Compreender erros de verificação de redundância cíclica em switches Nexus

Contents

Introduction

Este documento descreve os detalhes sobre erros de Cyclic Redundancy Check (CRC) observados nos contadores de interface e nas estatísticas dos switches Cisco Nexus.

Prerequisites

Requirements

A Cisco recomenda que você compreenda os conceitos básicos de switching Ethernet e a CLI (Command Line Interface, interface de linha de comando) do Cisco NX-OS. Para obter mais informações, consulte um destes documentos aplicáveis:

- Guia de configuração básica do Cisco Nexus 9000 NX-OS, versão 10.2(x)
- Guia de configuração básica do Cisco Nexus 9000 Series NX-OS, versão 9.3(x)
- Guia de configuração básica do Cisco Nexus 9000 Series NX-OS, versão 9.2(x)
- Guia de configuração básica do Cisco Nexus 9000 Series NX-OS, versão 7.x

- Troubleshooting de Ethernet

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Switches Nexus 9000 Series iniciando a partir do software NX-OS versão 9.3(8)
- Switches Nexus 3000 Series iniciando a partir do software NX-OS versão 9.3(8)

As informações apresentadas neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Este documento descreve detalhes sobre erros de Cyclic Redundancy Check (CRC) observados em contadores de interface em switches Cisco Nexus Series. Este documento descreve o que é um CRC, como ele é usado no campo Frame Check Sequence (FCS) dos quadros Ethernet, como os erros de CRC se manifestam nos switches Nexus, como os erros de CRC interagem nos cenários de switching Store-and-Forward e Cut-Through, as causas raiz mais prováveis dos erros de CRC e como solucionar e resolver erros de CRC.

Hardware aplicável

As informações neste documento aplicam-se a todos os switches Cisco Nexus Series. Algumas das informações neste documento também podem ser aplicáveis a outras plataformas de roteamento e comutação da Cisco, como roteadores e switches Cisco Catalyst.

Definição de CRC

Um CRC é um mecanismo de detecção de erros comumente usado em computadores e redes de armazenamento para identificar dados alterados ou corrompidos durante a transmissão. Quando um dispositivo conectado à rede precisa transmitir dados, o dispositivo executa um algoritmo de computação baseado em códigos cíclicos em relação aos dados que resultam em um número de comprimento fixo. Esse número de comprimento fixo é chamado de valor CRC, mas coloquialmente, é frequentemente chamado de CRC para abreviação. Esse valor de CRC é adicionado aos dados e transmitido através da rede em direção a outro dispositivo. Este dispositivo remoto executa o mesmo algoritmo de código cíclico em relação aos dados e compara o valor resultante com o CRC anexado aos dados. Se ambos os valores corresponderem, o dispositivo remoto assume que os dados foram transmitidos pela rede sem estarem corrompidos. Se os valores não corresponderem, o dispositivo remoto assume que os dados foram corrompidos durante a transmissão pela rede. Esses dados corrompidos não podem ser confiáveis e são descartados.

Os CRCs são usados para detecção de erros em várias tecnologias de rede de computadores, como Ethernet (variantes com e sem fio), Token Ring, ATM (Asynchronous Transfer Mode Modo de Transferência Assíncrona) e Frame Relay. Os quadros Ethernet têm um campo FCS (Frame

Check Sequence, Sequência de Verificação de Quadro) de 32 bits no final do quadro (imediatamente após o payload do quadro) em que um valor CRC de 32 bits é inserido.

Por exemplo, considere um cenário em que dois hosts chamados Host-A e Host-B estejam diretamente conectados um ao outro por meio de suas NICs (Network Interface Cards, placas de interface de rede). O Host-A precisa enviar a frase "Este é um exemplo" para o Host-B através da rede. O Host-A cria um quadro Ethernet destinado ao Host-B com um payload de "Este é um exemplo" e calcula que o valor CRC do quadro é um valor hexadecimal de 0xABCD. O Host-A insere o valor de CRC de 0xABCD no campo FCS do quadro Ethernet e, em seguida, transmite o quadro Ethernet da placa de rede do Host-A para o Host-B.

