

Common Error Messages on Catalyst 6500/6000 Series Switches Running Cisco IOS Software

Document ID: 41265

Introduction

Prerequisites

Requirements

Components Used

Conventions

%C6KPWR-SP-4-UNSUPPORTED: unsupported module in slot [num], power not allowed: [chars]

Problem

Description

Workaround

%DUAL-3-INTERNAL: IP-EIGRP 1: Internal Error

Problem

Description

Workaround

%EARL_L3_ASIC-SP-4-INTR_THROTTLE: Throttling "IP_TOO_SHRT"

Problem

Description

Workaround

%EARL_L3_ASIC-SP-3-INTR_WARN: EARL L3 ASIC: Non-fatal interrupt [chars]

Problem

Description

Workaround

%EARL_NETFLOW-4-TCAM_THRLD: Netflow TCAM threshold exceeded, TCAM

Utilization [[dec]%

Problem

Description

Workaround

%ETHCNTR-3-LOOP_BACK_DETECTED : Keepalive packet loop-back detected on [chars]

Problem

Description

Workaround

loadprog: error – on file open boot: cannot load "cisco2-Cat6k-MSFC"

Problem

Description

Workaround

%L3_ASIC-DFC3-4-ERR_INTRPT: Interrupt TF_INT:FI_DATA_INT

Problem

Description

%MLS_STAT-SP-4-IP_LEN_ERR: MAC/IP length inconsistencies

Problem

Description

%MLS_STAT-SP-4-IP_CSUM_ERR: IP checksum errors

Problem

Description

Workaround

%MCAST-SP-6-ADDRESS_ALIASING_FALLBACK

Problem
Description
c6k_pwr_get_fru_present(): can't find fru_info for fru type 6, #
Problem
Description
%MROUTE-3-TWHEEL_DELAY_ERR
Problem
Description
%MCAST-SP-6-GC_LIMIT_EXCEEDED
Problem
Description
Workaround
%MISTRAL-SP-3-ERROR: Error condition detected: TM_NPP_PARITY_ERROR
Problem
Description
%MLS_STAT-4-IP_TOO_SHRT: Too short IP packets received
Problem
Description
Processor [number] of module in slot [number] cannot service session requests
Problem
Description
**%PM_SCP-1-LCP_FW_ERR: System resetting module [dec] to recover from error:
[chars]**
Problem
Description
Workaround
**%PM_SCP-SP-4-UNK_OPCODE: Received unknown unsolicited message from
module [dec], opcode [hex]**
Problem
Description
Workaround
%QM-4-TCAM_ENTRY: Hardware TCAM entry capacity exceeded
Problem
Description
Workaround
**%slot_earl_icc_shim_addr: Slot [num] is neither SuperCard nor Supervisor – Invalid
slot**
Problem
Description
**%SYSTEM_CONTROLLER-SP-3-ERROR: Error condition detected:
TM_NPP_PARITY_ERROR**
Problem
Description
Workaround
**SP: Linecard endpoint of Channel 14 lost Sync. to Lower fabric and trying to recover
now!**
Problem
Description
%SYSTEM-1-INITFAIL: Network boot is not supported
Problem
Description
Resolution
CPU_MONITOR-3-TIMED_OUT or CPU_MONITOR-6-NOT_HEARD
Problem

Description
Workaround

% Invalid IDPROM image for linecard
Problem
Description
Workaround

%C6KPWR-4-DISABLED: Power to module in slot [dec] set [chars]
Problem
Description
Workaround

ONLINE-SP-6-INITFAIL: Module [dec]: Failed to [chars]
Problem
Description
Workaround

FM_EARL7-4-FLOW_FEAT_FLOWMASK_REQ_FAIL
Problem
Description
Workaround

MCAST-2-IGMP_SNOOP_DISABLE
Problem
Description
Workaround

C6KERRDETECT-2-FIFOCRITLEVEL: System detected an unrecoverable resources error on the active supervisor pinnacle
Problem
Description
Workaround

SP-RP Ping Test[7]: Test skipped due to high traffic/CPU utilization
Problem
Description
Workaround

SW_VLAN-4-MAX_SUB_INT
Problem
Description
Workaround

MCAST-6-L2_HASH_BUCKET_COLLISION
Problem
Description
Workaround

%QM-4-AGG_POL_EXCEEDED: QoS Hardware Resources Exceeded : Out of Aggregate policers
Problem
Description
Workaround

NetPro Discussion Forums – Featured Conversations
Related Information

Introduction

This document provides a brief explanation of common syslog and error messages that you see on Cisco Catalyst 6500/6000 series switches that run Cisco IOS® system software. Use the Output Interpreter Tool [\(](#) registered customers only) if you have an error message that does not appear in this document. The tool provides the meaning of error messages that Cisco IOS Software and Catalyst OS (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 runs on the Supervisor Engine.

Note: This minimum logging configuration on the Catalyst 6500/6000 is recommended:

- 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.

%C6KPWR-SP-4-UNSUPPORTED: unsupported module in slot [num], power not allowed: [chars]

Problem

The switch reports this error message:

- C6KPWR-SP-4-UNSUPPORTED: unsupported module in slot [num], power not allowed: [chars]

This example shows the console output that is displayed when this problem occurs:

```
Oct 14 16:50:13: %C6KPWR-SP-4-UNSUPPORTED: unsupported module in slot 2, power not allowed
Unknown Card Type
Oct 14 16:50:20: %C6KPWR-SP-4-UNSUPPORTED: unsupported module in slot 2, power not allowed
Unknown Card Type
```

Description

This message indicates that the module in the specified slot is not supported. The [num] is the slot number, and [chars] provides more details about the error.

Workaround

Upgrade the Supervisor Engine software to a version that supports the hardware module. Refer to the *Supported Hardware* section of the Cisco Catalyst 6500 Series Switches Release Notes for the relevant release. In order to resolve the issue that the message describes, perform one of these actions:

- Insert or replace the Switch Fabric Module.
- Move the unsupported module to a different slot.

