

Common CatOS Error Messages on Catalyst 5000/5500 Series Switches

Document ID: 30082

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Error Messages on Catalyst 5500/5000 Series Switches

- %CDP-4-NVLANMISMATCH: Native vlan mismatch detected on port [Mod]/[Port]
- DTP-1-ILGLCFG: Illegal config (on, isl—on,dot1q) on Port [mod/port]
- %IP-3-UDP_SOCKETOVFL:UDP socket overflow
- %IP-3-UDP_BADCKSUM:UDP bad checksum
- %KERNEL-5-UNALIGNACCESS:Alignment correction made
- %MCAST-4-RX_JNRANGE:IGMP: Rcvd Report in the range
- %MCAST-2-IGMP_FALLBACK:IGMP: Running in FALL BACK mode
- MGMT-5-LOGIN_FAIL:User failed to log in from Console
- %MLS-4-MOVEOVERFLOW:Too many moves, stop MLS for 5 sec
- %PAGP-5-PORTFROMSTP / %PAGP-5-PORTTOSTP
- %SPANTREE-3-PORTDEL_FAILNOTFOUND
- %SYS-3-PORT_ERR:
- %SYS-4-PORT_WARN:
 - convert_post_SAC_CiscoMIB:Nvram block [#] unconvertible
 - EARL-2:LKUPRAM Err / blkcmbParityErrHdlr
 - Earl2:Banff
 - EARL-3-BADCOLOR: Bad color [vlan_no] read from [hex] for a [chars] entry
- Module is not supported

Related Information

Introduction

This document provides a brief explanation of common system log (syslog) and error messages that you see on Catalyst 5500/5000 series switches that run Catalyst OS (CatOS) software.

Use the Error Message Decoder [↗](#) (registered customers only) tool 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 runs on the switch Supervisor Engine.

Cisco recommends this minimum logging configuration on the Catalyst 5500/5000 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 5500/5000 Series Switches

The messages in this section are common error messages that you see on Catalyst 5500/5000 series switches that run CatOS.

%CDP-4-NVLANMISMATCH: Native vlan mismatch detected on port [Mod]/[Port]

Problem

Frequent %CDP-4-NVLANMISMATCH syslog messages are generated on the switch.

Description

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

```
%CDP-4-NVLANMISMATCH:Native vlan mismatch detected on port 4/1
```

This message is generated whenever the switch port is physically connected to another switch or router. This message is generated on the switch because the configured native VLAN on the port is different than the one that is set on the connecting switch or router port.

A trunk port that is configured with IEEE 802.1Q tagging can receive both tagged and untagged traffic. By default, the switch forwards untagged traffic with the native VLAN configured for the port. If a packet has the same VLAN ID as the outgoing port native VLAN ID, the packet is transmitted 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 be transmitted correctly on the trunk. This can imply some connectivity issues in your network.

You can issue the **show trunk mod/port** command in order to verify the native VLAN that is configured on your switch. In the 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)

```

You can issue the **set vlan *vlan-id mod/port*** command in order to change the native VLAN that is configured on the trunk port. In the command, ***mod/port*** is the trunk port.

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

Problem

DTP-1-ILGLCFG: Illegal config (on, isl--on,dot1q) on Port [mod/port] errors are generated.

Description

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

%IP-3-UDP_SOCKETOVFL:UDP socket overflow

Problem

Periodic %IP-3-UDP_SOCKETOVFL:UDP socket overflow syslog messages are generated on the switch.

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_SOCKETOVFL:UDP socket 2353 overflow
%IP-3-UDP_SOCKETOVFL:UDP socket 2353 overflow
%IP-3-UDP_SOCKETOVFL:UDP socket 2353 overflow
%IP-3-UDP_SOCKETOVFL:UDP socket 2353 overflow

```

The switch generates this syslog message when the buffer that is allocated for incoming packets on the specified socket (UDP destination port) is full because the rate of traffic that is destined for that 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. Increase the polling interval on the network management station or reduce the number of MIB objects that are polled.

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 was full, the switch generated 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 on the specified destination UDP ports to the switch. If the switch generates an excessive number of these messages, use a network analyzer in order to identify the source of the traffic and 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. This identifies the internal interface for the Supervisor Engine. Refer to Catalyst Switched Port Analyzer (SPAN) Configuration Example for more information. Do not worry about the no such port counter. This counter is the number of UDP packets received that are destined for nonexistent ports.

