appears. The first [chars] is the port number, the second [chars] describes the state of the interface, the third [chars] is the current link state, and the fourth [chars] is the configured state of the interface.

Recommended Action No action is required.

Error Message PM-4-PVLAN_TYPE_CFG_ERR: Failed to set VLAN [dec] to a [chars] VLAN.

Explanation The platform did not set a private VLAN type. [dec] is the VLAN ID.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message PM-4-TOO_MANY_APP: application '[chars]' exceeded registration limit.

Explanation The port manager detected an invalid request. [chars] is the application.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message PM-4-UNKNOWN_HOST_ACCESS: Invalid Host access value ([dec]) is received.

Explanation The host access table is being accessed with an invalid host access value. [dec] is the value that is received.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message PM-4-VMPS_CFG: Dynamic access VLAN [dec] same as voice vlan on [chars].

Explanation The access VLAN ID on the VMPS server is the same as the voice VLAN ID on the interface. [dec] is the access VLAN ID, and [chars] is the physical interface.

Recommended Action Assign the access VLAN on the VMPS server to a VLAN ID that is different from the voice VLAN ID.

Error Message PM-6-EXT_VLAN_ADDITION: Extended VLAN is not allowed to be configured in VTP CLIENT mode.

Explanation The switch did not add a VLAN in VTP client mode.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

PORT SECURITY Messages

Error Message PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred caused by MAC [enet] on port [chars].

Explanation An unauthorized device attempted to connect on a secure port. [enet] is the MAC address of the unauthorized device, and [chars] is the secure port.

Recommended Action Identify the device that attempted to connect on the secure port. Notify your network system administrator of this condition.

Error Message PORT_SECURITY-2-PSECURE_VIOLATION_VLAN: Security violation on port [chars] due to MAC address [enet] on VLAN [dec]

Explanation An unauthorized device attempted to connect on a secure trunk port. [chars] is the secure port, [enet] is the MAC address of the unauthorized device, and [dec] is the VLAN ID.

Recommended Action Identify the device that attempted to connect through the secure trunk port. Notify your network system administrator of this condition.

Error Message PORT_SECURITY-6-ADDR_REMOVED: Address [dec]:[enet] exists on port [chars]. It has been removed from port [chars].

Explanation A routed port is reconfigured as a switch port. The address in the previous switch configuration conflicts with the running configuration and has been deleted. [dec]:[enet] is the MAC address of the port, and [chars] is the reconfigured port.

Recommended Action No action is required.

Error Message PORT_SECURITY-6-VLAN_FULL: Vlan [int] on port [chars] has reached its limit. Address [enet] has been removed.

Explanation The voice VLAN has become the access VLAN. Because the maximum number of addresses allowed on the access VLAN has been reached, the specified Ethernet address has been deleted. [int] is the VLAN number, [chars] is the port number, and [enet] is the Ethernet address.

Recommended Action No action is required.

Error Message PORT_SECURITY-6-VLAN_REMOVED: VLAN [int] is no longer allowed on port [chars]. Its port security configuration has been removed.

Explanation A configured VLAN has been excluded either due to a port-mode change or an allowed VLAN list change and is removed from the configuration. [int] is the VLAN ID, and [chars] is the switch port assigned to the VLAN.

Recommended Action No action is required.

QOSMGR Messages

Error Message QOSMGR-3-FEATURE_NOT_FOUND: Cannot find feature for [chars].

Explanation An internal software error has occurred. [chars] is the description of the feature that the software cannot find.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message QOSMGR-3-FILTERTYPE_INVALID: Internal Error Invalid Policy filtertype [dec].

Explanation An internal software error has occurred. [dec] is the invalid filter type identification.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message QOSMGR-3-MERGE_RES_COUNT: Internal Error Invalid count.

Explanation An internal software error has occurred.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message QOSMGR-3-NO_POLICER_QOSLABEL: Creating port Class Label Failed.

Explanation An internal software error has occurred.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message QOSMGR-3-NO_VMR_QOSLABEL: qm_generate_vmrs have no qos label.

Explanation An internal software error has occurred.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message QOSMGR-3-NULL_POLICER: Internal Error Invalid Policer.

Explanation An internal software error has occurred.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message QOSMGR-3-POLICER_RES_COUNT: Internal Error Invalid Policer count.

Explanation An internal software error has occurred.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message QOSMGR-3-POLICYMAP_NOT_FOUND: Cannot find policymap for [chars].

Explanation An internal software error has occurred. [chars] is the policy map name.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message QOSMGR-3-QUEUE_PTR_ERROR: queue pointers out of order [hex] [hex] [hex] [hex].

Explanation An internal software error has occurred. [hex] [hex] [hex] [hex] are the software-computed queue pointer values. The parameters provide error details for Cisco Technical Support.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message QOSMGR-3-RESERVE_COUNT_ERROR: Reserved Count Exceeding total [dec].

Explanation An internal software error has occurred in the allocated reserved buffers. [dec] is the reserved count computed by the software.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message QOSMGR-3-RESOURCE_INTERNAL: Internal Error in resource allocation.

Explanation An internal software error has occurred.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message QOSMGR-3-VMRSEQ_INVALID: Internal Error Invalid VMR sequence.

Explanation An internal software error has occurred.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message QOSMGR-4-ACTION_NOT_SUPPORTED: Action is not supported in policymap [chars].

Explanation An action other than the **set**, **trust**, and **police** policy-map class configuration commands was configured in a policy map. This is a hardware limitation. [chars] is the name of the policy map.

Recommended Action Configure only the supported actions of **set**, **trust**, and **police** when in policy-map class configuration mode.

Error Message QOSMGR-4-CLASS_NOT_SUPPORTED: Classification is not supported in classmap [chars].

Explanation An unsupported **match** class-map configuration command was configured in a policy map and attached to an egress interface or more than one **match** command was configured. This is a hardware limitation. [chars] is the class-map name.

Recommended Action Reconfigure the class map or the policy map. Use only the **match ip dscp dscp-list** class-map configuration command in a policy map that is attached to an egress interface. Only one match per class map is supported.

Error Message QOSMGR-4-COMMAND_FAILURE: Execution of [chars] command failed.

Explanation The command to configure a QoS setting failed. This is possibly due to lack of hardware resources. [chars] is the description of the command.

Recommended Action Look for any other messages that indicate resource failure. If other messages indicate that the hardware resources are exceeded, retry the command with a smaller configuration. Find out more about the error by using the **show tech-support** privileged EXEC command. Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message QOSMGR-4-HARDWARE_NOT_SUPPORTED: Hardware limitation has reached for policymap [chars].

Explanation The policy map configuration has exceeded the limitation of the hardware. You configured more QoS ACL entries than the number specified in the SDM template. [chars] is the policy-map name.

Recommended Action Reconfigure the class map or the policy map, and reduce the number of QoS ACLs.

Error Message QOSMGR-4-MATCH_NOT_SUPPORTED: Match type is not supported in classmap [chars].

Explanation An unsupported match type was entered. Only the **access-group** *acl-index-or-name*, **ip dscp** *dscp-list*, and **ip precedence** *ip-precedence-list* match types are supported with the **match** class-map configuration command. [chars] is the name of the class map.

Recommended Action Reconfigure the class map using only the **match access-group**, **match ip dscp**, and **match ip precedence** class-map configuration commands within the class map.

