Common CatOS Error Messages on Catalyst 6500/6000 Series Switches

Document ID: 29804

Contents

KERNEL−1−CREATEPROCESSFAILED
PI_CI_S_CBL_DROP_REG

Related Information

Introduction

This document provides a brief explanation of common syslog and error messages that you see on Catalyst 6500/6000 series switches that run Catalyst OS (CatOS) software.

Use the Error Message Decoder Tool (registered customers only) if you have an error message that does not appear in this document. This tool provides the meaning of error messages that Cisco IOS® Software and CatOS software generate.

Note: The exact format of the syslog and error messages that this document describes can vary slightly. The variation depends on the software release that you run on the switch Supervisor Engine.

Note: Cisco recommends this minimum logging configuration on the Catalyst 6500/6000 series switches:

- Issue the **set time** command in order to set the date and time on the switch. Or configure the switch to use the Network Time Protocol (NTP) in order to obtain the date and time from an NTP server.
- Ensure that logging and logging time stamps are enabled, which is the default.
- Configure the switch to log to a syslog server, if possible.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Error Messages on Catalyst 6500/6000 Series Switches

The messages in this section are common error messages that you see on Catalyst 6500/6000 series switches that run CatOS.

%CDP−4−NVLANMISMATCH: Native vlan mismatch detected on port [dec]/[dec]

Problem

The switch generates frequent `%CDP−4−NVLANMISMATCH` syslog messages.

Description

This example shows the console output that you see when this error message occurs on the switch:

```
2002 Jan 11 08:50:40 EST -05:00 %CDP-4-NVLANMISMATCH:
   Native vlan mismatch detected on port 4/1
2002 Jan 11 02:02:45 %CDP-4-NVLANMISMATCH:
   Native vlan mismatch detected on port 1/1
```

The switch generates this message whenever the switch port is physically connected to another switch or router. This message appears on the switch because the configured native VLAN on the port is different than the native VLAN on the connecting switch/router port.

A trunk port that you have configured with IEEE 802.1Q tagging can receive both tagged and untagged traffic. By default, the switch forwards untagged traffic with the native VLAN that is configured for the port. If a packet has a VLAN ID that is the same as the outgoing port native VLAN ID, the switch transmits the packet untagged. Otherwise, the switch transmits the packet with a tag.

Ensure that the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, the traffic of the native VLANs on both sides cannot transmit correctly on the trunk. This problem can imply some connectivity issues in your network.

Issue the **show trunk** *mod/port* command in order to verify the native VLAN that is configured on your switch. In this command, *mod/port* is the trunk port. Here is sample output:

```
Console> (enable) show trunk 5/24
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 5/24     desirable    dot1q          not-trunking  1

Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 5/24     1-1005

Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
 5/24     1

Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
 5/24

Console> (enable)
```

Issue the **set vlan** *vlan_id mod/port* command in order to change the native VLAN that is configured on the trunk port. In this command, *mod/port* is the trunk port.

Note: The syslog error message `"%CDP-4-NATIVE_VLAN_MISMATCH"` is an indication of a native VLAN mismatch in Catalyst switches that run Cisco IOS Software.

Note: If switches are connected with the use of the nontrunk ports, ensure that you configure the ports to be in the same VLAN. If the ports are not in the same VLAN, you get the error message `%CDP-4-NVLANMISMATCH: Native vlan mismatch detected on port [port num]`.

DTP−1−ILGLCFG: Illegal config (on, isl−−on,dot1q) on Port [mod/port]

Problem

The switch generates `DTP−1−ILGLCFG: Illegal config (on, isl−−on,dot1q) on Port [mod/port]` errors.

Description

This message can occur if you have set both sides of the trunk to `on`, but the encapsulation types (`isl`, `dot1q`) do not match. If you have set the trunk modes to `desirable`, the trunk does not come up because of this misconfiguration. Check the output of the **show trunk** command on both ends in order to troubleshoot. Be sure that the encapsulation types are the same.

%IP−3−UDP_SOCKOVFL:UDP socket overflow

Problem

The switch generates periodic `%IP−3−UDP_SOCKOVFL:UDP socket overflow` syslog messages.

Description

This example shows the console output that you see when this error occurs:

Note: The User Datagram Protocol (UDP) socket number that displays can vary or be consistently the same.

```
%IP−3−UDP_SOCKOVFL:UDP socket 2353 overflow
%IP−3−UDP_SOCKOVFL:UDP socket 2353 overflow
%IP−3−UDP_SOCKOVFL:UDP socket 2353 overflow
%IP−3−UDP_SOCKOVFL:UDP socket 2353 overflow
```

The switch generates this syslog message when the buffer that is allocated for incoming packets on the specified socket (the UDP destination port) is full. This buffer is full because the rate of traffic that is destined for the socket is too high. For example, this condition can happen when a network management station sends a large number of Simple Network Management Protocol (SNMP) queries. When UDP overflow happens, try to reduce the number of SNMP queries. In order to reduce the number of queries, increase the polling interval on the network management station or reduce the number of MIB objects that the network management station polls.

In the example in this section, the switch received an excessive number of packets that were destined for the switch IP address (or the broadcast address) with destination UDP socket 2353. Because the input buffer for this socket on the switch is full, the switch generates a syslog message. Issue the **show netstat udp** command in order to see the number of times that the switch reached the overflow condition.

```
Console> (enable) show netstat udp
udp:
        0 incomplete headers
        0 bad data length fields
        0 bad checksums
        0 socket overflows
        110483 no such ports
Console> (enable)
```

These syslog messages indicate that one or more stations send a large amount of UDP traffic to the switch on the specified destination UDP ports. If the switch generates an excessive number of these messages, use a network analyzer in order to identify the source of the traffic. Then, reduce the rate of traffic. Because the

UDP traffic is destined to the CPU of the switch, you can use the Switched Port Analyzer (SPAN) function and set the source port to sc0. The SPAN identifies the internal interface for the Supervisor Engine. Refer to Catalyst Switched Port Analyzer (SPAN) Configuration Example for more information.

Note: Do not worry about the `no such port` counter. This counter shows the number of UDP packets that the switch received that were destined for nonexistent ports.

%EC−SP−5−L3DONTBNDL1: TE (mod/port) suspended: PAgP not enabled on the remote port

Problem

The switch generates the `%EC−SP−5−L3DONTBNDL1: TE(mod/port)suspended: PAgP not enabled on the remote port` error message .

Description

This error message generally occurs when Port Aggregation Protocol (PAgP) is enabled on the Layer 3 (L3) interface, but the partner port is not enabled for PAgP. Here is an example:

```
%EC−SP−5−L3DONTBNDL1: Te(mod/port)suspended: PAgP not enabled on the remote port.
%EC−SP−5−L3DONTBNDL1: Te(mod/port)suspended: PAgP not enabled on the remote port.
%EC−SP−5−L3DONTBNDL1: Te(mod/port)suspended: PAgP not enabled on the remote port.
```

The error message most likely occurs because of configuration issues, but it can also be a result of hardware/cabling issues. Ensure that the configuration is in accordance with the configuration guide. If the error persists, troubleshoot the cabling and hardware. In order to troubleshoot the hardware, try these methods:

- Reseat the Gigabit Interface Converter (GBIC).
- Replace the GBIC.
- Test the hardware with a different line card.

