

Nexus スイッチでの巡回冗長検査エラーについて

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[該当ハードウェア](#)

[CRC の定義](#)

[CRC エラーの定義](#)

[CRC エラーの一般的な症状](#)

[Windows ホストでの受信エラー](#)

[Linux ホストでの RX エラー](#)

[ネットワークデバイスでの CRC エラー](#)

[ストアアンドフォワード ネットワーク デバイスでの入力エラー](#)

[カットスルー ネットワーク デバイスでの入出力エラー](#)

[CRC エラーのトレースおよび分離](#)

[CRC エラーの根本原因](#)

[CRC エラーの解決](#)

[関連情報](#)

はじめに

このドキュメントでは、インターフェイスカウンタで見られる巡回冗長検査(CRC)エラーと、Cisco Nexusスイッチの統計情報について説明します。

前提条件

要件

イーサネットスイッチングの基本と Cisco NX-OS CLI (コマンド ライン インターフェイス) について理解しておくことをお勧めします。詳細については、次の該当するドキュメントのいずれかを参照してください。

- [Cisco Nexus 9000 NX-OS の基礎の構成ガイド、リリース 10.2\(x\)](#)
- [Cisco Nexus 9000 シリーズ NX-OS の基礎の構成ガイド、リリース 9.3\(x\)](#)
- [Cisco Nexus 9000 シリーズ NX-OS の基礎の構成ガイド、リリース 9.2\(x\)](#)
- [Cisco Nexus 9000 シリーズ NX-OS の基礎の構成ガイド、リリース 7.x](#)
- [イーサネットのトラブルシューティング](#)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- NX-OSソフトウェアリリース9.3(8)以降のNexus 9000シリーズスイッチ
- NX-OSソフトウェアリリース9.3(8)以降のNexus 3000シリーズスイッチ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

このドキュメントでは、Cisco Nexusシリーズスイッチのインターフェイスカウンタで見られる巡回冗長検査(CRC)エラーについて詳しく説明します。このドキュメントでは、CRCの概要、イーサネットフレームのFrame Check Sequence (FCS ; フレームチェックシーケンス) フィールドでのCRCの使用方法、NexusスイッチでのCRCエラーの発生、ストアアンドフォワードスイッチングでのCRCエラーのインタラクションについて説明します。また、カットスルースイッチングのシナリオ、CRCエラーの根本原因として最も可能性が高いもの、およびCRCエラーのトラブルシューティングと解決方法についても説明します。

該当ハードウェア

このドキュメントの情報は、すべてのCisco Nexusシリーズスイッチに適用されます。このドキュメントの情報の一部は、Cisco Catalystルータやスイッチなど、他のシスコのルーティングおよびスイッチングプラットフォームにも適用できます。

CRC の定義

CRCは、送信中に変更または破損されたデータを識別するために、コンピュータおよびストレージネットワークで一般的に使用されるエラー検出メカニズムです。ネットワークに接続されたデバイスがデータを送信する必要がある場合、そのデバイスは固定長の数になるデータに対してサイクリックコードに基づいて計算アルゴリズムを実行します。この固定長の数値は CRC 値と呼ばれますが、口語的には、多くの場合、略して CRC と呼ばれます。この CRC 値は、データに付加され、ネットワークを介して別のデバイスに送信されます。このリモートデバイスは、データに対して同じ循環コードアルゴリズムを実行し、その結果の値をデータに付加されたCRCと比較します。両方の値が一致する場合、リモートデバイスはデータが破損することなくネットワーク経由で送信されたものと見なします。値が一致しない場合、リモートデバイスはネットワーク経由の送信でデータが破損しているとは見なします。この破損したデータは信頼されず、破棄されます。

CRCは、イーサネット (有線と無線の両方)、トークンリング、非同期転送モード(ATM)、フレームリレーなど、複数のコンピュータネットワークテクノロジーでのエラー検出に使用されます。イーサネットフレームには、32ビットのCRC値が挿入されるフレームの最後 (フレームの