Error Message QOSMGR-4-NOT_SUPPORTED: Action '[chars]' is not supported for a policymap attached to output side.

Explanation A **set** or **trust** policy-map class configuration command was configured in a policy map and attached to an egress interface. A warning message is logged, and the actions do not take affect. This is a hardware limitation. [chars] is either the set or trust action.

Recommended Action Do not configure a **set** or **trust** policy-map class configuration command in a policy map and attach it to an egress interface. These policy-map actions are supported only on ingress interfaces.

Error Message QOSMGR-4-POLICER_PLATFORM_NOT_SUPPORTED: Policer configuration has exceeded hardware limitation for policymap [chars].

Explanation The policy-map configuration has exceeded the limitation of the hardware. An attempt to configure more policers in all policy maps (by using the **police** or **police aggregate** policy-map class configuration command) than supported by the hardware, which is not allowed, caused this condition. [chars] is the policy-map name.

Recommended Action Reconfigure the class maps or the policy maps, or delete the policy map from some interfaces.

Error Message QOSMGR-4-POLICER_POLICY_NOT_SUPPORTED: Number of policers has exceeded per policy hardware limitation for policymap [chars].

Explanation The policy-map configuration has exceeded the limitation of the hardware. You configured more policers in a policy map (by using the **police** or **police aggregate** policy-map class configuration command) than supported. [chars] is the policy-map name.

Recommended Action Reconfigure the class map or the policy map, and reduce the number of policers.

REP Messages

Error Message REP-3-INVALIDPKT: received invalid pkt: [chars]

Explanation The switch received an invalid Resilient Ethernet Protocol (REP) packet. [chars] is information about the invalid packet.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still need assistance, open a case with the TAC, or provide your Cisco technical support representative with your information.

Error Message REP-3-NOPPPROC: [traceback] Failed to create REP LSL Fast Hello Process

Explanation The switch cannot exchange hello packets with its Resilient Ethernet Protocol (REP) neighbors because the Link Status Layer (LSL) age timer is set to longer than 3 seconds.

Recommended Action Reload the switch.

Error Message REP-4-LINKSTATUS: [chars] (segment [dec]) is [chars]

Explanation The REP-interface link status has changed. The first [chars] is the interface name. [dec] is the REP segment number of the interface, and the second [chars] is the new link status.

Recommended Action No action is required.

Error Message REP-5-PREEMPTIONFAIL: can not perform preemption on segment [dec] due to [char]

Explanation The REP preempt operation failed. This could be due to an invalid port ID or a neighbor_offset number specified with the **rep block port** interface configuration command. This could also be caused by entering the **rep block port preferred** interface configuration command if there is no REP port configured with the **preferred** keyword. [dec] is the segment number, and [char] is the reason for the REP preempt operation failed.

Recommended Action Correct the configuration. Run REP manual preemption on the primary edge port by entering the **rep preempt segment** command.

RMON Messages

Error Message RMON-5-FALLINGTRAP: Falling trap is generated because the value of [chars] has fallen below the falling-threshold value [dec].

Explanation A falling trap has been generated. The value of the specified MIB object is below the falling threshold value. [chars] is the MIB object, and [dec] is the threshold value.

Recommended Action Take appropriate action on the specified MIB object.

Error Message RMON-5-RISINGTRAP: Rising trap is generated because the value of [chars] exceeded the rising-threshold value [dec].

Explanation A rising trap has been generated. The value of the specified MIB object is above the rising threshold value. [chars] is the MIB object, and [dec] is the threshold value.

Recommended Action Take appropriate action on the specified object.

SCHED Messages

Error Message SCHED-3-UNEXPECTEDEVENT: [traceback] [process information] Process received unknown event (maj [hex], min [hex])

Explanation An event was not processed. The first [hex] is the major event number, and the second [hex] is the minor event number.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still need assistance, open a case with the TAC, or provide your Cisco technical support representative with your information.

SPAN Messages

Error Message SPAN-3-MEM_UNAVAIL: Memory was not available to perform the SPAN operation

Explanation The system could not perform a SPAN operation because of a lack of memory.

Recommended Action Reduce other system activity to ease the memory demands.

Error Message SPAN-3-UNKN_ERR: An internal error occurred during a SPAN operation.

Explanation SPAN detected an error in its internal operation.

Recommended Action The error might be transient. Try the SPAN operation again. If a second attempt also fails, reload the switch by using the **reload** privileged EXEC command to complete the operation.

Error Message SPAN-3-UNKN_ERR_PORT: An internal error occurred when configuring SPAN on port [chars].

Explanation SPAN detected an error in its internal operation. [chars] is the interface.

Recommended Action The error might be transient. Try the SPAN operation again. If the second attempt also fails, reload the switch by using the **reload** privileged EXEC command to complete the operation.

SPANTREE Messages

Error Message SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port [chars] with BPDU Guard enabled. Disabling port.

Explanation A bridge protocol data unit (BPDU) was received on an interface that has the spanning tree BPDU guard feature enabled. The interface was administratively shut down. [chars] is the name of the interface.

Recommended Action Either remove the device sending BPDUs, or disable the BPDUGuard feature. You can configure the BPDU guard feature locally on the interface or globally on all PortFast ports. To disable BPDU guard on an interface, use the **no spanning-tree bpduguard enable** interface configuration command. To disable BPDU guard globally, use the **no spanning-tree portfast bpduguard default** global configuration command. After you have removed the device or disabled BPDU guard, enter the no shutdown interface configuration command to re-enable the interface.

Error Message SPANTREE-2-BLOCK_BPDUGUARD_VP: Received BPDU on port [chars], vlan [dec] with BPDU Guard enabled. Disabling vlan.

Explanation A BPDU was received on an interface and the VLAN. The spanning tree BPDU guard feature was enabled and configured to shut down the VLAN. The VLAN was error disabled. [chars] is the interface, and [dec] is the VLAN.

Recommended Action Either remove the device sending BPDUs, or disable the BPDU guard feature. You can configure the BPDU guard feature locally on the interface or globally on all PortFast ports. Enter the **clear errdisable** privileged EXEC command to re-enable the interface and VLAN.

Error Message SPANTREE-2-BLOCK_PVID_LOCAL: Blocking [chars] on [chars]. Inconsistent local vlan.

Explanation The spanning-tree port associated with the listed spanning-tree instance and interface will be held in the spanning-tree blocking state until the port VLAN ID (PVID) inconsistency is resolved. The listed spanning-tree instance is that of the native VLAN ID of the listed interface. The first [chars] is the interface, and the second [chars] is the spanning-tree instance.

Recommended Action Verify that the configuration of the native VLAN ID is consistent on the interfaces on each end of the 802.1Q trunk connection. When corrected, spanning tree automatically unblocks the interfaces, as appropriate.

Error Message SPANTREE-2-BLOCK_PVID_PEER: Blocking [chars] on [chars]. Inconsistent peer vlan.

Explanation The spanning-tree port associated with the listed spanning-tree instance and interface will be held in the spanning-tree blocking state until the port VLAN ID (PVID) inconsistency is resolved. The listed spanning-tree instance is that of the native VLAN ID of the interface on the peer switch to which the listed interface is connected. The first [chars] is the interface, and the second [chars] is the spanning-tree instance.

