

Troubleshooting Common Issues on the Catalyst 2900XL and 3500XL Series Switches

Document ID: 29200

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Troubleshoot General Switch Issues

- Troubleshoot LEDs
- Troubleshoot and Understand POST Failure Messages
- Troubleshoot Fan Failures
- Troubleshoot System Error Messages
- Troubleshoot High CPU

Troubleshoot high Memory utilization

- High process Memory utilization

Troubleshoot Expansion Slots in the Catalyst 2900XL

- Expansion Slot Module Does Not Work
- ATM Module Fails POST Tests
- ATM Module Has Corrupt Module Software
- Password Recovery for the ATM Module

Troubleshoot Interface Issues

- Workstation cannot Log into the Network During Startup and cannot Obtain a DHCP Address
- Troubleshoot NIC Compatibility Issues
- Troubleshoot Interface Errors
- The CDP-4-DUPLEX_MISMATCH Error Message on an ISL Trunk Port on a C3524-PWR-XL
- Support for Loopback Interfaces

Troubleshoot GBIC Issues

- 1000BASE-T GBIC is not Recognized or does not Work
- GigaStack GBIC is not Recognized or does not Work Properly
- GigaStack GBIC Link Flaps and Never Stabilizes
- Troubleshoot GigaStack GBIC Based on LED Status
- Troubleshoot GigaStack GBIC Loop Configuration
- NO_LOOP_DETECT System Error Message with GigaStack GBIC
- GIGASTACK-6-LOOP_DETECTED System Error Message with GigaStack GBIC

Troubleshoot Console Connectivity Problems

- Unreadable Characters on the Management Console
- No Connectivity Through the Console
- Cisco Telnet Denial of Service

Troubleshoot General Software Issues

- Recover from Missing or Corrupted Software or Switch: Prompt
- Troubleshoot Cisco Visual Switch Manager or Cluster Management Suite
- Hardware and Software Compatibility or Software Feature Support
- Recover Lost Password

Diagnostic Commands

- show interface
- show controllers ethernet-controller

```
show env fan
show logging
show platform port-asic stats drop
```

Related Information

Introduction

This document discusses how to identify and troubleshoot potential hardware problems with Cisco Catalyst Layer 2 fixed configuration 2900XL and 3500XL series switches.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- General system and power requirements
- Proper installation procedure
- Switch management
- Software considerations for the Catalyst 2900XL and 3500XL switches

You can prevent many hardware problems that you encounter at the time of field installations or at the time of normal operation if you perform a thorough product overview ahead of time.

Components Used

The information in this document is based on these software and hardware versions:

- Catalyst 2900XL and 3500XL series switches

Note: This document is not specific to any Cisco IOS® Software Release.

Conventions

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

Troubleshoot General Switch Issues

Troubleshoot LEDs

In order to troubleshoot switches on the basis of LED information, refer to the documentation on these devices:

- Catalyst 2900XL
- Catalyst 3500XL

Troubleshoot and Understand POST Failure Messages

Each time you power up the switch, eight Power-On Self Tests (POSTs) run automatically. POSTs check the most important system components before the switch begins to forward packets. When the switch begins the POST, the port status LEDs display amber for two seconds, and then display green. As each test runs, the port status LEDs go out. 1x is the first to go out. The port status LEDs for ports 2x through 8x go out sequentially

as the system completes a test.

When the POST completes successfully, the port status LEDs go out. This indicates that the switch is operational. If a test fails, the port status LED associated with the test displays amber. The system LED also displays amber.

Note: From Cisco IOS Software Release 11.2(8.5)SA6 onwards, the port and system LEDs both remain amber after a POST failure. In the earlier Cisco IOS Software Releases, only the LEDs of failed linked ports remained amber.