%DUAL-3-INTERNAL: IP-EIGRP 1: Internal Error

Problem

The switch reports this error message:

- %DUAL-3-INTERNAL: IP-EIGRP 1: Internal Error

Description

The error message indicates that there is an internal bug in the Cisco IOS Software. The bug has been fixed in these releases:

- Cisco IOS Software Release 12.2(0.4)
- Cisco IOS Software Release 12.1(6.1)
- Cisco IOS Software Release 12.2(0.5)T
- Cisco IOS Software Release 12.1(6.5)E
- Cisco IOS Software Release 12.1(6.5)EC
- Cisco IOS Software Release 12.1(6)E02
- Cisco IOS Software Release 12.2(0.18)S
- Cisco IOS Software Release 12.2(2)B
- Cisco IOS Software Release 12.2(15)ZN

Workaround

Upgrade the Cisco IOS Software to one of these releases or to the latest release.

%EARL_L3_ASIC-SP-4-INTR_THROTTLE: Throttling "IP_TOO_SHRT"

Problem

The switch reports this error message:

- %EARL_L3_ASIC-SP-4-INTR_THROTTLE: Throttling "IP_TOO_SHRT"

This example shows the console output that is displayed when this problem occurs:

```
Jul 25 12:00:40.228 AEST: %EARL_L3_ASIC-SP-4-INTR_THROTTLE: Throttling "IP_TOO_SHRT" Intr.  
Exceeded permitted 1000/100 intrs/msec
```

Description

This message indicates that the switch forwarding engine receives an IP packet of a length that is shorter than the minimum allowed length. The switch drops the packet. In earlier versions, the packet is silently dropped and counted in the forwarding engine statistics. In later versions, the error message is recorded in the syslog once every 30 minutes. These issues can cause the switch forwarding engine to receive this type of IP packet:

- A bad network interface card (NIC) driver
- A NIC driver bug
- A bad application

The switch simply reports that it has received these "bad" packets and intends to drop them.

Workaround

The origin of the problem is external to the switch. Unfortunately, the forwarding engine does not keep track of the source IP address of the device that sends these bad packets. The only way to detect the device is to use a sniffer to track down the source and then replace the device.

%EARL_L3_ASIC-SP-3-INTR_WARN: EARL L3 ASIC: Non-fatal interrupt [chars]

Problem

The switch reports this error message:

- EARL_L3_ASIC-SP-3-INTR_WARN: EARL L3 ASIC: Non-fatal interrupt [chars]

This example shows the console output that is displayed when this problem occurs:

```
Apr 20 17:53:38: %EARL_L3_ASIC-SP-3-INTR_WARN: EARL L3 ASIC:  
Non-fatal interrupt Packet Parser block interrupt  
Apr 20 19:13:05: %EARL_L3_ASIC-SP-3-INTR_WARN: EARL L3 ASIC:  
Non-fatal interrupt Packet Parser block interrupt
```

Description

The error message %EARL_L3_ASIC-SP-3-INTR_WARN indicates that the Enhanced Address Recognition Logic (EARL) Layer 3 (L3) application-specific integrated circuit (ASIC) detected an unexpected non-fatal condition. This indicates that a bad packet, probably a packet which contains a Layer 3 IP checksum error, was received and dropped. The cause of the issue is a device on the network that sends out bad packets. These issues, among others, can cause the bad packets:

- Bad NICs
- Bad NIC drivers
- Bad applications

In older Cisco IOS Software releases, these packets are normally dropped without being logged. The feature of logging error messages about this problem is a feature found in Cisco IOS Software Release 12.2SX and later.

Workaround

This message is for informational purposes only. As a workaround, use one of these two options:

- Use a network sniffer in order to identify the source that sends out the erroneous packets. Then, resolve the issue with the source device or application.
- Disable Layer 3 error checks in the switch hardware for:

- ◆ Packet checksum errors

- ◆ Packet length errors
- ◆ Packets that have the same source and destination IP addresses

Use the **no mls verify** command to stop these error checks, as these examples show:

- ◆

```
Switch(config)#no mls verify ip checksum

!--- This configures the switch to discontinue checks for packet
!--- checksum errors.
```
- ◆

```
Switch(config)#no mls verify ip length {consistent | minimum}

!--- This configures the switch to discontinue checks for packet
!--- length errors.
```
- ◆

```
Switch(config)#no mls verify ip same-address

!--- This configures the switch to discontinue checks for packets that have t
!--- same source and destination IP addresses.
```

%EARL_NETFLOW-4-TCAM_THRLD: Netflow TCAM threshold exceeded, TCAM Utilization [[dec]%

Problem

The switch reports this error message:

- EARL_NETFLOW-4-TCAM_THRLD: Netflow TCAM threshold exceeded, TCAM Utilization [[dec]%

This example shows the console output that is displayed when this problem occurs:

```
Aug 24 12:30:53: %EARL_NETFLOW-SP-4-TCAM_THRLD: Netflow TCAM threshold exceeded,
TCAM Utilization [97%]
Aug 24 12:31:53: %EARL_NETFLOW-SP-4-TCAM_THRLD: Netflow TCAM threshold exceeded,
TCAM Utilization [97%]
```

Description

This message indicates that the NetFlow ternary content addressable memory (TCAM) is almost full. Aggressive aging will be temporarily enabled. If you change the NetFlow mask to FULL mode, TCAM for NetFlow can overflow because there are so many entries. Issue the **show mls netflow ip count** command in order to check this information.

The Supervisor Engine 720 checks how full the NetFlow table is every 30 seconds. The Supervisor Engine turns on aggressive aging when the table size reaches almost 90 percent. The idea behind aggressive aging is that the table is nearly full, so there are new active flows that cannot be created. Therefore, it makes sense to aggressively age-out the less active flows (or inactive flows) in the table in order to make space for more active flows.

The capacity for each policy feature card (PFC) NetFlow table (IPv4), for PFC3a and PFC3b, is 128,000 flows. For the PFC3bXL, the capacity is 256,000 flows.

Workaround

In order to prevent this problem, disable the FULL NetFlow mode. Issue the **no mls flow ip** command.

Note: Generally, the **no mls flow ip** command does not affect packet forwarding because TCAM for packet forwarding and TCAM for NetFlow accounting are separate.