Quando o Host-B receber esse quadro, ele calculará o valor CRC do quadro com o uso exato do mesmo algoritmo do Host-A. O Host-B calcula que o valor de CRC do quadro é um valor hexadecimal de 0xABCD, o que indica ao Host-B que o quadro Ethernet não foi corrompido enquanto o quadro foi transmitido ao Host-B.

Definição de erro CRC

Um erro de CRC ocorre quando um dispositivo (um dispositivo de rede ou um host conectado à rede) recebe um quadro Ethernet com um valor de CRC no campo FCS do quadro que não corresponde ao valor de CRC calculado pelo dispositivo para o quadro.

Este conceito é melhor demonstrado através de um exemplo. Considere um cenário em que dois hosts chamados Host-A e Host-B estejam diretamente conectados entre si por meio de suas NICs (Network Interface Cards, placas de interface de rede). O Host-A precisa enviar a frase "Este é um exemplo" para o Host-B através da rede. O Host-A cria um quadro Ethernet destinado ao Host-B com um payload de "Este é um exemplo" e calcula que o valor CRC do quadro é o valor hexadecimal 0xABCD. O Host-A insere o valor de CRC de 0xABCD no campo FCS do quadro Ethernet e, em seguida, transmite o quadro Ethernet da placa de rede do Host-A para o Host-B.

No entanto, danos no meio físico que conecta o Host-A ao Host-B corrompem o conteúdo do quadro de forma que a frase dentro do quadro mude para "Este foi um exemplo" em vez do payload desejado de "Este é um exemplo".

Quando o Host-B receber esse quadro, ele calculará o valor CRC do quadro, incluindo o payload corrompido. O Host-B calcula que o valor CRC do quadro é um valor hexadecimal de 0xDEAD, que é diferente do valor CRC 0xABCD dentro do campo FCS do quadro Ethernet. Essa diferença nos valores de CRC informa ao Host-B que o quadro Ethernet foi corrompido enquanto o quadro foi transmitido ao Host-B. Como resultado, o Host-B não pode confiar no conteúdo desse quadro Ethernet, então ele o descartará. O Host-B normalmente incrementará algum tipo de contador de erros em sua placa de rede (NIC), como os "erros de entrada", "erros de CRC" ou os contadores de "erros de RX".

Sintomas comuns de erros de CRC

Os erros de CRC geralmente se manifestam de duas maneiras:

1. Incrementando ou não zero contadores de erros em interfaces de dispositivos conectados à rede.
2. Perda de pacotes/quadros para o tráfego que atravessa a rede devido à queda de quadros

corrompidos por dispositivos conectados à rede.

Esses erros se manifestam de maneiras ligeiramente diferentes, dependendo do dispositivo com o qual você está trabalhando. Essas subseções entram em detalhes para cada tipo de dispositivo.

Erros Recebidos em Hosts do Windows

Erros de CRC em hosts Windows geralmente se manifestam como um contador de **Erros Recebidos** diferente de zero exibido na saída do comando **netstat -e** do prompt de comando. Um exemplo de um contador de Erros Recebidos diferente de zero do Prompt de Comando de um host do Windows está aqui:

```
>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
```

A placa de rede e seu respectivo driver devem suportar a contabilização de erros de CRC recebidos pela placa de rede para que o número de erros recebidos relatados pelo comando **netstat -e** seja exato. A maioria das placas de rede modernas e seus respectivos drivers suportam a contabilização precisa dos erros de CRC recebidos pela placa de rede.

Erros de RX em hosts Linux

Erros de CRC em hosts Linux geralmente se manifestam como um contador de "erros de RX" diferentes de zero exibido na saída do comando **ifconfig**. Um exemplo de um contador de erros de RX diferentes de zero de um host Linux está aqui:

```
$ 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
```

Erros de CRC em hosts Linux também podem se manifestar como um contador de "erros de RX" diferentes de zero exibido na saída do comando **ip -s link show**. Um exemplo de um contador de erros de RX diferentes de zero de um host Linux está aqui:

```
$ 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
```

A placa de rede e seu respectivo driver devem suportar a contabilização de erros de CRC recebidos pela placa de rede para que o número de erros de RX relatados pelos comandos **ifconfig** ou **ip -s link show** seja exato. A maioria das placas de rede modernas e seus respectivos drivers suportam a contabilização precisa dos erros de CRC recebidos pela placa de rede.