This table shows the LED and the component of the switch to which the LED corresponds:

LED	Components Tested
1x	DRAM
2x	Flash memory
3x	Switch CPU
4x	System board
5x	CPU interface Application-Specific Integrated Circuit (ASIC)
6x	Switch core ASIC
7x	Ethernet controller ASIC
8x	Ethernet interfaces

At the time of the switch bootup sequence (cold start or through the **reload** command), monitor the POST tests as they run through a console connection to the switch. Here is an example:

```
!--- Output is suppressed.

C2900 POST: System Board Test: Passed
C2900 POST: CPU Buffer Test: Passed
C2900 POST: CPU Notify RAM Test: Passed
C2900 POST: CPU Interface Test: Passed
C2900 POST: Testing Switch Core: Passed
C2900 POST: Testing Buffer Table: Passed
C2900 POST: Data Buffer Test: Passed
C2900 POST: Configuring Switch Parameters: Passed
C2900 POST: Ethernet Controller Test: Passed
C2900 POST FAILURE: front-end post: FastEthernet0/2:
C2900 POST FAILURE: looped-back packet not received
C2900 POST FAILURE: front-end post: FastEthernet0/4:
C2900 POST FAILURE: looped-back packet not received
C2900 POST: MII Test: Passed
```

```
!--- Output is suppressed.
```

This output shows one example of a failure on a Catalyst 2900XL switch at the time of the bootup sequence.

Alternatively, you can issue the **show post** command when the system runs, in order to see if any port had failed a POST test. This command, available in Cisco IOS Software Release 11.2(8.5)SA6, checks if the POST tests passed. If there is a failure, this command determines which POST test failed. This command is useful when you are able to get a link on a particular port, or the port LED is amber. For example, here is an

output from a Catalyst 2900XL which failed a POST test on FastEthernet interface 0/19:

```
2900XL# show post
POST FAILED: FastEthernet0/19 failed front-end loopback test
```

When there is no POST failure, you see this output. This output is captured from a Catalyst 3500XL switch:

```
3512xl#show post
Passed
```

See the Common Reasons and Solutions section for more information on POST failure messages.

Common Reasons and Solutions

A POST failure usually indicates physical damage to the interface. If an Ethernet Controller that controls four interfaces fails, those ports fail too. A common cause of such damage is ESD. For Catalyst 2900XL switches, the issue is documented in Cisco bug ID CSCdm13915 [🔗](#) (registered customers only) .

Failure of any of these diagnostic tests is normally fatal and usually requires a Return Material Authorization (RMA) to resolve the problem. In order to verify this, reset the switch with a console connection established and capture the actual bootup diagnostic information. Then open a service request with Cisco Technical Support.

Troubleshoot Fan Failures

Perform these actions if you suspect a fan failure:

1. Check the LEDs. If all of the LEDs are off, check the power to the switch. The fan can fail due to a power problem.
2. Check the system LED. The system LED is amber if the system detects a problem, and can indicate a fan problem if you cannot hear the fan in operation. If you use a Catalyst 3524-PWR-XL, issue the **show env fan** command to check the fan for failure.

Troubleshoot System Error Messages

System messages report any errors that the switch encounters. System messages can appear in the command line interface (CLI) while you are connected to the switch (through the console or Telnet). Syslogs are also recorded in the system message log of the switch. In order to view the system message log, issue the **show logging** command.

Refer to System Messages for syslog error message explanations and actions.

Troubleshoot High CPU

After you issue the **show processes cpu** command, the Catalyst 2900XL and Catalyst 3500XL switches report a high value for CPU utilization when idle. With other Cisco devices, high CPU utilization when idle is a cause for concern. However, such utilization is normal for Catalyst 2900XL and 3500XL switches. Refer to High CPU Utilization on Catalyst 2900XL/3500XL Switches for more information.

Troubleshoot high Memory utilization

High process Memory utilization

High process memory utilization occurs when you connect the Catalyst switch to IP phones on a port through the dot1q trunks. The switch can be configured with a number of VLANs. The switch sends spanning-tree BPDUs for all VLANs to the IP phone connected through trunk to the switch. This causes the memory utilization to increase on the switch.

