Troubleshooting WS−X6348 Module Port Connectivity on a Catalyst 6500/6000 Running Cisco IOS System Software

Document ID: 29423

Contents

Introduction
Prerequisites
Requirements
Components Used
Conventions
Before You Begin
WS−X6348 Module Architecture
Known Issues
Troubleshooting Catalyst 6500/6000 WS−X6348 Module Port Connectivity
Step−by−Step Instructions
Command Outputs to Collect Before Contacting TAC
Related Information

Introduction

This document discusses detailed troubleshooting for the WS−X6348 module on the Catalyst 6500/6000 running Cisco IOS® and the command outputs to collect before contacting TAC.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

- Catalyst 6500 with Supervisor II with Multilayer Switch Feature Card 2 (MSFC2)
- WS−X6348 module
- Cisco IOS version 12.1(11b)E4

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Before You Begin

WS−X6348 Module Architecture

Each WS−X6348 card is controlled by a single Application−Specific Integrated Circuit (ASIC) that connects the module to both the 32 GB data bus backplane of the switch and to a set of four other ASICs which controls groups of 12 10/100 ports.

An understanding of this architecture is important as it can help in troubleshooting interface problems. For example, if a group of 12 10/100 interfaces fails the online diagnostics (refer to Step 18 of this document to learn more about the **show diagnostic module** <*mod#*> command), this typically indicates one of the ASICs mentioned above has failed.

Known Issues

You may see a message similar to one or more of the following in the syslogs or **show log** command output:

- Coil Pinnacle Header Checksum
- Coil Mdtif State Machine Error
- Coil Mdtif Packet CRC Error
- Coil Pb Rx Underflow Error
- Coil Pb Rx Parity Error

If you see one or more of these messages, and you have a group of 12 ports stuck and not passing traffic, perform the following steps:

1. Disable and enable the interfaces.
2. Soft−reset the module (by issuing the **hw−module module** <*module#*> **reset** command).
3. Hard−reset the module by physically reseating the card or by issuing the **no power enable module** <*module#*> and the **power enable module** <*module#*> global configuration commands.

After performing steps 2 and/or 3, contact the Technical Assistance Center (TAC) with the above information if you encounter one or more of the following:

- The module does not come online.
- The module comes online, but a group of 12 interfaces fails diagnostics (as seen in the output from the **show diagnostic module** <*mod#*> command).
- The module is stuck in the other state when booting up.
- All port LEDs on the module become amber.
- All interfaces are in the err−disabled state as seen by issuing the **show interfaces status module** <*module#*> command.

Troubleshooting Catalyst 6500/6000 WS−X6348 Module Port Connectivity

Step−by−Step Instructions

In order to perform port connectivity troubleshooting on the Catalyst 6500/6000 WS−X6348 module, complete these steps:

1. Check the software version in use and make sure there are no known WS−X6348 issues with that code.

```
e-6509-a#show version
Cisco Internetwork Operating System Software
IOS (tm) c6sup2_rp Software (c6sup2_rp-DSV-M), Version 12.1(11b)E4, EARLY DEPLOY
MENT RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Thu 30-May-02 23:12 by hqluong
Image text-base: 0x40008980, data-base: 0x415CA000

ROM: System Bootstrap, Version 12.1(4r)E, RELEASE SOFTWARE (fc1)
BOOTLDR: c6sup2_rp Software (c6sup2_rp-DSV-M), Version 12.1(11b)E4, EARLY DEPLOY
MENT RELEASE SOFTWARE (fc1)

e-6509-a uptime is 3 weeks, 2 days, 23 hours, 29 minutes
System returned to ROM by power-on (SP by power-on)
System restarted at 20:50:55 UTC Wed Oct 23 2002
System image file is "bootflash:c6sup22-dsv-mz.121-11b.E4"

cisco Catalyst 6000 (R7000) processor with 112640K/18432K bytes of memory.
Processor board ID SAD054305CT
R7000 CPU at 300Mhz, Implementation 39, Rev 2.1, 256KB L2, 1024KB L3 Cache
Last reset from power-on
Bridging software.
X.25 software, Version 3.0.0.
24 Ethernet/IEEE 802.3 interface(s)
2 Virtual Ethernet/IEEE 802.3  interface(s)
120 FastEthernet/IEEE 802.3 interface(s)
10 Gigabit Ethernet/IEEE 802.3 interface(s)
381K bytes of non-volatile configuration memory.

16384K bytes of Flash internal SIMM (Sector size 512K).
Configuration register is 0x2102
```

2. Verify that the module is a WS−X6348 and that the status is Ok.

```
e-6509-a#show module 4

Mod Ports Card Type                              Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  4   48  48 port 10/100 mb RJ45                 WS-X6348-RJ-45     SAL05187Q59
```

```
Mod MAC addresses                          Hw    Fw           Sw           Status
--- ---------------------------------- ------ ------------ ------------ -------
  4  0005.3130.6bc8 to 0005.3130.6bf7   5.0   5.4(2)       7.2(0.35)    Ok

Mod Sub-Module                  Model           Serial           Hw     Status
--- --------------------------- --------------- ---------------- ------- -------
  4 Inline Power Module         WS-F6K-PWR                       1.0    Ok
e-6509-a#
```

In the command output above, check the status of the module. It could be in one of the following states:

- `Ok` − Everything is fine.
- `power-deny` − Not enough power is available to power the module.
- `other` − Most likely the Serial Communication Protocol (SCP) communication is broken.
- `faulty/unknown` − This indicates most likely a bad module or slot.
- `err-disabled` − View the output from the **show log** command (shown in Step 4) to see if there are any messages on why the module is in the `err-disabled` state.

