

Fehlerbehebung bei Schnittstellen-CRC-Fehlern auf IOS XR-Routern

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Funktionsweise von CRC](#)

[Problem](#)

[Identifizieren von Schnittstellen-CRC-Fehlern](#)

[Häufige Ursachen von Schnittstellen-CRC-Fehlern](#)

[Verfahren zur Behebung von Schnittstellen-CRC-Fehlern auf Cisco IOSXR-Routern](#)

Einleitung

In diesem Dokument wird die Fehlerbehebung bei CRC-Fehlern (Cyclic Redundancy Check) an Schnittstellen mit Cisco IOS® XR-Routern beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie mit der Cisco IOS XR-Plattform vertraut sind.



Anmerkung: Cisco empfiehlt, dass Sie über Cisco IOS XR und Zugriff auf die Admin-CLI verfügen müssen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco IOS XR-Plattformen, einschließlich, aber nicht beschränkt auf:

- Cisco Router der Serie ASR 9000 (z. B. ASR 9006 und ASR 9010)
- Cisco NCS Router der Serie 540
- Cisco NCS Router der Serie 560
- Cisco NCS Router der Serie 5500
- Cisco NCS Router der Serie 5700

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Ein CRC ist ein grundlegender Fehlererkennungscode, der in digitalen Netzwerken und Speichergeräten verwendet wird, um versehentliche Änderungen an Rohdaten während der Übertragung zu erkennen. Es stellt die Integrität von Daten sicher, indem es Beschädigungen identifiziert, die durch Rauschen oder Störungen auf dem Kommunikationskanal auftreten können.

Funktionsweise von CRC

CRC behandelt einen Datenblock als binäres Polynom. Am Ende des Senders teilt ein mathematischer Algorithmus dieses Datenpolynom durch ein vordefiniertes festes Divisorpolynom, das als Generatorpolynom bezeichnet wird. Der Rest dieser Polynomteilung ist eine kurze Binärsequenz fester Länge, die als CRC-Prüfsumme (oder Prüfwert) bezeichnet wird. Diese Prüfsumme wird dann an die ursprünglichen Daten angehängt und zusammen mit diesen übertragen.

Beim Empfang der Daten führt der Empfänger die gleiche CRC-Berechnung für die empfangenen Daten (einschließlich der angehängten Prüfsumme) durch. Wenn die Daten fehlerfrei übertragen wurden, muss der Rest dieser Division Null sein. Wenn der Rest ungleich null ist, weist dies darauf hin, dass bei der Übertragung Fehler festgestellt wurden und die Daten als beschädigt gelten. CRCs sind besonders effektiv bei der Erkennung von häufigen Fehlern, wie Burst-Fehlern (mehrere aufeinander folgende korrupte Bits), die in vielen Kommunikationskanälen vorherrschen.

Problem

Cisco IOS XR-Plattformen nutzen CRC-Prüfungen an physischen Schnittstellen (z. B. Ethernet, optische Verbindungen usw.), um die Zuverlässigkeit der Verbindungen aufrechtzuerhalten. Sie bieten Schnittstellenstatistiken mit CRC-Fehlerindikatoren. Hohe CRC-Fehlerzahlen weisen in der Regel auf Probleme auf physischer Ebene hin, z. B. fehlerhafte Kabel, Anschlüsse oder Transceiver. Mit den Cisco IOS XR-Diagnosebefehlen können Techniker CRC-Fehler in Echtzeit überwachen und sie mit anderen Schnittstellenfehlern korrelieren, um eine umfassende Fehlerbehebung zu ermöglichen. CRC-Fehlerdaten sind in Cisco IOS XR-Telemetrie- und Protokollierungssysteme integriert und ermöglichen so eine proaktive Überwachung des Netzwerkzustands.

Auf Plattformen wie der Serie NCS 5500/5700 und der Serie ASR 9000 können CRC-Fehlertrends Alarmer oder automatisierte Workflows auslösen, um Ausfallzeiten zu minimieren.