When memory utilization increases, you can see an error message in the tracebacks, which is similar to this:

```
Dec  5 15:51:31 MET: %SYS-2-MALLOCFAIL: Memory allocation of 568 bytes failed from 0x192C2
-Process= "STP Queue Handler", ipl= 6, pid= 56
```

As a workaround, configure only an allowed VLAN list on the ports through the **switchport trunk allowed vlan {add vlan-list / all / except vlan-list / remove vlan-list}** command.

The allowed VLAN list must include only the VLANs that are necessary on that port, which are usually the voice and data VLANs. Refer to Cisco bug ID CSCdw22282 (registered customers only) for more information.

Troubleshoot Expansion Slots in the Catalyst 2900XL

Expansion Slot Module Does Not Work

Perform these actions to troubleshoot possible expansion slot problems:

1. Issue the **show version** command to ensure that the switch recognizes the module ports. In order to ensure that the software you run supports the module, refer to the Release Notes for the Catalyst 2900 Series XL and Catalyst 3500 Series XL Switches, Cisco IOS Release 12.0(5)WC2.
2. If you run the appropriate level of software, and the LED is still amber, make sure that the module is seated properly and that the thumb screws are tightened on the front pane of the module.
3. If the module still does not appear to be operational, try the module in another slot in the same switch. Alternatively, try the module in another switch, if available.

ATM Module Fails POST Tests

Refer to Understanding ATM Module POST Results for information on how to troubleshoot POST test failure on the ATM module.

ATM Module Has Corrupt Module Software

Refer to Recovering from Corrupted Module Software.

Password Recovery for the ATM Module

Refer to Recovering from a Lost or Forgotten Password.

Troubleshoot Interface Issues

Workstation cannot Log into the Network During Startup and cannot Obtain a DHCP Address

When you power up or reboot a client machine, if you observe one of these symptoms, the problem can be due to an initial connectivity delay that the switch introduces:

- Microsoft networking client displays `No Domain Controllers Available`.
- Dynamic Host Configuration Protocol (DHCP) reports `No DHCP Servers Available`.
- A Novell Internetwork Packet Exchange (IPX) networking workstation does not have the **Novell Login Screen** upon bootup.
- An AppleTalk networking client displays `Access to your AppleTalk network has been interrupted. To re-establish your connection, open and close the AppleTalk control panel. Sometimes, the chooser application of the AppleTalk client either does not display a zone list, or displays an incomplete zone list.`
- IBM network stations can display one of these messages:
 - ◆ `NSB83619--Address resolution failed`
 - ◆ `NSB83589--Failed to boot after 1 attempt`
 - ◆ `NSB70519--Failed to connect to a server`

See the Common Reasons and Solutions section for information on common reasons for this problem, and the solutions to recover from the problem.

Common Reasons and Solutions

The reasons for these symptoms can be:

- An interface delay caused by Spanning Tree Protocol (STP)
- EtherChannel, Trunking, or auto-negotiation delay

Refer to [Using Portfast and Other Commands to Fix Workstation Startup Connectivity Delays](#) for more information about these delays and their solutions.

Contact Cisco Technical Support if you still face issues after you review and follow the procedure in this document.

Troubleshoot NIC Compatibility Issues

When a server or client connection to the switch does not come up, look for an autonegotiation issue. If you see errors on the port, check for a Network Interface Card (NIC) compatibility issue, or an improper configuration on the switch.

See the Common Reasons and Solutions section for more information.

Common Reasons and Solutions

The reasons for these symptoms can be:

- A known NIC driver issue
- A speed and duplex mismatch
- Autonegotiation issues
- Cabling problems

Refer to [Troubleshooting Cisco Catalyst Switches to NIC Compatibility Issues](#) for more information on how to troubleshoot these problems.

Troubleshoot Interface Errors

If you experience slow performance or intermittent connectivity, check for interface errors. Issue the **show controllers ethernet-controller** command in order to check for interface errors for the port you troubleshoot. The Diagnostic Commands section of this document explains this command.

Also issue the **show interface** command. The Diagnostic Commands section explains this command also. Refer to Understanding Data Link Errors for additional information on each counter and possible causes.

This table lists some of the known issues with counters on the Catalyst 2900XL and 3500XL series switches.