3. Verify that the configuration for the specific interface and any global configuration that might effect the interface is correct. Ensure that options such as spanning−tree portfast, are configured when appropriate.

```
e-6509-a#show running-config interface fastethernet 4/1
Building configuration...

Current configuration : 134 bytes
!
interface FastEthernet4/1
 no ip address
 switchport
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
end

e-6509-a#show running-config interface vlan 2
Building configuration...

Current configuration : 61 bytes
!
interface Vlan2
 ip address 192.168.2.2 255.255.255.0
end

e-6509-a#show running-config
Building configuration...
Current configuration : 9390 bytes
!
! Last configuration change at 20:23:32 UTC Sat Nov 16 2002
! NVRAM config last updated at 20:54:58 UTC Wed Oct 23 2002
!
version 12.1
service timestamps debug datetime
service timestamps log datetime
no service password-encryption
!
hostname e-6509-a
!
!
redundancy
 main-cpu
  auto-sync standard
```

```
!
vlan 2
vtp mode transparent
ip subnet-zero
!
!
 --More
<output truncated>
```

4. Check for any interface related messages in the log by issuing the **show log** command. With Integrated Cisco IOS (Native Mode), the log can display messages from both the Switch Processor (SP) (SP = Supervisor/Policy Feature Card (PFC)) and the Route Processor (RP) (RP = MSFC).

```
e-6509-a#show log
Syslog logging: enabled (2 messages dropped, 0 flushes, 0 overruns)
    Console logging: level debugging, 333 messages logged
    Monitor logging: level debugging, 0 messages logged
    Buffer logging: level debugging, 333 messages logged
    Trap logging: level informational, 132 message lines logged

Log Buffer (8192 bytes):

Nov 10 17:04:44: %C6KPWR-SP-4-ENABLED: power to module in slot 4 set on
Nov 10 17:05:33: %DIAG-SP-6-RUN_MINIMUM: Module 4: Running Minimum Online Diagnostic
Nov 10 17:05:38: %DIAG-SP-6-DIAG_OK: Module 4: Passed Online Diagnostics
Nov 10 17:05:38: %OIR-SP-6-INSCARD: Card inserted in slot 4, interfaces are now Onli
etc&
```

5. The following command can be used to determine the status of the interface as well as whether the interface is configured as a Layer 3 (L3) routed interface (the default), a trunk, or a Layer 2 (L2) switchport.

```
e-6509-a#show interfaces fastethernet 4/1 status

Port    Name               Status       Vlan       Duplex  Speed Type
Fa4/1                      connected    2          a-full  a-100 10/100BaseTX

e-6509-a#show interfaces fastethernet 4/2 status
Port    Name               Status       Vlan       Duplex  Speed Type
Fa4/2                      connected    trunk      a-full  a-100 10/100BaseTX

e-6509-a#show interfaces fastethernet 4/3 status
Port    Name               Status       Vlan       Duplex  Speed Type
Fa4/3                      connected    routed     a-full  a-100 10/100BaseTX
```

- The Status field can display the following states:
  - ◊ connected
  - ◊ notconnect
  - ◊ connecting
  - ◊ faulty
  - ◊ inactive
  - ◊ shutdown
  - ◊ disabled
  - ◊ err-disabled
  - ◊ monitor
  - ◊ active
  - ◊ dot1p
  - ◊ untagged
  - ◊ inactive
  - ◊ onhook

If an interface is in the notconnect state, check the cabling as well as the device connected to

the other end. If an interface is in the faulty state, it indicates a hardware problem; issue the **show diagnostic module** <*mod*> command for module diagnostic results. If the interface is an L2 interface and shows the inactive state, ensure its VLAN still exists by issuing the **show vlan** command and try to shut/no shut the interface. VLAN Trunk Protocol (VTP) problems can sometimes cause a VLAN to be deleted, which results in interfaces associated with that VLAN becoming inactive.

- The Vlan field displays routed if the interface is configured as an L3 routed interface. It displays trunk if the interface is configured as a trunk interface, or if the VLAN number that the interface is a member of is configured as an L2 access switchport.
- The Duplex and Speed fields have an a in front of the value displayed (such as a−full) if the value has been obtained through auto−negotiation. If the interface is hardcoded, the a will not be present for those fields. While not in a connected state, an auto−negotiation−enabled interface displays auto in these fields. Make sure that the device attached to this interface has the same settings as this interface regarding either hard−setting the speed and duplex or auto−negotiating the speed and duplex.

If your port is a routed port, skip to Step 10. Otherwise continue below.