In order to recover from this issue, enable MLS fast aging. While you enable MLS fast aging time, initially set the value to 128 seconds. If the size of the MLS cache continues to grow over 32 K entries, decrease the setting until the cache size remains less than 32 K. If the cache continues to grow over 32K entries, decrease the normal MLS aging time. Any aging-time value that is not a multiple of 8 seconds is adjusted to the closest multiple of 8 seconds.

```
Router#configure terminal
Router(config)#mls aging fast threshold 64 time 30
```

%ETHCNTR-3-LOOP_BACK_DETECTED : Keepalive packet loop-back detected on [chars]

Problem

The switch reports this error message, and the port is forced to linkdown:

- %ETHCNTR-3-LOOP_BACK_DETECTED : Keepalive packet loop-back detected on [chars]

This example shows the console output that is displayed when this problem occurs:

```
Oct 2 10:40:13: %ETHCNTR-3-LOOP_BACK_DETECTED: Keepalive packet loop-back detected on
GigabitEthernet0/1
Oct 2 10:40:13: %PM-4-ERR_DISABLE: loopback error detected on Gi0/1, putting Gi0/1 in
err-disable state
```

Description

The problem occurs because the keepalive packet is looped back to the port that sent the keepalive. Keepalives are sent on the Catalyst switches in order to prevent loops in the network. Keepalives are enabled by default on all interfaces. You see this problem on the device that detects and breaks the loop, but not on the device that causes the loop.

Workaround

Issue the **no keepalive** interface command in order to disable keepalives. A disablement of the keepalive prevents errdisablement of the interface, but it does not remove the loop.

Note: In Cisco IOS Software Release 12.2(x)SE-based releases and later, keepalives are not sent on fiber and uplink interfaces by default.

loadprog: error – on file open boot: cannot load "cisco2-Cat6k-MSFC"

Problem

The switch reports this error message:

- loadprog: error – on file open boot: cannot load "bootflash:c6msfc2–boot–mz.121–8a.EX"

Description

The problem occurs only at an unaligned write to the device that is close to an internal 64–byte boundary. The problem can occur under one of these circumstances:

- During the write of a crash dump file
 - Something causes the system to crash at the time of the write of the file.
- When code is corrupted during migration from CatOS to Cisco IOS Software

Workaround

The workaround is to modify the device driver so that it correctly handles unaligned access. If the error occurs because of a code corruption during migration from CatOS to Cisco IOS Software, erase the Flash and download a new, valid CatOS software image.

%L3_ASIC–DFC3–4–ERR_INTRPT: Interrupt TF_INT:FI_DATA_INT

Problem

The switch reports this error message:

- %L3_ASIC–DFC3–4–ERR_INTRPT: Interrupt TF_INT:FI_DATA_INT occurring in EARL %Layer 3 ASIC

Description

This error message indicates that there is an error in the Layer 3 (L3) forwarding application–specific integrated circuit (ASIC). Basically, the switch shows this message when some transient traffic passes through the ASIC and the software simply reports the occurrence of an interrupt condition. As soon as this condition is met, the counters that the **show earl statistics** command shows increase. Every time that the software tries to recover from such a state, the switch generates this syslog message. Generally, this message is informational if its occurrence remains low. But if the error message occurs frequently, there can be a problem with the hardware.

Check the counters value in the **show earl statistics** command output. If the counters increase rapidly, it indicates a possible problem with the hardware.

%MLS_STAT–SP–4–IP_LEN_ERR: MAC/IP length inconsistencies

Problem

The switch reports this error message:

- %MLS_STAT-SP-4-IP_LEN_ERR: MAC/IP length inconsistencies

This example shows the console output that is displayed when this problem occurs:

```
May 29 21:54:14 JST: %MLS_STAT-SP-4-IP_LEN_ERR: MAC/IP length inconsistencies
May 29 23:10:44 JST: %MLS_STAT-SP-4-IP_LEN_ERR: MAC/IP length inconsistencies
```

Description

These messages indicate that packets were received in which the IP length does not match the MAC length of the packet. The Supervisor Engine dropped these packets. There are no negative effects on the switch because it drops the packets. The switch reports the message for informational purposes. The cause of the issue is a device on the network that sends out bad packets. These issues, among others, can cause the bad packets:

- Bad NICs
- Bad NIC drivers
- Bad applications

Use a network sniffer in order to find the source that sends out the erroneous packets. Then, resolve the issue with the source device or application.

The other workaround is a switch configuration that stops the switch checks for:

- Packet checksum errors
- Packet length errors
- Packets that have the same source and destination IP addresses

Use these commands in order to stop the switch checks:

- ```
Switch(config)#no mls verify ip checksum
```

  
*!--- This configures the switch to discontinue checks for packet checksum errors.*
- ```
Switch(config)#no mls verify ip length
```


!--- This configures the switch to discontinue checks for packet length errors.
- ```
Switch(config)#no mls verify ip same-address
```

  
*!--- This configures the switch to discontinue checks for packets that have the same source and destination IP addresses.*

## %MLS\_STAT-SP-4-IP\_CSUM\_ERR: IP checksum errors

### Problem

The switch reports this error message:

- %MLS\_STAT-SP-4-IP\_CSUM\_ERR: IP checksum errors

This example shows the console output that is displayed when this problem occurs:

```
Jan 20 12:48:52: %MLS_STAT-SP-4-IP_CSUM_ERR: IP checksum errors
Jan 20 14:49:53: %MLS_STAT-SP-4-IP_CSUM_ERR: IP checksum errors
```

## Description

These messages indicate that the switch receives IP packets that have an invalid checksum value. There are no negative effects on the switch because the switch drops the packets. The switch reports the message for informational purposes. The cause of the issue is a device on the network that sends out bad packets. These issues, among others, can cause the bad packets:

- Bad NICs
- Bad NIC drivers
- Bad applications

## Workaround

As a workaround, use one of these two options:

- Use a network sniffer in order to identify the source that sends out the erroneous packets. Then, resolve the issue with the source device or application.
- Disable Layer 3 error checks in the switch hardware for both:
  - ◆ Packet checksum errors
  - ◆ Packet length errors

In order to stop these error checks, use the **no mls verify** command, as these examples show:

- ◆ 

```
Switch(config)#no mls verify ip checksum

!--- This configures the switch to discontinue checks for packet
!--- checksum errors.
```
- ◆ 

```
Switch(config)#no mls verify ip length {consistent | minimum}

!--- This configures the switch to discontinue checks for packet
!--- length errors.
```

## %MCAST-SP-6-ADDRESS\_ALIASING\_FALLBACK

### Problem

The switch reports this error message:

- %MCAST-SP-6-ADDRESS\_ALIASING\_FALLBACK:

This example shows the console output that is displayed when this problem occurs:

```
%MCAST-SP-6-ADDRESS_ALIASING_FALLBACK: Address Aliasing detected for
group 0100.5e00.0001 on vlan 632 from possible source ip 10.158.132.185 source
mac 0000.bea6.82e0
```

## Description

This message indicates that the switch receives excessive multicast traffic that is destined for a multicast MAC address in the 01-00-5e-00-00-xx range. This multicast range is reserved for Internet Group Management Protocol (IGMP) control traffic, for example:

- Leaves
- Joins
- General queries

The switch CPU normally processes all the IGMP control traffic. Therefore, Cisco IOS Software provides a mechanism to ignore excessive IGMP multicast traffic that is destined for reserved addresses. The mechanism ensures that the CPU does not become overwhelmed. Use of this mechanism is referred to as "fallback mode".