Identifizieren von Schnittstellen-CRC-Fehlern

Der erste Schritt bei der Fehlerbehebung besteht darin, zu bestätigen, dass CRC-Fehler

tatsächlich auftreten, und diese Fehler auf einer bestimmten Schnittstelle zu inkrementieren.

Schritt 1: Melden Sie sich in der CLI von Cisco IOS XR beim Router an, und führen Sie diesen Befehl aus, um festzustellen, ob die CRC-Fehleranzahl für eine Schnittstelle zunimmt.

Beispielausgabe für Befehle:

```
<#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
```

Suchen Sie nach dem CRC-Zähler unter Eingabefehlern. Wenn dieser Wert inkrementiert wird, wird bestätigt, dass CRC-Fehler vorliegen.

Schritt 2: Melden Sie sich in der CLI von Cisco IOS XR beim Router an, und führen Sie diesen Befehl aus, um zu überprüfen und zu bestätigen, ob die CRC-Fehleranzahl für eine Schnittstelle

zunimmt, und stellen Sie detailliertere Statistiken bereit.

Beispielausgabe für Befehle:

<#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
```

Die CRC-Zähler für Eingabefehler und CRC-Zähler für Eingabe-MIB geben einen klaren Hinweis auf CRC-Fehler.

Häufige Ursachen von Schnittstellen-CRC-Fehlern

Häufige Ursachen für CRC-Fehler in Cisco IOS XR und anderen Netzwerkgeräten sind in der Regel Probleme auf der physischen Ebene oder Fehlkonfigurationen. Die häufigsten Ursachen sind:

- Beschädigte oder defekte physische Medien: Hierzu gehören Kupfer- oder Glasfaserkabel oder Direct Attach Cables (DACs).
- Ausgefallene oder beschädigte Transceiver/optische Verbindungen: SFP, SFP+, QSFP usw. können sich verschlechtern oder ausfallen.
- Fehlerhafte Patchfeldanschlüsse: Anschlüsse an Patchfeldern können beschädigt oder verschmutzt werden.
- Defekte Hardware für Netzwerkgeräte: Hierzu können bestimmte Ports auf einer Linecard, Linecard-ASICs, Media Access Controls (MACs) oder Fabric-Module gehören.
- Fehlerhafte Netzwerkschnittstellenkarten (NICs) in angeschlossenen Hosts/Geräten: Die Hardware am Remote-Ende kann fehlerhaft sein.
- Konfigurationsdiskrepanzen: Hierzu zählen z. B. MTU-Größendiskrepanzen (Maximum Transmission Unit) zwischen Geräten, die dazu führen können, dass große Pakete nicht richtig abgeschnitten werden, was zu CRC-Fehlern führen kann.

Verfahren zur Behebung von Schnittstellen-CRC-Fehlern auf Cisco IOS XR-Routern

Führen Sie nach der Identifizierung von CRC-Fehlern diese Schritte aus, um das Problem

systematisch zu beheben und zu beheben.

Schritt 1: Löschen von Schnittstellenzählern

Bevor Sie mit der Fehlerbehebung fortfahren, löschen Sie die Schnittstellenzähler, um eine neue Baseline zu erhalten, und beobachten Sie, ob sich die CRC-Fehler weiter erhöhen. Melden Sie sich in der Cisco IOS XR CLI beim Router an, und führen Sie diesen Befehl aus, um die Schnittstellenzähler zu löschen.