%IP−3−UDP_BADCKSUM:UDP bad checksum

Problem

The switch generates periodic `%IP−3−UDP_SOCKOVFL:UDP socket overflow` syslog messages.

Description

This example shows the console output that you see when this error occurs:

Note: The UDP socket number that displays can vary or be consistently the same.

```
%IP−3−UDP_BADCKSUM:UDP bad checksum
```

The switch generates this syslog message when the switch detects a bad checksum on a UDP datagram, such as SNMP packets. The UDP datagram header carries a checksum that the receiving network device checks in order to verify that the datagram became corrupt during transit. If the received checksum does not match the checksum value in the header, the device drops the datagram and logs an error message. Issue the **show netstat udp** command in order to see the number of times that the switch detected a checksum datagram with an error.

```
Console> (enable) show netstat udp
```

```
udp:
        0 incomplete headers
        0 bad data length fields
        0 bad checksums
        0 socket overflows
        110483 no such ports
Console> (enable)
```

This message is informational only. A network device sends bad packets to the switch and causes the error message. Use a network analyzer in order to identify the source of the traffic. Because the UDP traffic is destined to the CPU of the switch, you can use the SPAN function and set the source port to sc0. The SPAN identifies the internal interface for the Supervisor Engine. Refer to Catalyst Switched Port Analyzer (SPAN) Configuration Example for more information.

Note: Do not worry about the `no such port` counter. This counter shows the number of UDP packets that the switch received that were destined for nonexistent ports.

%KERNEL−5−UNALIGNACCESS:Alignment correction made

Problem

The switch generates periodic `%KERNEL−5−UNALIGNACCESS:Alignment correction made` syslog messages.

Description

This example shows the syslog output that you see when this error occurs:

```
%KERNEL−5−UNALIGNACCESS:Alignment correction made at 0x80056B3C reading 0x81B82F36
%KERNEL−5−UNALIGNACCESS:Alignment correction made at 0x80056B88 reading 0x81B82F36
%KERNEL−5−UNALIGNACCESS:Alignment correction made at 0x80056B3C reading 0x81BF1DB6
%KERNEL−5−UNALIGNACCESS:Alignment correction made at 0x80056B88 reading 0x81BF1DB6
```

These syslog messages indicate that the switch CPU detected and corrected an alignment error during an attempt to access data in DRAM. These messages are informational only. The messages do not indicate a problem with the switch and do not affect system performance.

In some cases, you see an excessive number of these messages. For example, these messages can flood your syslog server log file or your switch console. If you receive an excess of the messages, consider an upgrade of the switch software to the latest maintenance release for your software release train. Or issue the **set logging level kernel 4 default** command in order to modify the logging level for the `Kernel` facility to 4 or lower.

If you upgrade to the latest maintenance release but still receive these syslog messages, create a service request with Cisco Technical Support.

%MCAST−4−RX_JNRANGE:IGMP: Rcvd Report in the range

Problem

The switch generates `Invalid traffic from multicast source address` messages.

Description

This example shows the syslog output that you see when this error occurs:

```
%MCAST−4−RX_JNRANGE:IGMP: Rcvd Report in the range 01−00−5e−00−00−xx
```

The `Rcvd Report in the range` syslog message is informational only. The switch generates this message at the receipt of Internet Group Management Protocol (IGMP) report packets with a multicast MAC address that starts with 01−00−5e−00−00−*xx*. This Layer 2 (L2) range of addresses is equivalent to a L3 multicast address range between 224.0.0.0 and 224.0.0.255. These addresses are reserved for the use of routing protocols and other low−level topology discovery or maintenance protocols. Examples of these protocols include gateway discovery and group membership reporting.

Use a packet capture tool such as a sniffer and filter on IGMP messages in order to troubleshoot this problem. In addition, you can use the Catalyst SPAN function in order to copy packets from a port that you suspect receives these messages from a network device. In order to suppress these messages, issue the command **set logging level mcast 2 default**. This command changes the logging level of multicast messages to 2.

Use the ports that the **show multicast router** command shows and/or any uplinks to the core of the network as the SPAN source ports. In the case that these ports are trunk ports, also configure the SPAN destination port as a trunk port. Issue the **show trunk** command in order to verify that the ports are trunk ports.

%MCAST−2−IGMP_FALLBACK:IGMP: Running in FALL BACK mode

Problem

A switch that has IGMP snooping enabled displays the `%MCAST−2−IGMP_FALLBACK:IGMP: Running in FALL BACK mode` error message.

Description

This example shows the syslog output that you see when this error occurs:

```
%MCAST−2−IGMP_ADDRAL:IGMP: Address Aliasing for 01−00−5e−00−00−01
%MCAST−2−IGMP_FALLBACK:IGMP: Running in FALL BACK mode
```

The switch generates this syslog message when the switch receives excessive multicast traffic that is destined for a multicast MAC address in the 01−00−5e−00−00−*xx* range. IGMP snooping does not support multicast streams to addresses in this MAC address range. This lack of support is because MAC addresses in this range are also used for IGMP control traffic, such as leaves, joins, and general queries. In the example in this section, the switch receives an excessive amount of traffic with the destination MAC address 01−00−5e−00−00−01. This message indicates that the Network Management Processor (NMP) detects a multicast data stream that disabled the protocol redirection escape logic. The stream is aliased to one of these special multicast addresses:

```
01−00−5e−00−00−01
01−00−5e−00−00−04
01−00−5e−00−00−05
01−00−5e−00−00−06
01−00−5e−00−00−0d
```

When the switch detects a high rate of such traffic, the switch stops snooping packets with the specified destination MAC address for a short period of time. This freeze is called fallback mode. Then, the switch starts snooping again, which is called normal mode. The switch generates the syslog message that this section describes when the switch runs in fallback mode.

Take either one of these approaches in order to detect which switch generates traffic to 01−00−5e−00−01:

- Issue the **set span sc0** *mod/port* command in order to monitor the sc0 port and send the traffic to a sniffer. The SPAN shows all traffic that is directed to the CPU of the switch.

Note: The traffic to these MAC addresses is only redirected to the CPU when the switch is not in fallback mode. When the switch is in fallback mode, the switch does not allow the packets to go to the CPU in order to avoid a traffic flood.

- If you run software version 6.3(10), 7.4(3), or later, there are additional syslog messages that tell you the offending source MAC address, source port, and source IP address. Refer to these syslog messages, which look similar to this:

```
2003 Jan 24 04:07:43 %MCAST−2−IGMP_ADDRAL:IGMP:
   Address Aliasing for 224.0.0.1
2003 Jan 24 04:07:43 %MCAST−2−IGMP_FALLBACK:IGMP:
   Running in FALL BACK mode
2003 Jan 24 04:07:43 %MCAST−2−IGMP_ADDRALDETAILS:IGMP:
   Multicast address aliasing: From 00−00−0c−11−22−33
   (3.3.3.33) on 1/2 to 01−00−5e−00−00−01 (224.0.0.1)
```

The solution is to isolate the host that generates this type of multicast traffic. Verify which address gets aliased. Try not to use this address for the multicast data feed. In the syslog message, you can find the location of the host in order to find out why the host sends this traffic. In this example, the location of the host is `3.3.3.33`.