Find the source of the illegal multicast traffic. Then, either stop the transmission or modify the characteristics of the stream so that the transmission no longer infringes upon the IGMP control data space. Also, use the error message in the Problem section, which provides a network source that potentially causes the problem.

## **c6k\_pwr\_get\_fru\_present(): can't find fru\_info for fru type 6, #**

### Problem

The switch reports this error message:

- c6k\_pwr\_get\_fru\_present(): can't find fru\_info for fru type 6, #

This example shows the console output that is displayed when this problem occurs:

```
Mar 10 08:30:53: SP: c6k_pwr_get_fru_present(): can't find fru_info for fru type 6, #38
Mar 10 08:30:53: SP: c6k_pwr_get_fru_present(): can't find fru_info for fru type 6, #38
Mar 10 08:30:53: SP: c6k_pwr_get_fru_present(): can't find fru_info for fru type 6, #43
Mar 10 08:30:53: SP: c6k_pwr_get_fru_present(): can't find fru_info for fru type 6, #43
```

## Description

This error message appears because of an erroneous response from the switch to Simple Network Management Protocol (SNMP) polling of the port adapters that Flex WAN modules use. This error message is cosmetic in nature, and there are no detrimental switch performance issues. Refer to Cisco bug ID CSCdx41473 [🔗](#) (registered customers only) for more details. The issue is fixed in these releases:

- Cisco IOS Software Release 12.1(11b)E4
- Cisco IOS Software Release 12.1(12c)E1
- Cisco IOS Software Release 12.1(13)E
- Cisco IOS Software Release 12.1(13)EC
- Later releases

## **%MROUTE-3-TWHEEL\_DELAY\_ERR**

## Problem

The switch reports this error message:

- %MROUTE-3-TWHEEL\_DELAY\_ERR:

This example shows the console output that is displayed when this problem occurs:

```
%MROUTE-3-TWHEEL_DELAY_ERR: Exceeded maximum delay (240000 ms) requested: 7200000
```

## Description

This message appears when the switch receives Protocol Independent Multicast (PIM) join/prune packets that advertise a high hold-time value. The packets advertise a higher hold-time value than the maximum delay that the OS of the switch allows, which is 4 minutes. These packets are multicast control packets, such as PIM, Distance Vector Multicast Routing Protocol (DVMRP), and other types.

Later releases of Cisco IOS Software for the Catalyst 6500/6000 have increased this maximum delay to 65,535 seconds, or approximately 17 minutes. Refer to Cisco bug ID CSCdw50542 [🔗](#) (registered customers only) for more details. The issue is fixed in these releases:

- Cisco IOS Software Release 12.1(12c)E
- Cisco IOS Software Release 12.2(12)T01
- Cisco IOS Software Release 12.1(13)E
- Cisco IOS Software Release 12.1(13)EC
- Later releases

## Workaround

Configure the third-party device that generates the PIM packets to use timers that are recommended by protocol standards.

## %MCAST-SP-6-GC\_LIMIT\_EXCEEDED

### Problem

The switch reports this error message:

- %MCAST-SP-6-GC\_LIMIT\_EXCEEDED

This example shows the console output that is displayed when this problem occurs:

```
%MCAST-SP-6-GC_LIMIT_EXCEEDED: IGMP snooping was trying to allocate more Layer 2 entries than what=allowed (13000)
```

## Description

This error message is logged when the IGMP snooping function on the switch has created the maximum number of allowed Layer 2 (L2) entries. The default maximum number of L2 entries that the switch can create for multicast groups is 15,488. In later versions of Cisco IOS Software, only the hardware-installed L2 multicast entries count toward the limit. Refer to Cisco bug ID CSCdx89380 [🔗](#) (registered customers only) for more details. The issue is fixed in Cisco IOS Software Release 12.1(13)E1 and later.

## Workaround

You can manually raise the L2 limit. Issue the `ip igmp l2-entry-limit` command.

## **%MISTRAL-SP-3-ERROR: Error condition detected: TM\_NPP\_PARITY\_ERROR**

### Problem

The switch reports this error message:

- %MISTRAL-SP-3-ERROR: Error condition detected: TM\_NPP\_PARITY\_ERROR

This example shows the console output that is displayed when this problem occurs:

```
Apr 19 22:14:18.237 EDT: %MISTRAL-SP-3-ERROR: Error condition detected:
TM_NPP_PARITY_ERROR
Apr 19 22:14:25.050 EDT: %MISTRAL-SP-3-ERROR: Error condition detected:
TM_NPP_PARITY_ERROR
Apr 19 22:15:20.171 EDT: %MISTRAL-SP-3-ERROR: Error condition detected:
TM_NPP_PARITY_ERROR
```

### Description

This error message indicates that there was a parity error in the next-page pointer of the internal Table Manager. If the switch runs Cisco IOS Software Release 12.1(8)E or later, the switch detects the parity error and resets the Mistral ASIC. The switch can then continue, without the need to reload. A random static discharge or other external factors can cause the memory parity error. If you see the error message only once or rarely, monitor the switch syslog in order to confirm that the error message is an isolated incident. If these error messages reoccur, create a service request with Cisco Technical Support.

## **%MLS\_STAT-4-IP\_TOO\_SHRT: Too short IP packets received**

### Problem

The switch reports this error message:

- %MLS\_STAT-4-IP\_TOO\_SHRT: Too short IP packets received

This example shows the console output that is displayed when this problem occurs:

```
*Apr 1 10:30:35 EST: %MLS_STAT-SP-4-IP_TOO_SHRT: Too short IP packets received
```

### Description

The message indicates that the switch forwarding engine receives an IP packet of a length that is shorter than the minimum allowed length. The switch drops the packet. In earlier versions, the packet is silently dropped and counted in the forwarding engine statistics. This applies to software releases that are earlier than 7.x or earlier than Cisco IOS Software Release 12.1(13E). In software releases that are later than 7.x or later than Cisco IOS Software Release 12.1(13E), the message is recorded in the syslog once every 30 minutes.

