Analyse von zyklischen Redundanzprüffehlern bei Nexus-Switches

Inhalt

Einleitung

In diesem Dokument werden Details zu CRC-Fehlern (Cyclische Redundancy Check) bei Schnittstellenzählern und Statistiken zu Cisco Nexus-Switches beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, die Grundlagen von Ethernet-Switching und der Cisco NX-OS-Befehlszeilenschnittstelle (CLI) zu verstehen. Weitere Informationen finden Sie in einem der folgenden Dokumente:

- Cisco Nexus 9000 NX-OS - Grundlegender Konfigurationsleitfaden, Version 10.2(x)
- Cisco Nexus NX-OS der Serie 9000 - Grundlegender Konfigurationsleitfaden, Version 9.3(x)
- Cisco Nexus NX-OS der Serie 9000 - Grundlegender Konfigurationsleitfaden, Version 9.2(x)
- Cisco Nexus NX-OS der Serie 9000 - Grundlegender Konfigurationsleitfaden, Version 7.x

- Fehlerbehebung für Ethernet

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Nexus Switches der Serie 9000 ab NX-OS Softwareversion 9.3(8)
- Nexus Switches der Serie 3000 ab NX-OS Softwareversion 9.3(8)

Die Informationen in diesem Dokument wurden von Geräten in einer bestimmten Laborumgebung erstellt. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Hintergrundinformationen

In diesem Dokument werden Details zu CRC-Fehlern (Cyclische Redundancy Check) bei Schnittstellenzählern auf Switches der Cisco Nexus-Serie beschrieben. In diesem Dokument wird beschrieben, was ein CRC ist, wie es im FCS-Feld (Frame Check Sequence) von Ethernet-Frames verwendet wird, wie CRC-Fehler auf Nexus-Switches auftreten, wie CRC-Fehler in Store-and-Forward Switching- und Cut-Through-Switching-Szenarien interagieren, die wahrscheinlichsten Ursachen von CRC-Fehlern und wie CRC-Fehler behoben und behoben werden.

Anwendbare Hardware

Die Informationen in diesem Dokument gelten für alle Switches der Cisco Nexus-Serie. Einige der in diesem Dokument enthaltenen Informationen können auch auf andere Routing- und Switching-Plattformen von Cisco, wie z. B. Cisco Catalyst Router und Switches, angewendet werden.

CRC-Definition

Ein CRC ist ein Fehlererkennungsmechanismus, der in Computern und Speichernetzwerken häufig zum Identifizieren von Daten verwendet wird, die während der Übertragung geändert oder beschädigt wurden. Wenn ein an das Netzwerk angeschlossenes Gerät Daten übertragen muss, wird auf der Grundlage zyklischer Codes ein Rechenalgorithmus ausgeführt, der mit den Daten übereinstimmt, die zu einer Zahl fester Länge führen. Diese Festlängennummer wird als CRC-Wert bezeichnet, wird aber kurz und bündig häufig als CRC bezeichnet. Dieser CRC-Wert wird an die Daten angehängt und über das Netzwerk an ein anderes Gerät übertragen. Dieses Remote-Gerät führt denselben zyklischen Code-Algorithmus für die Daten aus und vergleicht den resultierenden Wert mit dem an die Daten angehängten CRC. Wenn beide Werte übereinstimmen, geht das Remote-Gerät davon aus, dass die Daten ohne Beschädigung über das Netzwerk übertragen wurden. Wenn die Werte nicht übereinstimmen, geht das Remote-Gerät davon aus, dass die Daten bei der Übertragung über das Netzwerk beschädigt wurden. Diese beschädigten Daten können nicht vertrauenswürdig sein und werden verworfen.

CRCs werden für die Fehlererkennung in verschiedenen Netzwerktechnologien des Computers verwendet, z. B. Ethernet (kabelgebunden und drahtlos), Token Ring, Asynchronous Transfer Mode (ATM) und Frame Relay. Ethernet-Frames verfügen am Ende des Frames (unmittelbar nach der Nutzlast des Frames) über ein 32-Bit-FCS-Feld (Frame Check Sequence), in das ein 32-Bit-CRC-Wert eingefügt wird.

Betrachten Sie beispielsweise ein Szenario, in dem zwei Hosts mit den Namen Host-A und Host-B direkt über ihre Netzwerkschnittstellenkarten (NICs) miteinander verbunden sind. Host A muss den Satz "Dies ist ein Beispiel" über das Netzwerk an Host-B senden. Host-A erstellt einen Ethernet-Frame für Host-B mit der Nutzlast "This is an example" und berechnet, dass der CRC-Wert des Frames ein Hexadezimalwert von 0xABCD ist. Host-A fügt den CRC-Wert 0xABCD in das FCS-Feld des Ethernet-Frames ein und überträgt dann den Ethernet-Frame aus der NIC von Host-A an Host-B.