If the interface is in an err−disabled state, issue the following command option to determine the reason:

```
e−6509−a#show interfaces fastethernet 4/1 status err−disabled
Port    Name               Status       Reason
Fa4/1                      connected    none
```

- The reason (found under the Reason field) for an interface to be placed in an err−disabled state can be any of the following:

  ◊ bpduguard
  ◊ dtp−flap
  ◊ link−flap
  ◊ pagp−flap
  ◊ root−guard
  ◊ udld

  An error−disabled state is an operational state similar to a link down state. You must issue the **shutdown** and the **no shutdown** commands to manually recover an interface from err−disable after fixing the cause of the error. An interface displaying Reason = none implies that the interface is not currently in an err−disabled state.

6. If an interface is configured as a trunk, check to make sure it is in the correct status and that the appropriate VLANs are spanning−tree forwarding and not pruned by VTP. For a dot1q trunk, make sure that the native VLAN matches that of the device on the other side of the trunk.

```
e−6509−a#show interfaces fastethernet 4/2 trunk

Port      Mode         Encapsulation  Status        Native vlan
Fa4/2     on           802.1q         trunking      1

Port      Vlans allowed on trunk
Fa4/2     1−1005

Port      Vlans allowed and active in management domain
Fa4/2     1−2,1002−1005

Port      Vlans in spanning tree forwarding state and not pruned
Fa4/2     1,1002−1005
```

- In the above output, you can see that Fast Ethernet interface 4/2 is in the Status state of trunking and is a dot1q trunk with Native vlan = 1. The trunking mode has been hard−set to

on.

- **Note:** While VLAN 2 exists in the Vlans allowed and active in management domain list, it does not exist in the Vlans in spanning tree forwarding state and not pruned list, since Fast Ethernet interface 4/2 is actually spanning−tree blocking for VLAN 2.

```
e−6509−a#show spanning−tree interface fastethernet 4/2 state
VLAN1                forwarding
VLAN2                blocking
VLAN1002             forwarding
VLAN1003             forwarding
VLAN1004             forwarding
VLAN1005             forwarding
```

7. The following command can be used to check the configuration and status of an interface configured as a trunk or an L2 access switchport:

   The following is an example of an L2 access switchport:

```
e−6509−a#show interfaces fastethernet 4/1 switchport
Name: Fa4/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access

!−−− This is an L2 static access interface.

Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 2 (VLAN0002)

!−−− This interface is a member of VLAN 2.

Trunking Native Mode VLAN: 1 (default)
Administrative private−vlan host−association: none
Administrative private−vlan mapping: none
Operational private−vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2−1001

e−6509−a#show running−config interface fastethernet 4/1
Building configuration...

Current configuration : 134 bytes
!
interface FastEthernet4/1
 no ip address
 switchport
 switchport access vlan 2
 switchport mode access
 spanning−tree portfast
end
```

   The following is an example of an L2 trunk switchport:

```
e−6509−a#show interfaces fastethernet 4/2 switchport
Name: Fa4/2
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk

!−−− This interface is a trunk.

Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
```

```
!--- This interface is a dot1q trunk.

Negotiation of Trunking: On

!--- This interface became a dot1q trunk through
!--- negotiations with its link partner.

Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)

!--- The native VLAN = 1.

Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL

!--- No VLANs have been cleared from this trunk.

Pruning VLANs Enabled: 2-1001

!--- VLANs in this range are capable of being pruned
!--- by the VTP.


e-6509-a#show running-config interface fastethernet 4/2
Building configuration...

Current configuration : 121 bytes
!
interface FastEthernet4/2
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
end
```

8. Verify that dynamic Content Addressable Memory (CAM) entries are being created for any traffic entering the L2 switchport or trunk interface you are troubleshooting. Make sure that the CAM entry is associated with the correct VLAN.

```
e-6509-a#show mac-address-table interface fastethernet 4/1
Codes: * - primary entry

  vlan   mac address     type    qos            ports
------+---------------+--------+---+--------------------------------
*    2  00d0.0145.bbfc   dynamic  --  Fa4/1
```

9. Verify that an L2 switchport or trunk interface is forwarding for spanning-tree on the correct VLAN(s). Make sure that portfast is enabled or disabled where appropriate.

```
e-6509-a#show spanning-tree interface fastethernet 4/1
 Port 193 (FastEthernet4/1) of VLAN2 is forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.193.
   Designated root has priority 8192, address 00d0.0145.b801
   Designated bridge has priority 8192, address 00d0.0145.b801
   Designated port id is 129.1, designated path cost 0
   Timers: message age 2, forward delay 0, hold 0
   Number of transitions to forwarding state: 8483
   BPDU: sent 115, received 4368
   The port is in the portfast mode

e-6509-a#show spanning-tree interface fastethernet 4/1 state
VLAN2                forwarding

e-6509-a#show spanning-tree vlan 2
```

```
VLAN2 is executing the ieee compatible Spanning Tree protocol
 Bridge Identifier has priority 32768, address 0008.20f2.a002
 Configured hello time 2, max age 20, forward delay 15
 Current root has priority 8192, address 00d0.0145.b801
 Root port is 193 (FastEthernet4/1), cost of root path is 19
 Topology change flag not set, detected flag not set
 Number of topology changes 6 last change occurred 02:18:47 ago
 Times:  hold 1, topology change 35, notification 2
         hello 2, max age 20, forward delay 15
 Timers: hello 0, topology change 0, notification 0, aging 300

Port 193 (FastEthernet4/1) of VLAN2 is forwarding
  Port path cost 19, Port priority 128, Port Identifier 128.193.
  Designated root has priority 8192, address 00d0.0145.b801
  Designated bridge has priority 8192, address 00d0.0145.b801
  Designated port id is 129.1, designated path cost 0
  Timers: message age 1, forward delay 0, hold 0
  Number of transitions to forwarding state: 8543
  BPDU: sent 115, received 4398
  The port is in the portfast mode

Port 194 (FastEthernet4/2) of VLAN2 is blocking
  Port path cost 19, Port priority 128, Port Identifier 128.194.
  Designated root has priority 8192, address 00d0.0145.b801
  Designated bridge has priority 8192, address 00d0.0145.b801
  Designated port id is 129.2, designated path cost 0
  Timers: message age 2, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  BPDU: sent 230, received 4159
```