%MGMT−4−OUTOFNVRAM: Out of NVRAM space: ([dec],[dec],[dec],[dec])

Problem

The switch generates `MGMT−4−OUTOFNVRAM:Out of NVRAM space` syslog messages.

Description

You see a message that is similar to this when the system runs out of NVRAM space:

```
%MGMT−4−OUTOFNVRAM:Out of NVRAM space:  (62,39204,524288,24976)
```

This message indicates that an NVRAM write operation fails because of a lack of space. The four [dec] that appear in parentheses indicate:

- First [dec] The configuration block that is written to NVRAM
- Second [dec] The size of the configuration that is written to NVRAM
- Third [dec] The total NVRAM size in the system
- Fourth [dec] The amount of NVRAM space that is available

The workaround is to change the system configuration from the default binary mode to the text mode. You use text mode if the configuration is too large for storage in binary format in the NVRAM. The text−based method does not write the configuration changes to NVRAM as you type in the changes. Instead, this method stores the changes in DRAM until you issue the **write memory** command from the command line. Refer to the *Setting the Text File Configuration Mode* section of the document Working with the Flash File System for further configuration instructions.

Note: Only the QoS and security access control list (ACL) configuration and module−related configuration are deleted when you use the text mode. The rest of the configuration is saved in the NVRAM in binary format, as before.

Cannot enable text mode config if ACL config is cleared from nvram

Problem

The switch generates the `Cannot enable text mode config if ACL config is cleared from nvram` error message.

Description

The switch generates this message during an attempt to change from a binary mode configuration to text mode configuration at a time when the current committed ACL configuration is not saved in NVRAM..

In most cases, you can issue the **set config acl nvram** command in order to solve this problem. The command copies the current committed ACL configuration from DRAM back into NVRAM.

MGMT−5−LOGIN_FAIL:User failed to log in from Console

Problem

The switch generates `MGMT−5−LOGIN_FAIL:User failed to log in from Console` errors.

Description

This message possibly indicates a problem with the terminal server that connects to the console port of the switch. When the switch console is connected to an async line of a terminal server and you perform a soft reset on the switch, garbage (random characters) streams across the screen for several minutes. If TACACS is enabled on the switch, several minutes can turn into several days as TACACS buffers and processes the garbage piece by piece. The workaround is to issue the **no exec** command on the async line to which the switch connects.

Note: Even after you issue the **no exec** command, the messages continue until the buffer is clear.

%PAGP−5−PORTFROMSTP / %PAGP−5−PORTTOSTP

Problem

The switch generates frequent `%PAGP−5−PORTFROMSTP` and `%PAGP−5−PORTTOSTP` syslog messages.

Description

This example shows the console output that you see when the switch generates these syslog messages:

```
%PAGP−5−PORTFROMSTP:Port 3/3 left bridge port 3/3
%PAGP−5−PORTTOSTP:Port 3/3 joined bridge port 3/3
%PM_SCP−SP−4−LCP_FW_ABLC
```

The PAgP logging facility reports events that involve PAgP. You use PAgP to negotiate EtherChannel links between switches. The switch generates the `%PAGP−5−PORTFROMSTP` syslog message at the loss of a link on a switch port. The switch generates the `%PAGP−5−PORTTOSTP` syslog message at the detection of a link on a switch port. These syslogs are normal, informational messages that indicate the addition or removal of a port from the spanning tree.

Note: The enablement of channeling is not necessary for these messages to appear.

In the example in this section, the switch first lost the link on port 3/3, which removed the port from the spanning tree. Then, the switch again detected the link on the port, which added the port back into the spanning tree.

If you see these messages frequently for a particular port, the link is flapping, which means that the link is constantly lost and regained. Investigate the cause. Typical causes of link flapping on a switch port include:

- Speed/duplex mismatch
- Late collision
- Faulty cable
- Faulty Network Interface Card (NIC) or other end station problem
- Faulty switch port
- Other misconfiguration

If you want to suppress these syslog messages, issue the **set logging level pagp 4 default** command in order to modify the logging level for the PAgP facility to 4 or lower. The default logging level for PAgP is 5.

%SPANTREE−3−PORTDEL_FAILNOTFOUND

Problem

The switch generates periodic %SPANTREE−3−PORTDEL_FAILNOTFOUND syslog messages.

Description

This example shows the syslog output that you see when this error occurs:

```
%SPANTREE−3−PORTDEL_FAILNOTFOUND:9/5 in vlan 10 not found (PAgP_Group_Rx)
```

These syslog messages indicate that the PAgP attempted to remove a port from the spanning tree for the specified VLAN, but the port was not in the spanning tree data structure for that VLAN. Typically, another process, such as the Dynamic Trunking Protocol (DTP), has already removed the port from the spanning tree.

These messages typically accompany %PAGP−5−PORTFROMSTP messages. The messages are for debug purposes. The messages do not indicate a problem with the switch and do not affect switching performance. In addition, these messages are not logged unless you have changed the default SPANTREE facility logging configuration. The default logging level for SPANTREE is 2.

In some cases, you see an excessive number of these messages. For example, these messages can flood your switch console. If you receive an excess of the messages, consider an upgrade of the switch software to the latest maintenance release for your software release train. In most cases, later software releases suppress these messages.

%SYS−1−CFG_RESTORE:[chars] block restored from backup

Problem

The switch generates %SYS−1−CFG_RESTORE syslog messages.

Description

This example shows the console output that you see when this error message occurs on the switch:

```
2005 Oct 14 14:36:26 %SYS−1−CFG_RESTORE:Global block restored from backup
```

These messages are informational only. The NVRAM monitoring feature, which was introduced in version 6.4(x), generates these messages. The messages basically report that there was a corrupted block in NVRAM and that the configuration was restored from backup. The [chars] is the block type that the user or process can modify. Checks for corrupted blocks in NVRAM are performed by default. Any block that is corrupted is restored with the copy that is in DRAM. Therefore, the configuration is not lost.

%SYS−1−SYS_OVERPWRRTNG:System drawing more power than the power supply rating

Problem

The switch generates periodic `%SYS−1−SYS_OVERPWRRTNG` syslog messages.

Description

This example shows the console output that you see when this error occurs on the switch:

```
Oct 13 11:27:11 %SYS−1−SYS_OVERPWRRTNG:System drawing more power than the power supply
rating
Oct 13 11:27:11 %SYS−1−SYS_OVERPWRRTNG:System drawing more power than the power supply
rating
```

This message indicates that the system draws more power than the power supply rating. The power management LED is lit red. This condition occurs only when the system is fully configured and the Supervisor Engines draw unequal power.

The workaround is to reseat the power supplies and then upgrade the Supervisor Engine software to a version that supports the hardware. Refer to the *Supported Hardware* section of the Cisco Catalyst 6500 Series Switches Release Notes for the relevant release.