Symptom	Description	Fix or Workaround
Runts on a 802.1Q trunk port.	A Catalyst 2900XL or 3500XL switch that receives a 64 or 66 byte 802.1Q encapsulated frame on a trunk port counts the frame as a runt. However, the switch continues to forward the frame. This issue is commonly seen when you connect Cisco 7960 IP phones to the switch when you use auxiliary (voice) VLANs. This issue is cosmetic, and is due to an ASIC limitation. This issue does not cause any degradation in the performance of the switch. Refer to Cisco bug ID CSCds32999 ☞ (registered customers only) for more information.	Cisco IOS Software Release 12.0(5.4)WC1 or later
Cyclic Redundancy Check (CRC) on an Inter-Switch Link (ISL) trunk port.	A Catalyst 3500XL or 2900XL Enterprise switch, with ISL trunking to the Fast Ethernet interface of a 7200-I/O-FE, 7500 PA-FE-TX, 3600 or 2600, or KeepAlive Link State Packets (LSP) marked as CRC/Input errors on the switch. These errors do not cause any performance impact. Refer to Cisco bug ID CSCdr22809 ☞ (registered customers only) for more information.	The workaround is to disable KeepAlive on the router or use 802.1Q trunking. No fix is available.
CRC on an ISL trunk port	Trunking between a Catalyst 2900XL and a Catalyst	The workaround is to use the

<p>that connects to a Catalyst 5500/5000 or 6500/6000 series switch.</p>	<p>5500/5000 or 6500/6000, with trunking negotiation through Dynamic Trunking Protocol (DTP) enabled on the Catalyst 5500/5000, causes CRC errors on the 2900XL due to the reception of non-ISL (DTP) packets. DTP or Dynamic Inter-Switch Link Protocol (DISL) sends out Protocol Data Units (PDUs) with both ISL and non-ISL encapsulated frames in order to speed up recovery from an out-of-sync situation for the hardware. An out-of-sync situation occurs when one side is trunk, and the other is not. Refer to Cisco bug ID CSCdm31600 ↗ (registered customers only) for more information. Also, refer to Cisco bug ID CSCdr72128 ↗ (registered customers only) for a variation of this issue.</p>	<p>nonegotiate trunk mode on the Catalyst 5500/5000, so that DTP does not run . No fix is available.</p>
<p>Giants on ISL or 802.1Q trunk ports.</p>	<p>When a Catalyst 2900XL switch receives a legal max-size Ethernet frame encapsulated or tagged for ISL or 802.1Q, and the packet is not forwarded to any other ports, the frame is counted as an oversize frame in the statistics counters.</p> <p>Note: There are many valid reasons for a packet to be received and not forwarded to any other ports. For example, packets received in a port that STP blocks, are not forwarded.</p> <p>Refer to Cisco bug ID CSCdm34557 ↗ (registered customers only) for more information.</p>	<p>There is no workaround for this bug. This issue is cosmetic only and you can ignore this issue with switch performance</p>

problems. No fix is available.

The CDP-4-DUPLEX_MISMATCH Error Message on an ISL Trunk Port on a C3524-PWR-XL

If you receive a CDP-4-DUPLEX_MISMATCH error message on an ISL trunk port on a Catalyst 3524-PWR-XL, see the Common Reasons and Solutions section for common reasons for this problem, and the relevant solutions.

Common Reasons and Solutions

- Make sure you have configured both sides with the same duplex. Typically, trunk ports are configured as full duplex links. Make sure both sides auto-negotiate correctly. If you hardcode on one side and set auto-negotiation on the other side, a half-duplex configuration arises on the auto-negotiate side of the link. Issue the **show interface *interface id*** command to check the duplex status.
- You can encounter Cisco bug ID CSCdx85015 [🔗](#) (registered customers only) . The workaround for this bug is to issue the **no power inline never** interface configuration command. The fix for the bug is available in Cisco IOS Software Release 12.0(5)WC5a or later.

Support for Loopback Interfaces

The loopback interfaces are not supported in Cisco Catalyst 2900XL/3500XL Series Switches. Loopback interfaces are not supported in these Cisco devices as they are purely Layer 2 switches and there is no need for any loopback interfaces.