```
# clear counter interface
```

Beispiele:

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

Überwachen Sie nach dem Löschen die Schnittstelle erneut mit `show interfaces <Schnittstelle>` und `show controllers <Schnittstelle> stats`, um zu sehen, ob die CRC-Fehler noch inkrementiert werden.

Schritt 2: Überprüfen Sie die MTU-Größe (Configuration Mismatch).

CRC-Fehler treten seltener auf als physische Probleme, eine MTU-Fehlanpassung kann jedoch manchmal zu Frame-Kürzungen und anschließenden CRC-Fehlern führen.

Überprüfen Sie die MTU-Einstellungen:

Überprüfen Sie die auf der Schnittstelle des lokalen Routers und des angeschlossenen Peer-Geräts konfigurierte MTU.

Suchen Sie in der Ausgabe nach MTU <Wert> Byte.

Beispielausgabe für Befehle:

```
<#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

Aktion: Stellen Sie sicher, dass die MTU-Einstellungen an beiden Enden der Verbindung konsistent sind. Bei Bedarf anpassen.

Schritt 3: Fehlerbehebung bei Problemen auf physischer Ebene (Verkabelung und Transceiver)

Probleme auf der physischen Schicht sind die häufigste Ursache für CRC-Fehler.

- Überprüfen und Ersetzen physischer Medien:
 - Untersuchen Sie das Kabel (Glasfaser, Kupfer, DAC) auf Beschädigungen, Knicke oder spitze Biegungen.
 - Stellen Sie sicher, dass das Kabel sicher in der Router-Schnittstelle und im angeschlossenen Gerät sitzt.
 - Aktion: Ersetzen Sie das Kabel durch ein zweifelsfrei funktionierendes Kabel. Wenn die Fehler nicht mehr auftreten, ist das ursprüngliche Kabel fehlerhaft.
- Prüfung der optischen Leistungspegel (für Glasfaserschnittstellen):
 - Eine niedrige oder zu hohe optische Leistung kann zu Signalverschlechterung und CRC-Fehlern führen.
 - Verwenden Sie den Befehl `show controllers <interface> all`, um die optischen Leistungswerte des Transceivers (Tx Power und Rx Power) zu überprüfen.

Beispielausgabe für Befehle:

<#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

- Vergleichen Sie die Werte für Tx Power und Rx Power mit den Grenzwerten für Warning low/high und Alarm low/high. Wenn Werte außerhalb des normalen Betriebsbereichs liegen (wie durch 'Warnung niedrig' oder 'Alarm niedrig/hoch' im Ausgang angezeigt), beheben Sie das Problem mit dem optischen Pfad (z. B. Stecker reinigen, Glasfaser-Patchkabel austauschen, auf übermäßige Dämpfung prüfen).
- Transceiver/Optik ersetzen:

Wenn die optischen Leistungspegel akzeptabel sind oder Sie vermuten, dass der Transceiver selbst fehlerhaft ist, versuchen Sie, den Transceiver (SFP, SFP+, QSFP usw.) durch einen zweifelsfrei funktionierenden zu ersetzen.

Schritt 4: Beheben von Hardwareproblemen (Port oder Line Card)

Wenn physische Medien und Transceiver ausgeschlossen werden, muss das Problem bei der Hardware des Routers liegen.

- Interner Loopback-Test (Soft Loop):

Bei diesem Test wird der interne Schaltkreis der Schnittstelle überprüft, indem der Datenverkehr innerhalb des Ports unter Umgehung des externen Kabels und des Transceivers zurückgeleitet wird.

Schritt 4.1. Internes Loopback implementieren:

```
# clear counter interface
```

```
# conf t  
# interface
```

```
# loopback internal  
# commit
```

Schritt 4.2. Überprüfen Sie die CRC-Fehler:

- Überwachen Sie die Schnittstelle mithilfe von `show interfaces Te0/0/0/26` auf CRC-Fehler.
- Wenn CRC-Fehler aufhören zu inkrementieren, impliziert dies, dass das Problem beim externen optischen Modul oder beim externen optischen Pfad (z. B. Glasfaser, Patchpanel, Remote-Gerät) liegt. Fahren Sie mit Schritt 4 fort (Externes Loopback), oder konzentrieren Sie sich auf die externen Netzwerkkomponenten.
- Wenn CRC-Fehler weiter zunehmen, wird ein Problem mit dem internen Schaltkreis des

Routers für diesen Port oder diese Linecard dringend empfohlen. In diesem Fall müssen Sie die Linecard oder den Router selbst austauschen.