There is no effect on the switch side. The switch 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. Possible causes include:

- A bad NIC driver
- A NIC driver bug
- A bad application

Because of hardware limitations, the Supervisor Engine does not keep track of the source IP, MAC address, or port of the device that sends the bad packets. You must use a packet-sniffing application in order to detect these devices and track down the source address.

The message in the Problem section is simply a warning/informational message from the switch. The message does not provide any information about the source port, MAC address, or IP address.

Use a packet-sniffing application inside the network. Try to shut down some interface or remove some device from the network in order to determine if you can isolate the device that malfunctions.

## Processor [number] of module in slot [number] cannot service session requests

### Problem

The switch reports this error message:

- Processor [number] of module in slot [number] cannot service session requests

### Description

This error occurs when you issue the **session slot *number* processor *number*** command in an attempt to establish a session in these situations:

- You try to establish a session to a module in which a session has been already established while logging into the switch.
- You try to establish a session for an unavailable module in the slot.
- You try to establish a session for an unavailable processor in the module.

## %PM\_SCP-1-LCP\_FW\_ERR: System resetting module [dec] to recover from error: [chars]

### Problem

The switch reports this error message:

- %PM\_SCP-1-LCP\_FW\_ERR: System resetting module [dec] to recover from error: [chars]

These examples show the console output that is displayed when this problem occurs:

- %PM\_SCP-SP-1-LCP\_FW\_ERR: System resetting module 13 to recover from error: Linecard received system exception

or

- `%PM_SCP-SP-1-LCP_FW_ERR: System resetting module 4 to recover from error: Coil Pb Rx Parity Error - Port #14`

## Description

The message indicates that the firmware of the specified module has detected an error. The system automatically resets the module in order to recover from the error. The [dec] is the module number, and [chars] is the error.

## Workaround

Reseat the module or put the module in a different slot and allow the module to go through the complete bootup diagnostics test. For more information on online diagnostics on the Catalyst 6500 series switches, refer to Configuring Online Diagnostics. After the module passes the diagnostics test, monitor the recurrence of the error message. If the error occurs again or the diagnostics test detects any issues, create a service request with Cisco Technical Support for further troubleshooting.

## **%PM\_SCP-SP-4-UNK\_OPCODE: Received unknown unsolicited message from module [dec], opcode [hex]**

## Problem

The switch reports this error message:

- `%PM_SCP-SP-4-UNK_OPCODE: Received unknown unsolicited message from module [dec], opcode [hex]`

These examples show the console output that is displayed when this problem occurs:

- `Dec 10 12:44:18.117: %PM_SCP-SP-4-UNK_OPCODE: Received unknown unsolicited message from module 2, opcode 0x330`

or

- `Dec 10 12:44:25.210: %PM_SCP-SP-4-UNK_OPCODE: Received unknown unsolicited message from module 2, opcode 0x114`

## Description

This error message simply indicates that the Supervisor Engine does not understand the control message from the line card because of features that are not supported by the switch Cisco IOS Software release.

Line cards send out control messages to the active Supervisor Engine that indicate the features that the software supports. But if the software does not support any of the line card features, these control messages are not recognized and the error message is displayed. This message is a harmless occurrence and does not affect any functions on the Supervisor Engine or the line cards.

## Workaround

Upgrade the Supervisor Engine software to the latest version that has the maximum feature support. Because this error message does not affect production or traffic, you can ignore the message.

# %QM-4-TCAM\_ENTRY: Hardware TCAM entry capacity exceeded

## Problem

The switch reports this error message:

- %QM-4-TCAM\_ENTRY: Hardware TCAM entry capacity exceeded

## Description

TCAM is a specialized piece of memory designed for rapid table lookups by the ACL and QoS engines. This message indicates exhaustion of the TCAM resources and software switching of packets. This means that each interface has its own ID in TCAM and therefore uses more TCAM resources. Most likely this problem is caused either by the presence of the **mls qos marking statistics** command or when the hardware TCAM does not have the capacity to handle all of the configured ACLs.

## Workaround

- Disable the **mls qos marking statistics** command as it is enabled by default.
- Try to share the same ACLs across multiple interfaces in order to reduce the TCAM resource contention.

# %slot\_earl\_icc\_shim\_addr: Slot [num] is neither SuperCard nor Supervisor – Invalid slot

## Problem

The switch reports this error message:

- %slot\_earl\_icc\_shim\_addr: Slot [num] is neither SuperCard nor Supervisor – Invalid Slot

## Description

This message occurs when an SNMP Manager polls for the TCAM data of a line card which does not have any TCAM information. This occurs only for a line card in a Catalyst 6500 switch that runs Cisco IOS Software. If the line card has TCAM information during the SNMP poll, the data is given to the network management system (NMS) for further processing. Refer to Cisco bug ID CSCec39383 [↗](#) (registered customers only) for more details. This issue is fixed in Cisco IOS Software Release 12.2(18).

As a workaround, you can block the query of TCAM data by the NMSs. The MIB object that provides TCAM usage data is `cseTcamUsageTable`. Complete these steps on the router in order to avoid tracebacks:

1. Issue the **snmp-server view *tcamBlock cseTcamUsageTable excluded*** command.
2. Issue the **snmp-server view *tcamBlock iso included*** command.
3. Issue the **snmp-server community public view *tcamBlock ro*** command.
4. Issue the **snmp-server community private view *tcamBlock rw*** command.

# **%SYSTEM\_CONTROLLER-SP-3-ERROR: Error condition detected: TM\_NPP\_PARITY\_ERROR**

## **Problem**

The switch reports this error message:

- %SYSTEM\_CONTROLLER-SP-3-ERROR: Error condition detected: TM\_NPP\_PARITY\_ERROR

This example shows the console output that is displayed when this problem occurs:

```
Feb 23 21:55:00: %SYSTEM_CONTROLLER-SP-3-ERROR: Error condition detected: TM_NPP_PARITY_ER
Feb 23 22:51:32: %SYSTEM_CONTROLLER-SP-3-ERROR: Error condition detected: TM_NPP_PARITY_ER
Feb 23 23:59:01: %SYSTEM_CONTROLLER-SP-3-ERROR: Error condition detected: TM_NPP_PARITY_ER
```

## **Description**

The most common errors from the Mistral ASIC on the MSFC are TM\_DATA\_PARITY\_ERROR, SYSDRAM\_PARITY\_ERROR, SYSAD\_PARITY\_ERROR, and TM\_NPP\_PARITY\_ERROR. Possible causes of these parity errors are random static discharge or other external factors. This error message indicates that there was a parity error. Processor Memory Parity Errors (PMPEs) are broken down into two types: single event upset (SEU) and repeated errors.