The **interface loopback** command is a carry-over from the mainline Cisco IOS software releases and is not applicable to these device platforms. When you enter the CLI commands that refer to a loopback interface, it might trigger these messages to be displayed in the log:

```
Assert failure in ../src-l2-les-common/stp_les_shim.c line 2524
Assert failure in ../src-l2-les-common/stp_les_shim.c line 2592
Assert failure in ../src-l2-les-common/stp_les_cli_cfg.c line 1261
Assert failure in ../src-l2-les-common/stp_les_cli_cfg.c line 1358
Assert failure in ../src-l2-les-common/stp_les_shim.c line 2558
Assert failure in ../src-l2-les-common/stp_les_shim.c line 2748
```

This issue is documented in Cisco bug ID CSCsc43453 (registered customers only) .

Troubleshoot GBIC Issues

1000BASE-T GBIC is not Recognized or does not Work

- If you have a 1000Base-T Gigabit Interface Converter (GBIC), and the GBIC is not recognized or does not work, refer to 1000BASE-T GBIC Switch Compatibility Matrix to verify software support for the GBIC.
- If you run the appropriate level of software but the link still does not work, refer to Connector and Cable Specifications.

GigaStack GBIC is not Recognized or does not Work Properly

- If you have a GigaStack GBIC, which is not recognized or does not work, refer to Catalyst GigaStack Gigabit Interface Converter Switch Compatibility Matrix to verify software support for the GBIC.
- If you run the appropriate level of software but the link still does not work, refer to Troubleshooting GigaStack to troubleshoot further on the basis of the LED status:

GigaStack GBIC Link Flaps and Never Stabilizes

If your GigaStack GBIC link flaps and never stabilizes, refer to the *Link Flaps and Never Stabilizes* section of Catalyst Switch GigaStack Configuration and Implications.

Troubleshoot GigaStack GBIC Based on LED Status

If your GigaStack GBIC Interface LED is not solid green (which indicates normal function), refer to Troubleshooting GigaStack to troubleshoot on the basis of your LED status.

Troubleshoot GigaStack GBIC Loop Configuration

Software releases earlier than Cisco IOS Software Release 12.0(5)XU do not support the GigaStack GBIC loop configuration. Earlier releases cause excessive collision errors on the port and can cause the link to become unstable. This instability decreases performance on the links. Communication between the switches in the stack is adversely affected. Therefore, the loop configuration is supported only if every device in the stack runs Cisco IOS Software Release 12.0(5)XU or later.

Refer to the *Cabling Configuration* section of Catalyst Switch GigaStack Configuration and Implications.

Refer to GBIC Loop Configurations not Supported Before IOS Software Release 12.0(5)XU for a visual description of valid and invalid configurations.

The GigaStack GBIC module enables you to create a 1 Gbps stack configuration of up to nine supported switches. The GigaStack GBIC supports one full-duplex link (in a point-to-point configuration) or up to nine half-duplex links (in a stack configuration) to other GigaStack-compatible Ethernet devices. If you use the required Cisco proprietary signaling and cabling, the GigaStack GBIC-to-GigaStack GBIC connection does not exceed three feet (or one meter).

NO_LOOP_DETECT System Error Message with GigaStack GBIC

If you receive the `NO_LOOP_DETECT, GIGASTACK, LOG_ALERT, 0`, The link neighbor of link %d of GigaStack system message, and want to understand or troubleshoot, refer to the *Error Message: NO_LOOP_DETECT* section of Catalyst Switch GigaStack Configuration and Implications.

GIGASTACK-6-LOOP_DETECTED System Error Message with GigaStack GBIC

If you receive the `%GIGASTACK-6-LOOP_DETECTED: Gigastack GBIC in is selected as Master Loop Breaker` system message, refer to the *Message: %GIGASTACK-6-LOOP_DETECTED* section of Catalyst Switch GigaStack Configuration and Implications.

Troubleshoot Console Connectivity Problems

This section explains strategies to troubleshoot console connectivity problems.

