Troubleshoot Interface CRC Errors on IOS XR Routers

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

- How CRC Works

Problem

- Identifying Interface CRC Errors
- Common Causes of Interface CRC Errors

Procedure to Resolve Interface CRC Errors onCisco IOSXR Routers

Introduction

This document describes how to troubleshoot Cyclic Redundancy Check (CRC) errors on interfaces within Cisco IOS® XR routers.

Prerequisites

Requirements

Cisco recommends that you have knowledge of the Cisco IOS XR Platform.

Note: Cisco recommends that you must have Cisco IOS XR and admin CLI access.

Components Used

The information in this document is based on Cisco IOS XR platforms, including but not limited to:

- Cisco ASR 9000 Series Routers (for example, ASR 9006 and ASR 9010)
- Cisco NCS 540 Series Routers
- Cisco NCS 560 Series Routers
- Cisco NCS 5500 Series Routers
- Cisco NCS 5700 Series Routers

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, ensure that you understand the potential impact of any command.

Background Information

A CRC is a fundamental error-detecting code used in digital networks and storage devices in order to detect accidental changes to raw data during transmission. It ensures the integrity of data by identifying corruption that can occur due to noise or interference on the communication channel.

How CRC Works

CRC operates by treating a block of data as a binary polynomial. At the end of sender, a mathematical algorithm divides this data polynomial by a predefined fixed divisor polynomial, known as the generator polynomial. The remainder of this polynomial division is a short, fixed-length binary sequence called the CRC checksum (or check value). This checksum is then appended to the original data and transmitted along with it.

Upon receiving the data, the receiver performs the same CRC calculation on the received data (including the appended checksum). If the data was transmitted without error, the remainder of this division must be zero. If the remainder is non-zero, it indicates that errors were detected during transmission, and the data is considered corrupted. CRCs are particularly effective at detecting common errors, such as burst errors (multiple consecutive corrupted bits), which are prevalent in many communication channels.

Problem

Cisco IOS XR platforms leverage CRC checks on physical interfaces (for example, Ethernet, optical, and so on) in order to maintain link reliability. They provide interface statistics that include CRC error counters. High CRC error counts typically indicate physical layer issues such as faulty cables, connectors, or transceivers. Cisco IOS XR diagnostic commands allow engineers to monitor CRC errors in real-time and correlate them with other interface errors for comprehensive troubleshooting. CRC error data is integrated into Cisco IOS XR telemetry and logging systems, enabling proactive network health monitoring.

On platforms like the NCS 5500/5700 Series and ASR 9000 Series, CRC error trends can trigger alarms or automated workflows in order to minimize downtime.

Identifying Interface CRC Errors

The first step in troubleshooting is to confirm that CRC errors are indeed occurring and incrementing on a specific interface.

Step 1. Login to router in Cisco IOS XR CLI and run this command in order to identify if CRC error count is incrementing for an interface.

Sample Command Output:

<#root>

```
RP/0/RP0/CPU0:N540X-12Z16G-SYS-D#
```

show interfaces Te0/0/0/26

```
Mon Jul 21 19:50:25.842 WIB
TenGigE0/0/0/26 is up, line protocol is up
Interface state transitions: 39
Dampening enabled: penalty 0, not suppressed
half-life: 1 reuse: 750
```

```
suppress: 2000 max-suppress-time: 4
restart-penalty: 0
Hardware is TenGigE, address is xxx.xxx.xxx (bia xxx.xxx.xxx)
Description: 10G:
Internet address is Unknown
MTU 9212 bytes, BW 10000000 Kbit (Max: 10000000 Kbit)
reliability 255/255, txload 0/255, rxload 6/255
Encapsulation ARPA,
Full-duplex, 10000Mb/s, 10GBASE-LR, link type is force-up
output flow control is off, input flow control is off
Carrier delay (up) is 2000 msec, Carrier delay (down) is 100 msec
loopback not set,
Last link flapped 1w4d
Last input 00:00:00, output 00:00:00
Last clearing of "show interface" counters 01:35:40
30 second input rate 249013000 bits/sec, 27739 packets/sec
30 second output rate 34886000 bits/sec, 11563 packets/sec
152403495 packets input, 172646518724 bytes, 0 total input drops
0 drops for unrecognized upper-level protocol
Received 0 broadcast packets, 84723 multicast packets
13 runts, 0 giants, 0 throttles, 0 parity
3731 input errors,
```

3718 CRC

```
, 0 frame, 0 overrun, 0 ignored, 0 abort
66477366 packets output, 24050248792 bytes, 0 total output drops
Output 0 broadcast packets, 77461 multicast packets
0 output errors, 0 underruns, 0 applique, 0 resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
```

Look for the **CRC** counter under **input errors**. If this value is incrementing, it confirms the presence of CRC errors.