Wenn Host-B diesen Frame empfängt, berechnet er den CRC-Wert des Frames unter Verwendung des exakt gleichen Algorithmus wie Host-A. Host-B berechnet, dass der CRC-Wert des Frames ein hexadezimaler Wert von 0xABCD ist, der Host-B anzeigt, dass der Ethernet-Frame nicht beschädigt war, während der Frame an Host-B übertragen wurde.

CRC-Fehlerdefinition

Ein CRC-Fehler tritt auf, wenn ein Gerät (entweder ein Netzwerkgerät oder ein mit dem Netzwerk verbundener Host) einen Ethernet-Frame mit einem CRC-Wert im FCS-Feld des Frames empfängt, der nicht mit dem vom Gerät für den Frame berechneten CRC-Wert übereinstimmt.

Dieses Konzept lässt sich am besten anhand eines Beispiels demonstrieren. Nehmen wir als Beispiel ein Szenario, in dem zwei Hosts mit den Namen Host-A und Host-B direkt über ihre Netzwerkschnittstellenkarten (NICs) miteinander verbunden sind. Host A muss den Satz "Dies ist ein Beispiel" über das Netzwerk an Host-B senden. Host-A erstellt einen Ethernet-Frame für Host-B mit der Nutzlast "This is an example" und berechnet, dass der CRC-Wert des Frames der Hexadezimalwert 0xABCD ist. Host-A fügt den CRC-Wert 0xABCD in das FCS-Feld des Ethernet-Frames ein und überträgt dann den Ethernet-Frame aus der NIC von Host-A an Host-B.

Schäden an den physischen Medien, die Host-A mit Host-B verbinden, beschädigen jedoch den Frame-Inhalt, sodass der Satz im Frame zu "This was an example" (Dies war ein Beispiel) wechselt, anstatt zu der gewünschten Payload von "This is an example" (Dies ist ein Beispiel).

Wenn Host-B diesen Frame empfängt, berechnet er den CRC-Wert des Frames einschließlich der beschädigten Nutzlast. Host-B berechnet, dass der CRC-Wert des Frames ein Hexadezimalwert von 0xDEAD ist, der sich vom 0xABCD CRC-Wert innerhalb des FCS-Felds des Ethernet-Frames unterscheidet. Dieser Unterschied bei den CRC-Werten weist Host-B darauf hin, dass der Ethernet-Frame beschädigt war, während der Frame an Host-B übertragen wurde. Daher kann Host-B dem Inhalt dieses Ethernet-Frames nicht vertrauen, daher wird er gelöscht. Host-B erhöht in der Regel auch eine Art von Fehlerzähler auf seiner Netzwerkkarte (NIC), z. B. die Zähler "Eingabefehler", "CRC-Fehler" oder "RX-Fehler".

Häufige Symptome von CRC-Fehlern

CRC-Fehler manifestieren sich in der Regel auf zwei Arten:

1. Erhöhen oder Nicht-Null-Fehlerzähler auf Schnittstellen von mit dem Netzwerk verbundenen Geräten.
2. Paket-/Frame-Verlust für Datenverkehr, der das Netzwerk durchläuft, da mit dem Netzwerk verbundene Geräte beschädigte Frames verwerfen.

Diese Fehler treten je nach Gerät, mit dem Sie arbeiten, auf leicht unterschiedliche Weise auf. In diesen Unterabschnitten wird auf die einzelnen Gerätetypen eingegangen.

Empfangene Fehler auf Windows-Hosts

CRC-Fehler auf Windows-Hosts manifestieren sich in der Regel als **Zähler** für **empfangene Fehler** ungleich null, der in der Ausgabe des Befehls **netstat -e** von der Eingabeaufforderung angezeigt wird. Ein Beispiel eines Zählers für nicht null empfangene Fehler von der Eingabeaufforderung eines Windows-Hosts ist:

```
>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
```

Die Netzwerkkarte und der entsprechende Treiber müssen die Erfassung von CRC-Fehlern unterstützen, die von der Netzwerkkarte empfangen wurden, damit die Anzahl der vom Befehl **netstat -e** gemeldeten empfangenen Fehler korrekt ist. Die meisten modernen NICs und ihre jeweiligen Treiber unterstützen die präzise Erfassung von CRC-Fehlern, die von der Netzwerkkarte empfangen wurden.