%SYS−1−MOD_DCPWRMISMATCH:Module [num] DC power failure detected during polling

Problem

The switch generates periodic `%SYS−1−MOD_DCPWRMISMATCH:Module[num]DC power failure detected during polling` syslog messages.

Description

This example shows the console output that you see when this error occurs on the switch:

```
%SYS−1−MOD_DCPWRMISMATCH:Module[num]DC power failure detected during polling
```

This message occurs because of any of these issues:

- The line card is not properly seated in the chassis.

  Reseat the line card.
- The chassis slot is faulty.

  Check for bent pins. Test the line card in a different slot.
- The line card is faulty.

Contact Cisco Technical Support.

%SYS−1−MOD_SEQMISMATCH:Bus asic sequence mismatch occurred on module

Problem

On the Catalyst 6000 switches with redundant Supervisor Engines (Multilayer Switch Feature Card [MSFC] and Policy Feature Card [PFC]), this bus ASIC sequence mismatch can occur within a switchover:

```
SYS−1−MOD_SEQMISMATCH: Bus asic sequence mismatch occurred on module
[dec] (asic=[dec], srcidx=0x[hex], seq=[dec])
```

Description

This example shows the console output that you see when this error occurs on the switch:

```
%SYS−1−MOD_SEQMISMATCH:Bus asic sequence mismatch occurred on module 7
(asic=1, srcidx=0x0, seq=0)
```

The error is on the Switch−Module Configuration Protocol (SCP) bus that communicates between the Supervisor and the line cards. The Supervisor sends out a heartbeat to the line cards, and these line cards do not respond appropriately to the Supervisor.

These error messages can be caused by any of these reasons:

- The supervisor engine is excessively busy
- The Spanning Tree Protocol (STP) loops
- The ACLs and QoS policers throttle or drop traffic over the inband communications channel
- Port ASIC synchronization problems or Switch Fabric Module problems
- Hardware Failure or improperly seated module

In some cases, these messages are also observed in line cards: WS−X6348−RJ45 and WS−X6516−GBIC.

This message has no impact and can be ignored. As a workaround, physically reseat the module and re−insert it firmly. The line cards are hot swappable, and they can use the same slot as the original locations so that all ports match with the Supervisor configuration.

%SYS−3−EOBC_CHANNELREINIT

Problem

The switch generates `%SYS−3−EOBC_CHANNELREINIT` syslog messages.

Description

These examples show the syslog output that you see when this error occurs:

- CatOS version 6.3.8, 7.3.2, and 7.5.1:

  ```
  %SYS−3−EOBC_CHANNELREINIT:Ethernet out of band channel reinitialized (1)
  ```
- CatOS version 7.6(6):

  ```
  %SYS−5−EOBC_CHANNELREINIT:Ethernet out of band channel reinitialized (1)
  ```

CatOS versions 6.3.8, 7.3.2, and 7.5.1 introduced this message. The message displays for a nonfatal error condition. The message indicates that both these occurrences have taken place:

- The switch has detected an Ethernet out−of−band channel (EOBC) transmit (Tx) queue−stuck condition on the system controller application−specific integrated circuit (ASIC).
- The ASIC has been reinitialized without a reset of the switch.

Note: The presence of a card with a faulty EOBC buffer can also cause the message.

The EOBC is a 100 Mbps half−duplex connection that the supervisors and line cards use to communicate over the backplane. Because they are half−duplex, collisions are expected on this in the communication channel. It is normal if these messages are reported occasionally since it is part of the self−recovery process.

The data traffic continues to flow through the switch. This message is informational only and requires no action. Later software releases include a change in the severity level of the message so that the severity coincides with the severity of the error. If you see this message very frequently, there can be more chances for control traffic drops, which is a cause for concern. If re−initialized messages appear in a close interval, contact Cisco Technical Support for further investigation.

%SYS−3−SYS_MEMERR:[chars] while [chars] address 0x[hex]

Problem

These error messages appear in the syslog:

- `%SYS−3−SYS_MEMERR:Bad magic number while freeing address 0x82175564`

  or
- `%SYS−3−SYS_MEMERR:Bad process id while allocating address 0x80ea51a4`

Description

These error messages indicate that memory management has detected memory corruption. The first [chars] can be one of these phrases:

- `Out of range`
- `Bad alignment`
- `Block is not free`
- `Back pointer mismatch`
- `Bad magic number`
- `Succeeding block out of range`
- `Succeeding block improperly aligned`
- `Preceding block out of range`
- `Preceding block improperly aligned`
- `Bad process id`

The second [chars] can be either of these:

- `freeing`
- `allocating`

The [hex] field is the block address to be freed or allocated.

The %SYS−3−SYS_MEMERR error message indicates that during access of the memory block, memory management found that the information had become corrupted. This problem occurs occasionally, with no ill effects on the switch. If this error occurs several times over a short period of time, check to see if the block address that the error messages mention is the same. If the block address is the same, there is a possibility that that particular sector on the memory chip has gone bad and needs to be replaced.

SYS−3−SYS_LCPERR3: Module [dec]: Coil [dec] Port [dec] stuck [dec] times ([dec] due to lcol; [dec] due to notx)

Problem

SYS−3−SYS_LCPERR3: Module [dec]: Coil [dec] Port [dec] stuck [dec] times ([dec] due to lcol; [dec] due to notx) error messages appear in the syslog.

Description

These error messages indicate that the module has detected a problem with the port ASIC and that a port is locked up.

These error messages do not necessarily indicate a hardware problem. The error occurs for the first time if the switch has had a late collision because of a duplex mismatch or a long cable. However, there is a software bug in the CatOS 7.2(2) code that causes the switch to fail to check for incremental errors. The same error is logged repeatedly. Refer to Cisco bug ID CSCdx79107 (registered customers only) for more information about this issue. The problem is fixed in CatOS version 7.3(1).

The syslog error that is generated is similar to this:

- 2005 Aug 02 09:20:16 %SYS−3−SYS_LCPERR3:Module 5: Coil 3 Port 1: stuck 3 times(3 due to lcol; 0 due to notx)
- 2005 Aug 02 10:10:45 %SYS−3−SYS_LCPERR3:Module 5: Coil 3 Port 1: stuck 3 times(3 due to lcol; 0 due to notx)

This list defines elements of the error message:

- Module [dec] is the module that reports the error.
- Coil [dec] is the number of the ASIC that reports the error.
- Port [dec] is the ASIC port that has the error.
- stuck [dec] is the error duration.
- The last two [dec] are the lcol and notx counts.

In order to turn off these syslog error messages, issue the **set errordetection portcounters disable** privileged mode command.

Also, check the port physical status for any of these problems:

- A duplex mismatch
- Out−of−sync NICs on the attached workstations
- The error disable condition
- Late collisions
- Any link−level errors

In order to resolve the issues that result from any of these problems, refer to these documents:

- Troubleshooting Cisco Catalyst Switches to NIC Compatibility Issues
- Recovering From errDisable Port State on the CatOS Platforms

If the error occurs several times, contact Cisco Technical Support in order to address this issue further.

