

Troubleshooting de Errores CRC de Interfaz en Routers IOS XR

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Cómo funciona CRC](#)

[Problema](#)

[Identificación de Errores CRC de Interfaz](#)

[Causas comunes de errores CRC de interfaz](#)

[Procedimiento para resolver errores CRC de interfaz en routers Cisco IOSXR](#)

Introducción

Este documento describe cómo resolver problemas de errores de Verificación por redundancia cíclica (CRC) en interfaces dentro de routers Cisco IOS® XR.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento de la plataforma Cisco IOS XR.



Nota: Cisco recomienda que debe tener acceso CLI de administración y Cisco IOS XR.

Componentes Utilizados

La información de este documento se basa en las plataformas Cisco IOS XR, incluidas, entre otras:

- Routers de la serie ASR 9000 de Cisco (por ejemplo, ASR 9006 y ASR 9010)
- Routers de la serie Cisco NCS 540
- Routers de la serie Cisco NCS 560
- Routers de la serie Cisco NCS 5500
- Routers de la serie Cisco NCS 5700

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Un CRC es un código fundamental de detección de errores utilizado en redes digitales y dispositivos de almacenamiento para detectar cambios accidentales en datos sin procesar durante la transmisión. Garantiza la integridad de los datos mediante la identificación de la corrupción que puede ocurrir debido al ruido o la interferencia en el canal de comunicación.

Cómo funciona CRC

CRC actúa tratando un bloque de datos como un polinomio binario. Al final del remitente, un algoritmo matemático divide este polinomio de datos por un polinomio divisor fijo predefinido, conocido como el polinomio generador. El resto de esta división polinómica es una secuencia binaria corta de longitud fija llamada suma de comprobación CRC (o valor de comprobación). Esta suma de comprobación se añade a los datos originales y se transmite junto con ellos.

Al recibir los datos, el receptor realiza el mismo cálculo CRC en los datos recibidos (incluida la suma de comprobación adjunta). Si los datos se transmitieron sin errores, el resto de esta división debe ser cero. Si el resto es distinto de cero, indica que se detectaron errores durante la transmisión y que los datos se consideran dañados. Los CRC son particularmente efectivos en la detección de errores comunes, como los errores de ráfaga (múltiples bits corruptos consecutivos), que prevalecen en muchos canales de comunicación.

Problema

Las plataformas Cisco IOS XR aprovechan las comprobaciones CRC en las interfaces físicas (por ejemplo, Ethernet, óptica, etc.) para mantener la fiabilidad de los enlaces. Proporcionan estadísticas de interfaz que incluyen contadores de errores CRC. Los recuentos de errores CRC altos normalmente indican problemas de la capa física como cables, conectores o transceptores defectuosos. Los comandos de diagnóstico de Cisco IOS XR permiten a los ingenieros monitorear los errores CRC en tiempo real y correlacionarlos con otros errores de interfaz para una resolución de problemas completa. Los datos de error CRC están integrados en los sistemas de telemetría y registro de Cisco IOS XR, lo que permite una supervisión proactiva del estado de la red.

En plataformas como las series NCS 5500/5700 y ASR 9000, las tendencias de error de CRC pueden activar alarmas o flujos de trabajo automatizados para minimizar el tiempo de inactividad.

Identificación de Errores CRC de Interfaz

El primer paso en la resolución de problemas es confirmar que los errores de CRC realmente están ocurriendo e incrementándose en una interfaz específica.

Paso 1. Inicie sesión en el router en Cisco IOS XR CLI y ejecute este comando para identificar si el conteo de errores CRC está aumentando para una interfaz.

Salida del Comando de Ejemplo:

```
<#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
```

Busque el contador CRC en errores de entrada. Si este valor aumenta, confirma la presencia de errores CRC.

Paso 2. Inicie sesión en el router en Cisco IOS XR CLI y ejecute este comando para verificar y confirmar si el conteo de errores CRC está aumentando para una interfaz y proporciona estadísticas más detalladas.