These single bit errors occur when a bit in a data word changes unexpectedly due to external events (which causes, for example, a zero to spontaneously change to a one). SEUs are a universal phenomenon irrespective of vendor or technology. SEUs occur very infrequently, but all computer and network systems, even a PC, are subject to them. SEUs are also called soft errors, which are caused by noise and result in a transient, inconsistent error in the data, this is unrelated to a component failure – most often the result of cosmic radiation.

Repeated errors (often referred to as hard errors) are caused by failed components. A hard error is caused by a failed component or a board-level problem, such as an improperly manufactured printed circuit board that results in repeated occurrences of the same error.

## **Workaround**

If you see the error message only once or rarely, monitor the switch syslog in order to confirm that the error message is an isolated incident. If these error messages reoccur, reseal the supervisor engine blade. If the errors stop, it was a hard parity error. If these error messages continue to reoccur, open a case with the Technical Assistance Center.

# **SP: Linecard endpoint of Channel 14 lost Sync. to Lower fabric and trying to recover now!**

## **Problem**

The switch reports this error message:

- SP: Linecard endpoint of Channel 14 lost Sync. to Lower fabric and trying to recover now!

## Description

The error message usually points to a mis-seated linecard. In most cases, you can physically reseal the linecard in order to solve this problem. In some cases, the module is faulty.

1. Issue the **show fabric fpoe map** command in order to identify the module that causes this error message.

```
Switch#configure terminal
Switch(config)#service internal
Switch(config)#end
Switch#show fabric fpoe map
Switch#configure terminal
Switch(config)#no service internal
Switch(config)#end
```

This example is the result of the **show fabric fpoe map** command. From the output, you can identify that the module in slot 12 causes the error message.

```
switch#show fabric fpoe map
```

```
slot channel fpoe
 12 0 14 <<
```

There are also related errors in "show fabric channel-counters" :

| slot | channel | rxErrors | txErrors | txDrops | lbusDrops |
|------|---------|----------|----------|---------|-----------|
| 1    | 0       | 1        | 0        | 0       | 0         |
| 2    | 0       | 16       | 0        | 0       | 0         |
| 3    | 0       | 16       | 0        | 0       | 0         |

2. Reseat the module which causes the error message.

## %SYSTEM-1-INITFAIL: Network boot is not supported

### Problem

While a Cisco Catalyst 6000/6500 switch boots, it can throw a similar error message:

```
%SYSTEM-1-INITFAIL: Network boot is not supported.

Invalid device specified
Booting from default device
Initializing ATA monitor library...
monlib.open(): Open Error = -13
loadprog: error - on file open
boot: cannot load "bootdisk:s72033-ipervicesk9-mz.122-18.SXF7.bin"
```

## Description

This error occurs mostly when the boot variables are not configured properly to boot the switch from a valid flash device.

In the illustration, notice the last line of the message:

```
boot: cannot load "bootdisk:s72033-ipervicesk9-mz.122-18.SXF7.bin"
```

The name of the flash device mentioned is **bootdisk**, and the first part of the IOS filename, **s72033** notes that the IOS is for Supervisor module 720. The Supervisor 720 module does not have or support a flash device named **bootdisk**. Because the Supervisor 720 module does not have a local flash of that name, the switch thinks that you want to boot from the network, so it displays the error message.

## Resolution

Configure the boot variable with the correct flash device name and the valid software file name.

These flash devices are supported by the Supervisor modules:

- Supervisor Engine 1 and Supervisor Engine 2

| Flash Device Name | Description                        |
|-------------------|------------------------------------|
| bootflash:        | Onboard flash memory               |
| slot0:            | Linear Flash PC card (PCMCIA slot) |
| disk0:            | ATA Flash PC card (PCMCIA slot)    |

- Supervisor Engine 720

| Flash Device Name | Description                                  |
|-------------------|----------------------------------------------|
| bootflash:        | Onboard flash memory                         |
| disk0:            | CompactFlash Type II card only (disk 0 slot) |
| disk1:            | CompactFlash Type II card (disk 1 slot)      |

- Supervisor Engine 32

| Flash Device Name | Description                                  |
|-------------------|----------------------------------------------|
| bootdisk:         | Onboard flash memory                         |
| disk0:            | CompactFlash Type II card only (disk 0 slot) |

If this does not resolve the issue, refer to [Recovering a Catalyst 6500/6000 Running Cisco IOS System Software from a Corrupted or Missing Boot Loader Image or ROMmon Mode](#).

## CPU\_MONITOR-3-TIMED\_OUT or CPU\_MONITOR-6-NOT\_HEARD

### Problem

The switch reports these error messages:

```
CPU_MONITOR-3-TIMED_OUT: CPU monitor messages have failed, resetting system
CPU_MONITOR-6-NOT_HEARD: CPU monitor messages have not been heard for [dec] seconds
```

## Description

These messages indicate that CPU monitor messages have not been heard for a significant amount of time. A time-out most probably occurs, which resets the system. [dec] is the number of seconds.

The problem possibly occurs because of these reasons:

- Badly seated line card or module
- Bad ASIC or bad backplane
- Software bugs
- Parity error
- High traffic in the Ethernet out of band channel (EOBC) channel

The EOBC channel is a half duplex channel that services many other functions, which includes Simple Network Management Protocol (SNMP) traffic and packets that are destined to the switch. If the EOBC channel is full of messages because of a storm of SNMP traffic, then the channel is subjected to collisions. When this happens, EOBC is possibly not able to carry IPC messages. This makes the switch display the error message.

## Workaround

Reseat the line card or module. If a maintenance window can be scheduled, reset the switch in order to clear any transient issues.

## % Invalid IDPROM image for linecard

### Problem

The %Invalid IDPROM image for linecard error message is received in Catalyst 6500 series switches running Cisco IOS system software.