%SYS−3−SYS_LCPERR3:Module [dec]: Pinnacle #[dec], Frames with Bad Packet CRC Error (PI_CI_S_PKTCRC_ERR − 0xC7) = [dec]

This message indicates that the module has detected frames with a bad packet CRC received by the bus ASIC from the DBus. The first [dec] is the module number. The second [dec] is the ASIC number that reports the error. The third [dec] is the error count.

The bad CRC packets can be sent from any port across the data bus. Probable causes are mis−seated or faulty Line modules.

During the maintenance window, when you can troubleshoot the switch, re−seat all modules including the Supervisors and check if the error message recurs. If it does, there are two procedures you can use in order to determine which of the modules is the root of the bad packets and get the module replaced.

Procedure 1

Use Diagnostic level:

1. Configure the switch for complete POST analysis.

   ```
   set test diaglevel complete
   ```

2. Re−seat all the modules including the supervisor engines.
3. Get the POST analysis results.

   ```
   show test all
   ```

4. Contact the Cisco Technical Representative with the output of the **show test** *all* command.

Procedure 2

Use the Pinnacle ASIC counters:

1. Remove one module at a time.
2. Use this command and watch the counter `0xC7` for incrementing errors.

   ```
   show asicreg <mod>/<port> pinnacle errcounters
   ```

   This command displays all the counters for Pinnacle ASIC in that module. Counter `0xC7` is displayed in the third line of the output. Every time the command is executed, the counters are cleared. The ideal number is 0 errors.

   ```
   C6500> (enable) show asicreg 3/1 pinnacle errcounters

   00C5: PI_CI_S_HDR_FCS_REG                    = 0000
   00C6: PI_CI_S_RBUS_FCS_REG                   = 0000
   00C7: PI_CI_S_PKTCRC_ERR_REG                 = 0000
   00C8: PI_CI_S_PKTLEN_ERR_REG                 = 0000
   00C9: PI_CI_S_BPDU_OUTLOST_REG               = 0000
   00CE: PI_CI_S_HOLD_REG                       = 0000
   ```

```
00CA: PI_CI_S_QOS0_OUTLOST_REG                = 0000
00CE: PI_CI_S_HOLD_REG                        = 0000
00CB: PI_CI_S_QOS1_OUTLOST_REG                = 0000
00CE: PI_CI_S_HOLD_REG                        = 0000
00CC: PI_CI_S_QOS2_OUTLOST_REG                = 0000

!--- Output elided.
```

3. Repeat steps 1 and 2 until the error does not occur. Contact the Cisco Technical Representative for replacement of the faulty module.

%SYS−4−SUPERVISOR_ERR:

Problem

These error messages appear in the syslog:

```
%SYS−4−SUPERVISOR_ERR:Forwarding engine IP length error counter =4
%SYS−4−SUPERVISOR_ERR:Forwarding engine IP too short error counter =1
%SYS−4−SUPERVISOR_ERR:Forwarding engine IP check sum error counter = 38
```

Description

These messages indicate that the switch forwarding engine receives an IP packet of a length that is less than the minimum allowed length and then drops the packet. In code versions that are earlier than 7.x, the forwarding engine silently drops the packet and counts the packet in the forwarding engine statistics. In code versions that are 7.x or later, this message is recorded in the syslog once every 30 minutes.

There is no effect on the switch side. The switch side drops the bad packet, which the receiving device would have dropped consequently. The only concern is that there is a device that sends bad packets. The possible causes include a bad NIC driver, a NIC driver bug, or a bad application. The Supervisor Engine does not keep track of the source IP address of the device that sends the bad packets. The only way to detect these devices is to use a sniffer in order to track down the source address.

This message is only an informational message and warning from the switch. Issue the **set errordetection portcounters disable** command on the switch in order to disable these error messages.

%SYS−4−P2_WARN: 1/Invalid traffic from multicast source address

Problem

The switch generates `Invalid traffic from multicast source address` messages.

Description

This example shows the syslog output that you see when this error occurs:

```
SYS−4−P2_WARN: 1/Invalid traffic from multicast source address
```

This multicast source address syslog message is generated when the switch receives packets that have a multicast MAC address as the source MAC. The use of a broadcast or multicast MAC address as the source MAC for a frame is not standards−compliant behavior. However, the switch still forwards traffic that is sourced from a multicast MAC address. The syslog message indicates the multicast MAC address in the source MAC field of the frame, as well as the port on which the traffic was received. The workaround is to try to identify the end station that generates frames with a multicast source MAC address. Typically, one of these devices transmits such frames:

- A traffic generator, such as Spirent SmartBits
- Third−party devices that share a multicast MAC address, such as load−balancing firewall or server products

Workaround

The error does not cause any performance issues. In order to avoid the error message, disable the log of the messages. Another workaround is to track down the device that generates frames with a multicast source MAC address. Then, use a sniffer or a SPAN configuration to find the device, and check its configurations.

%SYS−4−PORT_ERR:Port 15/1 rxTotalDrops

Problem

These error messages appear in the syslog:

- `%SYS−4−PORT_ERR:Port 16/1 rxTotalDrops (7426859)`

  or
- `%SYS−4−PORT_ERR:Port 15/1 rxTotalDrops (2563127)`

Description

In the example in this section, `ERRORDETECTION PORTCOUNTERS` have been enabled and receive (Rx) errors occur on port 1/1. But the syslog (`SYS−4−PORT_ERR`) message reports `rxTotalDrops` on 15/1 instead of 1/1.

Note: `ERRORDETECTION PORTCOUNTERS` are disabled by default.

On some installations, software enables the feature and it remains enabled after upgrades. This issue has been resolved in 6.3(1) for a fresh install. If you see this message, check the first uplink port (1/1 or 2/1), not the port that the syslog reports (15/1 or 16/1). The **show counters** command output shows the errors that occur. If the only error counter that reports errors is `rxTotalDrops`, the drops that occur are most likely Color Blocking Logic (CBL) drops. Expect these drops if spanning tree is blocking for a VLAN on that port. CBL drops are packets that are received on a trunk for a VLAN that is blocked on that trunk. For example, broadcast, multicast, or unknown unicast can still be received on a blocked port.

If there are other error counters that report errors, the cause needs further investigation.

The workaround is to disable the `ERRORDETECTION PORTCOUNTERS`. Issue the **set errordetection portcounters disable** command.

%SYS−4−MODHPRESET:

Problem

The switch reports this error message to the switch console and syslog for a WS−X6608 line card:

```
2002 Aug 26 09:22:58 %SYS−4−MODHPRESET:
   Host process (860) 3/5 got reset asynchronously
```

Description

Active T1 or E1 ports on WS−X6608 modules reset on a random and infrequent basis. This reset results in the drop of all active calls to Public Switched Telephone Networks (PSTNs). Ports that are not configured but are enabled continuously reset in an attempt to connect to a Cisco CallManager. These reset messages can overlap to the active gateway ports and cause an unwanted reset. The overlap and reset are possible because all eight ports share the processor. This system message continually appears on your console screen and in your syslogs, if you have configured them. This behavior is expected for this blade. The behavior does not affect system performance.

