

Problemen oplossen Interface CRC-fouten op IOS XR Routers

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Hoe CRC werkt](#)

[Probleem](#)

[CRC-fouten in de interface identificeren](#)

[Oorzaken van CRC-fouten in de interface](#)

[Procedure voor het oplossen van CRC-fouten op Cisco IOSXR-routers](#)

Inleiding

In dit document wordt beschreven hoe u Cyclic Redundancy Check (CRC)-fouten kunt oplossen op interfaces binnen Cisco IOS® XR-routers.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van het Cisco IOS XR Platform.



Opmerking: Cisco raadt u aan Cisco IOS XR en CLI-toegang voor beheerders te hebben.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco IOS XR-platforms, waaronder, maar niet beperkt tot:

- Cisco ASR 9000 Series-routers (bijvoorbeeld ASR 9006 en ASR 9010)
- Cisco NCS 540-reeks routers
- Cisco NCS 560-reeks routers
- Cisco NCS 5500-reeks routers
- Cisco NCS 5700-reeks routers

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Een CRC is een fundamentele foutdetectiecode die wordt gebruikt in digitale netwerken en opslagapparaten om toevallige veranderingen in ruwe gegevens tijdens de overdracht te detecteren. Het zorgt voor de integriteit van gegevens door corruptie te identificeren die kan optreden als gevolg van ruis of interferentie op het communicatiekanaal.

Hoe CRC werkt

CRC werkt door een blok gegevens te behandelen als een binaire polynoom. Aan het einde van de afzender deelt een wiskundig algoritme deze gegevenspolynomiaal door een vooraf gedefinieerde vaste delerpolynomiaal, bekend als de generatorpolynomiaal. De rest van deze polynoom-deling is een korte binaire sequentie met een vaste lengte die de CRC-checksum (of controlewaarde) wordt genoemd. Deze checksum wordt vervolgens toegevoegd aan de oorspronkelijke gegevens en samen met deze verzonden.

Na ontvangst van de gegevens voert de ontvanger dezelfde CRC-berekening uit op de ontvangen gegevens (inclusief de bijgevoegde controlesom). Als de gegevens foutloos zijn verzonden, moet de rest van deze verdeling nul zijn. Als de rest niet-nul is, geeft dit aan dat er fouten zijn gedetecteerd tijdens de verzending en dat de gegevens als beschadigd worden beschouwd. CRC's zijn bijzonder effectief in het detecteren van veelvoorkomende fouten, zoals burst-fouten (meerdere opeenvolgende beschadigde bits), die in veel communicatiekanalen voorkomen.

Probleem

Cisco IOS XR-platforms maken gebruik van CRC-controles op fysieke interfaces (bijvoorbeeld Ethernet, optisch, enzovoort) om de betrouwbaarheid van koppelingen te behouden. Ze bieden interfacestatistieken die CRC-fouttellers bevatten. Hoge CRC-fouttellingen wijzen meestal op problemen met fysieke lagen, zoals defecte kabels, connectoren of transceivers. Cisco IOS XR diagnostische opdrachten kunnen ingenieurs CRC fouten in real-time te controleren en correleren met andere interface fouten voor uitgebreide probleemoplossing. CRC-foutgegevens zijn geïntegreerd in Cisco IOS XR-telemetrie- en registratiesystemen, waardoor proactieve bewaking van de netwerkstatus mogelijk is.

Op platforms zoals de NCS 5500/5700-serie en ASR 9000-serie kunnen trends in CRC-fouten leiden tot alarmen of geautomatiseerde workflows om downtime te minimaliseren.

CRC-fouten in de interface identificeren

De eerste stap bij het oplossen van problemen is om te bevestigen dat CRC-fouten inderdaad voorkomen en toenemen op een specifieke interface.

Stap 1. Meld u aan bij de router in Cisco IOS XR CLI en voer deze opdracht uit om te bepalen of het aantal CRC-fouten voor een interface toeneemt.

Voorbeeld opdrachtuitvoer:

```
<#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
```

Zoek naar de CRC-teller onder invoerfouten. Als deze waarde toeneemt, bevestigt dit de aanwezigheid van CRC-fouten.

Stap 2. Meld u aan bij de router in Cisco IOS XR CLI en voer deze opdracht uit om te controleren en te bevestigen of het aantal CRC-fouten toeneemt voor een interface en meer gedetailleerde statistieken biedt.