The error message can look similar to these messages:

```
% Invalid IDPROM image for daughterboard 1 in slot 4 (error = 4)
% Invalid IDPROM image for linecard in slot 5 (error = 4)
% Invalid IDPROM image for daughterboard 1 in slot 5 (error = 4)
```

## Description

This error indicates that the linecards installed did not boot correctly because the supervisor generated a bad signal onto control bus. In some scenarios, it is seen that improper seating can also cause the supervisor or linecards not to be recognized on Cat6500 chassis. Refer to Cisco bug ID CSCdz65855 (registered customers only) for more information.

## Workaround

If redundant supervisor setup is available, perform a force switchover and reseat the original active supervisor.

If it is a single supervisor setup, schedule a downtime, and complete these steps:

1. Move the supervisor module to another slot.
2. Reseat all the line cards and make sure that they are placed properly.

Refer to Online Insertion and Removal (OIR) of Modules in Cisco Catalyst Switches for more information on online insertion and removal of modules.

## **%C6KPWR-4-DISABLED: Power to module in slot [dec] set [chars]**

### **Problem**

The switch reports the error message:

```
%C6KPWR-4-DISABLED: Power to module in slot [dec] set [chars]
```

This example shows the console output that is displayed when this problem occurs:

```
%C6KPWR-SP-4-DISABLED: power to module in slot 10 set off (Fabric channel errors)
%C6KPWR-SP-4-DISABLED: power to module in slot 2 set off (Module Failed SCP dnld)
%C6KPWR-SP-4-DISABLED: power to module in slot 9 set off (Module not responding to Keep Al
```

### **Description**

This message indicates that the module in the indicated slot was powered off for the indicated reason. [dec] is the slot number, and [chars] indicates the power status.

The switch has its normal vibrations and over time those vibrations can cause a module to slightly come away from the backplane. When this happens, the supervisors keepalive polling does not receive a response from the module within the allotted time and the supervisor reboots the module in order to try to gain a better connection to it. If the module still does not respond to the polls, the supervisor continuously reboots the module, and eventually puts it into `error disable` and does not allow any power to reach this module.

### **Workaround**

A simple reseal of the module corrects this issue 90 percent of the time. If you reseal the module, it realigns the switch fabric and ensures a firm connection to the backplane.

If the concerned module is the Content Switching Module (CSM), consider the upgrade of the CSM software to a release 4.1(7) or later. This issue is documented at Cisco bug ID CSCei85928 (against CSM software) (registered customers only) and Cisco bug Id CSCek28863 (against Cisco IOS software) (registered customers only) .

The latest CSM software can be downloaded from the Cisco Catalyst 6000 Content Switching Module software download page.

## **ONLINE-SP-6-INITFAIL: Module [dec]: Failed to [chars]**

### **Problem**

The switch reports the error message:

```
ONLINE-SP-6-INITFAIL: Module [dec]: Failed to [chars]
```

This example shows the console output that is displayed when this problem occurs:

```
%ONLINE-SP-6-INITFAIL: Module 5: Failed to synchronize Port asic
```

## Description

The cause of the crash is that the Pinnacle ASIC failed to synchronize. This is usually caused by a bad contact or a badly seated card.

## Workaround

The system recovers without user intervention. If the error message recurs, then reseal the concerned line card or module.

## FM\_EARL7-4-FLOW\_FEAT\_FLOWMASK\_REQ\_FAIL

### Problem

The switch reports the error message:

```
%FM_EARL7-4-FLOW_FEAT_FLOWMASK_REQ_FAIL: Flowmask request for the flow based
feature [chars] for protocol [chars] is unsuccessful, hardware acceleration may be disabled
for the feature
```

This example shows the console output that is displayed when this problem occurs:

```
%FM_EARL7-4-FLOW_FEAT_FLOWMASK_REQ_FAIL: Flowmask request for the flow based
feature Reflexive ACL for protocol IPv4 is unsuccessful, hardware acceleration may be disabled
for the feature
```

## Description

The flow mask request for the flow-based feature is unsuccessful. This condition can occur because of a TCAM resource exception, a flow mask registers resource exception, or an unresolvable flow mask conflict with other NetFlow-based features. The NetFlow shortcut installation and hardware acceleration for the feature can be disabled under this condition, and the feature can be applied in the software.

If you have ingress reflexive ACL only, reflect and eval configured in the ingress direction on different interfaces, then reflexive ACL flowmask requirement is based on ingress reflexive ACLs. As long as the reflexive ACL is configured on a different interface than QoS micro-flow policing or does not overlap with micro-flow policing policy ACL, when on same interface, they can coexist in hardware. If they are on the same interface and the reflexive ACL and QoS policy overlap, then reflexive ACL disables NetFlow shortcut installation and traffic matching reflexive ACL is software switched. This is due to the conflicting flowmask requirements.

In case of egress reflexive ACL, the reflexive ACL flowmask requirement is global on all the interfaces, since there is only ingress NetFlow. If QoS user based micro-flow policing is configured in this case, reflexive ACL disables NetFlow shortcut installation and traffic matching reflexive ACL is software switched.

## Workaround

Issue the **show fm fie flowmask** command in order to determine the NetFlow shortcut installation enable / disable status for the feature. If the NetFlow shortcut installation and hardware acceleration is disabled for the feature, use only ingress reflexive access-lists in combination with micro-flow policing, and make sure that the micro-flow policer does not overlap with the reflexive access-list. Reapply the feature for the flow mask request to succeed, and re-enable the NetFlow shortcut installation for the feature.

# MCAST-2-IGMP\_SNOOP\_DISABLE

## Problem

The switch reports the error message:

```
%MCAST-2-IGMP_SNOOP_DISABLE:IGMP Snooping disabled due to excessive events/packets,
[dec]/[dec]; auto reenable in about 2 mins
```

This example shows the console output that is displayed when this problem occurs:

```
%MCAST-2-IGMP_SNOOP_DISABLE:IGMP Snooping disabled due to excessive events/packets,
0/19880; auto reenable in about 2 mins
```

## Description

IGMP snooping is disabled, but the system receives multicast traffic. This situation forces multicast packets to be directed to the route processor and possibly floods it. IGMP snooping can be disabled automatically due to excessive multicast traffic. IGMP snooping basically looks at these control packets that are exchanged between routers and hosts and based on the joins, leaves and queries update what ports receive the multicast.

This message normally occurs because the route processor receives a much higher than expected rate of IGMP join packets or normal multicast packets destined to reserved Layer3/Layer2 multicast address ranges. Therefore the switch runs out of resources and as the logging messages reports, the switch mitigates and disables IGMP snooping for a short period.