The workaround is to disable unused ports. Issue the **set port disable** *mod/port* command. Add all ports to the Cisco CallManager database. You can configure these ports as gateways, Media Termination Points (MTPs), or hardware conference bridges.

%SYS−4−NVLOG:SYNDIAGS:Bus ASIC sync error

Problem

The syslog reports this error message in the log:

```
2002 Aug 23 08:59:16 %SYS−4−NVLOG:SYNDIAGS:
   Bus ASIC sync error on Module 16, bus I/F register = 0xa0
2002 Aug 23 09:00:53 %SYS−4−NVLOG:SYNDIAGS:
   Bus ASIC sync error on Module 1, bus I/F register = 0x30
```

Description

This message can indicate that the Supervisor Engine ASIC was not in sync prior to the diagnostics run. When you get this message, try to reseat the module or move the module to a different slot and see if the message stops. If you still get the message, issue the **show test** *mod_number* command, collect the output, and contact Cisco Technical Support. This issue is a hardware problem. The solution is to replace the module that gives this error message.

SYS−4−PORT_GBICBADEEPROM: / %SYS−4−PORT_GBICNOTSUPP:

Problem

The GBIC modules WS−G5484, WS−G5486, and WS−G5487 appear to operate normally, but the modules report these software errors:

```
%SYS−4−PORT_GBICBADEEPROM: port bad gbic eeprom checksum
%SYS−4−PORT_GBICNOTSUPP: port gbic not supported
```

Description

When you use GBIC modules WS−G5484, WS−G5486, and WS−G5487 with a WS−X6408−GBIC card, error messages appear in the software log, although there are no problems. When you plug these same GBICs into other modules or Supervisor Engines, the errors may not appear, as long as the GBICs have a valid Cisco GBIC Supervisor Engine EEPROM (SEEPROM). This error message is visual only. The message does not affect traffic that passes through the module or GBIC.

This problem is a cosmetic software problem only. Do not replace the hardware. These available Catalyst software releases have fixed this problem when SEEPROMs are available on the Cisco GBIC:

- CatOS 5.5(5) and later

- CatOS 6.2(3) and later

If a GBIC does not have a Cisco SEEPROM, an upgrade of the CatOS software does not fix the error message. In this case, the error indicates that an earlier Cisco GBIC or a noncertified, non−Cisco GBIC is in place. You can only replace certified Cisco GBICs under a support contract or warranty. Look at the label on the top of the GBIC case in order to verify that the GBIC is a certified Cisco GBIC. Look for these items:

- A Cisco logo
- A Cisco part number that starts with 30
- GBIC vendor name

For more details, refer to Field Notice: G5484, G5486, G5487 GBICs Generate Bad EPROM Errors.

SYS−4−SYS_LCPERR4: Module [dec]: Pinnacle #[dec] PB parity error

Problem

The console or syslog reports these error messages:

```
%SYS−4−SYS_LCPERR4:Module 12: Pinnacle #1 PB parity error. Tx path.
      Status=0x0046: Module needs troubleshooting or TAC assistance.
%SYS−4−SYS_LCPERR4:Module 12: Pinnacle #1 PB parity error. Rx path.
      Status=0x0002: Module needs troubleshooting or TAC assistance.
```

Description

This message can indicate a transient Pinnacle ASIC packet buffer problem. The first [dec] is the module number. The second [dec] is the ASIC number. If the error is limited to a single module, reseat and then power cycle the module. If you see this error message frequently, contact Cisco Technical Support for further assistance.

%SYS−5−SYS_LCPERR5:Module module

Problem

The console or syslog reports these error messages:

```
%SYS−5−SYS_LCPERR5:Module 7: Coil Pinnacle Header Checksum Error − Port #32:
%SYS−5−SYS_LCPERR5:Module 7: Coil Mdtif Packet CRC Error − Port #32:
%SYS−5−SYS_LCPERR5:Module 7: Coil Mdtif State Machine Error − Port #32:
```

Description

This error message is specific to 6348 line cards. The log message in the Problem section can be the result of a hardware or a software problem. Complete the steps in this section in order to determine if the problem is a hardware or software problem.

Complete the steps if both these items are true:

- You only see the message that the Problem section shows and no other coil−related messages in the syslogs.
- You have transmit stuck on one port but not on a group of 12 ports.

1. Issue the **show mac** *mod/port* command twice in 2−second intervals in order to confirm that you have a transmit stuck.

Try to send traffic in between the issue of each command. Verify if the transmit counters have increased. If you see that the numbers have increased, the transmit is not stuck.

2. Disable/enable the ports and see if they recover.
3. Issue the **reset** *mod_number* command in order to soft reset the module.

   See if the module recovers.
4. Issue the **set module power {up | down}** *mod_number* command in order to hard reset the module.

   See if the module recovers.

You most likely face a software issue if all these items are true:

- You disable/enable the ports and either soft reset or hard reset the module, and the card comes on line.
- All the ports pass diagnostics in the **show test** command output.
- Traffic starts to pass without problems.

If all these items are true, refer to Cisco bug ID CSCdu03935 (registered customers only) . The issue is fixed in versions 5.5(18), 6.3(10), 7.4(3), and later.

In some cases, you see `%SYS-5-SYS_LCPERR5:Module 9: Coil Pinnacle Header Checksum Error - Port #37` error messages and one or more of these messages:

- `Coil Mdtif State Machine Error`
- `Coil Mdtif Packet CRC Error`
- `Coil Pb Rx Underflow Error`
- `Coil Pb Rx Parity Error`

If you see these messages, determine if some or all these items are true:

- After you soft reset or/and hard reset the module, it still does not come on line.
- The module comes on line, but a group of 12 ports has failed diagnostics in the **show test** command output.
- The module is stuck in `other` state when you boot.
- All port LEDs on the module become amber.
- All ports are in `errdisabled` state when you issue the **show port** *mod_number* command.

If you experience any of the problems in this list, you most likely face a hardware problem. You must replace the card.

SYS-4-NVLOG:convert_post_SAC_CiscoMIB:Nvram block [#] unconvertible

Problem

The switch generates periodic `convert_post_SAC_CiscoMIB:` syslog messages.

Description

This example shows the console output that you see when this message occurs:

```
SYS-4-NVLOG:convert_post_SAC_CiscoMIB:Nvram block 0 unconvertible: )
SYS-4-NVLOG:convert_post_SAC_CiscoMIB:Nvram block 1 unconvertible: )
SYS-4-NVLOG:convert_post_SAC_CiscoMIB:Nvram block 2 unconvertible: )
```

These console messages often appear when you upgrade or downgrade CatOS code versions. The messages can also occur when you load a switch configuration that another switch generates or when you use a switch configuration from another version of code. A failover to the standby Supervisor Engine can also generate these messages.

Different versions of code contain variables that the NVRAM stores. When the switch initially boots to a later or earlier version of CatOS, the switch converts the previous configuration to a version that is usable by the current boot image. During this process, a particular memory block that is not necessary or usable in the current form is deallocated rather than converted. This internal function generates the error message.