Unreadable Characters on the Management Console

An incorrect baud rate setting on the management console typically causes unreadable characters.

In order to resolve this problem, reset the emulation software on the management console to 9600 baud (the default console baud rate of the switch). If this action does not help, cycle through the various baud rate

options on the management console until you find one that works. The switch baud rate may have been changed from the default.

No Connectivity Through the Console

Check this connectivity equipment.

- Make sure that the management console line is connected to the console port on the switch.
- Make sure that the correct cable and connector are used. Refer to [Connecting a Terminal to Catalyst 2900/3500 XL Switches](#) for more information.

Cisco Telnet Denial of Service

A specifically crafted TCP connection to a Telnet or reverse Telnet port of a Cisco device that runs Internetwork Operating System (IOS)® can block further access to the device through Telnet, reverse Telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP). Data Link Switching (DLSw) and protocol translation connections can also be affected. However, any Telnet, reverse Telnet, RSH, SSH, DLSw and protocol translation sessions established before exploitation are not affected.

All other device services operate normally. Services like packet forwarding (excluding DLSw and protocol translation), routing protocols and all other communication to and through the device are not affected.

Refer to Cisco bug ID CSCef46191 (registered customers only) . This bug tracks this problem. Also refer to the related Security Advisory at [Cisco Telnet Denial of Service Vulnerability](#).

Troubleshoot General Software Issues

Recover from Missing or Corrupted Software or Switch: Prompt

You need to recover the switch in these scenarios:

- If your switch misses software
- If your switch has a corrupt software image
- If your switch is in `Switch: prompt` mode
- If you receive the `Error Loading Flash` error message

Refer to [Recovery From Corrupt or Missing Software Image on Cisco Catalyst 2900XL and 3500XL Series Switches](#).

Troubleshoot Cisco Visual Switch Manager or Cluster Management Suite

If you have problems with your Cisco Visual Switch Manager or Cluster Management Suite, refer to [Troubleshooting Cisco Visual Switch Manager or Cluster Management Suite Access on the Catalyst 2900XL/3500XL/2950 Switch](#) for procedures to troubleshoot (including Java and browser requirements).

Hardware and Software Compatibility or Software Feature Support

Refer to these documents to identify the necessary software level to support a certain hardware or software feature:

- [1000BASE-T GBIC Switch Compatibility Matrix](#)
- [Catalyst GigaStack Gigabit Interface Converter Switch Compatibility Matrix](#)

- Minimum Cisco IOS Release for Major Features

Recover Lost Password

Refer to Password Recovery Procedure for the Catalyst Layer 2 Fixed Configuration and 3550 Series Switches to recover a lost password.

Diagnostic Commands

- **show interface**
- **show controllers ethernet-controller**
- **show env fan**
- **show logging**
- **show platform port-asic stats drop**