RX-Fehler auf Linux-Hosts

CRC-Fehler auf Linux-Hosts manifestieren sich in der Regel als Nicht-Null-Zähler für "RX errors", der in der Ausgabe des Befehls **ifconfig** angezeigt wird. Ein Beispiel für einen Nicht-Null-RX-Fehlerzähler von einem Linux-Host ist:

```
$ 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-Fehler auf Linux-Hosts können auch als Nicht-Null-Zähler für "RX-Fehler" manifestiert werden, der in der Ausgabe des Befehls **ip -s link show** angezeigt wird. Ein Beispiel für einen Nicht-Null-RX-Fehlerzähler von einem Linux-Host ist:

```
$ 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
```

Die Netzwerkkarte und der entsprechende Treiber müssen die Erfassung von CRC-Fehlern unterstützen, die von der Netzwerkkarte empfangen wurden, damit die Anzahl der RX-Fehler, die

von der **ifconfig** oder der **ip -s-Verbindung** gemeldet wurden, die Befehle korrekt sind. Die meisten modernen NICs und ihre jeweiligen Treiber unterstützen die präzise Erfassung von CRC-Fehlern, die von der Netzwerkkarte empfangen wurden.

CRC-Fehler auf Netzwerkgeräten

Netzwerkgeräte arbeiten in einem der beiden Weiterleitungsmodi - Store-and-Forward (SnF)-Weiterleitungsmodus und Cut-Through Forwarding-Modus. Die Art und Weise, wie ein Netzwerkgerät einen empfangenen CRC-Fehler behandelt, hängt von seinen Weiterleitungsmodi ab. In den folgenden Unterabschnitten wird das spezifische Verhalten für die einzelnen Weiterleitungsmodi beschrieben.

Eingabefehler auf Speicher- und Weiterleitungsnetzwerkgeräten

Wenn ein Netzwerkgerät, das in einem SnF-Weiterleitungsmodus betrieben wird, einen Frame empfängt, puffert das Netzwerkgerät den gesamten Frame ("Store"), bevor Sie den CRC-Wert des Frames validieren, eine Weiterleitungsentscheidung für den Frame treffen und den Frame aus einer Schnittstelle ("Forward") übertragen. Wenn ein Netzwerkgerät, das im SnF-Weiterleitungsmodus betrieben wird, einen beschädigten Frame mit einem falschen CRC-Wert für eine bestimmte Schnittstelle empfängt, wird der Frame gelöscht und der Zähler "Input Errors" (Eingabefehler) auf der Schnittstelle erhöht.

Anders ausgedrückt: Korrupte Ethernet-Frames werden nicht von Netzwerkgeräten weitergeleitet, die im SnF-Weiterleitungsmodus betrieben werden. sie werden beim Eingang fallen gelassen.

Cisco Nexus Switches der Serien 7000 und 7700 werden im Store-and-Forward-Weiterleitungsmodus betrieben. Ein Beispiel für einen Leistungsindikator für Nicht-Null-Eingangsfehler und einen Nicht-Null-CRC/FCS-Zähler eines Switches der Serie Nexus 7000 oder 7700 ist hier:

```
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-Fehler können sich auch als Nicht-Nullzähler "FCS-Err" in der Ausgabe von Fehlern **bei** den **Anzeigen von Schnittstellenzählern** manifestieren. Der Zähler "Rcv-Err" in der Ausgabe dieses Befehls hat auch einen Wert von nicht null, d. h. die Summe aller Eingabefehler (CRC oder anders), die von der Schnittstelle empfangen werden. Ein Beispiel hierfür ist hier:

```
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
```

Eingabe- und Ausgabefehler bei Cut-Through-Netzwerkgeräten

Wenn ein Netzwerkgerät, das im Cut-Through-Weiterleitungsmodus betrieben wird, einen Frame empfängt, trifft das Netzwerkgerät eine Weiterleitungsentscheidung für den Frame-Header und beginnt, den Frame aus einer Schnittstelle zu übertragen, sobald er genug Frame empfängt, um eine gültige Weiterleitungsentscheidung zu treffen. Da Frame- und Paket-Header am Anfang des Frames stehen, wird diese Weiterleitungsentscheidung in der Regel getroffen, bevor die Nutzlast des Frames empfangen wird.