This message is generally informational only. Compare the previous configuration with the current configuration in order to verify the proper conversion of all configuration information.

If these messages display when no code upgrade, configuration change, or Supervisor Engine failover has occurred, create a service request with Cisco Technical Support.

%SYS−6−CFG_CHG:Module [dec] block changed by SecurityRx

Problem

The switch generates periodic `%SYS−6−CFG_CHG:Module [dec] block changed by SecurityRx` syslog messages.

Description

This example shows the console output that you see when this error occurs on the switch:

```
%SYS−6−CFG_CHG:Module 3 block changed by SecurityRx
%SYS−6−CFG_CHG:Module 4 block changed by SecurityRx
```

This message indicates that the configuration block has been modified. These messages are expected when port security is configured on the switch, and aging is enabled. A PSecure MAC is the MAC address that is learned from the port security process and is added to the CAM table as a static entry to secure the port. When you have an aging time on the port security configuration, the MAC address is removed from the CAM table and the NVRAM (where PSecure MACs are stored) at the aging time. The next packet that is received from the port after this aging out takes place aids in the repopulation of the CAM and NVRAM with the PSecure MAC address.

InbandPingProcessFailure:Module x not responding over inband

Problem

These error messages appear in the **show log** command output:

```
InbandPingProcessFailure:Module 2 not responding over inband
InbandPingProcessFailure:Module 2 not responding over inband
```

Description

This message indicates that the module does not respond to the Supervisor Engine requests over the in−band communication channel. One of these occurrences can cause the error:

- The Supervisor Engine is excessively busy.
- There are Spanning Tree Protocol (STP) loops.

- ACLs and QoS policers throttle or drop traffic over the in−band communication channel.
- There are port ASIC synchronization problems.
- There are switch fabric module problems.

The Supervisor Engine polls the Multilayer Switch Feature Card (MSFC) via a special ping every 10 seconds. The Supervisor Engine then resets the MSFC if the MSFC fails to respond to three consecutive pings. In addition, in CatOS version 6.2 and later, the active and standby Supervisor Engines poll each other over the in−band channel, and the switch fails over to the standby Supervisor Engine.

Note: If you have recently migrated to or from versions 6.3(10), 7.4(2), or 7.4(3), the switch can reset if you issue the **show log** command or the **show tech−support** command and if you have the `InbandPing` failure message in the log. The workaround is to issue the **clear log** command before you issue the **show log** command. Cisco bug ID CSCdz32730 (registered customers only) identifies this caveat. The issue is resolved in versions 6.4(1) , 7.5(1), and later.

Typically, these messages result from a failed port ASIC or an unreliable connection to the backplane. Complete these steps:

1. Remove the module that the messages reference.
2. Firmly reseat the module in its slot.

   Issue the **set test diaglevel complete** command in order to ensure that complete diagnostics mode is enabled.

   Issue the **show log** *mod_number* command and the **show test** *mod_number* command in order to find any failed tests.
3. If Step 2 does not resolve the problem, create a service request with Cisco Technical Support.

   Complete these steps in order to provide the necessary information:

   a. Capture the output from the appropriate **show** commands from the CatOS.

   ◊ If the referenced module is not an MSFC, capture the output of these commands:

   · **show tech−support**
   · **show log**
   · **show logging buffer 1024**
   · **show test** *mod_number*

   Note: Issue this command once for each line card.
   · **show scp mod** *mod_number*

   Note: Issue this command once for each line card.
   · **show mod**

   ◊ If the referenced module is an MSFC, capture the output of these commands:

   · **show inband**
   · **show test 0**
   · **show scp stat**
   · **show scp failcnt**
   · **show scp mod**
   · **show scp process**

   Note: The **show scp** commands are hidden.

In addition, check for any crashinfo files in the bootflash. Issue the **show bootflash:** command.

b. Determine when and how often the problem occurs.

   Does the problem occur when the in−band connection experiences congestion? Conduct a ping test between the sc0 interface on the Supervisor Engine and a VLAN interface on the MSFC in order to test for in−band congestion. If your Catalyst runs CatOS system software, perform these steps:

   a. Capture output from the **show inband** command at the Supervisor Engine command−line interface (CLI).
   b. Open a separate Telnet session to the MSFC directly and ping from a VLAN interface to the sc0 interface.
   c. Capture output again from the **show inband** command at the Supervisor Engine CLI.
   d. If several pings fail or time out, issue the **set span sc0** *mod/port* **both inpkts disable** command.

      This command configures a SPAN session for the sc0 interface. After you start the sniffer or similar software, perform an extended ping test between the sc0 and a VLAN interface.

c. Determine if the sc0 is assigned to a special management VLAN or to a VLAN with a large amount of traffic, particularly broadcasts and multicasts.
d. Monitor the output of the **show errordetection inband** command.

   The **set errordetection** command helps you monitor the switch. At the detection of an error, a syslog message informs you that a problem exists before noticeable performance degradation occurs. The **show errordetection inband** command displays the type of in−band failure occurrence, such as an in−band stuck, resource error, or in−band failure during bootup.

Invalid feature index set for module

Problem

The `Invalid feature index set for module` error message displays when you install a new switching module in a Catalyst 6500/6000 series switch.

Description

This example shows the console output that you see when this error occurs:

```
%SYS−5−MOD_INSERT:Module 4 has been inserted
Invalid feature index set for module 4
```

The `Invalid feature index set for module` error occurs when the software image version that currently runs on the Supervisor Engine does not support the piece of hardware that you inserted.

In the example in this section, a 48−port 10/100 Mbps switching module (WS−X6348−RJ−45) was inserted in a Catalyst 6000 switch that runs software release 5.3(2)CSX. The minimum software release that the WS−X6348−RJ−45 module requires is 5.4(2).

The workaround is to upgrade the Supervisor Engine software to a version that supports the hardware. Refer to the Release Notes for Catalyst 6000/6500 Software Release 5.x for a list of the minimum software versions for each module.

Pinnacle Synch Failed

Problem

The `Pinnacle Synch Failed` error message displays at bootup.

Description

This example shows the console output that you see when this error occurs:

```
System Power On Diagnostics Complete

Boot image: bootflash:cat6000−sup.5−4−4.bin

In Local Test Mode, Synch Failed. Retries: 4

Local Test Mode encounters Minor hardware problem in Module # 1

Running System Diagnostics from this Supervisor (Module 1)
This may take up to 2 minutes....please wait
Pinnacle Synch Failed. Retries: 4
Minor hardware problem in Module # 1
Use 'show test 1' to see results of tests.


Cisco Systems Console

Enter password:
```

The workaround is to turn off the switch and check for these items:

- You have firmly seated the Supervisor Engines and all switching modules in the chassis backplane.
- You have fully engaged the ejector levers on the left and right sides of the modules. Be sure that you press the levers completely against the front panel of the module.
- You have screwed the thumb screws on the left and right sides of the modules into the card cage and tightened the screws.

After you ensure that you have properly engaged all modules in the chassis, turn on the chassis.

If you still see `Pinnacle Synch Failed` messages, there can be a hardware problem with one of the modules.