Step 2. Login to router in Cisco IOS XR CLI and run this command in order to verify and confirm if CRC error count is incrementing for an interface and provides more detailed statistics.

Sample Command Output:

<#root>

```
RP/0/RP0/CPU0:N540X-12Z16G-SYS-D#
```

show controllers Te0/0/0/26 stats

```
Mon Jul 21 19:50:56.139 WIB
Statistics for interface TenGigE0/0/0/26 (cached values):

Ingress:
Input total bytes = 173638989945
Input good bytes = 173638989945

Input total packets = 153271045
Input 802.1Q frames = 0
Input pause frames = 0
Input pkts 64 bytes = 1332238
Input pkts 65-127 bytes = 14101870
Input pkts 128-255 bytes = 9711091
```

```
Input pkts 256-511 bytes = 4850242
Input pkts 512-1023 bytes = 4395212
Input pkts 1024-1518 bytes = 117306517
Input pkts 1519-Max bytes = 1577617
Input good pkts = 153271045
Input unicast pkts = 153185898
Input multicast pkts = 85158
Input broadcast pkts = 0
Input drop overrun = 0
Input drop abort = 0
Input drop invalid VLAN = 0
Input drop invalid DMAC = 0
Input drop invalid encap = 0
Input drop other = 0

Input error giant = 0
Input error runt = 13
Input error jabbers = 0
Input error fragments = 9
```

Input error CRC = 3729

```
Input error collisions = 0
Input error symbol = 370
Input error other = 0

Input MIB giant = 0
Input MIB jabber = 0
```

Input MIB CRC = 3729

```
Egress:
Output total bytes = 24170362757
Output good bytes = 24170362757

Output total packets = 66833308
Output 802.1Q frames = 0
Output pause frames = 0
Output pkts 64 bytes = 10113
Output pkts 65-127 bytes = 35246624
Output pkts 128-255 bytes = 14254990
Output pkts 256-511 bytes = 2888642
Output pkts 512-1023 bytes = 3779102
Output pkts 1024-1518 bytes = 10642390
Output pkts 1519-Max bytes = 11455

Output good pkts = 66833308
Output unicast pkts = 66755447
Output multicast pkts = 77865
Output broadcast pkts = 0

Output drop underrun = 0
Output drop abort = 0
Output drop other = 0

Output error other = 0
```

The **Input error CRC** and **Input MIB CRC** counters provide a clear indication of CRC errors.

Common Causes of Interface CRC Errors

Common causes of CRC errors on Cisco IOS XR and other network devices typically stem from physical layer issues or misconfigurations. The most frequent root causes include:

- Damaged or malfunctioning physical media: This includes copper or fiber cables or Direct Attach Cables (DACs).
- Failing or damaged transceivers/optics: SFP, SFP+, QSFP, and so on, can degrade or fail.
- Faulty patch panel ports: Connectors on patch panels can become damaged or dirty.
- Defective network device hardware: This can include specific ports on a line card, line card ASICs, Media Access Controls (MACs), or fabric modules.
- Malfunctioning network interface cards (NICs) in connected hosts/devices: The hardware at remote end can be faulty.
- Configuration mismatches: Such as Maximum Transmission Unit (MTU) size mismatches between devices, which can cause large packets to be truncated incorrectly, leading to CRC errors.

Procedure to Resolve Interface CRC Errors on Cisco IOS XR Routers

Once CRC errors are identified, perform these steps in order to systematically troubleshoot and resolve the issue.

Step 1. Clear Interface Counters

Before you proceed with troubleshooting, clear the interface counters to get a fresh baseline and observe if CRC errors continue to increment. Login to router in Cisco IOS XR CLI and run this command in order to clear interface counters.

```
# clear counter interface <interface-id>
```

For example:

```
# clear counter interface Te0/0/0/26
```

After you clear, monitor the interface again using **show interfaces <interface>** and **show controllers <interface> stats** to see if the CRC errors are still incrementing.