ペイロードの直後)に32ビットのFrame Check Sequence (FCS ; フレームチェックシーケンス) フィールドがあります。

たとえば、Host-AとHost-Bという2台のホストが、ネットワークインターフェイスカード(NIC)を介して相互に直接接続されているとします。Host-Aは、「This is an example」という文をネットワーク経由でHost-Bに送信する必要があります。Host-Aは、「This is an example」というペイロードを持つHost-B宛てのイーサネットフレームを作成し、フレームのCRC値が0xABCDという16進値になることを計算します。Host-AはCRC値0xABCDをイーサネットフレームのFCSフィールドに挿入し、ホストAのNICからホストBにイーサネットフレームを送信します。

ホストBはこのフレームを受信すると、ホストAとまったく同じアルゴリズムを使用してフレームのCRC値を計算できます。Host-Bでは、フレームのCRC値が16進数値0xABCDであると計算されています。これは、フレームがHost-Bに送信された際に、イーサネットフレームが破損しなかったことをHost-Bに示しています。

CRC エラーの定義

CRCエラーは、デバイス(ネットワークデバイスまたはネットワークに接続されたホスト)がイーサネットフレームを受信し、そのフレームのFCSフィールドに含まれるCRC値が、フレームに関してデバイスで計算されたCRC値と一致しない場合に発生します。

この概念がよく理解できるように、例を使用します。「Host-A」と「Host-B」という2つのホストがネットワークインターフェイスカード(NIC)を介して互いに直接接続されているシナリオについて説明します。Host-Aは、「This is an example」という文をネットワーク経由でHost-Bに送信する必要があります。Host-Aは、「This is an example」というペイロードを持つHost-B宛てのイーサネットフレームを作成し、フレームのCRC値が0xABCDという16進値になることを計算します。Host-AはCRC値0xABCDをイーサネットフレームのFCSフィールドに挿入し、ホストAのNICからホストBにイーサネットフレームを送信します。

ただし、Host-AとHost-Bを接続する物理メディアが損傷しているため、フレームの内容が破損し、フレーム内の文が「This is an example」という目的のペイロードではなく「This was an example」に変化しています。

Host-Bはこのフレームを受信すると、フレームのCRC値を計算し、破損したペイロードを計算に含めることができます。Host-Bでは、フレームのCRC値が、イーサネットフレームのFCSフィールド内の0xABCD CRC値とは異なる16進数値0xDEADであると計算されます。このCRC値の違いは、イーサネットフレームがホストBに送信される間にホストBにイーサネットフレームが破損したことを示します。その結果、ホストBはこのイーサネットフレームの内容を信頼できないため、廃棄できます。通常、ホストBは、「input errors」、「CRC errors」、または「RX errors」カウンタなど、ネットワークインターフェイスカード(NIC)上の何らかのエラーカウンタを増加させることができます。

CRC エラーの一般的な症状

CRCエラーは通常、次の2つの方法のいずれかで発生します。

1. ネットワークに接続されたデバイスのインターフェイスのエラーカウンタが増加するか 0

以外になる。

2. ネットワークに接続されたデバイスが破損したフレームをドロップしたために、ネットワークを通過するトラフィックでパケット/フレームが失われる。

これらのエラーは、その時点で使用しているデバイスに応じて、わずかに異なる方法で発生します。以下のサブセクションで、デバイスのタイプごとに詳しく説明します。

Windows ホストでの受信エラー

WindowsホストでのCRCエラーは通常、コマンドプロンプトからのnetstat -eコマンドの出力に表示される、0以外のReceived Errorsカウンタとして現れます。Windowsホストのコマンドプロンプトからのゼロ以外のReceived Errorsカウンタの例を次に示します。

```
<#root>
```

```
>
```

```
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	

netstat -e コマンドによってレポートされる受信エラーの数を正確にするために、NIC とそのそれぞれのドライバは、NIC が受信する CRC エラーの計算をサポートしている必要があります。最近のほとんどの NIC とそのそれぞれのドライバは、NIC が受信する CRC エラーの正確な計算をサポートしています。

Linux ホストでの RX エラー

LinuxホストのCRCエラーは、通常ifconfigコマンドの出力に表示される0以外の「RX errors」カウンタとして現れます。Linuxホストのゼロ以外のRXエラーカウンタの例を次に示します。