Schritt 4.3: Entfernen des internen Loopbacks nach Abschluss des Tests

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

Externer Loopback-Test (Hard Loop):

Bei diesem Test wird ein physischer Loopback-Anschluss verwendet, um das Signal am physischen Anschluss des Ports einschließlich des Transceivers zurückzuleiten. Dadurch kann festgestellt werden, ob ein Problem mit dem Transceiver oder der internen Verarbeitung des Ports vorliegt.

Schritt 4.4: Verwenden eines Loopback-Steckverbinders

Dies hilft, den Übertragungspfad (Tx) physisch mit dem Empfangspfad (Rx) am physischen Port der Schnittstelle zu verbinden.

Schritt 4.5: Verwenden Sie ein externes Loopback-Toolkit

Sie können dies auch verwenden, um den Übertragungs- (Tx) und Empfangspfad (Rx) am physischen Port der Schnittstelle zu verbinden und eine externe Schleife in der Befehlszeilenschnittstelle zu verwenden:

```
# clear counter interface
```

```
# conf t
```

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

```
# loopback external
```

```
# commit
```

Verwenden Sie einen externen Loopback, um die Hardware zu identifizieren, die CRC verursacht. Wenn CRC-Fehler aufhören, liegt das Problem wahrscheinlich weiter vorgelagert (z. B. Remote-Gerät, Kabel). Wenn sie fortgesetzt werden, ist der Transceiver oder die Port-Hardware fehlerhaft.

Schritt 4.6: Entfernen des externen Loopbacks nach Abschluss des Tests

Entfernen Sie auch den Loopback-Steckverbinder/das Toolkit.

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

- Schnittstelle an einen anderen Port/eine andere Linecard verschieben:
 - Versuchen Sie, wenn möglich, das Kabel und den Transceiver an einen anderen Port derselben Linecard anzuschließen. Bleiben Fehler bestehen, kann die Linecard selbst fehlerhaft sein.
 - Wenn keine Fehler mehr auftreten, war der ursprüngliche Port wahrscheinlich defekt.
 - Wenn über mehrere Ports auf derselben Linecard weiterhin Fehler auftreten, versuchen Sie, zu einer anderen Linecard zu wechseln (falls verfügbar). So kann ermittelt werden, ob ein Problem bei einem bestimmten Port, einer Linecard oder möglicherweise beim Chassis vorliegt.

Schritt 5: Überprüfen auf bekannte Probleme und Fehler

Bevor Sie mit dem Hardware-Ersatz fortfahren, ist es ratsam, nach allen bekannten Software- oder Hardware-Fehlern zu suchen.

1. Cisco Bug Search Tool: Suchen Sie im Cisco Bug Search Tool (BST) nach Ihrer Plattform, Schnittstellentyp und Softwareversion.
2. Cisco Support-Dokumentation: Überprüfen Sie die Problemhinweise, Versionshinweise und bekannten Hinweise von Cisco.

Wenn ein passender Fehler gefunden wird, führen Sie die empfohlene Problemumgehung oder den empfohlenen Upgrade-Pfad durch.

Schritt 6: Hardware-Ersatz

Wenn alle vorherigen Schritte zur Fehlerbehebung - einschließlich des Ausschlusses bekannter Softwarefehler - abgeschlossen sind und das Problem weiterhin besteht, kann die Hardware (optische Verbindungen, Transceiver, Linecard oder Gehäuse) fehlerhaft sein.

Erstellen Sie je nach Bedarf ein Ticket beim Cisco Technical Assistance Center (TAC) für die Retouren genehmigung (Return Merchandise Authorization, RMA) für die optischen Verbindungen oder Linecards.

Durch die systematische Durchführung dieser Schritte zur Fehlerbehebung können Sie CRC-

Schnittstellenfehler auf Cisco IOS XR-Plattformen effektiv diagnostizieren und beheben.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.