Das FCS-Feld eines Ethernet-Frames befindet sich am Ende des Frames, unmittelbar nach der Nutzlast des Frames. Daher hat ein Netzwerkgerät, das im Cut-Through-Weiterleitungsmodus betrieben wird, bereits begonnen, den Frame aus einer anderen Schnittstelle zu übertragen, bis er das CRC des Frames berechnen kann. Wenn der vom Netzwerkgerät für den Frame berechnete CRC-Wert nicht mit dem im FCS-Feld vorhandenen CRC-Wert übereinstimmt, bedeutet dies, dass das Netzwerkgerät einen beschädigten Frame in das Netzwerk weitergeleitet hat. In diesem Fall erhöht das Netzwerkgerät zwei Zähler:

1. Der Zähler "Input Errors" (Eingabefehler) auf der Schnittstelle, an der der beschädigte Frame ursprünglich empfangen wurde.
2. Der Zähler "Ausgabefehler" auf allen Schnittstellen, auf denen der beschädigte Frame übertragen wurde. Bei Unicast-Datenverkehr ist dies normalerweise eine einzige Schnittstelle. Bei Broadcast-, Multicast- oder unbekanntem Unicast-Datenverkehr kann es sich jedoch um eine oder mehrere Schnittstellen handeln.

Ein Beispiel hierfür ist hier dargestellt, wo die Ausgabe des Befehls **show interface** darauf hinweist, dass mehrere beschädigte Frames auf Ethernet1/1 des Netzwerkgeräts empfangen und aufgrund des Cut-Through-Weiterleitungsmodus des Netzwerkgeräts über Ethernet1/2 übertragen wurden:

```
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-Fehler können sich auch als Nicht-Nullzähler "FCS-Err" auf der Eingangs-Schnittstelle und Nicht-Nullzähler "Xmit-Err" auf Ausgangs-Schnittstellen in der Ausgabe von Fehlern **bei** Anzeigen **von Schnittstellenzählern** manifestieren. Der Zähler "Rcv-Err" in der Ausgabe dieses Befehls auf der Eingangs-Schnittstelle hat ebenfalls einen Wert von nicht null, d. h. die Summe aller Eingabefehler (CRC oder anders), die von der Schnittstelle empfangen werden. Ein Beispiel

hierfür ist hier:

```
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
```

Das Netzwerkgerät ändert außerdem den CRC-Wert im FCS-Feld des Frames in einer bestimmten Weise, die bedeutet, dass dieser Frame für Upstream-Netzwerkgeräte beschädigt ist. Dieses Verhalten wird als "Stomping" des CRC bezeichnet. Die genaue Art und Weise, in der das CRC geändert wird, variiert von Plattform zu Plattform, erfordert jedoch im Allgemeinen, den aktuellen CRC-Wert im FCS-Feld des Frames umzukehren. Hier ein Beispiel:

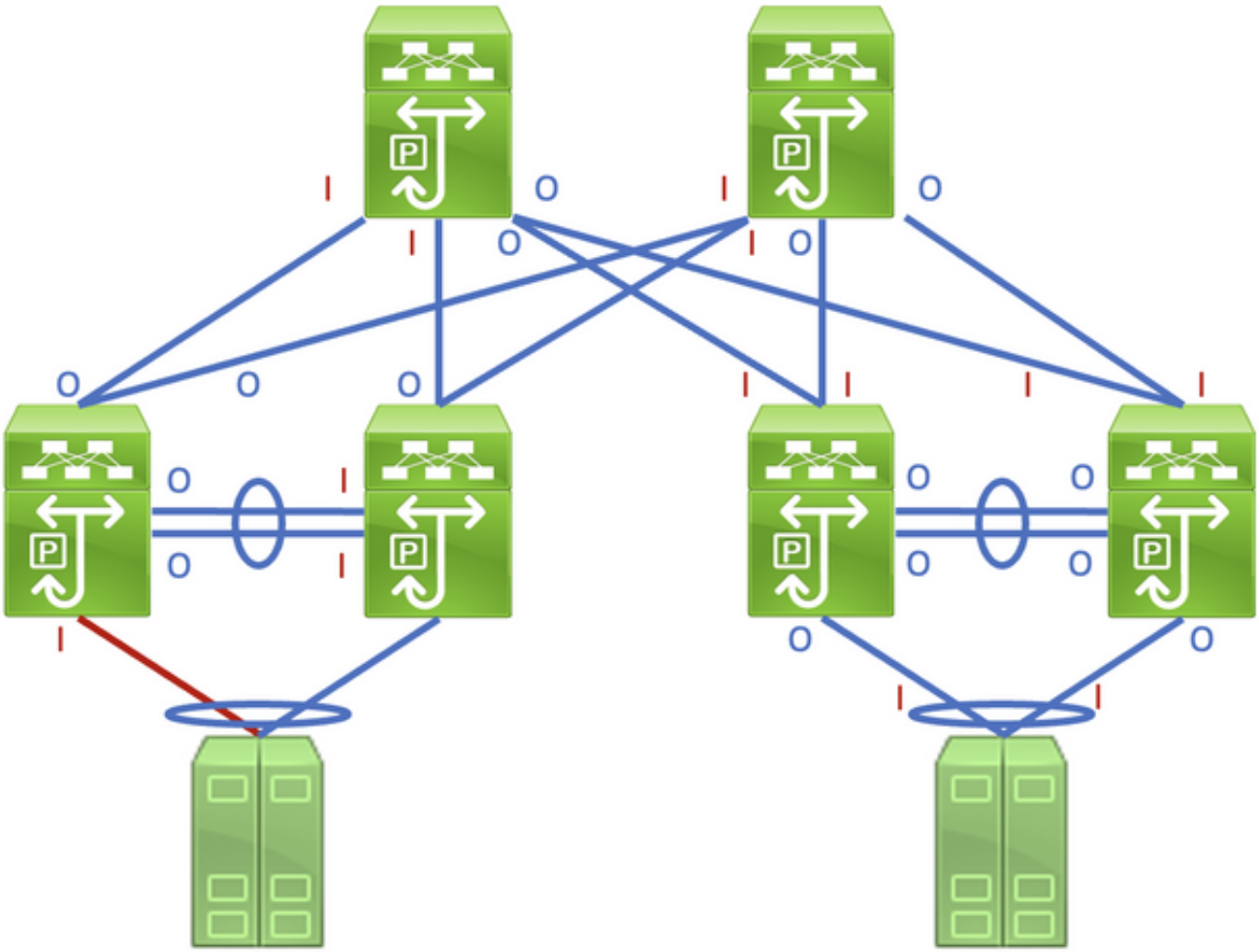
```
Original CRC: 0xABCD (1010101111001101)
Stomped CRC:  0x5432 (0101010000110010)
```

Aufgrund dieses Verhaltens können Netzwerkgeräte, die im Cut-Through-Weiterleitungsmodus betrieben werden, einen beschädigten Frame im gesamten Netzwerk verbreiten. Wenn ein Netzwerk aus mehreren Netzwerkgeräten besteht, die im Cut-Through-Weiterleitungsmodus betrieben werden, kann ein einzelner beschädigter Frame dazu führen, dass die Zähler für Eingangs- und Ausgangsfehler in mehreren Netzwerkgeräten im Netzwerk inkrementiert werden.

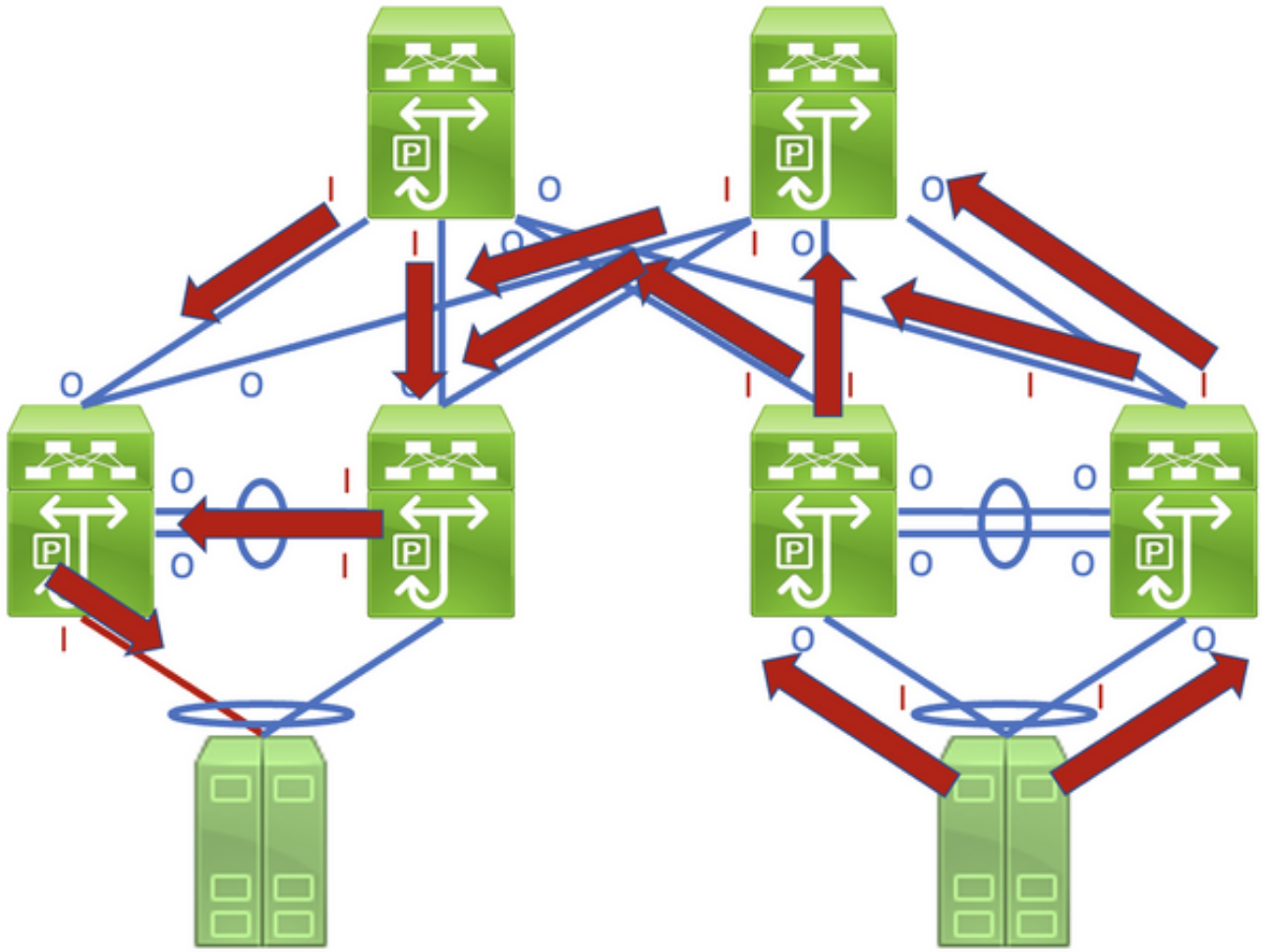
Nachverfolgen und Isolieren von CRC-Fehlern

Der erste Schritt zur Identifizierung und Behebung der Ursachen von CRC-Fehlern besteht darin, die Quelle der CRC-Fehler auf eine bestimmte Verbindung zwischen zwei Geräten in Ihrem Netzwerk zu isolieren. Ein Gerät, das mit dieser Verbindung verbunden ist, hat einen Fehler-Zähler für die Schnittstellenausgabe mit dem Wert Null oder erhöht nicht, während das andere Gerät, das mit dieser Verbindung verbunden ist, über einen Nicht-Null- oder Inkrementierungs-Fehlerzähler für die Schnittstelleneingabe verfügt. Dies legt nahe, dass der Datenverkehr die Schnittstelle eines Geräts intakt ausleitet, zum Zeitpunkt der Übertragung an das Remote-Gerät beschädigt ist und von der Eingangs-Schnittstelle des anderen Geräts an der Verbindung als Eingangsfehler gewertet wird.