```
<#root>
```

```
$
```

```
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
```

Linux ホストの CRC エラーは、`ip -s link show` コマンドの出力に 0 以外の RX エラーカウンタとして表示される場合もあります。Linuxホストのゼロ以外のRXエラーカウンタの例を次に示します。

```
<#root>
```

```
$
```

```
ip -s link show eth0
```

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DEFAULT group default qlen 1
    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
```

`ifconfig` コマンドまたは `ip -s link show` コマンドによってレポートされる RX エラーの数を正確にするために、NIC とそのそれぞれのドライバは、NIC が受信する CRC エラーの計算をサポートしている必要があります。最近のほとんどの NIC とそのそれぞれのドライバは、NIC が受信する CRC エラーの正確な計算をサポートしています。

ネットワークデバイスでの CRC エラー

ネットワークデバイスは、次の2つの転送モードのいずれかで動作します。

- ストアアンドフォワードフォワーディングモード
- カットスルーフォワーディングモード

ネットワークデバイスが受信したCRCエラーを処理する方法は、転送モードによって異なります。次のサブセクションでは、各転送モードの具体的な動作について説明します。

ストアアンドフォワード ネットワーク デバイスでの入力エラー

ストアアンドフォワードフォワーディングモードで動作しているネットワークデバイスは、フレ

ームを受信すると、フレームのCRC値を検証する前にフレーム全体をバッファリングし(「Store」)、フレームの転送を決定し、フレームをインターフェイスから送信します(「Forward」)。したがって、ストアアンドフォワードフォワーディングモードで動作しているネットワークデバイスが、特定のインターフェイス上で、不正なCRC値を持つ破損したフレームを受信すると、そのフレームをドロップし、インターフェイスの「入力エラー」カウンタを増やすことができます。

つまり、破損したイーサネットフレームは、ストアアンドフォワードフォワーディングモードで動作するネットワークデバイスによって転送されず、入力でドロップされます。

Cisco Nexus 7000 および 7700 シリーズ スイッチは、ストアアンドフォワード転送モードで動作します。Nexus 7000または7700シリーズスイッチの入力エラーカウンタとCRC/FCSカウンタの値がゼロ以外になる例を次に示します。

<#root>

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 runs 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 エラーは、show interface counters errors の出力に 0 以外の FCS エラー (FCS-Err) カウンタとして表示される場合もあります。このコマンドの出力にある「Rcv-Err」カウンタにも、ゼロ以外の値がある場合があります。この値は、インターフェイスが受信したすべての入力エラー (CRCなど) の合計です。次に例を示します。

<#root>

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

カットスルー ネットワーク デバイスでの入出力エラー

カットスルーフォワーディングモードで動作しているネットワークデバイスがフレームを受信し始めると、そのネットワークデバイスはフレームヘッダーで転送決定を行い、有効な転送決定を行うのに十分なフレームを受信するとすぐに、インターフェイスからフレームを送信し始めることができます。フレームヘッダーとパケットヘッダーはフレームの先頭にあるため、この転送判断は、通常、フレームのペイロードが受信される前に行われます。

イーサネットフレームの FCS フィールドは、フレームの最後 (フレームのペイロードの直後) にあります。したがって、カットスルーフォワーディングモードで動作しているネットワークデバイスでは、フレームのCRCを計算できる時点までに、すでに別のインターフェイスからフレームの送信を開始している場合があります。フレームに関してネットワークデバイスによって計算されたCRCが、FCSフィールドに存在するCRC値と一致しない場合は、ネットワークデバイスが破損したフレームをネットワークに転送したことを意味します。この場合、ネットワークデバイスは次の2つのカウンタを増分できます。

