Controleer cyclische redundantie op Nexus-Switches

Inhoud

Inleiding

Dit document beschrijft details rond cyclische redundantie (CRC) fouten die zijn waargenomen op interfacetellers en statistieken van Cisco Nexus-switches.

Voorwaarden

Vereisten

Cisco raadt u aan de basis van Ethernet-switching en de Cisco NX-OS opdrachtregel interface (CLI) te begrijpen. Raadpleeg voor meer informatie een van deze toepasselijke documenten:

- Cisco Nexus 9000 NX-OS fundamentals Configuration Guide, release 10.2(x)
- Cisco Nexus 9000 Series configuratie Guide uit het NX-OS systeem, release 9.3(x)
- Cisco Nexus 9000 Series NX-OS fundamentals Configuration Guide, release 9.2(x)
- Cisco Nexus 9000 Series configuratie Guide uit het NX-OS systeem, release 7.x

- Ethernet-probleemoplossing

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Nexus 9000 Series switches vanaf NX-OS softwarerelease 9.3(8)
- Nexus 3000 Series switches vanaf NX-OS softwarerelease 9.3(8)

De informatie in dit document is gemaakt van apparatuur in een specifieke labomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Dit document beschrijft details rond CRC-fouten (Cyclic Redundancy Control) die zijn waargenomen op interfacetellers op Cisco Nexus Series switches. Dit document beschrijft wat een CRC is, hoe het wordt gebruikt in het veld Frame Control Sequence (FCS) van Ethernet-frames, hoe CRC-fouten zich manifesteren op Nexus-switches, hoe CRC-fouten interacteren in Store-and-Forward-switching-scenario's, de meest waarschijnlijke oorzaken van CRC-fouten en hoe u CRC-fouten moet oplossen en oplossen.

Toepasselijke hardware

De informatie in dit document is van toepassing op alle switches van de Nexus van Cisco Nexus. Sommige informatie in dit document kan ook van toepassing zijn op andere de routing en switching platforms van Cisco, zoals Cisco Catalyst routers en switches.

CRC-definitie

Een CRC is een foutdetectiemechanisme dat veel wordt gebruikt in computer- en opslagnetwerken om gegevens te identificeren die tijdens de transmissie zijn gewijzigd of gecorrumpeerd. Wanneer een op het netwerk aangesloten apparaat gegevens moet verzenden, voert het apparaat een rekenalgoritme in dat is gebaseerd op cyclische codes op basis van de gegevens die in een getal met een vaste lengte resulteren. Dit vaste-lengte nummer wordt de CRC-waarde genoemd, maar informeel wordt het vaak de CRC-waarde genoemd. Deze CRC-waarde wordt toegevoegd aan de gegevens en via het netwerk naar een ander apparaat verzonden. Op dit externe apparaat wordt hetzelfde cyclische codealgoritme tegen de gegevens gebruikt en wordt de resulterende waarde vergeleken met de CRC die aan de gegevens is toegevoegd. Als beide waarden overeenkomen, dan gaat het afstandsapparaat ervan uit dat de gegevens over het netwerk zijn verzonden zonder dat ze beschadigd zijn. Als de waarden niet overeenkomen, dan veronderstelt het externe apparaat dat de gegevens tijdens transmissie over het netwerk zijn gecorrumpeerd. Deze gecorrumpeerde gegevens kunnen niet worden vertrouwd en worden verworpen.

CRCs worden gebruikt voor foutdetectie tussen meerdere computernetwerktechnologieën, zoals Ethernet (zowel bekabelde als draadloze varianten), Token Ring, Asynchronous Transfer Mode (ATM) en Frame Relay. Ethernet-frames hebben een veld met 32 bits Frame Control Sequence

(FCS) aan het eind van het frame (onmiddellijk na de payload van het frame) waar een 32-bits CRC-waarde wordt ingevoegd.

Denk bijvoorbeeld aan een scenario waarin twee hosts met de naam Host-A en Host-B direct met elkaar worden verbonden via hun netwerkinterfacekaarten (NIC's). Host-A moet de zin "Dit is een voorbeeld" naar Host-B via het netwerk verzenden. Host-A maakt een Ethernet-frame dat bestemd is voor Host-B met een lading van "Dit is een voorbeeld" en berekent dat de CRC-waarde van het frame een hexadecimale waarde van 0xABCD is. Host-A voegt de CRC-waarde van 0xABCD in het FCS-veld van het Ethernet-frame in en geeft vervolgens het Ethernet-frame van Host-A's NIC naar Host-B door.

Wanneer Host-B dit frame ontvangt, zal het de CRC-waarde van het frame berekenen met behulp van het exacte algoritme zoals Host-A. Host-B berekent dat de CRC-waarde van het frame een hexadecimale waarde van 0xABCD is, die aan Host-B aangeeft dat het Ethernet-frame niet gecorrumpeerd was terwijl het frame naar Host-B werd verzonden.