Recommended Action Verify that the configuration of the native VLAN ID is consistent on the interfaces on each end of the 802.1Q trunk connection. When interface inconsistencies are corrected, spanning tree automatically unblocks the interfaces.

Error Message SPANTREE-2-CHNL_MISCFG: Detected loop due to etherchannel misconfiguration of [chars] [chars].

Explanation A misconfiguration of a channel group has been detected. For example, the ports on one side of the EtherChannel either are not configured to be in the channel or did not bundle into the channel and the other side has successfully bundled the ports into the EtherChannel. The first [chars] is the port, and the second [chars] is the VLAN.

Recommended Action Identify the local ports using the **show interfaces status err-disabled** privileged EXEC command, and then check the EtherChannel configuration on the remote device by using the **show etherchannel summary** privileged EXEC command on the remote device. After the configuration is correct, enter the **shutdown** and then **no shutdown** interface configuration commands on the associated port-channel interfaces.

Error Message SPANTREE-2-LOOPGUARD_BLOCK: Loop guard blocking port [chars] on [chars].

Explanation The spanning-tree message age timer has expired because no BPDUs were received from the designated bridge. Because this condition could be caused by a unidirectional-link failure, the interface is put into the blocking state and marked as loop-guard-inconsistent to prevent possible loops from being created. The first [chars] is the name of this port, and the second [chars] is the spanning-tree mode displayed in the **show spanning-tree** privileged EXEC command.

Recommended Action Enter the **show spanning-tree inconsistentports** privileged EXEC command to review the list of interfaces with loop-guard inconsistencies. Determine why devices connected to the listed ports are not sending BPDUs. One reason might be that they are not running the STP. If so, you should disable loop guard on the inconsistent interfaces by using the **spanning-tree guard none** interface configuration command or by starting STP on the remote side of the links.

Error Message SPANTREE-2-LOOPGUARD_CONFIG_CHANGE: Loop guard [chars] on port [chars] on [chars].

Explanation The spanning-tree loop-guard configuration for the listed interface has been changed. If enabled, the interface is placed into the blocking state. It is marked as loop-guard-inconsistent when the message-age timer expires because no BPDUs were received from the designated bridge. This feature is mainly used to detect unidirectional links. The first [chars] is the loop-guard state (*enable* or *disable*), the second [chars] is the interface name, and the third [chars] is the spanning-tree instance.

Recommended Action Verify that this is the desired configuration for the listed interface. Correct it if this is not the desired configuration.

Error Message SPANTREE-2-LOOPGUARD_UNBLOCK: Loop guard unblocking port [chars] on [chars].

Explanation The interface has received a BPDU. If the inconsistency was caused by a unidirectional link failure, the problem no longer exists. The loop-guard-inconsistency is cleared for the interface, which is taken out of the blocking state, if appropriate. The first [chars] is the name of this port, and the second [chars] is the spanning-tree mode displayed in the **show spanning-tree** privileged EXEC command.

Recommended Action No action is required.

Error Message SPANTREE-2-PVSTSIM_FAIL: Superior PVST BPDU received on VLAN [dec] port [chars], claiming root [dec]:[enet]. Invoking root guard to block the port.

Explanation The root guard blocked a port that might cause a spanning-tree loop. When a PVST+ switch is connected to an multiple spanning-tree (MST) switch, the IST root (MSTOO) becomes the root for all PVST+ spanning trees. A loop can occur if any of the PVST+ spanning trees have a better root than IST. To prevent the loop, root guard blocks the port on the MST switch that receives the superior message from the PVST+ side. The first [dec] is the VLAN ID, [chars] is the short interface name, such as Gi0/1, the second [dec] is the root bridge priority, and [enet] is the root bridge MAC address.

Recommended Action When STP converges after a new switch or switch port is added to the topology, root guard might temporarily block the port and then automatically restore it. If the port remains blocked, identify the root bridge from this error message, and configure a less favorable priority for the VLAN spanning tree. There could be other superior PVST roots, and the port cannot recover until all such roots are cleared. Alternatively, try disabling and then enabling the VLAN port.

Error Message SPANTREE-2-RECV_1Q_NON_1QTRUNK: Received 802.1Q BPDU on non 802.1Q trunk [chars] [chars].

Explanation The interface that received a Shared Spanning Tree Protocol (SSTP) BPDU was in trunk mode but was not using 802.1Q encapsulation. The first [chars] is the interface, and the second [chars] is the VLAN.

Recommended Action Verify that the configuration and operational state of the listed interface and that of the interface to which it is connected are in the same mode (*access* or *trunk*). If the mode is trunk, verify that both interfaces have the same encapsulation (*ISL* or *802.1Q*). If the encapsulation types are different, use the **switchport trunk encapsulation** interface configuration command to make them consistent. When the encapsulation is consistent, spanning tree automatically unblocks the interface.

Error Message SPANTREE-2-RECV_BAD_TLV: Received SSTP BPDU with bad TLV on [chars] [chars].

Explanation The interface received an SSTP BPDU without the VLAN ID tag. The BPDU is discarded. The first [chars] is the interface, and the second [chars] is the VLAN that received the SSTP BPDU.

Recommended Action If this message recurs, copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer vlan id [dec] on [chars] [chars].

Explanation The listed interface received an SSTP BPDU that is tagged with a VLAN ID that does not match the VLAN ID that received the BPDU. This occurs when the native VLAN is not consistently configured on both ends of an 802.1Q trunk. [dec] is the VLAN ID, the first [chars] is the port, and the second [chars] is the VLAN.

Recommended Action Verify that the configurations of the native VLAN ID is consistent on the interfaces on each end of the 802.1Q trunk connection. When the configurations are consistent, spanning tree automatically unblocks the interfaces.

Error Message SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port [chars] on [chars].

Explanation The listed interface received a BPDU that advertises a superior spanning-tree root bridge (lower bridge ID, lower path cost, and so forth) than that in use. The interface is put into blocking state and marked as *root-guard inconsistent* to prevent a suboptimal spanning-tree topology from forming. The first [chars] is the name of this port, and the second [chars] is the spanning-tree mode displayed in the output of the **show spanning-tree** privileged EXEC command.

Recommended Action Enter the **show spanning-tree inconsistentports** privileged EXEC command to review the list of interfaces with root-guard inconsistencies. Determine why devices connected to the listed ports are sending BPDUs with a superior root bridge, and take action to prevent more occurrences. When the inaccurate BPDUs have been stopped, the interfaces automatically recover and resume normal operation. Make sure that it is appropriate to have root guard enabled on the interface.

Error Message SPANTREE-2-ROOTGUARD_CONFIG_CHANGE: Root guard [chars] on port [chars] on [chars].

Explanation The spanning-tree root guard configuration for the listed interface has changed. If enabled, any BPDU received on this interface that advertises a superior spanning-tree root bridge (lower bridge ID, lower path cost, and so forth) to that already in use causes the interface to be put into the blocking state and marked as *root-guard inconsistent*. The first [chars] is the root-guard state (*enable* or *disable*), the second [chars] is the interface, and the third [chars] is the spanning-tree instance.

Recommended Action Verify that this is the desired configuration for the listed interface. Correct it if it is not the desired configuration.

Error Message SPANTREE-2-ROOTGUARD_UNBLOCK: Root guard unblocking port [chars] on [chars].