1. 破損したフレームが最初に受信されたインターフェイスの入力エラー (Input Errors) カウンタ。
2. 破損したフレームが送信されたすべてのインターフェイスの出力エラー (Output Errors) カウンタ。ユニキャストトラフィックの場合、通常は単一のインターフェイスを使用します。ただし、ブロードキャスト、マルチキャスト、または不明なユニキャストトラフィックの場合は、1つ以上のインターフェイスを使用します。

この例を次に示します。ここで、show interfaceコマンドの出力は、ネットワークデバイスのカットスルー転送モードが原因で、複数の破損フレームがネットワークデバイスのEthernet1/1で受信され、Ethernet1/2から送信されたことを示しています。

```
<#root>
```

```
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 エラーは、show interface counters errors の出力で、入インターフェイスの 0 以外の FCS エラー (FCS-Err) カウンタおよび出インターフェイスの 0 以外の転送エラー (Xmit-Err) カウンタとして表示される場合もあります。このコマンドの出力にある入インターフェイスの「 Rcv-Err」カウンタにも、ゼロ以外の値がある場合があります。この値は、インターフェイスが受信したすべての入力エラー (CRCその他のエラー) の合計です。次に例を示します。

<#root>

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	0	0	0	0

```
-----
```

また、ネットワークデバイスは、アップストリームネットワークデバイスに対して、このフレームが破損していることを示す特定の方法で、フレームのFCSフィールドのCRC値を変更することもできます。この動作は、CRCの「ストンピング」と呼ばれます。CRCが変更される正確な方法はプラットフォームによって異なりますが、通常はフレームのFCSフィールドに存在する現在のCRC値が反転します。次に例を示します。