If your port is a L2 switchport or trunk, proceed to Step 11.

10. For L3 routed interfaces, make sure that you are learning IP routes and Address Resolution Protocol (ARP) entries. Ensure that routing protocol neighbors are being formed correctly through the interface in question.

```
e-6509-a#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - ISIS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    200.200.200.0/24 is directly connected, Loopback1
     160.10.0.0/24 is subnetted, 1 subnets
C       160.10.10.0 is directly connected, Vlan1
     130.130.0.0/16 is variably subnetted, 2 subnets, 2 masks
D       130.130.0.0/16 is a summary, 01:24:53, Null0
C       130.130.130.0/24 is directly connected, FastEthernet4/3
C    192.168.2.0/24 is directly connected, Vlan2
D    120.0.0.0/8 [90/130816] via 192.168.2.1, 01:14:39, Vlan2
D    150.150.0.0/16 [90/130816] via 192.168.2.1, 01:14:39, Vlan2

e-6509-a#show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.2.2              -   0008.20f2.a00a  ARPA   Vlan2
Internet  192.168.2.1             85   00d0.0145.bbfc  ARPA   Vlan2
Internet  130.130.130.2           74   00d0.0145.bbfc  ARPA   FastEthernet4/3
Internet  130.130.130.1            -   0008.20f2.a00a  ARPA   FastEthernet4/3
Internet  160.10.10.1              -   0008.20f2.a00a  ARPA   Vlan1

e-6509-a#show ip arp 130.130.130.2
```

```
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  130.130.130.2          86   00d0.0145.bbfc  ARPA   FastEthernet4/3

e-6509-a#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address                 Interface   Hold Uptime   SRTT   RTO  Q  Seq Type
                                        (sec)         (ms)       Cnt Num
1   130.130.130.2           Fa4/3         14 01:14:54    1  3000  0  2
0   192.168.2.1             Vl2           13 01:25:10    1   200  0  1
```

11. If the interface is connected to another Cisco device, use Cisco Discovery Protocol (CDP) to check if this interface can see that device.

    Note: CDP must be enabled on this switch and the other Cisco device. Also, note that CDP is Cisco proprietary, and therefore does not work with non-Cisco devices.

    Make sure CDP is enabled globally on this switch by issuing the following command.

    ```
    e-6509-a#show cdp
    Global CDP information:
            Sending CDP packets every 60 seconds
            Sending a holdtime value of 180 seconds
            Sending CDPv2 advertisements is enabled
    ```

    Make sure CDP is enabled on the interface by issuing the command below. If CDP is disabled on the interface, the following command will not provide any output. You can also issue the **show running-config interface fastethernet** <*mod/port*> command to ensure that the **no cdp enable** command is not present on the interface.

    ```
    e-6509-a#show cdp interface fastethernet 4/1
    FastEthernet4/1 is up, line protocol is up
      Encapsulation ARPA
      Sending CDP packets every 60 seconds
      Holdtime is 180 seconds
    ```

    In the following example, Fast Ethernet interface 4/1 on the Catalyst 6509 switch directly connects to Fast Ethernet interface 5/1 on another Catalyst 6509. The neighbor Catalyst 6500 is running hybrid CatOS 6.3(9), and is named "e-6509-b." It has an IP address of 192.168.2.3. This information was learned through a CDP version 2 advertisement.

    ```
    e-6509-a#show cdp neighbors fastethernet 4/1 detail
    -------------------------
    Device ID: SCA041601ZB(e-6509-b)
    Entry address(es):
      IP address: 192.168.2.3
    Platform: WS-C6509,  Capabilities: Trans-Bridge Switch IGMP
    Interface: FastEthernet4/1,  Port ID (outgoing port): 5/1
    Holdtime : 174 sec

    Version :
    WS-C6509 Software, Version McpSW: 6.3(9) NmpSW: 6.3(9)
    Copyright (c) 1995-2002 by Cisco Systems

    advertisement version: 2
    VTP Management Domain: 'test'
    Native VLAN: 2
    Duplex: full
    ```

    The following command can be used to check if the interface is transmitting and receiving CDP version 1 or version 2 packets and whether any errors have been experienced:

    ```
    e-6509-a#show cdp traffic
    ```

```
CDP counters :
        Total packets output: 30781, Input: 30682
        Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
        No memory: 0, Invalid packet: 0, Fragmented: 0
        CDP version 1 advertisements output: 0, Input: 0
        CDP version 2 advertisements output: 30781, Input: 30682
```

- Most non−Cisco devices as well as Cisco devices with CDP disabled allow CDP packets to pass through them. This can sometimes lead you to believe that two Cisco CDP enabled devices are directly connected when, in fact, they are not. CDP uses multicast destination address 01−00−0C−CC−CC−CC, which is typically flooded throughout the VLAN of a switch that is not CDP enabled or that does not support CDP.