Die Identifizierung dieser Verbindung in einem Netzwerk, das aus SnF-Netzwerkgeräten besteht, ist eine einfache Aufgabe. Die Identifizierung dieser Verbindung in einem Netzwerk, das aus Cut-Through-Netzwerkgeräten besteht, ist jedoch schwieriger, da viele Netzwerkgeräte über Nicht-Nullpunkt-Fehlerzähler für Eingabe- und Ausgabe verfügen. Ein Beispiel für dieses Phänomen ist die Topologie, in der der rot hervorgehobene Link so beschädigt ist, dass der über den Link laufende Datenverkehr beschädigt ist. Die mit einem roten "I" beschrifteten Schnittstellen weisen auf Schnittstellen hin, die Nicht-Nulleingabefehler aufweisen können, während Schnittstellen mit einem blauen "O" Schnittstellen mit Nicht-Nullausgabefehlern angeben.



Um die fehlerhafte Verbindung zu identifizieren, müssen Sie die beschädigten "path" Frames im Netzwerk rekursiv mithilfe von Nicht-Null-Eingabe- und -Ausgabe-Fehlerzählern verfolgen, wobei Nicht-Null-Eingabefehler Upstream auf die beschädigte Verbindung im Netzwerk hinweisen. Dies wird im Diagramm hier veranschaulicht.



Ein detailliertes Verfahren zur Nachverfolgung und Identifizierung einer beschädigten Verbindung wird am besten anhand eines Beispiels demonstriert. Betrachten Sie die Topologie hier:

In dieser Topologie ist die Schnittstelle Ethernet1/1 eines Nexus-Switches mit dem Namen Switch-1 über die Netzwerkkarte (NIC) eth0 von Host 1 mit einem Host namens Host-1 verbunden. Die Schnittstelle Ethernet1/2 des Switch-1 ist über die Schnittstelle Ethernet1/2 des Switch-2 mit einem zweiten Nexus-Switch namens Switch-2 verbunden. Die Schnittstelle Ethernet1/1 des Switch-2 ist über die Netzwerkkarte eth0 des Host-2 mit dem Host-2 verbunden.

Die Verbindung zwischen Host-1 und Switch-1 über die Ethernet1/1-Schnittstelle des Switch-1 ist beschädigt, wodurch der Datenverkehr, der die Verbindung passiert, periodisch beschädigt wird. Wir wissen jedoch noch nicht, dass dieser Link beschädigt ist. Wir müssen den Pfad verfolgen, den die beschädigten Frames im Netzwerk hinterlassen, indem wir die Eingabe- und Ausgabefehler nicht null oder erhöhen, um die beschädigte Verbindung in diesem Netzwerk zu lokalisieren.

In diesem Beispiel meldet die Netzwerkkarte von Host-2, dass sie CRC-Fehler empfängt.