Step 2. Check for Configuration Mismatches (MTU)

While less common for CRC errors than physical issues, an MTU mismatch can sometimes lead to frame truncation and subsequent CRC errors.

Verify MTU Settings:

Check the MTU configured on the interface of the local router and the connected peer device.

Look for MTU <value> bytes in the output.

Sample Command Output:

<#root>

```
RP/0/RP0/CPU0:N540X-12Z16G-SYS-D#
```

show interfaces Te0/0/0/26

```
Mon Jul 21 19:50:25.842 WIB
TenGigE0/0/0/26 is up, line protocol is up
Interface state transitions: 39
Dampening enabled: penalty 0, not suppressed
half-life: 1 reuse: 750
suppress: 2000 max-suppress-time: 4
restart-penalty: 0
Hardware is TenGigE, address is xxx.xxx.xxx (bia xxx.xxx.xxx)
Description: 10G:
Internet address is Unknown
```

MTU 9212 bytes

```
, BW 10000000 Kbit (Max: 10000000 Kbit)
reliability 255/255, txload 0/255, rxload 6/255
Encapsulation ARPA,
Full-duplex, 10000Mb/s, 10GBASE-LR, link type is force-up
output flow control is off, input flow control is off
Carrier delay (up) is 2000 msec, Carrier delay (down) is 100 msec
loopback not set,
Last link flapped 1w4d
Last input 00:00:00, output 00:00:00
Last clearing of "show interface" counters 01:35:40
30 second input rate 249013000 bits/sec, 27739 packets/sec
30 second output rate 34886000 bits/sec, 11563 packets/sec
152403495 packets input, 172646518724 bytes, 0 total input drops
0 drops for unrecognized upper-level protocol
Received 0 broadcast packets, 84723 multicast packets
13 runts, 0 giants, 0 throttles, 0 parity
3731 input errors,
```

3718 CRC

```
, 0 frame, 0 overrun, 0 ignored, 0 abort
66477366 packets output, 24050248792 bytes, 0 total output drops
Output 0 broadcast packets, 77461 multicast packets
0 output errors, 0 underruns, 0 applique, 0 resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
```

Action: Ensure the MTU settings are consistent across both ends of the link. Adjust if necessary to match.

Step 3. Troubleshoot Physical Layer Issues (Cabling and Transceivers)

Physical layer problems are the most common cause of CRC errors.

- Inspect and Replace Physical Media:
  - Visually inspect the cable (fiber, copper, DAC) for any damage, kinks, or sharp bends.
  - Ensure the cable is securely seated in both the router interface and the connected device.
  - Action: Replace the cable with a known good one. If the errors stop, the original cable was

faulty.

- Check Optical Power Levels (for fiber interfaces):
  - Low or excessively high optical power can cause signal degradation and CRC errors.
  - Use the **show controllers <interface> all** command to check the optical power values of transceiver (Tx Power and Rx Power).

Sample Command Output:

<#root>

```
RP/0/RP0/CPU0:N540X-12Z16G-SYS-D# show controller Te0/0/0/26 all
Mon Jul 21 19:50:32.643 WIB
Operational data for interface TenGigE0/0/0/26:

State:
Administrative state: enabled
Operational state: Up
LED state: Green On

Phy:
Media type: R fiber over 1310nm optics
Optics:
Vendor: CISCO-ACCELINK
Part number: RTXM228-401-C88
Serial number: ACW26040HE6
Wavelength: 1310 nm
Digital Optical Monitoring:
Transceiver Temp: 39.000 C
Transceiver Voltage: 3.265 V

Alarms key: (H) Alarm high, (h) Warning high
(L) Alarm low, (l) Warning low
Wavelength Tx Power Rx Power Laser Bias
Lane (nm) (dBm) (mW) (dBm) (mW) (mA)
-- ----- ------ ------ ------ ------ ------

0 n/a -2.5 0.5603 -17.2 0.0192l 35.250



DOM alarms:
Receive Power: Warning low

Alarm Alarm Warning Warning Alarm
Thresholds High High Low Low
------- ------- ------- -------
Transceiver Temp (C): 75.000 70.000 0.000 -5.000
Transceiver Voltage (V): 3.630 3.465 3.135 2.970
Laser Bias (mA): 75.000 70.000 18.000 15.000

Transmit Power (mW): 2.239 1.122 0.151 0.060



Transmit Power (dBm): 3.500 0.500 -8.202 -12.204



Receive Power (mW): 2.239 1.122 0.036 0.015



Receive Power (dBm): 3.500 0.500 -14.413 -18.386
```

```
Alarms:
Current:
No alarms
Statistics:
FEC:
Corrected Codeword Count: 0
Uncorrected Codeword Count: 0
```