show interface

Enter the **show interface** command to check for speed and duplex settings, error counters, input and output queues, input and output rates, and to display the administrative and operational status of the interface. Use the `packets input` and `packets output` fields (from the output) to determine whether traffic enters or leaves the interface.

```
switch#show interface
```

```
FastEthernet0/1 is down, line protocol is down
Hardware is Fast Ethernet, address is 00d0.5868.f181 (bia 00d0.5868.f181)
MTU 1500 bytes, BW 0 Kbit, DLY 0 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive not set
Full-duplex, 100Mb/s, 100BaseTX/FX
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output 3w6d, output hang never
Last clearing of "show interface" counters 2w6d
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 0 multicast
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

Here are the counters that help you troubleshoot a problem on the interface:

Input Errors

`Input errors` provide a count of any errors that occurred during an attempt to receive packets from this port. The counter includes both CRC and frame errors. However, this counter does not include ignored packets. This is a list of input errors:

- **CRC Errors** These errors occur when the received packets fail the CRC check.

- **Frame Errors** Frame errors occur when the receiving frame is not complete.
- **Ignored Counter** This counter counts the number of frames dropped on input due to resource exhaustion in the switch fabric.
- **Overruns Counter** Overruns occur when Inter-Frame Gaps (IFG) are too short. In this case, a new Ethernet frame arrives before the previous one is completely stored in shared memory.

Output Errors

Output errors provide a count of any error that occurred while during an attempt to transmit packets from this port.

- **Collisions Counter** This counter shows the number of times a collision occurred during an attempt to transmit a packet from this port. This counter must be 0 for a port that operates in full-duplex mode.
- **Interface Resets Counter** This counter counts the number of times the port resets, generally due to link up or link down transitions.
- **Underruns Counter** Underruns occur when packets are not retrieved quickly enough from shared memory to be transmitted.

Babbles and Late Collisions

Babble errors occur due to the transmission of frames in excess of 1518 bytes in size. A late collision occurs outside of the collision window and occurs due to a duplex mismatch or a wire that exceeds the distance limitations (100 meters for 10/100 ports). The deferred counter tabulates the number of times the port waits to transmit due to traffic on the wire.

Lost Carrier and No Carrier

A carrier is an electrical signal that Ethernet devices use to detect whether another transmitting station uses the wire currently. The `lost carrier` counter increases when the carrier sense loss occurs when the hardware transmits a frame onto the wire and does not see its own carrier wave on the Ethernet. Absence of the carrier signal increments the `no carrier` counter.

show controllers ethernet-controller

The `show controllers ethernet-controller` command provides in-depth information about a specific interface as shown here:

```
Switch# show controllers ethernet-controller fa0/4

Transmit                               Receive
26869777 Bytes                          402753236 Bytes
460 Unicast frames                       1 Unicast frames
45408 Multicast frames                   198165 Multicast frames
12207 Broadcast frames                   0 Broadcast frames
Discarded frames                          0 No bandwidth frames
Too old frames                            0 No buffers frames
Deferred frames                           0 No dest, unicast
0 1 collision frames                      0 No dest, multicast
0 2 collision frames                      0 No dest, broadcast
0 3 collision frames                      1 Alignment errors
0 4 collision frames                      0 FCS errors
0 5 collision frames                      0 Collision fragments
0 6 collision frames
0 7 collision frames                      0 Undersize frames
0 8 collision frames                      198166 Minimum size frames
0 9 collision frames                      65 to 127 byte frames
0 10 collision frames                     28 to 255 byte frames
```

0 11 collision frames	256 to 511 byte frames
0 12 collision frames	512 to 1023 byte frames
0 13 collision frames	1024 to 1518 byte frames
0 14 collision frames	0 Oversize frames
0 15 collision frames	
0 16 Excessive collisions	1102 Late collisions

Most of the fields in the output are self-explanatory. This table explains platform-specific counters:

Fields	Explanation	Action
Discarded frames	The total number of frames whose transmission attempt is abandoned due to insufficient resources (such as underrun). This total includes frames of all destination types.	Reduce the traffic load destined to that interface if you see a rise in the number of packets in this field.
Too old frames	Number of frames that took longer than two seconds to travel through the switch, and the switch discarded the frames. This situation only occurs under extreme, high stress conditions.	Reduce the switch load if you see a rise in the number of packets in this field.
Deferred frames	The total number of frames whose first transmission attempt had to be delayed due to traffic on the network media. This total includes only those frames that are subsequently transmitted without error and without a collision.	Reduce the switch load if you see a rise in the number of packets in this field.
No bandwidth frames and No buffers frames	The number of times a port received a packet from the network. However, the switch does not have the resources to receive the packet. This situation occurs only under stress conditions, but can occur with bursts of traffic on several ports. So, a small number in the No bandwidth frames field is not a cause for concern. Ensure that this value is far less than 1 percent of the frames received.	Reduce the traffic load on the particular interface.
No dest, unicast	Number of times that a unicast packet is received. The port	See below.

	determines that the packet must not be forwarded to any other ports.	
No dest, multicast	Number of times that a multicast packet is received. The port determines that the multicast packet must not be forwarded to any other ports.	See below.
No dest, broadcast	Number of times that a broadcast packet is received. The port determines that the broadcast packet must not be forwarded to any other ports.	See below.

This is a brief description of example scenarios to receive an increase in the No dest counter.

- If STP blocks a port, most packets are not forwarded. This results in No dest packets.
- If a port just acquired a link, there is a very brief (less than one second) period where incoming packets are not forwarded.
- If a port is an access port, and the port is connected to an ISL trunk port, the No dest counter shows a very large value. All the incoming ISL packets are not forwarded. This is an invalid configuration.
- If a lone port is in a VLAN, and no other ports on the switch belong to that VLAN, the port drops incoming packets.
- Port A receives a packet with destination MAC address X. The switch has already learned that the MAC address X resides on port A. This situation arises if a hub is connected to port A. One workstation connected to the hub transmits packets to another workstation connected to the hub. This scenario is also possible if a switch is connected to port A, and the other switch temporarily floods packets to all ports while it learns the addresses.
- If a static address is set up on another port in the same VLAN, and no static address is set up for the receiving port, the packet is dropped. For example, if a static address is set up to specify that if the destination MAC address X is received on port f0/2, the packet must be forwarded to port f0/3. If a packet with the destination MAC address X is received on any port other than f0/2, but in the same VLAN as f0/2, the packet is dropped.
- If the port is a secure port, packets with disallowed source MAC addresses are not forwarded.

show env fan

The **show env fan** command is applicable only to the Catalyst 3524PWR–XL switches. This command helps to identify whether the system fan is faulty. If so, replace the switch.