```
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
```

Sie wissen, dass die Netzwerkkarte von Host 2 über die Schnittstelle Ethernet1/1 mit Switch-2 verbunden ist. Sie können mithilfe des Befehls **show interface** bestätigen, dass die Schnittstelle Ethernet1/1 einen Ausgabefehler-Zähler von nicht null aufweist.

```
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
```

Da der Fehlerzähler für die Ausgabe der Schnittstelle Ethernet1/1 nicht null ist, gibt es höchstwahrscheinlich eine andere Schnittstelle des Switch-2, die einen Nicht-Nulleingangsfehler-Zähler aufweist. Mit dem Befehl **show interface counter errors non-zero (Schnittstellenfehler anzeigen) können Sie** ermitteln, ob an den Schnittstellen von Switch-2 ein Eingabefehler von nicht null vorliegt.

```
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
```

```
--------------------------------------------------------------------------------
```

Wie Sie sehen, hat Ethernet1/2 von Switch-2 einen Nicht-Nulleingangsfehler-Zähler. Dies deutet darauf hin, dass Switch-2 beschädigten Datenverkehr an dieser Schnittstelle empfängt. Sie können mithilfe der Funktionen Cisco Discovery Protocol (CDP) oder Link Local Discovery Protocol (LLDP) überprüfen, welches Gerät mit Ethernet1/2 von Switch-2 verbunden ist. Ein Beispiel hierfür ist hier mit dem Befehl **show cdp neighbors** dargestellt.

```
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
```

Sie wissen jetzt, dass Switch-2 über seine Ethernet1/2-Schnittstelle beschädigten Datenverkehr von der Ethernet1/2-Schnittstelle des Switch-1 empfängt. Sie wissen jedoch noch nicht, ob die Verbindung zwischen Ethernet1/2 des Switch-1 und Ethernet1/2 des Switch-2 beschädigt ist und die Beschädigung verursacht oder ob Switch-1 ein Cut-Through-Switch ist, der korrupten Datenverkehr weiterleitet. Sie müssen sich bei Switch-1 anmelden, um dies zu überprüfen.

Mit dem Befehl **show interfaces** können Sie bestätigen, dass die Ethernet1/2-Schnittstelle des Switch-1 einen Ausgabefehler-Zähler von nicht null aufweist.

```
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
```

Sie sehen, dass Ethernet1/2 von Switch-1 einen Ausgabefehler-Zähler von nicht null aufweist. Dies deutet darauf hin, dass die Verbindung zwischen dem Ethernet1/2-Switch und dem Ethernet1/2-Switch-2 nicht beschädigt ist. Stattdessen ist Switch-1 ein Switch, der den auf einer anderen Schnittstelle empfangenen Cut-Through-Switch-Verkehr weiterleitet und beschädigte Daten weiterleitet. Wie bereits mit Switch-2 gezeigt, können Sie den Befehl **show interface counters errors non-zero** verwenden, um zu ermitteln, ob irgendeine Schnittstelle von Switch-1

einen Nicht-Nulleingabefehler aufweist.

```
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
--------------------------------------------------------------------------------
```

Wie Sie sehen, hat Ethernet1/1 von Switch-1 einen Nicht-Nulleingangsfehler-Zähler. Dies deutet darauf hin, dass der Switch-1 beschädigten Datenverkehr an dieser Schnittstelle empfängt. Wir wissen, dass diese Schnittstelle eine Verbindung zur eth0 NIC des Host-1 herstellt. Wir können die eth0 NIC-Schnittstellenstatistiken von Host-1 überprüfen, um zu bestätigen, dass Host-1 beschädigte Frames aus dieser Schnittstelle sendet.