CRC-foutendefinitie

Een CRC-fout treedt op wanneer een apparaat (een netwerkapparaat of een host die met het netwerk is verbonden) een Ethernet-frame ontvangt met een CRC-waarde in het FCS-veld van het frame dat niet overeenkomt met de CRC-waarde die door het apparaat voor het frame is berekend.

Dit concept kan het beste worden aangetoond door een voorbeeld te geven. Overweeg een scenario waar twee hosts genaamd Host-A en Host-B rechtstreeks met elkaar worden verbonden via hun netwerkinterfacekaarten (NIC’s). Host-A moet de zin "Dit is een voorbeeld" naar Host-B via het netwerk verzenden. Host-A maakt een Ethernet-frame dat bestemd is voor Host-B met een lading van "Dit is een voorbeeld" en berekent dat de CRC-waarde van het frame de hexadecimale waarde 0xABCD is. Host-A voegt de CRC-waarde van 0xABCD in het FCS-veld van het Ethernet-frame in en geeft vervolgens het Ethernet-frame van Host-A's NIC naar Host-B door.

Schade aan de fysieke media die Host-A met Host-B verbinden corrumpeert de inhoud van het frame zodanig dat de zin in het frame verandert in "Dit was een voorbeeld" in plaats van de gewenste lading van "Dit is een voorbeeld".

Wanneer Host-B dit frame ontvangt, berekent het de CRC-waarde van het frame inclusief de gecorrumpeerde lading. Host-B berekent dat de CRC-waarde van het frame een hexadecimale waarde van 0xDEAD is, die anders is dan de 0xABCD CRC-waarde binnen het FCS-veld van het Ethernet-frame. Dit verschil in CRC-waarden vertelt Host-B dat het Ethernet-frame gecorrumpeerd was terwijl het frame naar Host-B werd verzonden. Als resultaat hiervan kan Host-B de inhoud van dit Ethernet-kader niet vertrouwen, zodat het wordt teruggebracht. Host-B zal gewoonlijk ook een soort foutmelding op de Network Interface Card (NIC) verhogen, zoals de "invoerfouten", de "CRC-fouten" of de "RX-fouten" tellers.

Vaak voorkomende symptomen van CRC-fouten

CRC-fouten manifesteren zich doorgaans op een van twee manieren:

1. Toename of niet-nul foutentellers op interfaces van netwerk aangesloten apparaten.
2. Packet/Frame Relay-verlies voor verkeer dat het netwerk overslaat door met het netwerk verbonden apparaten die gecorrumpeerde frames laten vallen.

Deze fouten manifesteren zich op lichtjes verschillende manieren, afhankelijk van het apparaat waarmee u werkt. Deze subsecties gaan in detail voor elk type apparaat in.

Ontvangen fouten op Windows hosts

CRC-fouten op Windows-hosts manifesteren doorgaans als een **teller** die niet op nul **staat** en die **wordt** weergegeven in de uitvoer van het **netstat -e** opdracht van de opdracht. Een voorbeeld van een teller die niet op nul is ontvangen, is hier:

```
>netstat -e
Interface Statistics

                          Received            Sent
Bytes                   1116139893      3374201234
Unicast packets          101276400        49751195
Non-unicast packets              0               0
Discards                         0               0
Errors                       47294               0
Unknown protocols                0
```

De NIC en haar respectieve bestuurder moeten de boekhouding ondersteunen van door de NIC ontvangen CRC-fouten, zodat het aantal door de **netstat-e**-opdracht gerapporteerde fouten nauwkeurig is. De meeste moderne NIC's en hun respectieve bestuurders ondersteunen een nauwkeurige boekhouding van door de NIC ontvangen CRC-fouten.

RX-fouten op Linux-hosts

CRC-fouten op Linux-hosts vertonen doorgaans als een niet-nulteller van "RX-fouten" die in de uitvoer van de opdracht **iffig** wordt weergegeven. Een voorbeeld van een niet-nuloptie RX-foutteller van een Linux-host is hier aanwezig:

```
$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.0.2.10  netmask 255.255.255.128  broadcast 192.0.2.255
       inet6 fe80::10  prefixlen 64  scopeid 0x20<link>
       ether 08:62:66:be:48:9b  txqueuelen 1000  (Ethernet)
       RX packets 591511682  bytes 214790684016 (200.0 GiB)
        RX errors 478920  dropped 0  overruns 0  frame 0
       TX packets 85495109  bytes 288004112030 (268.2 GiB)
       TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

CRC-fouten op Linux-hosts kunnen ook worden weergegeven als een niet-nulteller van "RX-fouten" die in de uitvoer van **ip -s link show-**opdracht wordt weergegeven. Een voorbeeld van een niet-nul RX-foutteller van een Linux-host is hier:

```
$ ip -s link show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DEFAULT group
default qlen 1000
   link/ether 08:62:66:84:8f:6d brd ff:ff:ff:ff:ff:ff
    RX: bytes  packets  errors  dropped overrun mcast
   32246366102 444908978 478920       647     0       419445867
   TX: bytes  packets  errors  dropped carrier collsns
   3352693923 30185715 0       0       0       0
   altname enp11s0
```

De NIC en haar respectieve bestuurder moeten de boekhouding van door de NIC ontvangen

CRC-fouten ondersteunen, zodat het aantal RX-fouten dat door de **link iffig** of **ip -s** wordt gemeld, nauwkeurig is. De meeste moderne NIC's en hun respectieve bestuurders ondersteunen een nauwkeurige boekhouding van door de NIC ontvangen CRC-fouten.

CRC-fouten in netwerkapparaten

Netwerkapparaten werken in één van de twee verzendmodi - Store-and-Forward expediteur, en Cut-Through Forwarding. De manier waarop een netwerkapparaat een ontvangen CRC-fout verwerkt, verschilt afhankelijk van de verzendmodi. De subsecties hier zullen het specifieke gedrag voor elke verzendmodus beschrijven.

Invoerfouten op opslaan-en-doorsturen netwerkapparaten

Wanneer een netwerkapparaat dat in een Store-and-Forward door-sturen modus werkt een kader ontvangt, zal het netwerkapparaat het gehele frame ("Store") bufferen voordat u de CRC-waarde van het frame valideert, een geforceerde beslissing op het frame nemen en het frame uit een interface ("Voorwaarts") verzenden. Daarom, wanneer een netwerkapparaat dat in een Store-and-Forward-verzendmodus werkt een gecorrumpeerd frame met een incorrecte CRC-waarde op een specifieke interface ontvangt, zal het het frame laten vallen en de "Input Errag" teller op de interface verhogen.

Met andere woorden, corrupte Ethernet-frames worden niet doorgestuurd door netwerkapparaten die in een Store-and-Forward-verzendmodus werken; ze worden bij hun ingangen laten vallen .

Cisco Nexus 7000 en 7700 Series switches werken in een Store-and-Forward-verzendmodus. Hier is een voorbeeld van een teller die geen ingangsfouten bevat en een teller die geen nulpunt is voor CRC/FCS vanaf een switch van Nexus 7000 of 7700 Series:

```
switch# show interface
<snip>
Ethernet1/1 is up
 RX
   241052345 unicast packets  5236252 multicast packets  5 broadcast packets
   245794858 input packets  17901276787 bytes
   0 jumbo packets  0 storm suppression packets
   0 runts  0 giants  579204 CRC/FCS  0 no buffer
   579204 input error  0 short frame  0 overrun   0 underrun  0 ignored
   0 watchdog  0 bad etype drop  0 bad proto drop  0 if down drop
   0 input with dribble  0 input discard
   0 Rx pause
```

CRC-fouten kunnen zich ook manifesteren als een "FCS-Err"-teller van niet-nul in de uitvoer van **show interface tellers** fouten. De "Rcv-Err"-teller in de uitvoer van deze opdracht zal ook een niet-nulwaarde hebben, wat de som is van alle invoerfouten (CRC of anderszins) die door de interface worden ontvangen. Hier is een voorbeeld van:

```
switch# show interface counters errors
<snip>
--------------------------------------------------------------------------------
Port          Align-Err    FCS-Err   Xmit-Err    Rcv-Err  UnderSize OutDiscards
--------------------------------------------------------------------------------
Eth1/1                0     579204          0     579204          0           0
```

I/O-fouten op cut-Through-netwerkapparaten

Wanneer een netwerkapparaat dat in een Doorvoermodus voor cut-Through werkt een frame begint te ontvangen, neemt het netwerkapparaat een doorvoerbeslissing over de kop van het frame en begint het frame uit een interface te verzenden zodra het voldoende van het frame ontvangt om een geldige doorsturen beslissing te maken. Aangezien frame en pakketheader aan het begin van het frame zijn, wordt deze verzendingsbeslissing meestal genomen voordat de lading van het frame wordt ontvangen.

Het FCS-veld van een Ethernet-frame bevindt zich aan het einde van het frame, onmiddellijk na de lading van het frame. Daarom zal een netwerkapparaat dat in een Doorvoermodus voor cut-Through werkt het frame vanuit een andere interface al zijn verzonden op het moment dat het de CRC van het frame kan berekenen. Als de CRC die door het netwerkapparaat voor het frame wordt berekend niet overeenkomt met de CRC-waarde die in het FCS-veld aanwezig is, betekent dat het netwerkapparaat dat een gecorrumpeerd frame in het netwerk wordt doorgestuurd. Wanneer dit gebeurt, verhoogt het netwerkapparaat twee tellers:

1. De "Invoerfouten" teller op de interface waar het gecorrumpeerde frame oorspronkelijk werd ontvangen.
2. De "Uitloopfouten" tellen op alle interfaces waar het gecorrumpeerde frame is overgebracht. Voor unicastverkeer zal dit meestal één interface zijn - maar voor uitzending, multicast of onbekend eenastverkeer kan dit één of meer interfaces zijn.

Een voorbeeld hiervan wordt hier getoond, waar de output van het bevel van de **show interface** erop wijst dat er meerdere gecorrumpeerde frames zijn ontvangen op Ethernet1/1 van het netwerkapparaat en vanuit Ethernet1/2 zijn verzonden door de cut-Through versturende modus van het netwerkapparaat:

```
switch# show interface
<snip>
Ethernet1/1 is up
 RX
   46739903 unicast packets  29596632 multicast packets  0 broadcast packets
   76336535 input packets  6743810714 bytes
   15 jumbo packets  0 storm suppression bytes
   0 runts  0 giants  47294 CRC  0 no buffer
   47294 input error  0 short frame  0 overrun   0 underrun  0 ignored
   0 watchdog  0 bad etype drop  0 bad proto drop  0 if down drop
   0 input with dribble  0 input discard
   0 Rx pause

Ethernet1/2 is up
 TX
   46091721 unicast packets  2852390 multicast packets  102619 broadcast packets
   49046730 output packets  3859955290 bytes
   50230 jumbo packets
   47294 output error  0 collision  0 deferred  0 late collision
   0 lost carrier  0 no carrier  0 babble  0 output discard
   0 Tx pause
```

CRC-fouten kunnen zich ook manifesteren als een niet-nul "FCS-Err"-teller op de ingangsinterface en niet-nul "Xmit-Err"-tellers op **spanning interfaces** in de uitvoer van fouten **van** de **showinterface**. De "Rcv-Err"-teller op de invoerinterface in de uitvoer van deze opdracht zal ook een niet-nulwaarde hebben, wat de som is van alle invoerfouten (CRC of anderszins) die door de interface worden ontvangen. Hier is een voorbeeld van:

```
switch# show interface counters errors
<snip>
```

```
--------------------------------------------------------------------------------
Port          Align-Err    FCS-Err   Xmit-Err    Rcv-Err  UnderSize OutDiscards
--------------------------------------------------------------------------------
Eth1/1                0      47294          0      47294          0           0
Eth1/2                0          0      47294          0          0           0
```

Het netwerkapparaat zal ook de CRC-waarde in het FCS-veld van het frame op een specifieke manier wijzigen, wat betekent dat de upstream-netwerkapparaten beschadigd zijn. Dit gedrag staat bekend als "stompen" van de CRC. De precieze wijze waarop de CRC wordt aangepast, varieert van platform tot platform, maar in het algemeen houdt het in dat de huidige CRC-waarde in het FCS-veld van het frame wordt omgekeerd. Hier is een voorbeeld van:

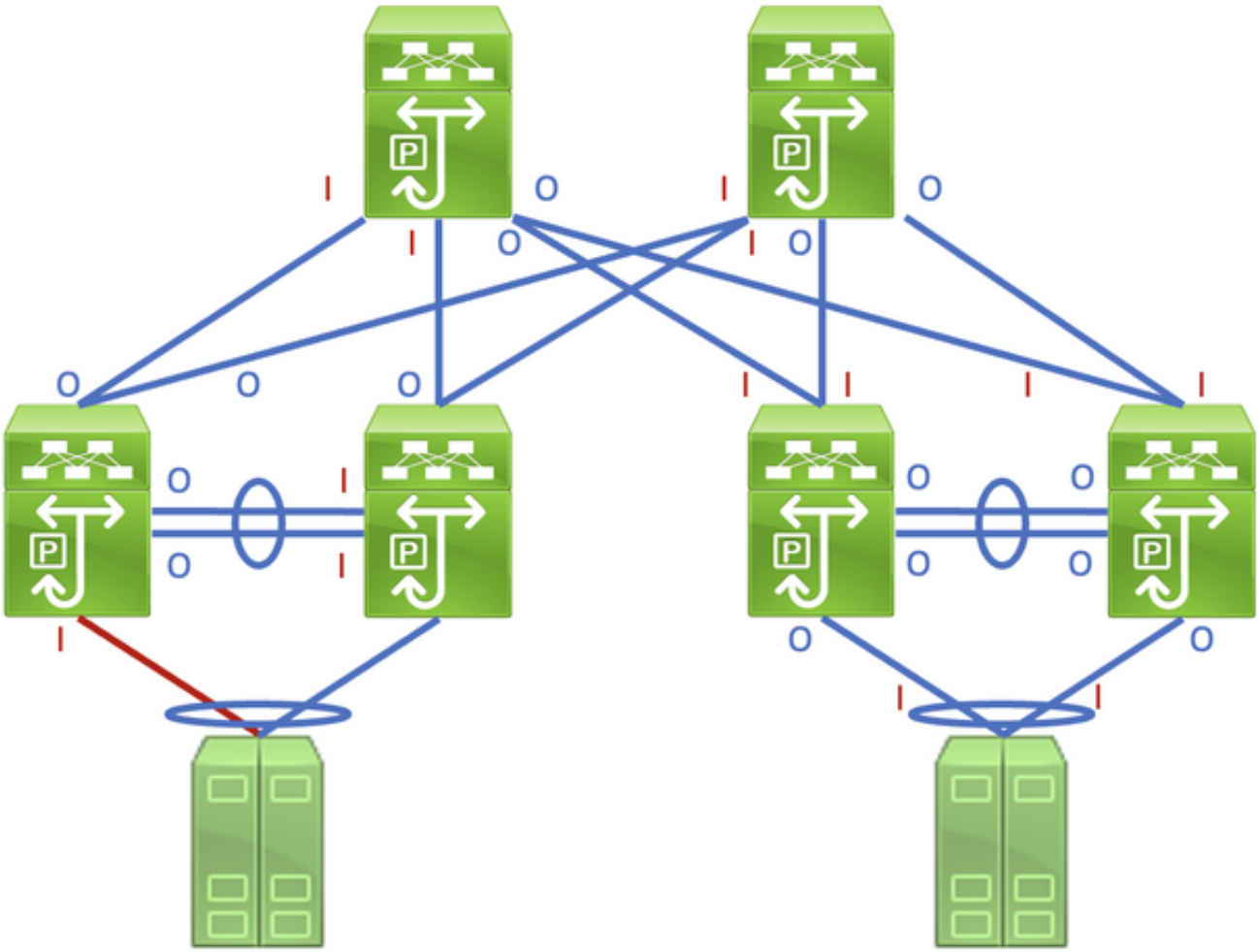
```
Original CRC: 0xABCD (1010101111001101)
Stomped CRC:  0x5432 (0101010000110010)
```

Als resultaat van dit gedrag, kunnen netwerkapparaten die in een cut-Through-verzendmodus werken een corrupt frame door een netwerk propageren. Als een netwerk bestaat uit meerdere netwerkapparaten die in een Cut-Through-verzendmodus werken, kan één corrupt frame invoerfouten en uitvoerfouttellers doen toenemen op meerdere netwerkapparaten binnen uw netwerk.

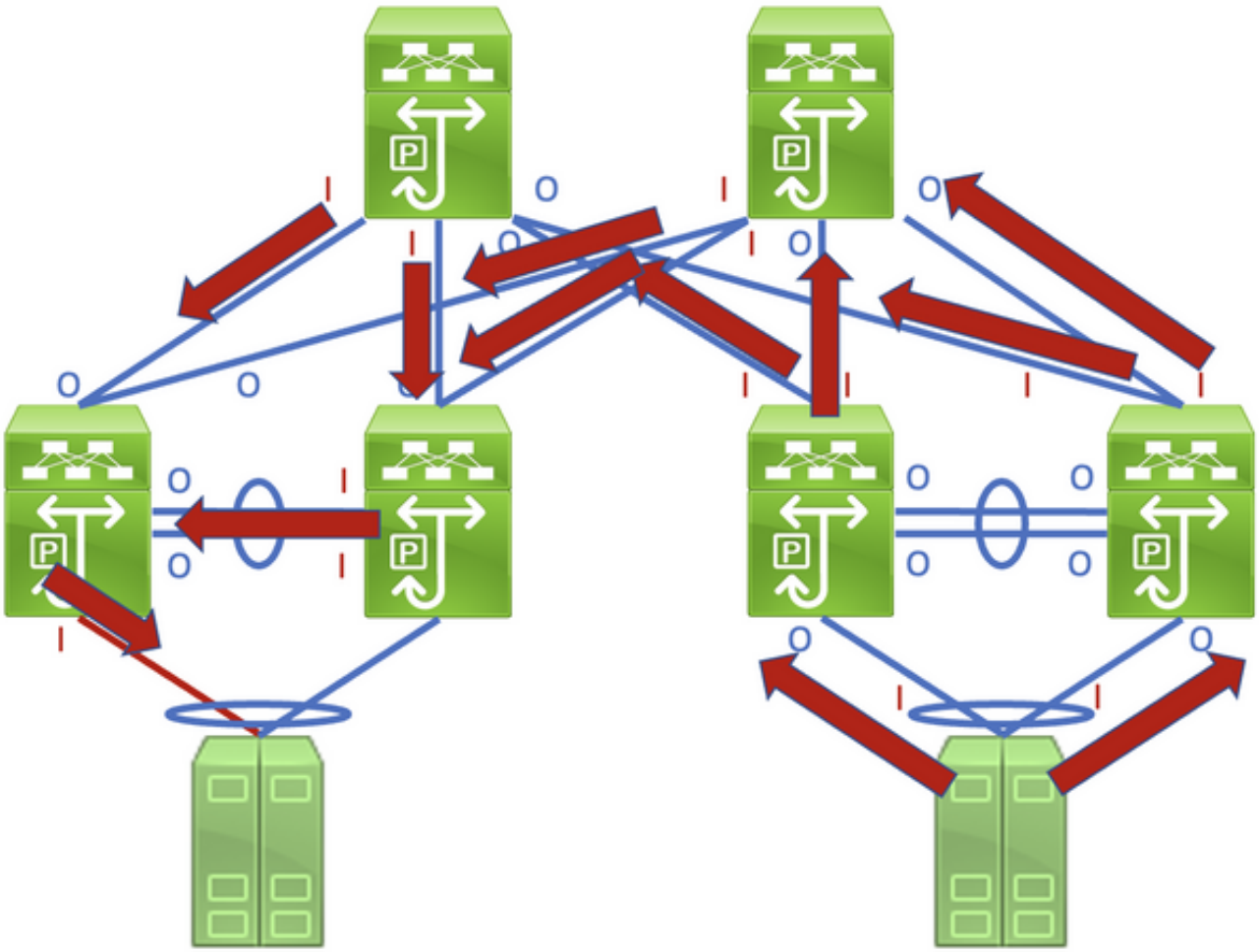
CRC-fouten traceren en isoleren

De eerste stap om de oorzaak van CRC-fouten te identificeren en op te lossen, is het isoleren van de bron van de CRC-fouten in een specifieke verbinding tussen twee apparaten binnen uw netwerk. Een apparaat dat op deze link is aangesloten, heeft een interface-uitvoerfouten teller met een waarde van nul of wordt niet verhoogd, terwijl het andere apparaat dat op deze link is aangesloten een niet-nul of een stijgende interface-invoerfoutteller heeft. Dit suggereert dat het verkeer de interface van één apparaat intact overschrijdt op het moment van de transmissie naar het afstandsapparaat, en als ingangsfout geteld wordt door de ingangsinterface van het andere apparaat op de link.