## Workaround

You can enable multicast rate limiting feature and set the threshold to a greater number.

Rate limiting is a more desirable method so that the queue is not overrun and also means that valid IGMP packets have less chance of being dropped and therefore the snooping process on the switch is still able to update appropriately.

Complete these steps in order to troubleshoot this issue:

1. Disable IGMP snooping with the command **no ip igmp snooping**.
2. Setup a SPAN session on the management VLAN interface on your Catalyst 6500 in order to determine that the MAC address belongs to the source from where the excessive traffic comes.
3. Look into the CAM table in order to identify the source, and remove that source.
4. Re-enable IGMP snooping.

# C6KERRDETECT-2-FIFOCRITLEVEL: System detected an unrecoverable resources error on the active supervisor pinnacle

## Problem

The switch reports these error messages. The error message can be one of these two types:

```
C6KERRDETECT-2-FIFOCRITLEVEL: System detected an unrecoverable resources error on the active supervisor
```

## Description

The root cause of this error is possibly a defective module or a mis-seated module. It can also be a chassis problem with this particular slot. This can be a transient issue if it is due to a mis-seated module.

These messages indicate that the system detected unrecoverable resources, which is due to the First In, First Out [FIFO] problem, on the indicated Pinnacle ASIC or specified port ASIC.

## Workaround

Issue the **remote command switch show platform hardware asicreg pinnacle slot 1 port 1 err** command in order to resolve this error, and configure the switch to run enhanced hardware tests with these steps:

**Note:** Type the entire command and hit the **Enter** key. You cannot write the command with the Tab key.

1. Issue the **diagnostic bootup level complete** command in order to set the diagnostic level to complete, and save the configuration.
2. Reseat the supervisor and firmly insert it
3. Once the supervisor comes online, issue the **show diagnostic** command in order to monitor the switch and check whether the error message still persists

## SP-RP Ping Test[7]: Test skipped due to high traffic/CPU utilization

### Problem

This error message is received when inband test pings failed due to high CPU:

```
SP-RP Ping Test[7]: Test skipped due to high traffic/CPU utilization
```

### Description

The SP-RP in band ping is an online diagnostic test and the message that SP-RP ping test failed is purely informational. It is indicative of high CPU utilization and can be the result of much traffic passing to the Route Processor or of switching traffic flowing to the switch processor. This can also happen during any route updates. It is normal to have Route Processor CPU used up to 100 percent sometimes.

### Workaround

The error message is purely informational and does not have any impact on the device performance.

## SW\_VLAN-4-MAX\_SUB\_INT

### Problem

The switch reports this error message:

```
%SW_VLAN-4-MAX_SUB_INT : The number of sub-interfaces allocated for interface [chars] has exceeded recommended limits of [dec]
```

This example shows the console output that is displayed when this problem occurs:

```
%SW_VLAN-4-MAX_SUB_INT: The number of sub-interfaces allocated for interface Gi1/1 has exceeded recommended limits of 1000
```

## Description

The number of Layer 3 sub-interfaces is limited by the internal VLANs in the switch. Catalyst 6500 series has 4094 VLANs that are used for various purposes. Issue the **show platform hardware capacity vlan** command in order to know the current status VLAN availability.

```
Switch#show platform hardware capacity vlan

VLAN Resources
 VLANs: 4094 total, 9 VTP, 0 extended, 17 internal, 4068 free
```

## Workaround

Recommended limit of sub interfaces is 1000 for each interface and 2000 for each module. Reduce the number of sub-interfaces allocated for the interface as it has exceeded the recommended limit.

**Note:** The console can get locked up due to the flood of these messages that are displayed at switch reload. This issue is documented in Cisco bug ID CSCek73741 (registered customers only) and the issue is resolved in Cisco IOS Software Releases 12.2(18)SXF10 and Cisco IOS Software Releases 12.2(33)SXH or later.

## MCAST-6-L2\_HASH\_BUCKET\_COLLISION

### Problem

The switch reports this error message:

```
MCAST-6-L2_HASH_BUCKET_COLLISION: Failure installing (G,C)->index:
([enet],[dec])->[hex] Protocol :[dec] Error:[dec]
```

This example shows the console output that is displayed when this problem occurs:

```
%MCAST-SP-6-L2_HASH_BUCKET_COLLISION: Failure installing (G,C)->index:
(0100.5e31.d522,802)->0xDA4 Protocol :0 Error:3
```

This error message is normally seen along with this message:

```
%MCAST-SP-6-GC_LIMIT_EXCEEDED: IGMP snooping was trying to allocate
more Layer 2 entries than what allowed (15488)
```

## Description

This message indicates that a Layer 2 entry was not installed in the hardware because there is not enough space in the hash bucket. Multicast packets are flooded on the incoming VLAN because the Layer 2 entry installation failed. When limit is exceeded, flooding occurs for additional group MACs.

## Workaround

If you do not use multicast, then you can disable IGMP snooping. Otherwise, you can increase the hash entry limit with the use of the **ip igmp snooping l2-entry-limit** command.

# %QM-4-AGG\_POL\_EXCEEDED: QoS Hardware Resources Exceeded : Out of Aggregate policers

## Problem

The switch reports this error message:

```
%QM-4-AGG_POL_EXCEEDED: QoS Hardware Resources Exceeded : Out of Aggregate policers
```

## Description

Only a limited number of aggregate policers can be supported. On EARL7-based switches, this limit is 1023.

## Workaround

Instead of port based QoS, you can configure VLAN based QoS. Complete these steps:


1. Apply the service-policy to each VLAN configured on the Layer 2 switchport.
2. Remove the service-policy from each port that belongs to the specific VLAN.
3. Configure each Layer 2 switchport for VLAN based QoS with the **mls qos vlan-based** command.

## NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

|                                                           |
|-----------------------------------------------------------|
| NetPro Discussion Forums – Featured Conversations for LAN |
| Network Infrastructure: LAN Routing and Switching         |
| Network Infrastructure: Getting Started with LANs         |

## Related Information

- [Message and Recovery Procedures for Catalyst 6500/6000 Cisco IOS Software Release 12.1E](#)
- [Cisco Catalyst 6500 Series Switches](#)
- [Error Message Decoder](#)  (registered customers only)
- [LAN Product Support](#)
- [LAN Switching Technology Support](#)
- [Technical Support & Documentation – Cisco Systems](#)

---

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Feb 27, 2008

Document ID: 41265

---