Erros de CRC em dispositivos de rede

Os dispositivos de rede operam em um de dois modos de encaminhamento: modo de encaminhamento Store-and-Forward e modo de encaminhamento Cut-Through. A maneira como um dispositivo de rede lida com um erro de CRC recebido varia dependendo de seus modos de encaminhamento. As subseções aqui descreverão o comportamento específico para cada modo de encaminhamento.

Erros de entrada em dispositivos de rede store-and-forward

Quando um dispositivo de rede operando em um modo de encaminhamento Store-and-Forward recebe um quadro, o dispositivo de rede armazenará o quadro inteiro em buffer ("Loja") antes que você valide o valor CRC do quadro, tome uma decisão de encaminhamento no quadro e transmita o quadro a partir de uma interface ("Encaminhar"). Portanto, quando um dispositivo de rede operando em um modo de encaminhamento Store-and-Forward recebe um quadro corrompido com um valor de CRC incorreto em uma interface específica, ele descartará o quadro e incrementará o contador "Erros de entrada" na interface.

Em outras palavras, quadros Ethernet corrompidos não são encaminhados por dispositivos de rede que operam em um modo de encaminhamento Store-and-Forward; eles são abandonados na entrada.

Os switches Cisco Nexus 7000 e 7700 Series operam em um modo de encaminhamento Store-and-Forward. Um exemplo de um contador de erros de entrada diferentes de zero e um contador CRC/FCS diferente de zero de um switch Nexus 7000 ou 7700 Series está aqui:

```
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
```

Os erros de CRC também podem se manifestar como um contador "FCS-Err" diferente de zero na saída de erros **show interface counters**. O contador "Rcv-Err" na saída desse comando também terá um valor diferente de zero, que é a soma de todos os erros de entrada (CRC ou outros) recebidos pela interface. Um exemplo disso é mostrado aqui:

```
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
```

Erros de entrada e saída em dispositivos de rede cut-through

Quando um dispositivo de rede operando em um modo de encaminhamento Cut-Through começa a receber um quadro, o dispositivo de rede tomará uma decisão de encaminhamento no cabeçalho do quadro e começará a transmitir o quadro a partir de uma interface assim que receber o suficiente do quadro para tomar uma decisão de encaminhamento válida. Como os cabeçalhos do quadro e do pacote estão no início do quadro, essa decisão de encaminhamento é geralmente tomada antes do recebimento do payload do quadro.

O campo FCS de um quadro Ethernet está no final do quadro, imediatamente após o payload do quadro. Portanto, um dispositivo de rede operando em um modo de encaminhamento Cut-Through já terá começado a transmitir o quadro de outra interface quando puder calcular o CRC do quadro. Se o CRC calculado pelo dispositivo de rede para o quadro não corresponder ao valor CRC presente no campo FCS, isso significa que o dispositivo de rede encaminhou um quadro corrompido para a rede. Quando isso acontece, o dispositivo de rede incrementará dois contadores:

1. O contador "Erros de entrada" na interface onde o quadro corrompido foi originalmente recebido.
2. O contador "Erros de saída" em todas as interfaces em que o quadro corrompido foi transmitido. Para o tráfego unicast, isso geralmente será uma única interface - no entanto, para tráfego de broadcast, multicast ou unicast desconhecido, isso pode ser uma ou mais interfaces.