Voorbeeld opdrachtuitvoer:

<#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
```

De ingangsfout CRC- en ingangsmib CRC-tellers geven een duidelijke indicatie van CRC-fouten.

Oorzaken van CRC-fouten in de interface

Veelvoorkomende oorzaken van CRC-fouten op Cisco IOS XR en andere netwerkapparaten komen meestal voort uit fysieke laagproblemen of verkeerde configuraties. De meest voorkomende oorzaken zijn:

- Beschadigde of slecht werkende fysieke media: dit omvat koperen of glasvezelkabels of Direct Attach-kabels (DAC's).
- Falen of beschadigde transceivers/optica: SFP, SFP+, QSFP, enzovoort, kunnen degraderen of falen.
- Defecte patchpaneelpoorten: connectors op patchpanelen kunnen beschadigd of vies worden.
- Defecte netwerkapparaathardware: dit kan specifieke poorten op een lijnkaart, lijnkaart-ASIC's, Media Access Controls (MAC's) of fabric-modules omvatten.
- Slecht werkende netwerkinterfacekaarten (NIC's) in aangesloten hosts/apparaten: de hardware aan het externe uiteinde kan defect zijn.
- Mismatches in de configuratie: zoals mismatches in de grootte van de Maximum Transmission Unit (MTU) tussen apparaten, waardoor grote pakketten onjuist kunnen worden afgekapt, wat leidt tot CRC-fouten.

Procedure voor het oplossen van CRC-fouten in de interface op Cisco IOS XR-routers

Zodra CRC-fouten zijn geïdentificeerd, voert u deze stappen uit om het probleem systematisch op te lossen en op te lossen.

Stap 1. Interfacetellers wissen

Voordat u doorgaat met het oplossen van problemen, moet u de interfacetellers wissen om een nieuwe basislijn te krijgen en te observeren of CRC-fouten blijven toenemen. Meld u aan bij de router in Cisco IOS XR CLI en voer deze opdracht uit om de interfacetellers te wissen.

```
# clear counter interface
```

Voorbeeld:

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

Nadat u de interface hebt gewist, controleert u de interface opnieuw met behulp van `show interfaces <interface>` en toont u `controllers <interface> stats` om te zien of de CRC-fouten nog steeds toenemen.

Stap 2. Controleren op mismatches in de configuratie (MTU)

Hoewel minder vaak voor CRC-fouten dan fysieke problemen, kan een MTU mismatch soms leiden tot frame truncation en daaropvolgende CRC fouten.

MTU-instellingen controleren:

Controleer de MTU die is geconfigureerd op de interface van de lokale router en het aangesloten peer-apparaat.

Zoek naar MTU <value> bytes in de uitvoer.

Voorbeeld opdrachtuitvoer:

```
<#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
```

Actie: Zorg ervoor dat de MTU-instellingen aan beide uiteinden van de koppeling consistent zijn. Indien nodig aanpassen om overeen te komen.

Stap 3. Problemen met fysieke lagen oplossen (bekabeling en transceivers)

Fysieke laagproblemen zijn de meest voorkomende oorzaak van CRC-fouten.

- Fysieke media controleren en vervangen:
 - Controleer de kabel (glasvezel, koper, DAC) visueel op beschadigingen, knikken of scherpe bochten.
 - Zorg ervoor dat de kabel stevig in zowel de router-interface als het aangesloten apparaat zit.
 - Actie: Vervang de kabel door een bekende goede kabel. Als de fouten stoppen, is de oorspronkelijke kabel defect.
- Controleer de optische vermogensniveaus (voor glasvezelinterfaces):
 - Laag of te hoog optisch vermogen kan leiden tot signaaldegradatie en CRC-fouten.
 - Gebruik de opdracht `show controllers <interface> all` om de optische vermogenswaarden van de transceiver (Tx Power en Rx Power) te controleren.

Voorbeeld opdrachtuitvoer:

<#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

- Vergelijk de waarden van Tx Power en Rx Power met de drempelwaarden Waarschuwing

laag/hoog en Alarm laag/hoog. Als de waarden buiten het normale werkingsbereik vallen (zoals aangegeven door 'Waarschuwing laag' of 'Alarm laag/hoog' in de uitvoer), moet u het probleem met het optische pad aanpakken (bijvoorbeeld connectoren schoonmaken, glasvezelpatchkabel vervangen, controleren op overmatige demping).

- Transceiver/optisch vervangen:

Als de optische vermogensniveaus aanvaardbaar zijn, of als u vermoedt dat de transceiver zelf defect is, probeer dan de transceiver (SFP, SFP+, QSFP, enzovoort) te vervangen door een bekende goede.

Stap 4. Problemen met hardware oplossen (poort- of lijnkaart)

Als fysieke media en transceivers worden uitgesloten, moet het probleem liggen bij de hardware van de router.

- Interne loopback-test (zachte lus):

Deze test controleert de interne circuits van de interface door het verkeer terug te leiden in de poort zelf, waarbij de externe kabel en transceiver worden omzeild.

Stap 4.1. Interne loopback implementeren:

```
# clear counter interface
```

```
# conf t  
# interface
```

```
# loopback internal  
# commit
```

Stap 4.2. CRC-fouten controleren:

- Monitor de interface voor CRC-fouten met behulp van `show interfaces Te0/0/0/26`.
- Als CRC-fouten stoppen met verhogen, betekent dit dat het probleem zich voordoet bij de externe optische module of het externe optische pad (bijvoorbeeld glasvezel, patchpaneel, extern apparaat). Ga verder met stap 4. (Externe loopback) of focus op de externe netwerkcomponenten.
- Als CRC-fouten blijven toenemen, duidt dit sterk op een probleem met het interne circuit van de router voor die poort of lijnkaart. In dit geval moet u doorgaan met het vervangen van de lijnkaart of de router zelf.

Stap 4.3. Verwijder de interne loopback zodra de test is voltooid

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

Externe loopback-test (harde lus):

Deze test maakt gebruik van een fysieke loopback-connector om het signaal terug te leiden naar de fysieke connector van de poort, inclusief de transceiver. Dit helpt bij het isoleren of het probleem zich voordoet bij de transceiver of de interne verwerking van de poort.

Stap 4.4. Gebruik een loopback-connector

Dit helpt bij het fysiek aansluiten van de transmissie (Tx) op het ontvangst (Rx) pad op de fysieke poort van de interface.

Stap 4.5. Een externe loopback-toolkit gebruiken

U kunt dit ook gebruiken om het transmissie- (Tx) en ontvangstpad (Rx) fysiek aan te sluiten op de fysieke poort van de interface en externe loopback toe te passen in de opdrachtregelinterface:

```
# clear counter interface
```

```
# conf t
```

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

```
# loopback external
```

```
# commit
```

Gebruik externe loopback verstandig om de hardware te identificeren die CRC veroorzaakt. Als CRC-fouten stoppen, is het probleem waarschijnlijk verder stroomopwaarts (bijvoorbeeld extern apparaat, kabel). Als ze doorgaan, is de transceiver of de poorthardware verdacht.

Stap 4.6. Verwijder externe loopback zodra de test is voltooid

Verwijder ook de loopback-connector/toolkit.

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

- Interface verplaatsen naar een andere poort/lijnkaart:
 - Probeer indien mogelijk de kabel en de transceiver naar een andere poort op dezelfde lijnkaart te verplaatsen. Als er fouten blijven bestaan, kan de lijnkaart zelf defect zijn.
 - Als fouten stoppen, is de oorspronkelijke poort waarschijnlijk defect.
 - Als er fouten blijven bestaan tussen meerdere poorten op dezelfde lijnkaart, probeer dan naar een andere lijnkaart te gaan (indien beschikbaar). Dit helpt te isoleren of het probleem zich voordoet bij een specifieke poort, een lijnkaart of mogelijk het chassis.

Stap 5. Controleer op bekende problemen en bugs

Voordat u doorgaat met het vervangen van hardware, is het raadzaam om te controleren op bekende software- of hardwarefouten.

1. Cisco Bug Search Tool: Zoek de Cisco Bug Search Tool (BST) voor uw platform, interfacetype en softwareversie.
2. Cisco-ondersteuningsdocumentatie: controleer Cisco-veldmeldingen, releasenotities en bekende waarschuwingen.

Als een overeenkomende bug wordt gevonden, voert u de aanbevolen oplossing of upgradepad uit.

Stap 6. Hardwarevervanging

Als alle voorgaande stappen voor probleemoplossing zijn doorlopen (inclusief het uitsluiten van bekende softwarebugs) en het probleem zich blijft voordoen, kan de hardware (optica, transceiver, lijnkaart of chassis) defect zijn.

Een zaak aanhangig maken bij het Cisco Technical Assistance Center (TAC) voor Return Merchandise Authorization (RMA) van de optica of lijnkaarten, indien van toepassing.

Door deze stappen voor probleemoplossing systematisch uit te voeren, kunt u CRC-fouten in de interface op Cisco IOS XR-platforms effectief diagnosticeren en oplossen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.