%IP-3-UDP_BADCKSUM:UDP bad checksum

Problem

Periodic %IP-3-UDP_BADCKSUM:UDP bad checksum syslog messages are generated on the switch.

Description

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

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

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

```
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 that sends bad packets to the switch causes the 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. This identifies the internal interface for the Supervisor Engine. Refer to Catalyst Switched Port Analyzer (SPAN) Configuration Example for more information. Do not worry about the no such port counter. This counter

is the number of UDP packets received that are destined for nonexistent ports.

%KERNEL-5-UNALIGNACCESS:Alignment correction made

Problem

Periodic %KERNEL-5-UNALIGNACCESS:Alignment correction made syslog messages are generated on the switch.

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 when it attempted to access data in DRAM. These messages are informational only. They 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 an upgrade to the latest maintenance release does not eliminate the generation of these syslog messages, create a service request [☞](#) (registered customers only) with Cisco Technical Support.

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

Problem

The %MCAST-4-RX_JNRANGE:IGMP: Rcvd Report in the range 01-00-5e-00-00-xx error message is displayed on a switch with Internet Group Management Protocol (IGMP) snooping enabled.

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 when it receives 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 Layer 3 (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 **set logging level mcast 2 default** command. 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

The %MCAST-2-IGMP_FALLBACK:IGMP: Running in FALL BACK mode error message is displayed on a switch with IGMP snooping enabled.

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
```

This syslog message is generated 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 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 destination MAC 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. This switch generates this syslog message when the switch runs in fallback mode.

The resolution is to use a sniffer in order 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.

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

Problem

MGMT-5-LOGIN_FAIL:User failed to log in from Console errors are generated.

Description

This message possibly indicates a problem with the terminal server that is connected 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.

%MLS-4-MOVEOVERFLOW:Too many moves, stop MLS for 5 sec

Problem

Sporadic or constant %MLS-4-MOVEOVERFLOW:Too many moves, stop MLS for 5 sec syslog messages are generated on the switch.

Description

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

```
%MLS-4-MOVEOVERFLOW:Too many moves, stop MLS for 5 sec(20000000)
%MLS-4-RESUMESC:Resume MLS after detecting too many moves
%MLS-4-MOVEOVERFLOW:Too many moves, stop MLS for 5 sec(20000000)
%MLS-4-RESUMESC:Resume MLS after detecting too many moves
```

These syslog messages indicate that the switch relearns one or more MAC addresses on multiple ports in rapid succession. For example, on an access switch with two uplinks to the core of the network, the switch may learn a given MAC address first on one uplink and then on the other very rapidly.

If you see these messages infrequently, the problem is most likely a transitory L2 (spanning tree) loop. The loop results in packet flooding in one or more VLANs.

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, the cause can be one of these issues:

- A permanent L2 (spanning tree) loop
- One or more faulty switch ports
- A bad cable (for example, a unidirectional fiber link)
- Other bad hardware

Note: The bad hardware is not necessarily on the switch that generates the messages.

- Misconfigured device

An example is a traffic generator that sends traffic to two switch ports that use the same MAC address.

If you are confident that there is no L2 loop or faulty hardware, you do not use Multilayer Switching (MLS) on the switch, and you want to eliminate these messages, disable MLS on the switch. Issue the **set mls disable** command. Or you can issue the **set logging level mls 3 default** command in order to modify the logging level for the MLS facility to 3 or lower. However, these solutions simply mask the problem.

If you receive these messages after you issue the **set mls disable** command, create a service request [🔗](#) (registered customers only) with Cisco Technical Support.

%PAGP-5-PORTFROMSTP / %PAGP-5-PORTTOSTP

Problem

Frequent %PAGP-5-PORTFROMSTP and %PAGP-5-PORTTOSTP syslog messages are generated on the switch.

Description

This example shows the console output that you see when these syslog messages are generated:

```
%PAGP-5-PORTFROMSTP:Port 3/3 left bridge port 3/3
%PAGP-5-PORTTOSTP:Port 3/3 joined bridge port 3/3
```

The Port Aggregation Protocol (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
- 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

Periodic %SPANTREE-3-PORTDEL_FAILNOTFOUND syslog messages are generated on the switch.

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-3-PORT_ERR:

Problem

The syslog logs these error messages:

```
%SYS-3-PORT_ERR:Port 6/20 swBusCRCErrorDrop (241)
%SYS-3-PORT_ERR:Port 6/21 swBusCRCErrorDrop (241)
%SYS-3-PORT_ERR:Port 6/23 dmaXferLengthErrors (236)
%SYS-3-PORT_ERR:Port 6/23 swBusCRCErrorDrop (731)
```

Description

These syslog messages are mainly for informational purposes and are unique to the CatOS 6.x versions.