Um exemplo disso é mostrado aqui, onde a saída do comando **show interface** indica que vários quadros corrompidos foram recebidos em Ethernet1/1 do dispositivo de rede e transmitidos para fora da Ethernet1/2 devido ao modo de encaminhamento Cut-Through do dispositivo de rede:

```
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
```

Os erros de CRC também podem se manifestar como um contador "FCS-Err" diferente de zero na interface de entrada e contadores "Xmit-Err" diferentes de zero nas interfaces de saída na saída de erros **show interface counters**. O contador "Rcv-Err" na interface de entrada na saída desse

comando também terá um valor diferente de zero, que é a soma de todos os erros de entrada (CRC ou outros) recebidos pela interface. Um exemplo disso é mostrado aqui:

```
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
```

O dispositivo de rede também modificará o valor de CRC no campo FCS do quadro de uma maneira específica que significa para dispositivos de rede upstream que esse quadro está corrompido. Esse comportamento é conhecido como "piscar" o CRC. A maneira precisa como o CRC é modificado varia de uma plataforma a outra, mas geralmente envolve a inversão do valor atual de CRC presente no campo FCS do quadro. Um exemplo disso está aqui:

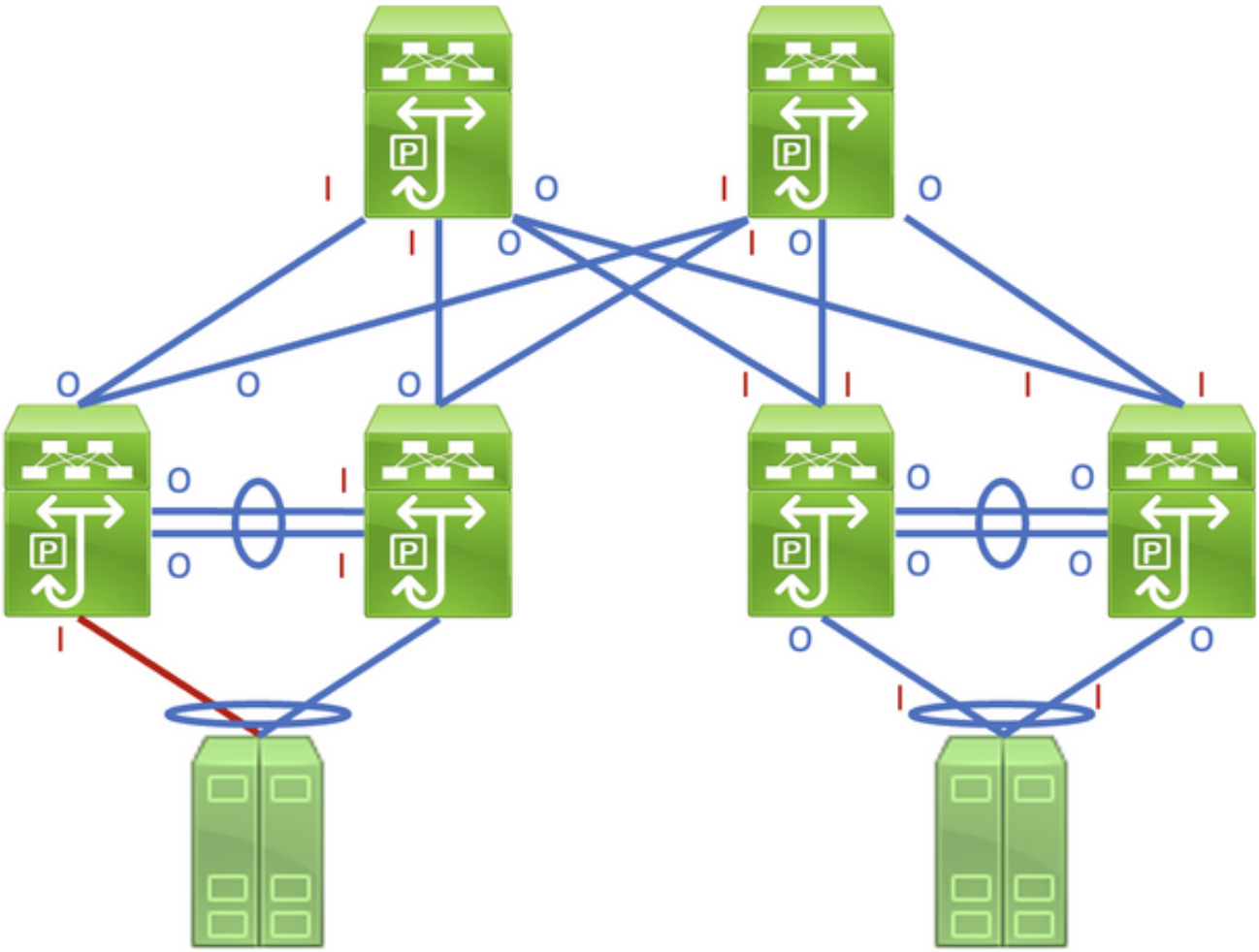
```
Original CRC: 0xABCD (1010101111001101)
Stomped CRC:  0x5432 (0101010000110010)
```