Salida del Comando de Ejemplo:

<#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
```

Los contadores Input error CRC y Input MIB CRC proporcionan una indicación clara de errores CRC.

Causas comunes de errores CRC de interfaz

Las causas comunes de los errores CRC en Cisco IOS XR y otros dispositivos de red generalmente provienen de problemas de capa física o configuraciones erróneas. Las causas principales más frecuentes son:

- Medios físicos dañados o con funcionamiento incorrecto: Esto incluye cables de cobre o fibra o cables de conexión directa (DAC).
- Transmisores/ópticos defectuosos o dañados: SFP, SFP+, QSFP, etc., pueden degradarse o fallar.
- Puertos de panel de conexión defectuosos: Los conectores de los paneles de conexión pueden dañarse o ensuciarse.
- Hardware de dispositivo de red defectuoso: puede incluir puertos específicos en una tarjeta de línea, ASIC de tarjeta de línea, controles de acceso a medios (MAC) o módulos de fabric.
- Tarjetas de interfaz de red (NIC) con fallos en hosts/dispositivos conectados: el hardware del extremo remoto puede ser defectuoso.
- Discordancias de configuración: como las discordancias de tamaño de la unidad de transmisión máxima (MTU) entre dispositivos, que pueden provocar que los paquetes grandes se trunquen incorrectamente, lo que provoca errores CRC.

Procedimiento para resolver errores CRC de interfaz en routers Cisco IOS XR

Una vez que se identifican los errores CRC, realice estos pasos para resolver el problema de manera sistemática.

Paso 1. Borrar contadores de interfaz

Antes de continuar con la resolución de problemas, borre los contadores de la interfaz para obtener una nueva línea de base y observe si los errores CRC continúan aumentando. Inicie sesión en el router en Cisco IOS XR CLI y ejecute este comando para borrar los contadores de la interfaz.

```
# clear counter interface
```

Por ejemplo:

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

Después de borrar, monitoree la interfaz nuevamente usando `show interfaces <interface>` y `show controllers <interface> stats` para ver si los errores CRC siguen aumentando.

Paso 2. Comprobar las discrepancias de configuración (MTU)

Si bien es menos común para los errores CRC que para los problemas físicos, una discordancia de MTU a veces puede llevar a truncamiento de tramas y subsiguientes errores CRC.

Verificar configuración de MTU:

Verifique la MTU configurada en la interfaz del router local y el dispositivo par conectado.

Busque bytes MTU <value> en la salida.

Salida del Comando de Ejemplo:

```
<#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
```

Acción: asegúrese de que la configuración de MTU sea coherente en ambos extremos del vínculo. Ajústelo si es necesario para que coincida.

Paso 3. Resolución de problemas de capa física (cableado y transceptores)

Los problemas de la capa física son la causa más común de errores CRC.

- Inspección y sustitución de medios físicos:
 - Inspeccione visualmente el cable (fibra, cobre, DAC) para ver si está dañado, aplastado o doblado.
 - Asegúrese de que el cable esté bien colocado tanto en la interfaz del router como en el dispositivo conectado.
 - Acción: Sustituya el cable por otro que se sepa que es correcto. Si se detienen los errores, el cable original era defectuoso.
- Comprobar los niveles de potencia óptica (para interfaces de fibra):
 - Una potencia óptica baja o excesivamente alta puede causar degradación de la señal y errores CRC.
 - Utilice el comando `show controllers <interface> all` para verificar los valores de potencia óptica del transceptor (potencia Tx y potencia Rx).

Salida del Comando de Ejemplo:

<#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: RTX228-401-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 0.01921 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 los valores de Tx Power y Rx Power con los umbrales Warning low/high y Alarm low/high. Si los valores están fuera del rango de funcionamiento normal (como se indica en 'Advertencia baja' o 'Alarma baja/alta' en la salida), resuelva el problema de trayectoria óptica (por ejemplo, limpie los conectores, reemplace el cable de interconexión de fibra, verifique si hay una atenuación excesiva).
- Sustitución del transceptor/óptica:

Si los niveles de potencia óptica son aceptables, o si sospecha que el propio transceptor es defectuoso, intente sustituir el transceptor (SFP, SFP+, QSFP, etc.) por otro que se sepa que es correcto.

Paso 4. Resolución de problemas de hardware (puerto o tarjeta de línea)

Si se descartan los medios físicos y los transceptores, el problema debe estar en el hardware del router.

- Prueba de loopback interno (bucle suave):

Esta prueba verifica la circuitería interna de la interfaz mediante un loop de tráfico dentro del puerto mismo, omitiendo el cable externo y el transceiver.

Paso 4.1. Implementación del loopback interno:

```
# clear counter interface
```

```
# conf t
# interface
```

```
# loopback internal
# commit
```

Paso 4.2. Verifique los errores CRC:

- Monitoree la interfaz para detectar errores de CRC usando show interfaces Te0/0/0/26.
- Si los errores CRC dejan de aumentar, implica que el problema está en el módulo óptico externo o en la trayectoria óptica externa (por ejemplo, fibra, panel de parches, dispositivo remoto). Vaya al paso 4 (Loopback externo) o céntrese en los componentes de red externos.
- Si los errores CRC continúan aumentando, sugiere fuertemente un problema con el circuito interno del router para ese puerto o tarjeta de línea. En este caso, debe continuar con la sustitución de la tarjeta de línea o del router en sí.

Paso 4.3. Eliminar el loopback interno una vez finalizada la prueba

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

Prueba de loopback externo (bucle duro):

Esta prueba utiliza un conector de loopback físico para volver a colocar la señal en el conector físico del puerto, incluido el transceptor. Esto ayuda a aislar si el problema está con el transceiver o el procesamiento interno del puerto.

Paso 4.4. Uso de un conector de loopback

Esto ayuda a conectar físicamente la ruta de transmisión (Tx) a la ruta de recepción (Rx) en el puerto físico de la interfaz.

Paso 4.5. Uso de un kit de herramientas de loopback externo

También puede utilizar esto para conectar físicamente la trayectoria de transmisión (Tx) y recepción (Rx) en el puerto físico de la interfaz y aplicar el loopback externo en la interfaz de línea de comandos:

```
# clear counter interface
```

```
# conf t
```

```
# interface Te0/0/0/26
```

```
# loopback external
```

```
# commit
```

Utilice el loopback externo sensiblemente para identificar el hardware que está causando el CRC. Si se detienen los errores de CRC, es probable que el problema siga en sentido ascendente (por ejemplo, dispositivo remoto o cable). Si continúan, el transceptor o el hardware del puerto son sospechosos.

Paso 4.6. Eliminar el loopback externo una vez finalizada la prueba

Retire también el conector/kit de herramientas de bucle invertido.

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

- Mover interfaz a un puerto/tarjeta de línea diferente:
 - Si es posible, intente mover el cable y el transceptor a un puerto diferente en la misma tarjeta de línea. Si persisten los errores, la tarjeta de línea puede ser defectuosa.
 - Si se detienen los errores, es probable que el puerto original sea defectuoso.
 - Si persisten errores en varios puertos de la misma tarjeta de línea, intente cambiar a una tarjeta de línea diferente (si está disponible). Esto ayuda a aislar si el problema está en un puerto específico, una tarjeta de línea o, potencialmente, en el chasis.

Paso 5. Compruebe si hay problemas y errores conocidos

Antes de proceder con la sustitución del hardware, se recomienda comprobar si hay algún error de software o hardware conocido.

1. Herramienta de búsqueda de errores de Cisco: busque la plataforma, el tipo de interfaz y la versión de software en la herramienta de búsqueda de errores de Cisco (BST).
2. Documentación de soporte de Cisco: revise los avisos de campo, las notas de la versión y las advertencias conocidas de Cisco.

Si se encuentra un error coincidente, realice la solución alternativa o la ruta de actualización recomendadas.

Paso 6. Sustitución de hardware

Si se han agotado todos los pasos previos de resolución de problemas (incluidos los errores de software conocidos) y el problema persiste, el hardware (óptica, transceptor, tarjeta de línea o chasis) puede ser defectuoso.

Plantee un caso ante el centro de asistencia técnica Cisco Technical Assistance Center (TAC) para obtener la autorización de devolución de material (RMA) de la óptica o las tarjetas de línea, según corresponda.

Al realizar sistemáticamente estos pasos de solución de problemas, puede diagnosticar y resolver eficazmente los errores CRC de la interfaz en las plataformas Cisco IOS XR.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).