Explanation The listed interface is no longer receiving BPDUs advertising a superior root bridge (lower bridge ID, lower path cost, and so forth). The root-guard inconsistency is cleared for the interface, and the blocking state is removed from the interface. The first [chars] is the name of this port, and the second [chars] is the spanning-tree mode displayed in **show spanning-tree** privileged EXEC command.

Recommended Action No action is required.

Error Message SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking [chars] on [chars]. Port consistency restored.

Explanation The port VLAN ID or port type inconsistencies have been resolved, and spanning tree will unblock the listed interface of the listed spanning-tree instance. The first [chars] is the interface, and the second [chars] is the spanning-tree instance.

Recommended Action No action is required.

Error Message SPANTREE-3-BAD_PORTNUM_SIZE: Rejected an attempt to set the port number field size to [dec] bits (valid range is [dec] to [dec] bits).

Explanation An error occurred in the platform-specific code that caused it to request more or less bits than are possible. The spanning-tree port identifier is a 16-bit field, which is divided evenly between the port priority and port number, with each subfield being 8 bits. This allows the port number field to represent port numbers between 1 and 255. However, on systems with more than 255 ports, the size of port number portion of the port ID must be increased to support the number of ports. This is performed by the STP subsystem at system initialization because the maximum number of ports on a particular platform will not change. This error occurs because of an error in the platform-specific code, which causes it to request more or less bits than are possible. The first [dec] is the number of bits for the port number, and the second and third [dec] describe the valid range.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message SPANTREE-3-PORT_SELF_LOOPED: [chars] disabled.- received BPDU src mac ([enet]) same as that of interface.

Explanation The interface received a BPDU with a source MAC address that matches the one assigned to the listed interface. This means that a port might be looped back to itself, possibly because of an installed diagnostic cable. The interface will be administratively shut down. [chars] is the interface that received the BPDU, and [enet] is the source MAC address.

Recommended Action Verify the interface configuration, and test any cable connected to the interface. When the problem is resolved, re-enable the interface by entering the **no shutdown** interface configuration command.

Error Message SPANTREE-3-PRESTD_NEIGH: pre-standard MST interaction not configured ([chars]). Please, configure: 'spanning-tree mst pre-standard' on ports connected to MST pre-standard switches.

Explanation The switch has received a prestandard MST BPDU on a port that is not configured for prestandard MST BPDU transmission. In most cases, the switch automatically adjusts its mode of operation on this port and starts sending prestandard BPDUs. However, because auto-detection of prestandard neighbors might fail, we recommend that you explicitly configure the port for prestandard MST BPDU transmission. This warning message only appears once. [chars] is the interface.

Recommended Action Configure the **spanning-tree mst pre-standard** interface configuration command on all ports connected to switches running the Cisco prestandard version of MST. Cisco recommends migrating all the switches in the network to the 802.1x standard MST version.

Error Message SPANTREE-4-PORT_NOT_FORWARDING>: [chars] [chars] [chars] [chars].

Explanation The port is not forwarding packets. For example, it might not be forwarding state information. The first [chars] is the mode, the second [chars] is the severity, the third [chars] is the interface name, and the fourth [chars] is the alarm string.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message SPANTREE-5-EXTENDED_SYSID: Extended SysId [chars] for type [chars].

Explanation The extended system ID feature is either enabled or disabled for the given type of spanning tree. If enabled, the spanning-tree instance identifier is stored in the lower portion of the bridge ID priority field and limits the allowed values for the bridge priority from 0 to 61440, in increments of 4096. If disabled, the bridge ID priority field consists only of the configured priority but some spanning-tree features might not be available on a given platform (for example, support for 4096 VLANs). On some platforms, this feature might be mandatory. The first [chars] is the extended system ID state (*enable* or *disable*), and the second [chars] is the spanning-tree instance.

Recommended Action No action is required.

Error Message SPANTREE-5-ROOTCHANGE: Root Changed for [chars] [dec]: New Root Port is [chars]. New Root Mac Address is [enet].

Explanation The root switch changed for a spanning-tree instance. The first [chars] and [dec] is the interface ID for the previous root port, the second [chars] is the interface ID for the new root port, and [enet] is the Ethernet address of the new root port.

Recommended Action No action is required.

Error Message SPANTREE-5-TOPOTRAP: Topology Change Trap for [chars] [dec].

Explanation A trap was generated because of a topology change in the network. [chars] and [dec] is the interface ID.

Recommended Action No action is required.

Error Message SPANTREE-6-PORTADD_ALL_VLANS: [chars] added to all Vlans

Explanation The interface has been added to all VLANs. [chars] is the added interface.

Recommended Action No action is required.

Error Message SPANTREE-6-PORTDEL_ALL_VLANS: [chars] deleted from all Vlans

Explanation The interface has been deleted from all VLANs. [chars] is the deleted interface.

Recommended Action No action is required.

Error Message SPANTREE-6-PORT_STATE: Port [chars] instance [dec] moving from [chars] to [chars].

Explanation The port state changed. The first [chars] is the interface name. [dec] is the spanning-tree instance ID. The second [chars] is the old state (such as listening, learning, or forwarding, and so forth), and the third [chars] is the new state.

Recommended Action No action is required.

Error Message SPANTREE-7-BLOCK_PORT_TYPE: Blocking [chars] on [chars]. Inconsistent port type.

Explanation The interface is in the spanning-tree blocking state until the port-type inconsistency is resolved. The first [chars] is the interface, and the second [chars] is the spanning-tree instance.

Recommended Action Verify that the configuration and operational states of the listed interface and those of the interface to which it is connected are in the same mode (*access* or *trunk*). If the mode is trunk, verify that both interfaces have the same encapsulation (*ISL* or *802.1Q*). When these parameters are consistent, spanning tree automatically unblocks the interface.

Error Message SPANTREE-7-PORTDEL_SUCCESS: [chars] deleted from Vlan [dec].

Explanation The interface has been deleted from VLAN. [chars] is the interface, and [dec] is the VLAN ID.

Recommended Action No action is required.

Error Message SPANTREE-7-RECV_1Q_NON_TRUNK: Received 802.1Q BPDU on non trunk [chars] [chars].

Explanation An SSTP BPDU was received on the listed interface, which is not an operational trunking interface. The first [chars] is the port name, and the second [chars] is the VLAN name.

Recommended Action Verify that the configuration and operational state of the listed interface and that of the interface to which it is connected are in the same mode (*access* or *trunk*). If the mode is trunk, verify that both interfaces have the same encapsulation (*none*, *ISL*, or *802.1Q*). When these parameters are consistent, spanning tree automatically unblocks the interface.

SPANTREE_FAST Messages

Error Message SPANTREE_FAST-7-PORT_FWD_UPLINK: [chars] [chars] moved to Forwarding (UplinkFast).

Explanation The listed interface has been selected as the new path to the root switch for the listed spanning-tree instance. The first [chars] is the spanning-tree instance, and the second [chars] is the interface.

Recommended Action No action is required.

SPANTREE_VLAN_SW Messages

Error Message SPANTREE_VLAN_SW-2-MAX_INSTANCE: Platform limit of [dec] STP instances exceeded. No instance created for [chars] (port [chars]).

Explanation The number of currently active VLAN spanning-tree instances has reached a platform-specific limit. No additional VLAN instances are created until the existing number of instances drops below the platform limit. [dec] is the spanning-tree instance limit, the first [chars] is the smallest VLAN number of those VLANs that cannot have STP instances created, and the second [chars] is the port number.