Como resultado desse comportamento, os dispositivos de rede que operam em um modo de encaminhamento Cut-Through podem propagar um quadro corrompido em toda a rede. Se uma rede consiste em vários dispositivos de rede operando em um modo de encaminhamento Cut-Through, um único quadro corrompido pode causar erros de entrada e contadores de erro de saída para incrementar em vários dispositivos de rede dentro da rede.

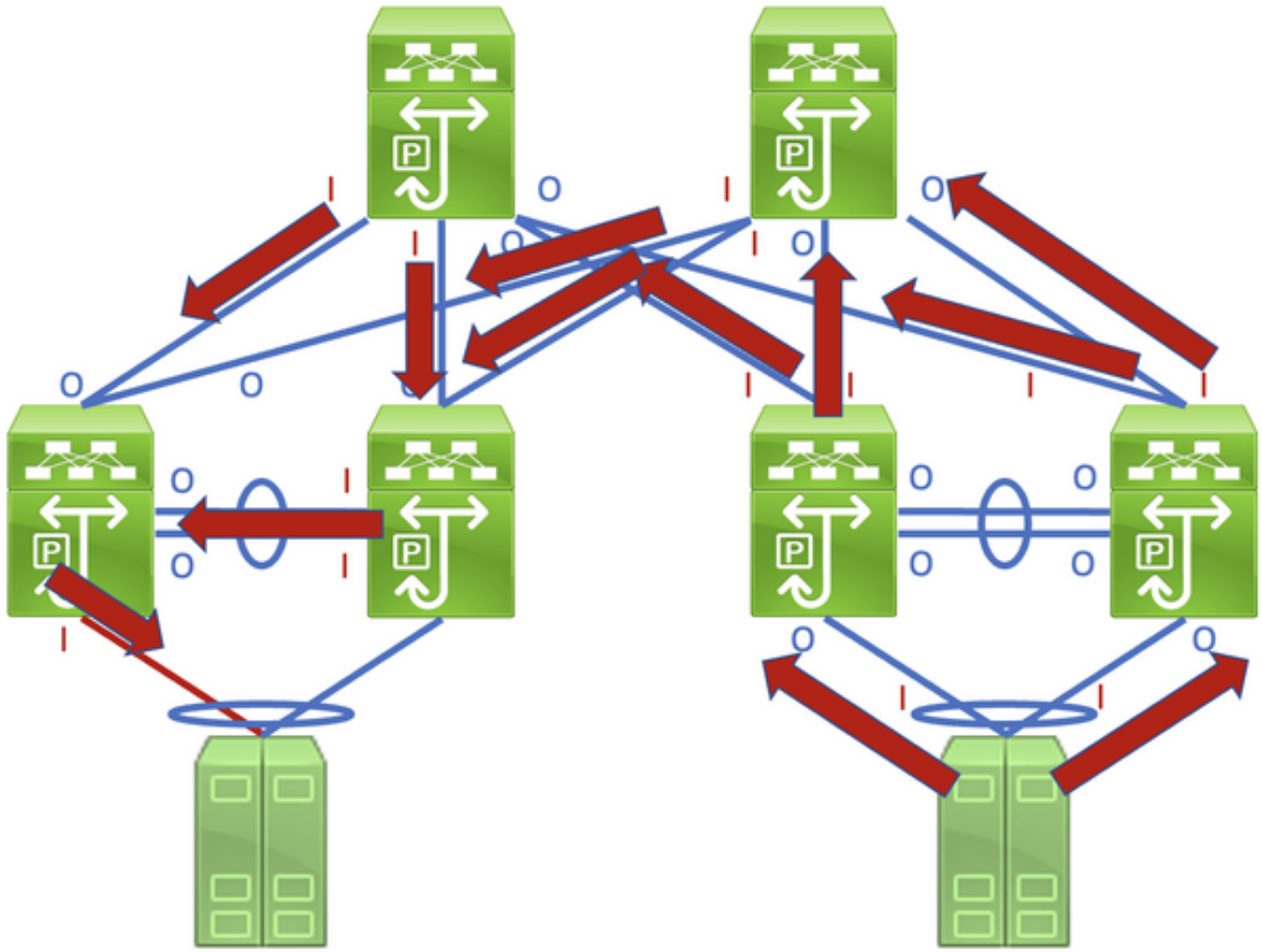
Rastrear e isolar erros de CRC

A primeira etapa para identificar e resolver a causa raiz dos erros de CRC é isolar a origem dos erros de CRC em um link específico entre dois dispositivos na rede. Um dispositivo conectado a esse link terá um contador de erros de saída de interface com um valor zero ou não está aumentando, enquanto o outro dispositivo conectado a esse link terá um contador de erros de entrada de interface diferente de zero ou incrementando. Isso sugere que o tráfego deixa a interface de um dispositivo intacto corrompida no momento da transmissão para o dispositivo remoto e é contado como um erro de entrada pela interface de entrada do outro dispositivo no link.

Identificar esse link em uma rede que consiste em dispositivos de rede operando em um modo de encaminhamento Store-and-Forward é uma tarefa simples. No entanto, é mais difícil identificar esse link em uma rede que consiste em dispositivos de rede operando em um modo de encaminhamento Cut-Through, já que muitos dispositivos de rede terão contadores de erro de entrada e saída diferentes de zero. Um exemplo desse fenômeno pode ser visto na topologia aqui, onde o link destacado em vermelho é danificado de forma que o tráfego que atravessa o link seja corrompido. As interfaces rotuladas com um "I" vermelho indicam interfaces que podem ter erros de entrada diferentes de zero, enquanto as interfaces rotuladas com um "O" azul indicam interfaces que podem ter erros de saída diferentes de zero.