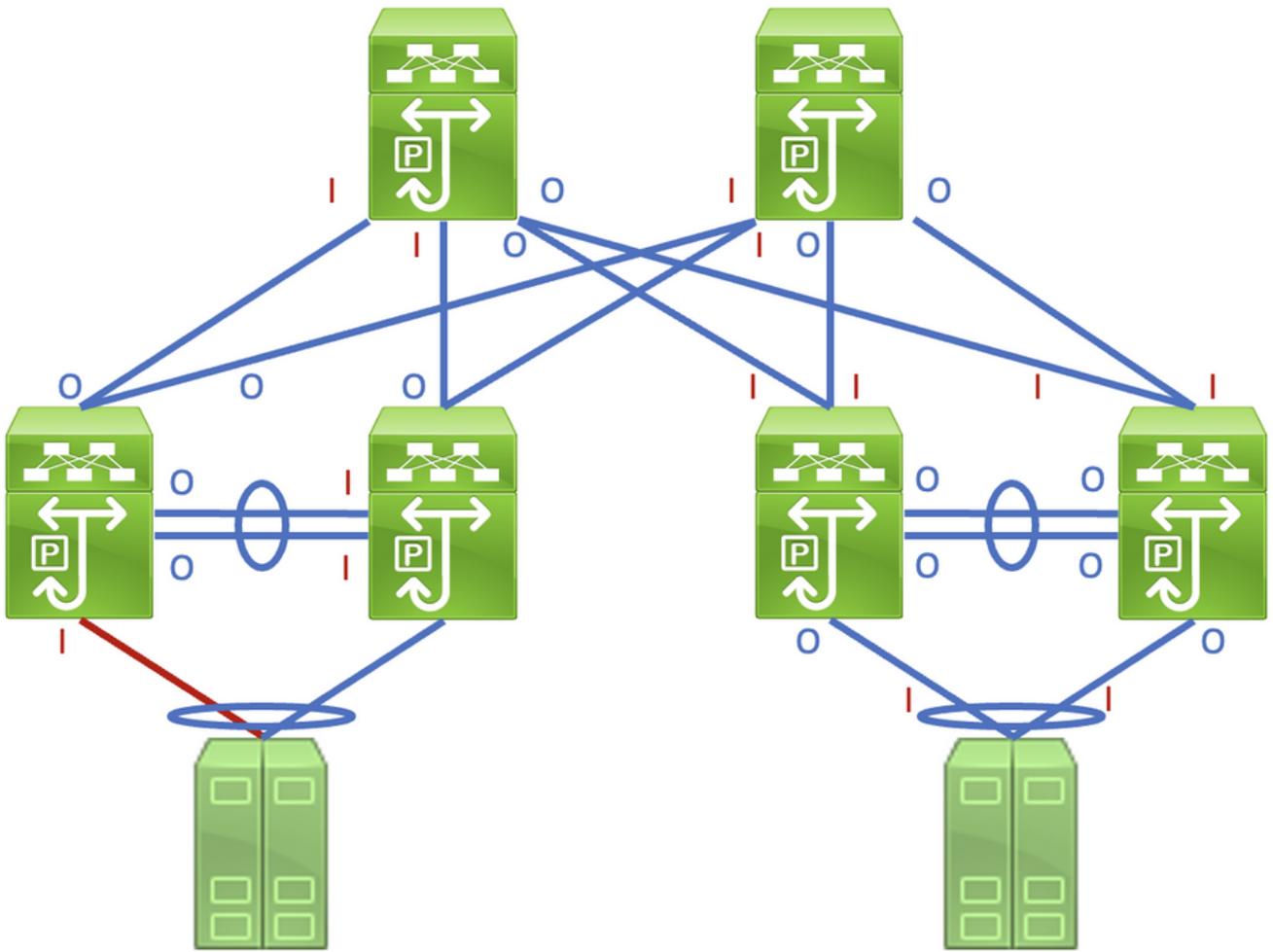
Original CRC: 0xABCD (1010101111001101)
Stomped CRC: 0x5432 (0101010000110010)

この動作の結果として、カットスルーフォワーディングモードで動作するネットワークデバイスは、ネットワーク全体に破損フレームを伝播する可能性があります。ネットワークがカットスルーフォワーディングモードで動作する複数のネットワークデバイスで構成されている場合、単一の破損したフレームによって、ネットワーク内の複数のネットワークデバイスで入力エラーと出力エラーカウンタが増加する可能性があります。

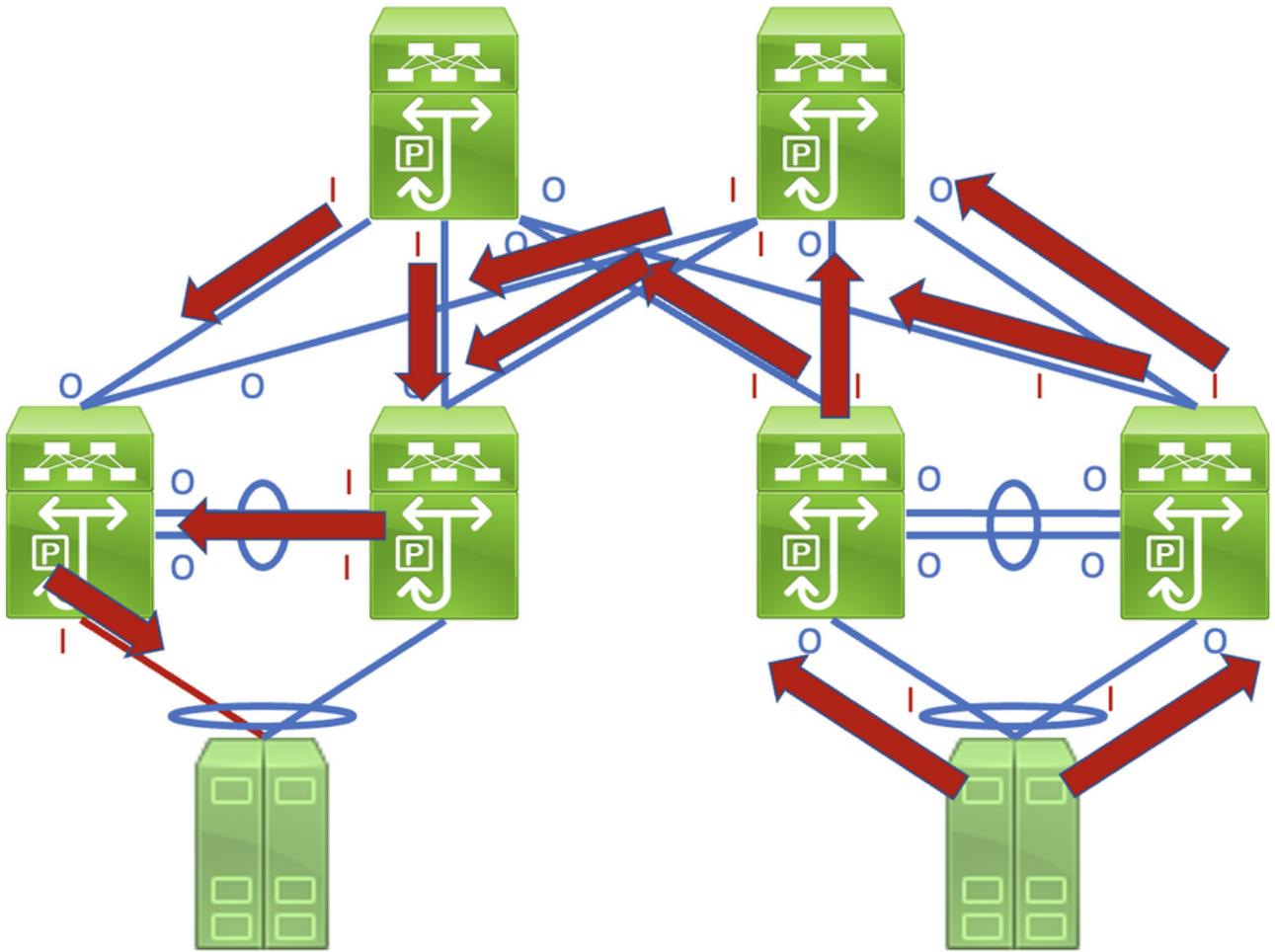
CRC エラーのトレースおよび分離

CRCエラーの根本原因を特定して解決するための最初のステップは、CRCエラーの原因をネットワーク内の2つのデバイス間の特定のリンクに切り分けることです。このリンクに接続された一方のデバイスでは、値がゼロのインターフェイス出力エラーカウンタまたは増加していないインターフェイス出力エラーカウンタが表示される場合があります。一方、このリンクに接続された他方のデバイスでは、ゼロ以外のインターフェイス出力エラーカウンタまたは増加しているインターフェイス入力エラーカウンタが表示される場合があります。これは、一方のデバイスのインターフェイスから出力されたトラフィックがそのままリモートデバイスへの送信時に破損しており、リンク上の他方のデバイスの入力インターフェイスによって入力エラーとしてカウントされることを示唆します。

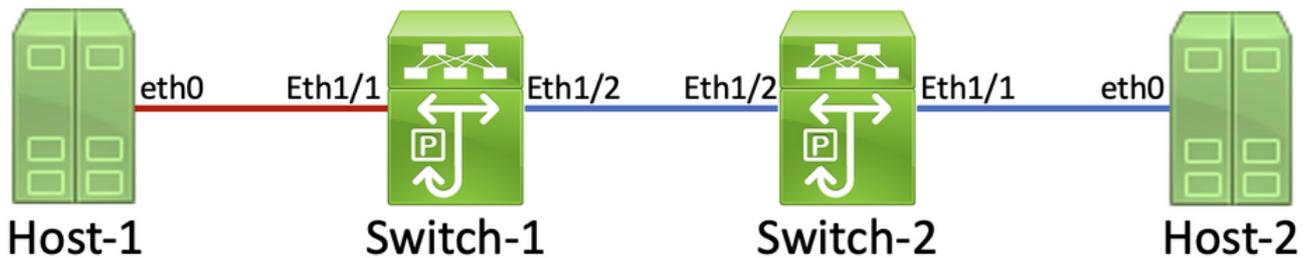