  Note: The **clear cdp table** and **clear cdp counters** commands are available and can be used to clear the CDP table and counters if needed.

12. Check the state and health of the interface that is encountering problems, and whether traffic is passing through it.

```
e−6509−a#show interfaces fastethernet 4/1
FastEthernet4/1 is up, line protocol is up
  Hardware is C6k 100Mb 802.3, address is 0005.3130.6bc8 (bia 0005.3130.6bc8)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Full−duplex, 100Mb/s
  input flow−control is off, output flow−control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:02, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     7915 packets input, 571304 bytes, 0 no buffer
     Received 7837 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     3546 packets output, 332670 bytes, 0 underruns
     0 output errors, 0 collisions, 4 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

- `FastEthernet4/1 is up` − This indicates that the interface hardware is currently active. It can also indicate that the interface has been taken down by an administrator by issuing the **shut interface** command, if the status reads administratively down.
- `line protocol is up` − This indicates whether the software processes that handle the line protocol for the interface consider the line usable.
- `MTU` − The Maximum Transmission Unit (MTU) is 1500 bytes for Ethernet by default (the maximum data portion size of a standard Ethernet frame). For jumbo frame support, the MTU can be increased to a maximum of 9216 bytes by issuing the **MTU** <*bytes*> **interface** command.
- `Full−duplex, 100Mb/s` − The current speed and duplex setting of the interface. Issue the **show interfaces FastEthernet** <*mod/port*> **status** (as shown in Step 5) to determine if this setting has been hard−set in the configuration, or obtained through auto−negotiation with the link partner. Also make sure that the device attached to this interface has the same settings as the interface regarding either hard−setting the speed and duplex or auto−negotiating the speed and duplex.

- `Last input, output` − The number of hours, minutes, and seconds since the last packet was successfully received or transmitted by the interface. This is useful for knowing when a dead interface failed.
- `Last clearing of "show interface" counters` − The last time the **clear counters** command was issued since the last time the switch was rebooted. The **clear counters** command is used to reset all of the statistics displayed through issuing the **show interfaces FastEthernet** <*mod/port*> command.

  Note: Variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared.
- `Input queue` − The number of packets in the input queue. Size/max/drops means the current number of frames in the queue/the max number of frames the queue can hold before it must start dropping frames/the actual number of frames dropped because the max queue size was exceeded. The input queue size can be modified by issuing the **hold−queue** <*queue size*> **in interface** command. Be careful when increasing the size of the queue as this may result in traffic delays because the frames get stuck in the queue for a longer period of time.
- `Total output drops` − The number of packets dropped because the output queue is full. A common cause of this might be traffic from a high bandwidth link being switched to a lower bandwidth link or traffic from multiple inbound links being switched to a single outbound link. For example, if a large amount of bursty traffic comes in on a gigabit interface and is switched out to a 100Mbps interface, this might cause output drops to increment on the 100Mbps interface. This is because the output queue on that interface is overwhelmed by the excess traffic due to the speed mismatch between the incoming and outgoing bandwidths.
- `Output queue` − The number of packets in the output queue. Size/max means the current number of frames in the queue/the max number of frames the queue can hold before it is full and must start dropping frames. The output queue size can be modified by issuing the **hold−queue** <*queue size*> **out interface** command. Be careful when increasing the size of the queue as this may result in traffic delays because the frames get stuck in the queue for a longer period of time.
- `5 minute input/output rate` − The average input and output rate seen by the interface in the last five minutes. To get a more accurate reading by specifying a shorter period of time (to better detect traffic bursts for example), issue the **load−interval** <*seconds*> **interface** command.
- `packets input/output` − The total error free packets received and transmitted on the interface. Monitoring these counters for increments is useful in determining whether traffic is flowing properly through the interface. The bytes counter includes both the data and MAC encapsulation in the error free packets received and transmitted by the system.