A identificação do link defeituoso exige que você rastreie recursivamente os quadros corrompidos do "caminho" seguidos na rede por meio de contadores de erro de entrada e saída diferentes de zero, com erros de entrada diferentes de zero apontando para upstream em direção ao link danificado na rede. Isso é demonstrado no diagrama aqui.



Um processo detalhado para rastrear e identificar um link danificado é melhor demonstrado por meio de um exemplo. Considere a topologia aqui:

Nesta topologia, a interface Ethernet1/1 de um switch Nexus chamado Switch-1 está conectada a um host chamado Host-1 através da NIC (Network Interface Card, placa de interface de rede) eth0 do Host-1. A interface Ethernet1/2 do Switch-1 está conectada a um segundo switch Nexus, chamado Switch-2, através da interface Ethernet1/2 do Switch-2. A interface Ethernet1/1 do Switch-2 está conectada a um host chamado Host-2 através da NIC eth0 do Host-2.

O link entre o Host-1 e o Switch-1 através da interface Ethernet1/1 do Switch-1 está danificado, fazendo com que o tráfego que atravessa o link seja corrompido intermitentemente. No entanto, ainda não sabemos se esta ligação está danificada. Devemos rastrear o caminho que os quadros corrompidos deixam na rede por meio de contadores de erro de entrada e saída diferentes de zero ou incrementando os contadores de erro de entrada e saída para localizar o link danificado nessa rede.

Neste exemplo, a placa de rede do Host 2 relata que está recebendo erros de CRC.

```
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
```

Você sabe que a placa de rede do Host-2 se conecta ao Switch-2 através da interface Ethernet1/1. Você pode confirmar se a interface Ethernet1/1 tem um contador de erros de saída diferente de zero com o comando **show interface**.

```
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
```

Como o contador de erros de saída da interface Ethernet1/1 é diferente de zero, é provável que outra interface do Switch-2 tenha um contador de erros de entrada diferente de zero. Você pode usar o comando **show interface counters errors non-zero** para identificar se alguma interface do Switch-2 tem um contador de erros de entrada diferente de zero.