Symptom 1

```
%SYS-3-PORT_ERR:Port 6/20 swBusCRCErrorDrop (241)
```

This counter is incremented when the switch detects errors during a check of the integrity of the full packet between the data bus and the internal receive (Rx) FIFO before it goes into transmit (Tx) packet buffers. At this point, the switch also checks the length of the packet against the length field. This error message means that this module detects packets that have cyclic redundancy check (CRC) errors. These packets come from another device. For example, when there is an Inter-Switch Link (ISL) trunk, the switch (port) does not check the integrity of the full packet. Therefore, try to find the device that sends the corrupt packets. Hard code the speed and duplex settings on ports that show this error, as well as on the other end of these ports.

Symptom 2

```
%SYS-3-PORT_ERR:Port 6/23 dmaXferLengthErrors (236)
```

Generally, this message is logged when you have issued the **set errordetection portcounters enable** command in order to enable error detection for port counters. This command is only useful with a problem that impacts the network. By default, this command is disabled. The code dictates that these counters should be 0, but if the counters reach a certain threshold, a syslog message is generated. The cause of the oversubscription can be a spanning tree loop which can have oversubscribed the port. As a result, the Direct Memory Access (DMA) queue is full. Issue the **set errordetection portcounters disable** command in order to disable the error detection, and see if the message disappears. If you disable the error detection counters and still receive this message, create a service request [🔗](#) (registered customers only) with Cisco Technical Support.

%SYS-4-PORT_WARN:

Problem

The syslog reports this error message:

```
2002 Sep 21 11:07:20 %SYS-4-PORT_WARN:Port 5/29 dmaTxFull (0)
dmaRetry (0) dmaLevel2Request (0)
```

Description

This message occurs when multiple errors mount on the ports. If the `dmaTXfull` counter increments, the port is overloaded, or a collision causes the problem. Hard code the speed and duplex on the switch ports as well as on workstation NICs. Do not set the speed and duplex mode to `auto`. This solves 99 percent of traffic problems with workstations. If there are any hubs or old cables in between the switch and the workstation, test them for integrity. Also, you can upgrade the firmware of the NICs that are installed in critical workstations and servers. This upgrade solves many performance issues. Refer to [Troubleshooting Cisco Catalyst Switches to NIC Compatibility Issues](#) for known NIC issues.

If you still receive these messages, create a service request [🔗](#) (registered customers only) with Cisco Technical Support.

convert_post_SAC_CiscoMIB:Nvram block [#] unconvertible

Problem

Periodic `convert_post_SAC_CiscoMIB: syslog` messages are generated on the switch.

Description

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

```
convert_post_SAC_CiscoMIB:Nvram block 0 unconvertible: )
convert_post_SAC_CiscoMIB:Nvram block 1 unconvertible: )
convert_post_SAC_CiscoMIB:Nvram block 2 unconvertible: )
```

These console messages are often generated 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 [🔗](#) (registered customers only) with Cisco Technical Support.

EARL-2:LKUPRAM Err / blkcmbParityErrHdlr

Problem

A `EARL-2:LKUPRAM Err` error is generated when you issue the **show cam** command. In addition, `blkcmbParityErrHdlr` errors appear in the NVRAM log when you issue the **show log** command. In some cases, the switch resets when you issue the **show cam** command.

Description

This example shows the syslog message that you see when you issue the **show cam** command:

```
EARL-2:LKUPRAM Err: Addr 3d93d, Data 1000002-0, Cnt 1
```

This example shows the NVRAM log output that you see when you issue the **show log** command:

```
01. blkcmbParityErrHdlr:LKUPRAM, intr=40, addr x16c61, data 801-0, cnt 1
02. blkcmbParityErrHdlr:LKUPRAM, intr=40, addr x16c61, data 801-0, cnt 2
03. blkcmbParityErrHdlr:LKUPRAM, intr=41, addr x16c61, data 801-0, cnt 3
```

These messages are printed in the NVRAM log when the software detects a parity error in an Enhanced Address Recognition Logic (EARL) memory location (content-addressable memory [CAM] entry). The switch can reset at the detection of such a parity error, which depends on the software version on the switch Supervisor Engine.

For more detailed information, refer to the release notes that Cisco bug ID CSCdk75035 [↗](#) (registered customers only) documents. For additional information, refer to the Bug Toolkit [↗](#) (registered customers only).