- `no buffer` − The number of received packets discarded because there is no buffer space. Compare with ignored count. Broadcast storms can often be responsible for these events.
- `Received broadcasts` − The total number of broadcasts and multicasts received on the interface.
- `runts` − The frames received that are smaller than the minimum IEEE 802.3 frame size (64 bytes for Ethernet) and with a bad Cyclic Redundancy Check (CRC). This can be caused by a duplex mismatch and physical problems such as a bad cable, port, or Network Interface Card (NIC) on the attached device.
- `giants` − The frames received that exceed the maximum IEEE 802.3 frame size (1518 bytes for non−jumbo Ethernet) and have a bad Frame Check Sequence (FCS). Try to find the offending device and remove it from the network. In many cases it is the result of a bad NIC.
- `throttles` − The number of times the interface requested another interface within the switch to slow down in sending information to the interface.
- `input errors` − This includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts. Other input−related errors can also cause the input errors count to be increased, and some datagrams may have more than one error. Therefore, this sum may not balance with the sum of enumerated input error counts.

- `CRC` − This increments when the CRC generated by the originating LAN station or far−end device does not match the checksum calculated from the data received. This usually indicates noise or transmission problems on the LAN interface or the LAN itself. A high number of CRCs is usually the result of collisions but can also indicate a physical issue (such as cabling, bad interface or NIC) or a duplex mismatch.
- `frame` − The number of packets received incorrectly having a CRC error and a non−integer number of octets (alignment error). This is usually the result of collisions or a physical problem (such as cabling, bad port or NIC) but can also indicate a duplex mismatch.
- `overrun` − The number of times the receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
- `ignore` − The number of received packets ignored by the interface because the interface hardware ran low on internal buffers. Broadcast storms and bursts of noise can cause the ignored count to be increased.
- `Input packets with dribble` − A dribble bit error indicates that a frame is slightly too long. This frame error counter is incremented for informational purposes, since the switch accepts the frame.
- `underruns` − The number of times that the transmitter has been running faster than the switch can handle.
- `output errors` − The sum of all errors that prevented the final transmission of datagrams out of the interface.

  Note: This may not equal the sum of the enumerated output errors, as some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.
- `collision` − The number of times a collision occurred before the interface transmitted a frame to the media successfully. Collisions are normal for interfaces configured as half duplex, but should not be seen on full duplex interfaces. If collisions are increasing dramatically, this points to a highly utilized link or possibly a duplex mismatch with the attached device.
- `interface resets` − The number of times an interface has been completely reset. This can happen if packets queued for transmission are not sent within several seconds. Interface resets can also occur when an interface is looped back or shut down.
- `babble` − The transmit jabber timer expired. A jabber is a frame longer than 1518 octets (excluding framing bits, but including FCS octets), which does not end with an even number of octets (alignment error) or has a bad FCS error.
- `late collision` − The number of times that a collision is detected on a particular interface late in the transmission process. For a 10Mbit/s port this is later than 512 bit−times into the transmission of a packet. Five hundred and twelve bit−times corresponds to 51.2 microseconds on a 10 Mbit/s system. This error can indicate a duplex mismatch among other things. For the duplex mismatch scenario, the late collision is seen on the half duplex side. As the half duplex side is transmitting, the full duplex side does not wait its turn and transmits simultaneously causing a late collision. Late collisions can also indicate an Ethernet cable or segment that is too long. Collisions should not be seen on interfaces configured as full duplex.
- `deferred` − The number of frames that have been transmitted successfully after waiting because the media was busy. This is usually seen in half duplex environments where the carrier is already in use when trying to transmit a frame.
- `lost carrier` − The number of times the carrier was lost during transmission.
- `No carrier` − The number of times the carrier was not present during the transmission.
- `Output buffer` − The number of failed buffers and the number of buffers swapped out.

13. Check that traffic counters are incrementing both inbound and outbound on the port.