- Compare the **Tx Power** and **Rx Power** values against the **Warning low/high** and **Alarm low/high** thresholds. If values are outside the normal operating range (as indicated by 'Warning low' or 'Alarm low/high' in the output), address the optical path issue (for example, clean connectors, replace fiber patch cable, check for excessive attenuation).

- Replace Transceiver/Optic:

If optical power levels are acceptable, or if you suspect the transceiver itself is faulty, try replacing the transceiver (SFP, SFP+, QSFP, and so on) with a known good one.

Step 4. Troubleshoot Hardware Issues (Port or Line Card)

If physical media and transceivers are ruled out, the issue must lie with the hardware of router.

- Internal Loopback Test (Soft Loop):

This test checks the internal circuitry of the interface by looping traffic back within the port itself, bypassing the external cable and transceiver.

Step 4.1. Implement internal loopback:

```
# clear counter interface <interface-id>

# conf t
# interface <interface-id>
# loopback internal
# commit
```

Step 4.2. Verify CRC errors:

- Monitor the interface for CRC errors using **show interfaces Te0/0/0/26**.
- If CRC errors stop incrementing, it implies the issue is with the external optics module or the external optical path (for example, fiber, patch panel, remote device). Proceed to Step 4. (External Loopback) or focus on the external network components.
- If CRC errors continue to increment, it strongly suggests an issue with the internal circuit of the router for that port or line card. In this case, you must proceed with replacing the line card or the router itself.

Step 4.3. Remove internal loopback once test is completed

```
# conf t
# interface <interface-id>
# no loopback internal
# commit
```

External Loopback Test (Hard Loop):

This test uses a physical loopback connector to loop the signal back at the physical connector of the port, including the transceiver. This helps isolate whether the issue is with the transceiver or the internal processing of port.

Step 4.4. Use a loopback connector

This helps to physically connect the transmit (Tx) to the receive (Rx) path on the physical port of the interface.

Step 4.5. Use an external loopback toolkit
You can also use this to physically connect the transmit (Tx) and receive (Rx) path on the physical port of the interface and apply external loopback in command line interface:

```
# clear counter interface <interface-id>

# conf t
# interface Te0/0/0/26
# loopback external
# commit
```

Use external loopback sensibly to identify the hardware that is causing CRC. If CRC errors stop, the issue is likely further upstream (for example, remote device, cable). If they continue, the transceiver or the port hardware is suspect.

Step 4.6. Remove external loopback once test is completed

Also remove the loopback connector/toolkit.

```
# conf t
# interface Te0/0/0/26
# no loopback external
# commit
```

- Move Interface to a Different Port/Line Card:
  - If possible, try moving the cable and transceiver to a different port on the same line card. If errors persist, the line card itself can be faulty.
  - If errors stop, the original port was likely defective.
  - If errors persist across multiple ports on the same line card, try moving to a different line card (if available). This helps isolate whether the problem is with a specific port, a line card, or potentially the chassis.

Step 5. Check for known issues and bugs

Before proceeding with hardware replacement, it is advisable to check for any known software or hardware bugs.

1. Cisco Bug Search Tool: Search the Cisco Bug Search Tool (BST) for your platform, interface type,

and software version.
2. Cisco Support Documentation:Review Cisco Field Notices, Release Notes, and known Caveats.

If a matching bug is found, perform the recommended workaround or upgrade path.

Step 6. Hardware Replacement

If all previous troubleshooting steps have been exhausted—including excluding any known software bugs — and the issue still persists, the hardware (optics, transceiver, line card, or chassis) can be faulty.

Raise a case with Cisco Technical Assistance Center (TAC) for Return Merchandise Authorization (RMA) of the optics or line cards, as appropriate.

By systematically performing these troubleshooting steps, you can effectively diagnose and resolve interface CRC errors on Cisco IOS XR platforms.