ストアアンドフォワードフォワーディングモードで動作するネットワークデバイスで構成されるネットワークでこのリンクを特定するのは、簡単な作業です。ただし、カットスルーフォワーディングモードで動作するネットワークデバイスで構成されるネットワークでこのリンクを識別する場合は、多くのネットワークデバイスでゼロ以外の入力および出力エラーカウンタを持つことができるため、より困難です。この現象の例は、次のトポロジで確認できます。このトポロジでは、赤で強調表示されているリンクが損傷を受けているため、リンクを通過するトラフィックが破損しています。赤色の「I」のラベルが付いたインターフェイスは、入力エラーカウンタが0以外になる可能性のあるインターフェイスを示し、青色の「O」のラベルが付いたインターフェイスは、出力エラーカウンタが0以外になる可能性のあるインターフェイスを示しています。



このドキュメントでは、インターフェイスカウンタで見られる巡回冗長検査(CRC)エラーと、Cisco Nexusスイッチの統計情報について説明します。



損傷したリンクをトレースして特定する詳細なプロセスは、例を使用して示すのが最も効果的です。次のトポロジについて考えてみます。



このトポロジでは、Switch-1という名前のNexusスイッチのインターフェイスEthernet1/1が、Host-1のネットワークインターフェイスカード(NIC)eth0を介してHost-1という名前のホストに接続されています。Switch-1のインターフェイスEthernet1/2は、Switch-2のインターフェイスEthernet1/2を介して、Switch-2という名前の2番目のNexusスイッチに接続されています。スイッチ2のインターフェイスEthernet1/1は、ホスト2のNIC eth0を介してホスト2という名前のホストに接続されています。

スイッチ1のEthernet1/1インターフェイスを経由するホスト1とスイッチ1の間のリンクが破損し、リンクを通過するトラフィックが断続的に破損する。ただし、リンクが損傷しているかどうかは、現時点では不明です。破損したフレームがネットワーク内に残るパスを、ゼロ以外の入力および出力エラーカウンタまたは増分された入力および出力エラーカウンタでトレースして、この

ネットワーク内の破損したリンクを見つける必要があります。

この例では、ホスト2 NICはCRCエラーを受信していることを報告します。