Recommended Action Reduce the number of currently active spanning-tree instances by either disabling some of the currently active spanning-tree instances or deleting the VLANs associated with them. You must manually enable the spanning trees that could not be created because of limited instances.

Error Message SPANTREE_VLAN_SHIM-3-ADD_REGISTRY_FAILED: Subsystem [chars] fails to add callback function [chars]

Explanation A subsystem did not add its callback functions. Use this message only for debugging. The first [chars] is the subsystem name, and the second [chars] is the function name.

Recommended Action No action is required.

Error Message SPANTREE_VLAN_SHIM-2-MAX_INSTANCE: Platform limit of [dec] STP instances exceeded. No instance created for [chars] (port [chars]).

Explanation The number of VLAN spanning-tree instances has reached the maximum. No more VLAN instances are created until instances are less than the maximum. [dec] is the maximum, the first [chars] is the VLAN for which an STP instance is not created, and the second [chars] is the port number.

For example, when you are configuring spanning tree and the maximum is 128 instances:

- If the switch has already created 128 instances and you enter the **vlan 200-1000** global interface configuration command, the first [chars] is 200, and an STP instance for VLAN 200 is not created. STP instances are also not created for the remainder of the VLANs in the range.
- If the switch has already created 100 instances and you enter the **vlan 200-1000** global interface configuration command, the first [chars] is 228. The switch creates STP instances for VLAN 200 to VLAN 227 but not for VLAN 228. STP instances are also not created for the remainder of the VLANs in the range.

Recommended Action Reduce the number of active spanning-tree instances by either disabling some or deleting the VLANs associated with them. To create STP instances, manually create them. If you do not, the switch automatically creates an STP instances when a VLAN is created.

For example, if the switch has already created 128 instances and you want to create an STP instance for VLAN 200, remove a spanning-tree instance with one of these commands:

- To delete one of the VLANs with an STP instance, enter the **no vlan *vlan-id*** global configuration command.
- To disable spanning tree on a per-VLAN basis, enter the **no spanning-tree *vlan-id*** global configuration command.

Enter the **spanning-tree 200** global configuration command to create an instance for VLAN 200.

STORM_CONTROL Messages

Error Message STORM_CONTROL-3-FILTERED: A [chars] storm detected on [chars]. A packet filter action has been applied on the interface.

Explanation The amount of traffic detected on the interface has exceeded the configured threshold values. The system is filtering the excess traffic. The first [chars] is the traffic type, and the second [chars] is the interface.

Recommended Action Determine and fix the root cause of the excessive traffic on the interface.

Error Message STORM_CONTROL-3-SHUTDOWN: A packet storm was detected on [chars]. The interface has been disabled.

Explanation The amount of traffic detected on the interface has exceeded the configured threshold values. Because the interface is configured to shutdown if a packet storm event is detected, it has been placed in an error-disabled state. [chars] is the affected interface.

Recommended Action You can enable error-disabled recovery by using the **errdisable recovery** global configuration command to automatically re-enable the interface. You should determine and fix the root cause of the excessive traffic on the interface.

SUPERVISOR Messages

Error Message SUPERVISOR-3-FATAL: [chars]

Explanation An internal error occurred in the supervisor ASIC. [chars] is the detailed error message.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

SUPQ Messages

Error Message SUPQ-3-THROTTLE_CPU_QUEUE: Invalid application ID [dec] used for throttling

Explanation An application has passed an invalid application ID for throttle check. [dec] is the internal application identifier.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message SUPQ-4-CPUHB_RECV_STARVE: [chars].

Explanation The system has detected that messages directed to the CPU are delayed. [chars] is the detailed error message.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message SUPQ-4-CPUHB_SLOW_TRANSMIT: [chars].

Explanation The system is warning you about a slowdown of the sending interface. [chars] is the detailed error message.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message SUPQ-4-CPUHB_TX_FAIL:CPU Heartbeat TX Failed.

Explanation The system is warning you about the sending interface discarding the heartbeat message.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message SUPQ-4-PORT_QUEUE_STUCK: Port queue Stuck for ASIC [dec] port [dec] queue [dec].

Explanation The system has detected that an interface queue is not being cleared in a reasonable time. The first [dec] is the ASIC, the second [dec] is the interface, and the third [dec] is the queue number.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message SUPQ-4-RECV_QUEUE_STUCK: Receive queue Stuck for ASIC [dec] queue [dec].

Explanation The system has detected that the receive queue is not being cleared in a reasonable time. The first [dec] is the ASIC, and the second [dec] is the queue number.

Recommended Action Find out more about the error by using the **show tech-support** privileged EXEC command. Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5 for more information.

SW_DAI Messages

Error Message SW_DAI-4-ACL_DENY: [dec] Invalid ARPs ([chars]) on [chars], vlan [dec]. ([enet]/[chars]/[enet]/[chars]/[time-of-day]).

Explanation The switch has received ARP packets considered invalid by ARP inspection. The packets are erroneous, and their presence shows that administratively denied packets were seen in the network. This log message appears when packets have been denied by ACLs either explicitly or implicitly (with static ACL configuration). These packets show attempted man-in-the-middle attacks in the network. The first [dec] is the number of invalid ARP packets. The first [chars] is either Req (request) or Res (response), and the second [chars] is the short name of the ingress interface. The second [dec] is the ingress VLAN ID. [enet]/[chars]/[enet]/[chars]/[time-of-day] is the MAC address of the sender, the IP address of the sender, the MAC address of the target, the IP address of the target, and the time of day.

Recommended Action No action is required.

Error Message SW_DAI-4-DHCP_SNOOPING_DENY: [dec] Invalid ARPs ([chars]) on [chars], vlan [dec]. ([enet]/[chars]/[enet]/[chars]/[time-of-day]).

Explanation The switch has received ARP packets considered invalid by ARP inspection. The packets are erroneous, and their presence might show attempted man-in-the-middle attacks in the network. This log message appears when the IP of the sender and MAC address binding for the received VLAN is not present in the DHCP snooping database. The first [dec] is the number of invalid ARP packets. The first [chars] is either Req (request) or Res (response), and the second [chars] is the short name of the ingress interface. The second [dec] is the ingress VLAN ID. [enet]/[chars]/[enet]/[chars]/[time-of-day] is the MAC address of the sender, the IP address of the sender, the MAC address of the target, the IP address of the target, and the time of day.

Recommended Action No action is required.

Error Message SW_DAI-6-DHCP_SNOOPING_PERMIT: [dec] ARPs ([chars]) on [chars], vlan [dec]. ([enet]/[chars]/[enet]/[chars]/[time-of-day]).

Explanation The switch has received ARP packets that have been permitted because the IP and MAC address of the sender match the DHCP snooping database for the received VLAN. The first [dec] is the number of valid ARP packets. The first [chars] is either Req (request) or Res (response), and the second [chars] is the short name of the ingress interface. The second [dec] is the ingress VLAN ID. [enet]/[chars]/[enet]/[chars]/[time-of-day] is the MAC address of the sender, the IP address of the sender, the MAC address of the target, the IP address of the target, and the time of day.

Recommended Action No action is required.