Het identificeren van deze verbinding in een netwerk dat bestaat uit netwerkapparaten die in een Store-and-Forward expediteits-modus werken is een eenvoudige taak. Het is echter moeilijker deze link in een netwerk te identificeren dat bestaat uit netwerkapparaten die in een Doorvoermodus werken, aangezien veel netwerkapparaten niet-nul input- en uitvoerfouttellers hebben. Een voorbeeld van dit fenomeen kan in de topologie hier worden gezien, waar de link in rood wordt gemarkeerd zo beschadigd is dat het verkeer dat de link oversteekt wordt gecorrumpeerd. Interfaces die zijn voorzien van een rode I-code geven aan interfaces die niet-nul invoerfouten kunnen hebben, terwijl interfaces met een blauwe O-code aangeven dat interfaces niet-nul uitvoerfouten kunnen hebben.



Voor het identificeren van de foutieve link moet u de "pad" gecorrumpeerde frames recursief overtrekken in het netwerk via niet-nul input- en uitvoerfouttellers, waarbij niet-nul invoerfouten upstream naar de beschadigde link in het netwerk wijzen. Dit wordt in het diagram hier aangetoond.



Een gedetailleerd proces voor het traceren en identificeren van een beschadigde link kan het beste worden aangetoond door middel van een voorbeeld. Denk hier aan de topologie:

In deze topologie wordt interface Ethernet1/1 van een Nexus switch genaamd Switch-1 aangesloten op een host genaamd Host-1 door Host-1's Network Interface Card (NIC) eth0. Interface Ethernet1/2 van Switch-1 is verbonden met een tweede Nexus-switch, Switch-2 genoemd, door Switch-2's interface Ethernet1/2. Interface Ethernet1/1 van Switch-2 is verbonden met een host genaamd Host-2 door Host-2's NIC eth0.

De verbinding tussen Host-1 en Switch-1 door de Ethernet1/1-interface van Switch-1 wordt beschadigd, waardoor verkeer dat de link oversteekt, periodiek gecorrumpeerd wordt. We weten echter nog niet dat deze link beschadigd is. We moeten het pad dat de gecorrumpeerde frames in het netwerk doorhalen via niet-nul of stijgende input- en uitvoerfouttellers om de beschadigde link in dit netwerk te vinden.

In dit voorbeeld meldt Host-2's NIC dat het CRC-fouten ontvangt.