```
<#root>
```

```
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
```

ホスト2 NICがインターフェイスEthernet1/1を介してスイッチ2に接続していることがわかっています。show interfaceコマンドを使用すると、インターフェイスEthernet1/1の出力エラーカウンタがゼロ以外になっていることを確認できます。

```
<#root>
```

```
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
```

インターフェイス Ethernet1/1 の出力エラーカウンタが 0 ではないため、Switch-2 では、高い確率で別のインターフェイスが 0 以外の入力エラーカウンタを持ちます。Switch-2 のインターフェイスに 0 以外の入力エラーカウンタがあるかどうかを確認するには、show interface counters errors non-zero コマンドを使用します。

```
<#root>
```

```
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
```

Switch-2 の Ethernet1/2 に 0 以外の入力エラーカウンタがあることが分かります。これは、

Switch-2 がこのインターフェイスで破損したトラフィックを受信していることを示しています。どのデバイスが Switch-2 の Ethernet1/2 に接続されているかは、Cisco Discovery Protocol (CDP) または Link Local Discovery Protocol (LLDP) 機能によって確認できます。この例として、show cdp neighbors コマンドを使用した場合を次に示します。

```
<#root>
```

```
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
```

```
(FD012345678)
```

```
Eth1/2
```

```
125    R S I s    N9K-C93180YC-
```

```
Eth1/2
```

これで、Switch-2がEthernet1/2インターフェイスでSwitch-1のEthernet1/2インターフェイスから破損したトラフィックを受信していることがわかりましたが、Switch-1のEthernet1/2とSwitch-2のEthernet1/2間のリンクが破損して破損を引き起こしているかどうかはまだわかりません。また、Switch-1が破損したトラフィックを転送するカットスルースイッチである場合は、受信していることがわかります。これを確認するには、Switch-1 にログインする必要があります。

show interfaces コマンドを使用すると、Switch-1 の Ethernet1/2 インターフェイスに 0 以外の出力エラーカウンタがあることを確認できます。