```
e−6509−a#show interfaces fastethernet 4/1 counters

Port            InOctets   InUcastPkts   InMcastPkts   InBcastPkts
Fa4/1             575990            78          7902             1
```

```
Port           OutOctets  OutUcastPkts  OutMcastPkts  OutBcastPkts
Fa4/1             335122            76          3456            41
```

- The above command shows the total unicast, multicast, and broadcast packets received (In) and transmitted (Out) on an interface.

  Note: If the interface is configured as an Inter−Switch Link Protocol (ISL) trunk, all traffic will be multicast (all ISL headers use a destination multicast address of 01−00−0C−CC−CC−CC).
- Issue the **clear counters [fastethernet** <*mod/port*>**]** command to reset these statistics.

14. Check for errors associated with the interface.

```
e−6509−a#show interfaces fastethernet 4/1 counters errors

Port        Align−Err    FCS−Err   Xmit−Err    Rcv−Err UnderSize OutDiscards
Fa4/1               0          0          0          0         0           0

Port      Single−Col Multi−Col  Late−Col Excess−Col Carri−Sen     Runts    Giants
Fa4/1              0         0         0          0         0         0         0

Port       SQETest−Err Deferred−Tx IntMacTx−Err IntMacRx−Err Symbol−Err
Fa4/1                0           0            0            0          0
```

- `Align−Err` − The number of frames with alignment errors (frames that do not end with an even number of octets and have a bad CRC) received on the interface. These usually indicate a physical problem (such as cabling, bad interface or NIC), but can also indicate a duplex mismatch. When the cable is first connected to the interface, some of these errors may occur. Also, if there is a hub connected to the interface, collisions between other devices on the hub may cause these errors.
- `FCS−Err` − The number of valid size frames with FCS errors but no framing errors. This is typically a physical issue (such as cabling, bad interface or NIC) but can also indicate a duplex mismatch.
- `Xmit−Err and Rcv−Err` − These indicate that the internal interface send (Tx) and receive (Rx) buffers are full. A common cause of Xmit−Err might be traffic from a high bandwidth link being switched to a lower bandwidth link, or traffic from multiple inbound links being switched to a single outbound link. For example, if a large amount of bursty traffic comes in on a gigabit interface and is switched out to a 100Mbps interface, this might cause Xmit−Err to increment on the 100Mbps interface. This is because the interface s output buffer is overwhelmed by the excess traffic due to the speed mismatch between the incoming and outgoing bandwidths.
- `Undersize` − The frames received that are smaller than the minimum IEEE 802.3 frame size of 64 bytes (excluding framing bits, but including FCS octets) that are otherwise well formed. Check the device sending out these frames.
- `Out−Discard` − The number of outbound packets chosen to be discarded even though no errors have been detected. One possible reason for discarding such a packet could be to free up buffer space.
- `Single−coll` (single collision) − The number of times one collision occurred before the interface transmitted a frame to the media successfully. Collisions are normal for interfaces configured as half duplex but should not be seen on full duplex interfaces. If collisions are increasing dramatically, this points to a highly utilized link or possibly a duplex mismatch with the attached device.
- `Multi−coll` (multiple collision) − The number of times multiple collisions occurred before the interface transmitted a frame to the media successfully. Collisions are normal for interfaces configured as half duplex but should not be seen on full duplex interfaces. If collisions are increasing dramatically, this points to a highly utilized link or possibly a duplex

mismatch with the attached device.

- `Late-coll` (late collisions) − The number of times that a collision is detected on a particular interface late in the transmission process. For a 10Mbit/s port, this is later than 512 bit−times into the transmission of a packet. Five hundred and twelve bit−times correspond to 51.2 microseconds on a 10 Mbit/s system. This error can indicate a duplex mismatch among other things. For the duplex mismatch scenario, the late collision is seen on the half duplex side. As the half duplex side is transmitting, the full duplex side does not wait its turn and transmits simultaneously causing a late collision. Late collisions can also indicate an Ethernet cable or segment that is too long. Collisions should not be seen on interfaces configured as full duplex.
- `Excess-coll` (excessive collisions) − A count of frames for which transmission on a particular interface fails due to excessive collisions. An excessive collision happens when a packet has a collision 16 times in a row. The packet is then dropped. Excessive collisions are typically an indication that the load on the segment needs to be split across multiple segments but can also point to a duplex mismatch with the attached device. Collisions should not be seen on interfaces configured as full duplex.
- `Carri-Sen` (carrier sense) − This occurs every time an Ethernet controller wants to send data on a half duplex connection. The controller senses the wire and checks if it is not busy before transmitting. This is normal on an half duplex Ethernet segment.
- `Runts` − The frames received that are smaller than the minimum IEEE 802.3 frame size (64 bytes for Ethernet) and with a bad CRC. This can be caused by a duplex mismatch and physical problems such as a bad cable, port, or NIC on the attached device.
- `Giants` − The frames received that exceed the maximum IEEE 802.3 frame size (1518 bytes for non−jumbo Ethernet) and have a bad FCS. Try to find the offending device and remove it from the network. In many cases it is the result of a bad NIC.
- `IntMacRx-Err` − The IntMacRx−Err counts non−network related errors on the MAC level, meaning the packet might have been fine, but the frame was dropped due to internal problems.
- Issue the **clear counters [fastethernet** <*mod/port*>**]** command to reset these statistics.

15. On a L2 trunk port, check the total number of trunk frames transmitted and received on the interface as well as the number of frames that had a trunk encapsulation error.

```
e-6509-a#show interfaces fastethernet 4/2 counters trunk

Port        TrunkFramesTx  TrunkFramesRx  WrongEncap

Fa4/2               20797          23772           1
```

Issue the **clear counters [fastethernet** <*mod/port*>**]** command to reset these statistics.

16. Check for packets dropped due to the broadcast suppression feature (if enabled).

```
e-6509-a#show interfaces fastethernet 4/1 counters broadcast

Port      BcastSuppDiscards

Fa4/1                     0
```

Issue the **clear counters [fastethernet** <*mod/port*>**]** command to reset these statistics.

17. The output of the **show spanning−tree interface FastEthernet** <*mod/port*> or **show spanning−tree vlan** <*vlan#*> commands can be used to verify that whether a particular port is forwarding or blocking with respect to spanning−tree protocol. Blocking ports will not forward traffic.

```
e-6509-a#show spanning-tree vlan 2

 VLAN2 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, address 0008.20f2.a002
  Configured hello time 2, max age 20, forward delay 15
```

```
 Current root has priority 8192, address 00d0.0145.b801
 Root port is 193 (FastEthernet4/1), cost of root path is 19
 Topology change flag not set, detected flag not set
 Number of topology changes 6 last change occurred 04:17:58 ago
 Times:  hold 1, topology change 35, notification 2
         hello 2, max age 20, forward delay 15
 Timers: hello 0, topology change 0, notification 0, aging 300

Port 193 (FastEthernet4/1) of VLAN2 is forwarding
  Port path cost 19, Port priority 128, Port Identifier 128.193.
  Designated root has priority 8192, address 00d0.0145.b801
  Designated bridge has priority 8192, address 00d0.0145.b801
  Designated port id is 129.1, designated path cost 0
  Timers: message age 2, forward delay 0, hold 0
  Number of transitions to forwarding state: 15695
  BPDU: sent 115, received 7974
  The port is in the portfast mode