```
Host-2$ ip -s link show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DEFAULT group
default qlen 1000
   link/ether 00:50:56:84:8f:6d brd ff:ff:ff:ff:ff:ff
    RX: bytes  packets  errors  dropped overrun mcast
   32246366102 444908978 478920       647     0       419445867
   TX: bytes  packets  errors  dropped carrier collsns
   3352693923 30185715 0       0       0       0
   altname enp11s0
```

U weet dat Host-2's NIC met Switch-2 verbonden is via interface Ethernet1/1. U kunt bevestigen dat interface Ethernet1/1 een niet-nul uitvoerfouten teller heeft met de **show interface** opdracht.

```
Switch-2# show interface
<snip>
Ethernet1/1 is up
admin state is up, Dedicated Interface
    RX
      30184570 unicast packets  872 multicast packets  273 broadcast packets
      30185715 input packets  3352693923 bytes
      0 jumbo packets  0 storm suppression bytes
      0 runts  0 giants 0 CRC  0 no buffer
      0 input error  0 short frame  0 overrun   0 underrun  0 ignored
      0 watchdog  0 bad etype drop  0 bad proto drop  0 if down drop
      0 input with dribble  0 input discard
      0 Rx pause
    TX
      444907944 unicast packets  932 multicast packets  102 broadcast packets
      444908978 output packets  32246366102 bytes
      0 jumbo packets
      478920 output error  0 collision  0 deferred  0 late collision
      0 lost carrier  0 no carrier  0 babble  0 output discard
      0 Tx pause
```

Aangezien de uitvoerfouten teller van interface Ethernet1/1 niet-nul is, is er waarschijnlijk een andere interface van Switch-2 die een teller van niet-nul ingangsfouten heeft. U kunt de opdracht **Show interface tellers fouten niet-nul** gebruiken om te identificeren of om het even welke interfaces van Switch-2 een teller van niet-nul ingangsfouten hebben.

```
Switch-2# show interface counters errors non-zero
<snip>
--------------------------------------------------------------------------------
Port          Align-Err    FCS-Err   Xmit-Err    Rcv-Err  UnderSize OutDiscards
--------------------------------------------------------------------------------
Eth1/1                0          0     478920          0          0           0
Eth1/2                0     478920          0     478920          0           0

--------------------------------------------------------------------------------
Port         Single-Col  Multi-Col   Late-Col  Exces-Col  Carri-Sen       Runts
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Port          Giants SQETest-Err Deferred-Tx IntMacTx-Er IntMacRx-Er Symbol-Err
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Port         InDiscards
--------------------------------------------------------------------------------
```

U kunt zien dat Ethernet1/2 van Switch-2 een niet-nul ingangsfoutteller heeft. Dit suggereert dat Switch-2 gecorrumpeerd verkeer op deze interface ontvangt. U kunt bevestigen welk apparaat op Ethernet1/2 van Switch-2 is aangesloten via de functies Cisco Discovery Protocol (CDP) of Link Local Discovery Protocol (LLDP). Een voorbeeld hiervan wordt hier getoond met de opdracht **tonen cdp buren**.

```
Switch-2# show cdp neighbors
<snip>
    Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
    S - Switch, H - Host, I - IGMP, r - Repeater,
    V - VoIP-Phone, D - Remotely-Managed-Device,
    s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform      Port ID
Switch-1(FDO12345678)
                    Eth1/2         125    R S I s   N9K-C93180YC- Eth1/2
```

U weet nu dat Switch-2 gecorrumpeerd verkeer op zijn Ethernet1/2 interface van Switch-1's Ethernet1/2 interface ontvangt, maar u weet nog niet of het verband tussen Switch-1's Ethernet1/2 en Ethernet1/2 van Switch-2 beschadigd is en de corruptie veroorzaakt, of als Switch-1 een doorsnede switch is die gecorrumpeerd verkeer door te sturen dat het ontvangt. U moet in Switch-1 loggen om dit te verifiëren.

U kunt bevestigen dat de Ethernet1/2-interface van Switch-1 een niet-nul uitvoerfouten teller heeft met de opdracht **showinterfaces**.

```
Switch-1# show interface
<snip>
Ethernet1/2 is up
admin state is up, Dedicated Interface
    RX
      30581666 unicast packets  178 multicast packets  931 broadcast packets
      30582775 input packets  3352693923 bytes
      0 jumbo packets  0 storm suppression bytes
      0 runts  0 giants 0 CRC  0 no buffer
      0 input error  0 short frame  0 overrun   0 underrun  0 ignored
      0 watchdog  0 bad etype drop  0 bad proto drop  0 if down drop
      0 input with dribble  0 input discard
      0 Rx pause
    TX
      454301132 unicast packets  734 multicast packets  72 broadcast packets
      454301938 output packets  32246366102 bytes
      0 jumbo packets
      478920 output error  0 collision  0 deferred  0 late collision
      0 lost carrier  0 no carrier  0 babble  0 output discard
      0 Tx pause
```

U kunt zien dat Ethernet1/2 van Switch-1 een niet-nul uitvoerfouten teller heeft. Dit suggereert dat het verband tussen Switch-1's Ethernet1/2 en Switch-2's Ethernet1/2 niet beschadigd is - in plaats daarvan is Switch-1 een doorsnede switch door te sturen gecorrumpeerd verkeer dat het op een andere interface ontvangt. Zoals eerder aangetoond met Switch-2, kunt u de **van de tonen** opdracht van de **fouten van de** interfacetellers **niet-nul gebruiken** om te identificeren of om het even welke interfaces van Switch-1 een teller van de niet-nul ingangsfouten hebben.