Error Message SW_DAI-4-INVALID_ARP: [dec] Invalid ARPs ([chars]) on [chars], vlan [dec]. ([enet]/[chars]/[enet]/[chars]/[time-of-day]).

Explanation The switch has received ARP packets considered invalid by ARP inspection. The packets do not pass one or more validation checks of the source or destination MAC address or the IP address. The first [dec] is the number of invalid ARP packets. The first [chars] is either Req (request), Res (response), or Invalid Opcode. The second [chars] is the short name of the ingress interface. The second [dec] is the ingress VLAN ID. [enet]/[chars]/[enet]/[chars]/[time-of-day] is the MAC address of the sender, the IP address of the sender, the MAC address of the target, the IP address of the target, and the time of day.

Recommended Action No action is required.

Error Message SW_DAI-4-PACKET_BURST_RATE_EXCEEDED: [dec] packets received in [dec] seconds on [chars].

Explanation The switch has received the given number of ARP packets in the specified burst interval. The interface is in the error-disabled state when the switch receives packets at a higher rate than the configured packet rate every second over the configured burst interval. The message is logged just before the interface is placed in the error-disabled state and if the configured burst interval is more than a second. The first [dec] is the number of packets, the second [dec] is the number of seconds, and [chars] is the affected interface.

Recommended Action No action is required.

Error Message SW_DAI-4-PACKET_RATE_EXCEEDED: [dec] packets received in [dec] milliseconds on [chars].

Explanation The switch has received the given number of ARP packets for the specified duration on the interface. This message is logged just before the port is placed in the error-disabled state because of the exceeded packet rate and when the burst interval is set to 1 second. The first [dec] is the number of packets, the second [dec] is the number of milliseconds, and [chars] is the affected interface.

Recommended Action No action is required.

Error Message SW_DAI-4-SPECIAL_LOG_ENTRY: [dec] Invalid ARP packets [[time-of-day]].

Explanation The switch has received ARP packets considered invalid by ARP inspection. The packets are erroneous, and their presence might show attempted man-in-the-middle attacks in the network. This message differs from other SW_DAI messages in that this message captures all messages when the rate of incoming packets exceeds the dynamic ARP inspection logging rate. [dec] is the number of invalid ARP packets, and [time-of-day] is the time of day.

Recommended Action No action is required.

Error Message SW_DAI-6-ACL_PERMIT: [dec] ARPs ([chars]) on [chars], vlan [dec]. ([enet]/[chars]/[enet]/[chars]/[time-of-day])).

Explanation The switch has received ARP packets that are permitted as a result of an ACL match. The first [dec] is the number of valid ARP packets. The first [chars] is either Req (request) or Res (response), and the second [chars] is the short name of the ingress interface. The second [dec] is the ingress VLAN ID. [enet]/[chars]/[enet]/[chars]/[time-of-day] is the MAC address of the sender, the IP address of the sender, the MAC address of the target, the IP address of the target, and the time of day.

Recommended Action No action is required.

Error Message SW_DAI-6-DHCP_SNOOPING_PERMIT: [dec] ARPs ([chars]) on [chars], vlan [dec]. ([enet]/[chars]/[enet]/[chars]/[time-of-day])).

Explanation The switch has received ARP packets that have been permitted because the IP and MAC address of the sender match the DHCP snooping database for the received VLAN. The first [dec] is the number of valid ARP packets. The first [chars] is either Req (request) or Res (response), and the second [chars] is the short name of the ingress interface. The second [dec] is the ingress VLAN ID. [enet]/[chars]/[enet]/[chars]/[time-of-day] is the MAC address of the sender, the IP address of the sender, the MAC address of the target, the IP address of the target, and the time of day.

Recommended Action No action is required.

SW_VLAN Messages

Error Message SW_VLAN-3-MALLOC_FAIL: Failed to allocate [dec] bytes

Explanation Memory allocation failed. [dec] is the number of bytes.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message SW_VLAN-3-VLAN_DAT_CACHE_SEQUENCE: Out of sequence vlan.dat sync message. Expected: [dec]; received: [dec].

Explanation The vlan.dat file is synchronized to the STANDBY through one or more checkpoint messages from ACTIVE. The sequence number for each set of checkpoint messages starts with 1. These messages are cached at the STANDBY until the end-of-set indicator is received. The STANDBY received a checkpoint message with a sequence number that does not match the expected sequence number. The first [dec] is the expected checkpoint message sequence number, and the second [dec] is the received checkpoint message sequence number.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message SW_VLAN-3-VLAN_PM_NOTIFICATION_FAILURE: VLAN Manager synchronization failure with Port Manager over [chars].

Explanation The VLAN manager dropped a notification from the port manager because of a lack of ready pool space. [chars] is the type of port manager notification.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message SW_VLAN-3-VTP_PROTOCOL_ERROR: VTP protocol code internal error: [chars].

Explanation The VTP code encountered an unexpected error while processing a configuration request, a packet, or a timer expiration. [chars] is the internal error.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message SW_VLAN-4-BAD_PM_VLAN_COOKIE_RETURNED: VLAN manager unexpectedly received a bad PM VLAN cookie from the Port Manager, VLAN indicated: [dec].

Explanation The VLAN manager received an upcall and a VLAN cookie from the port manager that translated to a bad VLAN number. [dec] is the VLAN ID.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message SW_VLAN-4-BAD_STARTUP_VLAN_CONFIG_FILE: Failed to configure VLAN from startup-config. Fallback to use VLAN configuration file from non-volatile memory.

Explanation The VLAN software did not use the VLAN configuration from the startup-configuration file. It will use the binary VLAN configuration file in NVRAM.

Recommended Action No action is required.

Error Message SW_VLAN-4-BAD_VLAN_CONFIGURATION_FILE: VLAN configuration file contained incorrect verification word: [hex].

Explanation The VLAN configuration file read by the VLAN manager did not begin with the correct value. The VLAN configuration file is invalid, and it has been rejected. [hex] is the incorrect verification value.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message SW_VLAN-4-BAD_VLAN_CONFIGURATION_FILE_VERSION: VLAN configuration file contained unknown file version: [dec].

Explanation The VLAN configuration file read by the VLAN manager contained an unrecognized file version number, which might mean an attempt to regress to an older version of the VLAN manager software. [dec] is the file version number.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message SW_VLAN-4-BAD_VLAN_TIMER_ACTIVE_VALUE: Encountered incorrect VLAN timer active value: [chars].

Explanation As a result of a software error, a VLAN timer was detected as active when it should have been inactive or as inactive when it should have been active. [chars] is the VLAN timer active value.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message SW_VLAN-4-EXT_VLAN_INTERNAL_ERROR: Extended VLAN manager received an internal error [dec] from [chars]: [chars].

Explanation An unexpected error code was received by the VLAN manager from the extended-range VLAN configuration software. [dec] is the error code. The first [chars] is the function, and the second [chars] describes the error code.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message SW_VLAN-4-EXT_VLAN_INVALID_DATABASE_DATA: Extended VLAN manager received bad data of type [chars]: value [dec] from function [chars].

Explanation Invalid data was received by the extended-range VLAN manager from an extended-range VLAN configuration database routine. The first [chars] is the data type, [dec] is the number received, and the second [chars] is the function name.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message SW_VLAN-4-IFS_FAILURE: VLAN manager encountered file operation error: call = [chars] / file = [chars] / code = [dec] ([chars]) / bytes transferred = [dec].