Turn off the switch and remove all switching modules. Turn on the switch with just the Supervisor Engine in the chassis. Add one module at a time and repeat the process until you identify the problem module.

RxSBIF_SEQ_NUM_ERROR:slot=x

Problem

These error messages appear in the syslog:

```
RxSBIF_SEQ_NUM_ERROR:slot=9, pinnacleMask=0X1,
   errSeqNum=b,source Index=0X1, errorType=0X2
RxSBIF_SEQ_NUM_ERROR:slot=3, pinnacleMask=0X1,
   errSeqNum=b,source Index=0X1, errorType=0X2
```

Description

The Catalyst 6500/6000 line cards as well as the Supervisor Engine module use port ASICs when they switch packets at high speeds between ports. The pinnacle ASIC provides a Gigabit Ethernet interface to the Catalyst 6500/6000 data bus. In order to support high forwarding rates, the switching bus of the Catalyst 6500/6000 supports pipelining. Pipelining enables the Catalyst 6500/6000 to switch multiple frames onto the bus before it obtains the results of the first frame. Each frame is prepended with an internal bus header that includes a sequence number. The switch uses the number to keep track of the multiple frames that await a forwarding decision. All line cards and the Supervisor Engines must have a common understanding of the current and next sequence number. This understanding is very important.

The `RXSBIF` error message reports the appearance of a sequence error on the switching bus. Such errors include a sequence mismatch and an invalid sequence. An invalid sequence means that the current packet on the switching bus has a sequence number which is different from the number that the ASICs expected. Here are sample error messages that report invalid sequence numbers:

```
%SYS-1-MOD_INVALIDSEQ:Bus asic invalid sequence occurred
   on module 1 (asic=1, srcidx=0x0, seq=14)
```

One of these problems typically causes the error messages:

- **Incorrectly seated module** Reseat the modules in their slots.

  Note: The module that detects the bus sequence number errors is not necessarily the module at fault. One incorrectly seated module can lead to the report of bus sequence number issues by any other module. Therefore, a reseat of all the modules can be necessary.

  Ensure that you lock the ejector levers in tightly and tighten the screws.
- **Faulty hardware** This cause is not as common. Reseat the modules. If you observe a failure, inspect the line cards for connector damage and inspect the backplane slot in the chassis for bent pins. If necessary, use a flashlight when you inspect the connector pins on the chassis backplane.

  If the problem persists after you reseat all the cards, capture output from the **show tech-support** command and the **show scp mod** or **show scp failcnt** hidden commands. Create a service request with Cisco Technical Support and provide this information.
- **Known issue** When the Catalyst 6500/6000 system is loaded with CatOS system software image release 6.1(1b), synchronization error messages can occur on the Supervisor Engine 2. Refer to the Field Notice: Continuous Synchronization Errors with Supervisor Engine 2 on Catalyst 6000 for more information.

lyra_ft_par_err_intr_hdlr: LKUPRAM error in NVRAM log

Problem

The NVRAM log displays the Forwarding Table Parity Error (ft_par_err).

```
lyra_ft_par_err_intr_hdlr: LKUPRAM, addr [hex], data [hex]
```

This error message indicates that a parity error has been detected in the forwarding table. The error message indicates the location of the error in the memory (`first [hex]`) and the data at that location (`second [hex]`).

Description

The probable cause for this error message is when a line card is not properly inserted and it replaces a different type of line card in that slot.

Complete these steps to resolve the issue:

1. Remove the module from the switch.
2. Inspect the backplane pins and reinsert the module.
3. If the issue persists, contact the Cisco Technical Representative.

In order to avoid the issue, execute the **module clear−config** command before you remove any modules. This command automatically removes the configuration that belongs to a module, once the module is removed from the chassis. For more information, refer to the Even After You Remove the Modules, the show run Command Still Shows Information About the Removed Module Interfaces section of Troubleshooting Hardware and Common Issues on Catalyst 6500/6000 Series Switches Running Cisco IOS System Software.

Note: The command does not clear the configurations of modules that have already been removed from the slot.

KERNEL−1−CREATEPROCESSFAILED

Problem

This error message appears in the logs:

```
%KERNEL−1−CREATEPROCESSFAILED:Error in creating process:
Unavailable free stack; stack type: 2; Name: tnetproc
```

The %KERNEL−1−CREATEPROCESSFAILED: Error in creating process: [chars]; stack type:[dec]; Name: [chars] error message indicates that the create process has failed; the system is out of processes. The Catalyst operating system allows a limited number of processes based on the number of stacks available. When stacks are unavailable, this message is generated. The first [chars] is the process ID; the [dec] is the stack type, and the second [chars] is the process name.

Description

The CatOS switch allows only a limited number of processes with a type 2 stack in the system, for example, Console, snmpdm, VtpRx, THREAD, or telnet145. The maximum number of processes with a type 2 stack is 13. Telnet or Secure Shell (SSH) is one of the processes which requires a type 2 stack. When all type 2 stacks are used, any attempt to connect through Telnet results in this error message.

This possibly occurred because the old Telnet or SSH sessions did not timeout on the switch or consume the process.

In order to resolve this issue, issue the **show users** command to check how many Telnet sessions have opened for the switch. Disconnect the Telnet sessions opened by the remote device with the **disconnect** *ip_address* command.

PI_CI_S_CBL_DROP_REG

Problem

```
Switch> (enable) show asicreg 4/28 pinnacle err
00C7: PI_CI_S_PKTCRC_ERR_REG                    = FFFF
016F: PI_CI_S_CBL_DROP_REG                      = 1619
```

Description

This register/counter does not indicate any hardware issue. It increments if a packet with specific VLAN tags is received on the port and this particular VLAN is not configured on the port. As a result, the packet is dropped, and the counter is incremented. Color Blocking Logic (CBL) refers to VLAN tagging on trunks. VLANs that are pruned from trunks have their traffic dropped. This state occurs when one side of the trunk has a higher number of VLANs in the spanning tree forward state.

The PI_CI_S_CBL_DROP_REG counters can increment in any mode; if the port transits the STP modes, you can see hits on an access port. If there is any negotiation on the port (default), this can also be seen as a normal behavior or function of the switch.

This counter counts packets dropped due to CBL lookup in a Complementary Bipolar Integrated Circuit (CBIC) block. The switch wants to send a packet out on a particular port for some VLAN, and the CBL logic says that the port is blocking/disabled/learning. This is not a big problem since these packets are dropped in the CBIC logic before they consume any packet buffers. You can disable/enable the port to see if it clears the counter.

Related Information

- **Common CatOS Error Messages on Catalyst 4500/4000 Series Switches**
- **Common CatOS Error Messages on Catalyst 5000/5500 Series Switches**
- **Catalyst 6500 Series System Message Guide, 8.7**
- **Configuring System Message Logging**
- **Cisco Catalyst 6000 Series Switches Product Support**
- **Error Message Decoder Tool (registered customers only)**
- **LAN Product Support**
- **LAN Switching Technology Support**
- **Technical Support & Documentation − Cisco Systems**

Updated: Nov 28, 2008 Document ID: 29804