```
Switch# show env fan
FAN 1 is OK

FAN 2 is OK

FAN 3 is OK

FAN 4 is OK

FAN 5 is OK
```

show logging

The **show logging** command helps to check the logged system messages. Make sure logging is enabled if you do not see any messages in the output of this command, in the console, or in the syslog server. Enable timestamps with the **service timestamps** global configuration command.

```
3500XL>show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
Console logging: level debugging, 102 messages logged
Monitor logging: level debugging, 0 messages logged
Buffer logging: level debugging, 102 messages logged
File logging: disabled
Trap logging: level informational, 108 message lines logged

Log Buffer (4096 bytes):
by console
00:09:55: %LINK-3-UPDOWN: Interface FastEthernet0/48, changed state to down
00:09:56: %LINEPROTO-5-UPDOWN:
    Line protocol on Interface FastEthernet0/48, changed state to down
00:13:30: %SYS-5-CONFIG_I: Configured from console by console
00:50:27: %CMP-CLUSTER_MEMBER_2-5-ADD:
    The Device is added to the cluster (Cluster Name:
    CH-3500-8, CMDR IP Address 10.10.10.101)
1w3d: %SYS-CLUSTER_MEMBER_2-5-CONFIG_I: Configured from console by console
3500XL>
```

show platform port-asic stats drop

The **show platform port-asic stats drop** command provides the real drops and indicates towards-traffic microbursts which cause the egress buffer to exhaust.

```
Switch#sh platform port-asic stats drop gig1/0/1
```

```
Interface Gi1/0/1 TxQueue Drop Statistics
Queue 0
  Weight 0 Frames 0
  Weight 1 Frames 0
  Weight 2 Frames 0
Queue 1
  Weight 0 Frames 0
  Weight 1 Frames 43472041
  Weight 2 Frames 1
Queue 2
  Weight 0 Frames 0
  Weight 1 Frames 0
  Weight 2 Frames 0
Queue 3
  Weight 0 Frames 0
  Weight 1 Frames 0
  Weight 2 Frames 3631857
Queue 4
  Weight 0 Frames 0
  Weight 1 Frames 0
  Weight 2 Frames 0
Queue 5
  Weight 0 Frames 0
  Weight 1 Frames 0
  Weight 2 Frames 0
```

Related Information

- [Cisco Catalyst 2900 Series LRE XL Switches Release Notes](#)
 - [Cisco Catalyst 3500 XL Series Switches Release Notes](#)
 - [Switches Product Support](#)
 - [LAN Switching Technology Support](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

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

© 2011 – 2012 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Mar 01, 2007

Document ID: 29200