```
<#root>
```

```
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
```

Switch-1 の Ethernet1/2 に 0 以外の出力エラーカウンタがあることが分かります。このことは、スイッチ1のEthernet1/2とスイッチ2のEthernet1/2の間のリンクが破損していないことを示しています。その代わりに、スイッチ1は、他のインターフェイスで受信する破損トラフィックを転送するカットスルースイッチです。前にSwitch-2で示したように、show interface counters errors non-zeroコマンドを使用して、Switch-1のインターフェイスのいずれかにゼロ以外の入力エラーカウンタがあるかどうかを確認できます。

<#root>

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-Co1	Multi-Co1	Late-Co1	Exces-Co1	Carri-Sen	Runts

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

Port	InDiscards					

Switch-1 の Ethernet1/1 に 0 以外の入力エラーカウンタがあることが分かります。これは、Switch-1 がこのインターフェイスで破損したトラフィックを受信していることを示しています。このインターフェイスはホスト1のeth0 NICに接続しています。Host-1のeth0 NICインターフェイスの統計情報を調べると、Host-1がこのインターフェイスから破損したフレームを送信しているかどうかを確認できます。

<#root>

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
```

Host-1のeth0 NIC統計情報は、ホストが破損したトラフィックを送信していないことを示しています。これは、Host-1 の eth0 と Switch-1 の Ethernet1/1 の間のリンクが損傷しており、このトラフィック破損の発生源となっていることを示しています。このリンクをトラブルシューティングして、この破損を引き起こしている障害のあるコンポーネントを特定し、交換する必要があります。

CRC エラーの根本原因

CRC エラーの最も一般的な根本原因は、2 つのデバイス間にある物理リンクのコンポーネントの損傷または誤動作です。次に例を示します。

- 物理メディア (銅線または光ファイバ) や直接接続ケーブル (DAC) の障害または損傷。
- トランシーバ/光学部品の障害または損傷。
- パッチパネルポートの障害または損傷。
- ネットワークデバイスハードウェアの障害 (特定のポート、ラインカードの特定用途向け集積回路[ASIC]、メディアアクセス制御[MAC]、ファブリックモジュールなど) 。
- ホストに挿入されたネットワーク インターフェイス カードの誤動作。

また、1つまたは複数の不適切に設定されたデバイスが、ネットワーク内で意図しない CRC エラーを発生させる可能性もあります。この例としては、ネットワーク内の2つ以上のデバイス間で最大伝送ユニット(MTU)の設定が一致していないために、大きなパケットが正しく切り捨てられないことがあります。この設定の問題を特定して解決すると、ネットワーク内のCRCエラーも修正できます。

CRC エラーの解決

特定の誤動作コンポーネントは、消去法によって特定できます。

- 物理メディア (銅線または光ファイバ) や DAC を、問題のないことが分かっている同じタイプの物理メディアと交換します。
- 1つのデバイスインターフェイスに挿入されたトランシーバを、同じモデルの正常なトランシーバと交換します。それでもCRCエラーが解決しない場合は、他のデバイスインターフェイスに挿入されたトランシーバを、同じモデルの正常なトランシーバと交換します。
- 損傷したリンクの一部としてパッチパネルが使用されている場合は、リンクを、そのパッチパネルの問題のないことが分かっているポートに移動させます。または、パッチパネルを使用せずにリンクを接続して、可能であればパッチパネルを根本的な原因から除外します。
- 損傷したリンクを、各デバイスの問題のないことが分かっている別のポートに移動させます。MAC、ASIC、またはラインカードの障害を切り分けるために、複数の異なるポートをテストする必要がある場合があります。
- 損傷したリンクにホストが関係している場合は、リンクをホストの別の NIC に移動させます。または、破損したリンクを正常なホストに接続し、ホストNICの障害を切り分けます。

誤動作しているコンポーネントがシスコ製品 (シスコのネットワークデバイスやトランシーバなど) で、有効なサポート契約でカバーされている場合は、[Cisco TACでサポートケースをオープンし](#)、問題の詳細を記入して、Return Material Authorization(RMA)で誤動作しているコンポーネントを交換してください。

関連情報

- [『Nexus 9000 Cloud Scale ASIC CRC Identification & Tracing Procedure』](#)

- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。