Explanation The VLAN manager received an unexpected error return from a Cisco IOS file system (IFS) call while reading the VLAN database. The first [chars] is the name of the function call, the second [chars] is the file name, [dec] is the error code, the third [chars] is the textual interpretation of the error code, and the second [dec] is the number of bytes transferred.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message SW_VLAN-4-NO_PM_COOKIE_RETURNED: VLAN manager unexpectedly received a null [chars] type cookie from the Port Manager, data reference: [chars].

Explanation The VLAN manager queried the port manager for a reference cookie but received a NULL pointer instead. The first [chars] is the type of port manager cookie, and the second [chars] is the interface or VLAN that is the source of the problem.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message SW_VLAN-4-STARTUP_EXT_VLAN_CONFIG_FILE_FAILED: Failed to configure extended range VLAN from startup-config. Error [chars].

Explanation The VLAN software did not use an extended-range VLAN configuration from the startup configuration file. All extended-range VLAN configurations are lost after the system boots up. [chars] is a description of the error code.

Recommended Action No action is required.

Error Message SW_VLAN-4-VLAN_CREATE_FAIL: Failed to create VLANs [chars]: [chars].

Explanation The specified VLANs could not be created. The port manager might not have completed the VLAN creation requests because the VLANs already exist as internal VLANs. The first [chars] is the VLAN ID, and the second [chars] describes the error.

Recommended Action Check the internal VLAN usage by using **show vlan internal usage** privileged EXEC command, reconfigure the feature that is using the internal VLANs, and try to create the VLANs again. If this message appears again, copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message SW_VLAN-4-VTP_INTERNAL_ERROR: VLAN manager received an internal error [dec] from vtp function [chars]: [chars].

Explanation The VLAN manager received an unexpected error code from the VTP configuration software. [dec] is the error code, the first [chars] is the VTP function, and the second [chars] is the error-code description.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports” section on page 1-5](#).

Error Message SW_VLAN-4-VTP_INVALID_DATABASE_DATA: VLAN manager received bad data of type [chars]: value [dec] from vtp database function [chars].

Explanation The VLAN manager received invalid data from a VTP configuration database routine. The first [chars] is the data type, and [dec] is the inappropriate value that was received, and the second [chars] is the VTP database function.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message SW_VLAN-4-VTP_INVALID_EVENT_DATA: VLAN manager received bad data of type [chars]: value [dec] while being called to handle a [chars] event.

Explanation The VLAN manager received invalid data from the VTP configuration software. The first [chars] is the data type, [dec] is the value of that data, and the second [chars] is the VTP event.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message SW_VLAN-4-VTP_SEM_BUSY: VTP semaphore is unavailable for function [chars]. Semaphore locked by [chars].

Explanation The VTP database is not available. You should access the VTP database later. The first [chars] is the function name that you want to configure, and the second [chars] is the function name that is using the VTP database.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message SW_VLAN-6-OLD_CONFIG_FILE_READ: Old version [dec] VLAN configuration file detected and read OK. Version [dec] files will be written in the future.

Explanation The VLAN software detected an old version of the VLAN configuration file format. It interpreted the file but it will use the new format in the future. The first [dec] is the old version number, and the second [dec] is the new version number.

Recommended Action No action is required.

Error Message SW_VLAN-6-VLAN_DAT_CACHE_EXISTS: Unexpected vlan.dat cache exists. Removing the cache and continuing the sync with new set.

Explanation The switch functionality is unaffected.

Recommended Action No action is required.

Error Message SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to [chars].

Explanation The VTP domain name was changed through the configuration to the name specified in the message. [chars] is the changed domain name.

Recommended Action No action is required.

Error Message SW_VLAN-6-VTP_MODE_CHANGE: VLAN manager changing device mode from [chars] to [chars].

Explanation An automatic VTP-mode device-change occurred upon receipt of a VLAN configuration database message containing more than a set number of VLANs. The first [chars] is the previous mode, and the second [chars] is the current mode.

Recommended Action No action is required.

SWITCH_QOS_TB Messages

Error Message SWITCH_QOS_TB-5-TRUST_DEVICE_DETECTED: [chars] detected on port [chars], port's configured trust state is now operational.

Explanation A trusted boundary detected a device matching the trusted device setting for the port and has modified the port trust state. The first [chars] is the trusted device, and the second [chars] is the port.

Recommended Action No action is required.

Error Message SWITCH_QOS_TB-5-TRUST_DEVICE_LOST: [chars] no longer detected on port [chars], operational port trust state is now untrusted.

Explanation A trusted boundary lost contact with a trusted device and has set the port trust state to untrusted. The first [chars] is the trusted device, and the second [chars] is the port.

Recommended Action No action is required.

TCAMMGR Messages

Error Message TCAMMGR-3-GROW_ERROR: cam region [dec] can not grow.

Explanation The specified CAM region is configured as a static region with a fixed number of entries, and a caller requested to add more CAM entries. [dec] is the CAM region.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message TCAMMGR-3-HANDLE_ERROR: cam handle [hex] is invalid.

Explanation The CAM handle used by the caller is not valid. [hex] is the handle value.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message TCAMMGR-3-INDEX_ERROR: cam value/mask index [dec] is invalid.

Explanation The CAM index used by the caller is not valid. [dec] is the index value.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message TCAMMGR-3-MOVE_ERROR: cam entry move from index [int] to index [int] failed.

Explanation Moving a CAM entry from one index to another failed. [int] is the index value.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message TCAMMGR-3-REGION_ERROR: cam region [dec] is invalid.

Explanation CAM region is not valid. [dec] is the region.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

Error Message TCAMMGR-3-REGMASK_ERROR: invalid cam region [dec] mask [dec] pair.

Explanation A caller attempted to install an entry with an invalid mask for the region. Only a predetermined set of masks is allowed in a region. The first [dec] is the region, and the second [dec] is the mask.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

UDLD Messages

Error Message UDLD-0-STOPPED:UDLD process stopped:[chars].

Explanation The UDLD process stopped because it cannot read the unique system identifier that is being used by UDLD. The system identifier is used to identify the device that is sending the UDLD packets. [chars] is the UDLD process name.

Recommended Action Reload the switch by using the **reload** privileged EXEC command. If the problem persists, copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the [“Error Message Traceback Reports”](#) section on page 1-5.

VQPCIENT Messages

Error Message VQPCIENT-2-TOOMANY: Interface [chars] shutdown by active host limit.

Explanation The system has shut down the specified interface because too many hosts have requested access to that interface. [chars] is the interface name.

Recommended Action To enable the interface, remove the excess hosts, and enter the **no shutdown** interface configuration command.

Error Message VQPCIENT-3-VLANNAME: Invalid VLAN ([chars]) in response.

Explanation The VLAN membership policy server (VMPS) has specified an unknown VLAN name. [chars] is the VLAN name.

Recommended Action Ensure that the VLAN exists on the switch. Verify the VMPS configuration by entering the **show vmps** privileged EXEC command.