Port 194 (FastEthernet4/2) of VLAN2 is blocking
  Port path cost 19, Port priority 128, Port Identifier 128.194.
  Designated root has priority 8192, address 00d0.0145.b801
  Designated bridge has priority 8192, address 00d0.0145.b801
  Designated port id is 129.2, designated path cost 0
  Timers: message age 1, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  BPDU: sent 230, received 7736
```

18. The **show diagnostic module** <*module#*> command can be used to check the results of the online diagnostic test performed at switch boot time or when a module is reset. The results of these tests can be used to determine if a hardware component failure has been detected on the module. It is important to set the diagnostic mode to complete, otherwise all or some of the diagnostic tests will be skipped. If a hardware component failure has occurred between now and the last switch or module reset, the diagnostics must be run again through a switch or module reset in order to detect the failure.

    In order to run the diagnostic tests for a module follow these three steps.

    a. Set the diagnostic mode to complete.

```
e-6509-a#config t
Enter configuration commands, one per line.  End with CNTL/Z.
e-6509-a(config)#diagnostic level complete
e-6509-a(config)#^Z
e-6509-a#show diagnostic level
Current Online Diagnostic Level = Complete
```

    b. Reset the module.

```
e-6509-a#hw-module module 4 reset
Proceed with reload of module? [confirm]
% reset issued for module 4
```

    c. View the diagnostic test result for the interfaces on the module for any indication of a failure. Also, look for failures in groups of 12 interfaces which would suggest a Coil ASIC failure or Pinnacle interface failure.

```
e-6509-a#show diagnostic module 4
Current Online Diagnostic Level = Complete

Online Diagnostic Result for Module 4 : PASS
Online Diagnostic Level when Line Card came up = Complete

Test Results: (. = Pass, F = Fail, U = Unknown)

1 . TestLoopback :
    Port  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23
   ----------------------------------------------------------------------------
```

```
      . . . . . . . . . . . . . . . . . . . . . . . . .

   Port 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47
   ------------------------------------------------------------------------
      . . . . . . . . . . . . . . . . . . . . . . . . .

2 . TestNetflowInlineRewrite :

   Port  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23
   ------------------------------------------------------------------------
      . . . . . . . . . . . . . . . . . . . . . . . . .

   Port 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47
   ------------------------------------------------------------------------
      . . . . . . . . . . . . . . . . . . . . . . . . .

e-6509-a#
```

Command Outputs to Collect Before Contacting TAC

The following is a list of commands that was used in the above troubleshooting the WS−X6348 module connectivity issues in this document. Please log the troubleshooting output collected using these commands before opening up a TAC case to provide to the TAC engineer for analysis.

- **show version**
- **show module** <*mod#*>
- **show running−config**
- **show log**
- **show interfaces fastethernet** <*mod/port*> **status**
- **show interfaces fastethernet** <*mod/port*> **trunk**
- **show interfaces fastethernet** <*mod/port*> **switchport**
- **show mac−address−table dynamic interfaces fastethernet** <*mod/port*>
- **show spanning−tree interfaces fastethernet** <*mod#/port*>
- **show ip route**
- **show ip arp**
- **show ip [eigrp/ospf] neighbors**
- **show cdp neighbors fastethernet** <*mod/port*> **detail**

Repeat the following five commands three times to monitor counter increments (Steps 12−16 only):

- **show interfaces fastethernet** <*mod/port*>
- **show interfaces fastethernet** <*mod/port*> **counters**
- **show interfaces fastethernet** <*mod/port*> **counters errors**
- **show interfaces fastethernet** <*mod/port*> **counters trunk**
- **show interfaces fastethernet** <*mod/port*> **counters broadcast**

- **diagnostic level complete** (global configuration command)

  hw−module module <*module#*> **reset**

  show diagnostic module <*mod#*>

Below is list of additional commands which can be collected before opening up a TAC case for further troubleshooting by the TAC engineers or development engineers. These commands are hidden commands and should be used exactly as shown for troubleshooting the WS−X6348 module issues by the TAC engineers. You can alternatively provide these commands at the request of the TAC engineer handling the case.

- **remote command switch show asicreg pinnacle slot** <*slot#*> **port** <*port#*>
- **remote command switch show asicreg coil slot** <*slot#*> **port** <*port#*>
- **show table ltl module** <*module#*> **start** <*LTL index*> **end** <*LTL index*>
- **remote command switch show table cbl slot** <*slot#*> **vlan** <*vlan#*>

Related Information

- **Troubleshooting Hardware and Common Issues on Catalyst 6500/6000 Series Switches Running Cisco IOS System Software**
- **Troubleshooting Hardware and Related Issues on the MSFC, MSFC2, and MSFC2a**
- **Troubleshooting Catalyst 6500/6000 Series Switches Running CatOS on the Supervisor Engine and Cisco IOS on the MSFC**
- **LAN Product Support**
- **LAN Switching Technology Support**
- **Technical Support & Documentation − Cisco Systems**

Updated: Sep 01, 2005 Document ID: 29423