If you run a software release that is earlier than 4.5(5), upgrade to these latest releases:

- 4.5(5)
- 5.2(2)
- 5.4(1)

If the switch consistently logs these messages after you upgrade the software, create a service request [↗](#) (registered customers only) with Cisco Technical Support.

Earl2:Banff

Problem

Numerous `Earl2:Banff` errors appear in the NVRAM log when you issue the **show log** command.

Description

This example shows the NVRAM log output that you see when you issue the **show log** command:

```
01. 6/2/2000,14:23:26: Earl2:Banff (2) pkt d-status=6, stat1=10, stat2=0
02. 6/2/2000,14:23:29: Earl2:Banff (2) MEQ status h=7 t=172 pg=3df
03. 6/2/2000,14:24:25: Earl2:Banff (2) pkt d-status=6, stat1=0, stat2=0
04. 6/2/2000,14:24:28: Earl2:Banff (2) MEQ status h=247 t=2ea pg=3df
```

These messages are printed in the NVRAM log when the software detects that one of the application-specific integrated circuits (ASICs) in the Banff chipset is stuck. The Banff chipset consists of three Banff ASICs. The Banff chipset on the Supervisor Engine is used to perform packet rewrites for MLS. If one of the Banff ASICs is stuck, the software resets the Banff and logs a message to the NVRAM log.

These messages do not indicate a problem unless an excessive number of resets occur. You can issue the hidden **show banff-reset** command in order to see the number of times each Banff ASIC in the chipset was reset since the last reload. There can be a problem if the reset count for a given Banff ASIC constantly increases.

This example shows the output of the **show banff-reset** command:

```
Console> (enable) show banff-reset

Banff reset counts:
-----
Banff 1: 1
Banff 2: 2772
Banff 3: 1
Console> (enable)
```

This example shows that Banff ASIC 2 has been reset 2772 times. If you see an excessive number of Banff resets on your switch, create a service request [🔗](#) (registered customers only) with Cisco Technical Support.

If you see these messages on a Supervisor Engine that cannot do IP MLS and/or Internetwork Packet Exchange (IPX) MLS (without Banff ASICs), ignore these messages. The messages do not affect your switch.

EARL-3-BADCOLOR: Bad color [vlan_no] read from [hex] for a [chars] entry

Problem

EARL-3-BADCOLOR: Bad color [vlan_no] read from [hex] for a [chars] entry errors are generated.

Description

The error indicates that a frame was seen with a VLAN ID for which the switch is not configured. In order to resolve the issue, you must understand how the invalid VLAN ID was learned. One strategy is to issue the **set length 0** command and capture the entire **show cam dynamic** command output to a file. Run that file through a sort utility in order to sort by VLAN number. Any VLAN numbers that are present in the CAM for which the switch is not configured point to the suspicious port. Issue the **show vlan** command in order to check this VLAN configuration. The suspicious port is often a trunk. In this case, investigate the other end of the trunk. The network impact can be from negligible to severe, which depends on how the VLAN ID became bogus. The impact is severe if other elements of frame corruption took place. If your network performance is affected, check for any other messages in the log in order to further troubleshoot. Otherwise, ignore this message.

Module is not supported

Problem

The `Module is not supported` error message is displayed when you install a new switching module in a Catalyst 5500/5000 series switch.

Description

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

```
Module 6 is not supported (46)
```

The `Module is not supported` 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 24-port 10BASE-FL Ethernet MT-RJ switching module (WS-X5015-MT) was inserted in a Catalyst 5500/5000 switch that runs software release 4.5(1). The minimum software release that is required for the WS-X5015-MT module is 5.1(1).

The workaround is to upgrade the Supervisor Engine software version to a software release that supports the hardware. The Catalyst 5000 Family Release Notes list the minimum software versions for each module. Also, you can use the Software Advisor [☐](#) (registered customers only) tool in order to determine the minimum software version that is required for the given hardware.

Related Information

- **System Message Guide – Catalyst Family Switches, 6.3 and 6.4**
 - **Common CatOS Error Messages on Catalyst 4500/4000 Series Switches**
 - **Common CatOS Error Messages on Catalyst 6500/6000 Series Switches**
 - **Catalyst 5000 Series Switches Product Support Page**
 - **Configuring System Message Logging**
 - **LAN Product Support Pages**
 - **LAN Switching Support Page**
 - **Technical Support & Documentation – Cisco Systems**
-

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

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Aug 09, 2006

Document ID: 30082