INDEX

Numerics

802.1x authentication messages

See DOT1X messages

A

abbreviations

char, variable field [1-5](#)

chars, variable field [1-5](#)

dec, variable field [1-5](#)

enet, variable field [1-5](#)

hex, variable field [1-5](#)

inet, variable field [1-5](#)

access control list manager messages

See ALCMGR messages

ACLMGR messages [2-3](#)

authentication messages

See DOT1X messages

B

BACKUP_INTERFACE messages [2-9](#)

BADTRANSCEIVER messages [2-9](#)

boot loader patch messages

See BSPATCH messages

BSPATCH messages [2-9](#)

bug toolkit [1-6](#)

C

Catalyst 3750-specific messages [2-47](#)

Cisco Gigabit Interface Converter messages

See GBIC_SECURITY messages

Cluster Membership Protocol messages

See CMP messages

CMP messages [2-10](#)

D

date/time-stamp designations [2-1](#)

DHCP messages [2-11](#)

DOT1Q_TUNNELLING messages [2-14](#)

DOT1X_SWITCH messages [2-20](#)

DOT1X messages [2-14](#)

DTP messages [2-23](#)

dynamic ARP inspection

See SW_DAI messages

Dynamic Host Configuration Protocol messages

See DHCP messages

Dynamic Trunking Protocol messages

See DTP messages

E

EC messages [2-25](#)

enhanced services forwarding messages

See ESF messages

ESF messages [2-30](#)

ETHCNTR messages [2-30](#)

EtherChannel controller messages

See ETHCNTR messages

EtherChannel messages

See EC messages

EXPRESS_SETUP messages [2-31](#)

F

facility codes [1-1](#)

fallback bridging manager messages
See PLATFORM_FBM messages

Flex Link messages
See BACKUP_INTERFACE messages

format of system messages [1-1](#)

FRNTEND_CTRLR messages [2-32](#)

G

GBIC_SECURITY_CRYPT messages [2-34](#)

GBIC_SECURITY_UNIQUE messages [2-35](#)

GBIC_SECURITY messages [2-32](#)

H

HARDWARE messages [2-35](#)

HLFM messages [2-37](#)

I

IDBMAN messages [2-38](#)

interface database manager messages
See IDBMAN messages

L

local forwarding manager messages
See HLFM messages

M

MAC_LIMIT messages [2-42](#)

MAC_MOVE messages [2-43](#)

MAC address table messages [2-42](#)

message codes [1-1](#)

message mnemonic code [1-5](#)

messages

802.1x [2-14](#)

ACLMGR [2-3](#)

BACKUP_INTERFACE [2-9](#)

BADTRANSCEIVER [2-9](#)

BSPATCH [2-9](#)

CMP [2-10](#)

DHCP [2-11](#)

DOT1Q_TUNNELLING [2-14](#)

DOT1X [2-14](#)

DOT1X_SWITCH [2-20](#)

DTP [2-23, 2-25](#)

EC [2-25](#)

ESF [2-30](#)

ETHCNTR [2-30](#)

EXPRESS_SETUP [2-31](#)

FRNTEND_CTRLR [2-32](#)

GBIC_SECURITY [2-32](#)

GBIC_SECURITY_CRYPT [2-34](#)

GBIC_SECURITY_UNIQUE [2-35](#)

HARDWARE [2-35](#)

HLFM [2-37](#)

IDBMAN [2-38](#)

MAC_LIMIT [2-42](#)

MAC_MOVE [2-43](#)

PAGP_DUAL_ACTIVE [2-43](#)

PHY [2-44](#)

PIMSN [2-46](#)

PLATFORM [2-46](#)

PLATFORM_CAT3750 [2-47](#)

PLATFORM_FBM [2-47](#)

PLATFORM_PBR [2-48](#)

PLATFORM_PM [2-50](#)

PLATFORM_SPAN [2-51](#)

PLATFORM_UCAST [2-51](#)

PLATFORM_VLAN [2-53](#)

PM [2-54](#)

PORT_SECURITY [2-62](#)

QOSMGR [2-63](#)
 REP [2-68](#)
 RMON [2-69](#)
 SPAN [2-70](#)
 SPANTREE [2-71](#)
 SPANTREE_FAST [2-78](#)
 SPANTREE_VLAN_SW [2-79](#)
 SPANTREE_VLAN_SWITCH [2-79](#)
 STORM_CONTROL [2-80](#)
 SUPERVISOR [2-80](#)
 SUPQ [2-81](#)
 SW_DAI [2-83](#)
 SW_VLAN [2-85](#)
 SWITCH_QOS_TB [2-91](#)
 TCAMMGR [2-92](#)
 UDLD [2-93](#)
 VQPCCLIENT [2-94](#)

message severity levels [1-4](#)

O

output interpreter [1-6](#)

P

PAGP_DUAL_ACTIVE messages [2-43](#)
 PHY messages [2-44](#)
 PIMSN messages [2-46](#)
 PIM snooping messages [2-46](#)
 PLATFORM_FBM messages [2-47](#)
 PLATFORM_PBR messages [2-48](#)
 PLATFORM_PM messages [2-50](#)
 PLATFORM_SPAN messages [2-51](#)
 PLATFORM_UCAST messages [2-51](#)
 PLATFORM_VLAN messages [2-53](#)
 PLATFORM messages [2-46](#)
 PM messages [2-54](#)
 policy-based routing messages

See PLATFORM_PBR messages

PORT_SECURITY messages [2-62](#)

port manager messages

See PM messages

port manager messages, platform

See PLATFORM_PM messages

Q

QOSMGR messages [2-63](#)

quality of service manager messages

See QOSMGR messages

R

REP messages [2-68](#)

Resilient Ethernet Protocol messages

See REP messages

RMON messages [2-69](#)

S

SFP security messages

See GBIC_SECURITY messages

SPAN messages [2-70](#)

spanning-tree fast-convergence

See SPANTREE_FAST messages

spanning-tree messages

See SPANTREE messages

spanning-tree per-VLAN messages

See SPANTREE_VLAN_SWITCH messages

SPANTREE_FAST messages [2-78](#)

SPANTREE_VLAN_SWITCH messages [2-79](#)

SPANTREE_VLAN_SW messages [2-79](#)

SPANTREE messages [2-71](#)

STORM_CONTROL messages [2-80](#)

SUPERVISOR messages [2-80](#)

SUPQ messages [2-81](#)

SW_DAI messages [2-83](#)
 SWITCH_QOS_TB messages [2-91](#)
 Switched Port Analyzer messages
 See SPAN messages
 Switched Port Analyzer messages, platform
 See PLATFORM_SPAN messages
 system messages
 facility codes [1-1](#)
 format [1-1](#)
 message text definition [1-5](#)
 mnemonic code [1-5](#)
 severity levels [1-4](#)
 variable fields [1-5](#)

T

tables
 facility codes [1-1](#)
 variable fields [1-5](#)
 TAC, contacting [1-6](#)
 TCAM manager messages [2-92](#)
 TCAMMGR messages [2-92](#)
 ternary content addressable memory manager messages
 See TCAMMGR messages
 time-stamp information [1-1](#)
 traceback reports [1-5](#)
 transceiver messages [2-9](#)
 trusted boundary messages
 See SWITCH_QOS_TB messages

U

UDLD messages [2-93](#)
 unicast routing messages
 See PLATFORM_UCAST messages
 UniDirectional Link Detection messages
 See UDLD messages

V

VLAN manager messages [2-85](#)
 VLAN Query Protocol messages
 See VQPCLIENT messages
 VQPCLIENT messages [2-94](#)
 VTP messages
 See SW_VLAN messages