```
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
```

Die eth0 NIC-Statistiken von Host-1 legen nahe, dass der Host keinen beschädigten Datenverkehr überträgt. Dies deutet darauf hin, dass die Verbindung zwischen dem eth0 des Host-1 und dem Ethernet1/1 des Switch-1 beschädigt ist und die Ursache für diese Beschädigung des Datenverkehrs ist. Darüber hinaus muss für diesen Link eine Fehlerbehebung durchgeführt werden, um die fehlerhafte Komponente zu identifizieren, die diese Beschädigung verursacht, und um sie zu ersetzen.

Ursachen von CRC-Fehlern

Die häufigste Ursache für CRC-Fehler ist eine beschädigte oder fehlerhafte Komponente einer physischen Verbindung zwischen zwei Geräten.

Beispiele:

- Fehlerhaftes oder beschädigtes physisches Medium (Kupfer oder Glasfaser) oder Direct Attach Cables (DACs).
- Fehlerhafte oder beschädigte Transceiver/optische Verbindungen.

- Patchfeld-Anschlüsse fehlerhaft oder beschädigt.
- fehlerhafte Hardware für Netzwerkgeräte (einschließlich spezifischer Ports, Line Card Application-Specific Integrated Circuits (ASICs), Media Access Controls (MACs), Fabric-Module usw.),

- Fehlerhafte Netzwerkschnittstellenkarte, die in einen Host eingesetzt ist.

Es ist auch möglich, dass ein oder mehrere falsch konfigurierte Geräte versehentlich CRC-Fehler in einem Netzwerk verursachen. Ein Beispiel hierfür ist eine MTU-Konfigurationsungleichheit (Maximum Transmission Unit) zwischen zwei oder mehr Geräten im Netzwerk, die dazu führt, dass große Pakete falsch abgeschnitten werden. Durch die Identifizierung und Behebung dieses Konfigurationsproblems können auch CRC-Fehler innerhalb eines Netzwerks behoben werden.

Beheben von CRC-Fehlern

Sie können die fehlerhafte Komponente durch einen Eliminationsprozess identifizieren:

1. Ersetzen Sie das physische Medium (Kupfer oder Glasfaser) oder den DAC durch ein zweifelsfrei funktionierendes physisches Medium desselben Typs.
2. Ersetzen Sie den Transceiver, der in die Schnittstelle eines Geräts eingefügt wurde, durch einen zweifelsfrei funktionierenden Transceiver desselben Modells. Wenn die CRC-Fehler dadurch nicht behoben werden, ersetzen Sie den Transceiver, der in die Schnittstelle des anderen Geräts eingefügt wurde, durch einen zweifelsfrei funktionierenden Transceiver desselben Modells.
3. Wenn Patchfelder als Teil der beschädigten Verbindung verwendet werden, ziehen Sie die Verbindung an einen zweifelsfrei funktionierenden Anschluss an der Patchbox. Alternativ können Sie das Patchfeld als mögliche Ursache beseitigen, indem Sie den Link anschließen, ohne das Patchfeld zu verwenden, wenn möglich.
4. Schließen Sie die beschädigte Verbindung an einen anderen, zweifelsfrei funktionierenden Anschluss an jedem Gerät an. Möglicherweise müssen Sie mehrere verschiedene Ports testen, um einen MAC-, ASIC- oder Line Card-Fehler zu isolieren.
5. Wenn die beschädigte Verbindung einen Host umfasst, verschieben Sie den Link auf eine andere Netzwerkkarte auf dem Host. Alternativ können Sie die beschädigte Verbindung mit einem zweifelsfrei funktionierenden Host verbinden, um einen Ausfall der Netzwerkkarte des Hosts zu isolieren.

Wenn es sich bei der fehlerhaften Komponente um ein Cisco Produkt (z. B. ein Cisco Netzwerkgerät oder Transceiver) handelt, das durch einen aktiven Support-Vertrag abgedeckt ist, können Sie beim Cisco TAC ein Support-Ticket erstellen, in dem Ihre Fehlerbehebung beschrieben wird, damit die fehlerhafte Komponente durch eine Retourengenehmigung (Return Material Authorization, RMA) ersetzt wird.

Zugehörige Informationen

- Verfahren zur Identifizierung und Verfolgung von ASIC CRC in der Nexus 9000 Cloud-Skalierung
- **Technischer Support und Dokumentation für Cisco Systeme**