```
Switch-1# show interface counters errors non-zero
<snip>
--------------------------------------------------------------------------------
Port          Align-Err    FCS-Err   Xmit-Err    Rcv-Err  UnderSize OutDiscards
--------------------------------------------------------------------------------
Eth1/1                0     478920          0     478920          0           0
Eth1/2                0          0     478920          0          0           0

--------------------------------------------------------------------------------
Port         Single-Col  Multi-Col   Late-Col  Exces-Col  Carri-Sen       Runts
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Port          Giants SQETest-Err Deferred-Tx IntMacTx-Er IntMacRx-Er Symbol-Err
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Port         InDiscards
--------------------------------------------------------------------------------
```

U kunt zien dat Ethernet1/1 van Switch-1 een niet-nul ingangsfoutteller heeft. Dit suggereert dat Switch-1 gecorrumpeerd verkeer op deze interface ontvangt. We weten dat deze interface verbonden is met Host-1's eth0-NIC. We kunnen de eth0 NIC interfacestatistieken van Host-1 bekijken om te bevestigen of Host-1 gecorrumpeerde frames uit deze interface verstuurt.

```
Host-1$ ip -s link show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DEFAULT group
default qlen 1000
   link/ether 00:50:56:84:8f:6d brd ff:ff:ff:ff:ff:ff
    RX: bytes  packets  errors dropped overrun mcast
   73146816142 423112898 0       0     0       437368817
   TX: bytes  packets  errors  dropped carrier collsns
   3312398924 37942624 0       0       0       0
   altname enp11s0
```

De eth0 NIC-statistieken van Host-1 suggereren dat de host geen gecorrumpeerd verkeer doorgeeft. Dit suggereert dat het verband tussen Host-1's eth0 en Switch-1's Ethernet1/1 beschadigd is en de bron van deze verkeerscorruptie is. Er zal verdere problemen oplossen bij deze link moeten worden uitgevoerd om de foutieve component te identificeren die deze corruptie veroorzaakt en deze te vervangen.

Groot veroorzaakt CRC-fouten

De meest voorkomende oorzaak van CRC-fouten is een beschadigd of slecht functionerend onderdeel van een fysieke verbinding tussen twee apparaten. Voorbeelden zijn:

- Falen of beschadigen van fysiek medium (koper of vezel) of Direct Attach Cable (DAC's).
- Het niet of niet goed werken van transceivers/glasvezelkabels.
- Geen of beschadigde patchpaneel poorten.
- hardware van het defecte netwerkapparaat (met inbegrip van specifieke poorten, toepassingsspecifieke geïntegreerde schakelingen voor lijnkaart [ASIC's], toegangscontroles voor media [MAC's], netwerkmodules enz.);
- Slecht functionerend netwerk interfacekaart in een host ingevoerd.

Het is ook mogelijk voor een of meer verkeerd geconfigureerd apparaten om onopzettelijk CRC-fouten in een netwerk te veroorzaken. Eén voorbeeld hiervan is een Maximum Transmission Unit

(MTU)-configuratie niet goed afgestemd tussen twee of meer apparaten binnen het netwerk, waardoor grote pakketten onjuist zijn ingekort. Het identificeren en oplossen van dit configuratieprobleem kan ook CRC fouten in een netwerk corrigeren.

CRC-fouten oplossen

U kunt de specifieke defecte component identificeren door middel van een proces van eliminatie:

1. Vervang het fysische medium (koper of vezel) of DAC door een bekend fysiek medium van hetzelfde type.
2. Vervang de transceiver die in de interface van één apparaat is ingebracht met een bekende transceiver van hetzelfde model. Als dit de CRC fouten niet oplost, vervang de transceiver die in de interface van het andere apparaat is opgenomen door een bekende transceiver van het zelfde model.
3. Als een patchpaneel gebruikt wordt als onderdeel van de beschadigde link, verplaats de link naar een bekende poort op het patchpaneel. U kunt ook het patchpaneel als mogelijke oorzaak elimineren door de link aan te sluiten zonder het patchpaneel indien mogelijk te gebruiken.
4. Verplaats de beschadigde link naar een andere, bekende poort op elk apparaat. U moet meerdere verschillende poorten testen om een MAC-, ASIC- of lijnkaartstoring te isoleren.
5. Als de beschadigde link een host betreft, verplaatst u de link naar een andere NIC op de host. In plaats hiervan kunt u de beschadigde link ook aansluiten op een bekende goede host om een storing van de NIC van de host te isoleren.

Als de defecte component een Cisco-product (zoals een Cisco-netwerkapparaat of transceiver) is dat door een actief ondersteuningscontract wordt gedekt, kunt u een ondersteuningscase met Cisco TAC openen waarin u specificeert hoe u de slecht functionerende component wilt laten vervangen door een Return Material Authorization (RMA).

Gerelateerde informatie

- Nexus 9000 ASIC CRC-identificatie en traceringsprocedure voor cloudschaal
- Technische ondersteuning en documentatie – Cisco Systems