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

Você pode ver que Ethernet1/2 do Switch-2 tem um contador de erros de entrada diferente de zero. Isso sugere que o Switch-2 recebe tráfego corrompido nessa interface. Você pode confirmar qual dispositivo está conectado à Ethernet1/2 do Switch-2 através dos recursos do Cisco Discovery Protocol (CDP) ou Link Local Discovery Protocol (LLDP). Um exemplo disso é mostrado aqui com o comando **show cdp neighbors**.

```
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
```

Você agora sabe que o Switch-2 está recebendo tráfego corrompido em sua interface Ethernet1/2 da interface Ethernet1/2 do Switch-1, mas ainda não sabe se o link entre Ethernet1/2 do Switch-1 e Ethernet1/2 do Switch-2 está danificado e causa corrupção, ou se o Switch-1 é um switch cut-through que encaminha tráfego corrompido que ele recebe. Você deve fazer login no Switch-1 para verificar isso.

Você pode confirmar que a interface Ethernet1/2 do Switch-1 tem um contador de erros de saída diferente de zero com o comando **show interfaces**.

```
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
```

Você pode ver que Ethernet1/2 do Switch-1 tem um contador de erros de saída diferente de zero. Isso sugere que o link entre a Ethernet1/2 do Switch-1 e a Ethernet1/2 do Switch-2 não está danificado - em vez disso, o Switch-1 é um switch cut-through que encaminha tráfego corrompido recebido em alguma outra interface. Como demonstrado anteriormente com o Switch-2, você pode usar o comando **show interface counters errors non-zero** para identificar se alguma interface do Switch-1 tem um contador de erros de entrada diferente de zero.

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

Você pode ver que Ethernet1/1 do Switch-1 tem um contador de erros de entrada diferente de zero. Isso sugere que o Switch-1 está recebendo tráfego corrompido nessa interface. Sabemos que essa interface se conecta à NIC eth0 do Host-1. Podemos revisar as estatísticas da interface NIC eth0 do Host-1 para confirmar se o Host-1 envia quadros corrompidos para fora dessa interface.

```
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
```

As estatísticas da placa de rede eth0 do Host-1 sugerem que o host não está transmitindo tráfego corrompido. Isso sugere que o link entre a Ethernet1/1 do Host-1 e a Ethernet do Switch-1 está danificado e é a fonte desse tráfego corrompido. Será necessário executar mais a solução de problemas neste link para identificar o componente defeituoso que está causando essa corrupção e substituí-lo.

Causas raiz de erros de CRC

A causa raiz mais comum de erros de CRC é um componente danificado ou com mau funcionamento de um link físico entre dois dispositivos. Os exemplos incluem:

- Meio físico com falha ou danificado (cobre ou fibra) ou cabos de conexão direta (DACs).
- Transceivers/ópticos com falha ou danificados.
- Portas do patch panel com falha ou danificadas.
- Hardware de dispositivo de rede defeituoso (incluindo portas específicas, ASICs (Application-Specific Integrated Circuits) de placa de linha, MACs (Media Access Controls), módulos de estrutura, etc.),
- Placa de interface de rede com mau funcionamento inserida em um host.

Também é possível que um ou mais dispositivos mal configurados causem inadvertidamente erros de CRC em uma rede. Um exemplo disso é uma incompatibilidade de configuração da Unidade de Transmissão Máxima (MTU - Maximum Transmission Unit) entre dois ou mais dispositivos na rede, fazendo com que pacotes grandes sejam truncados incorretamente. Identificar e resolver esse problema de configuração pode corrigir erros de CRC em uma rede também.

Resolver erros de CRC

Você pode identificar o componente de mau funcionamento específico por meio de um processo de eliminação:

1. Substitua o meio físico (cobre ou fibra) ou o DAC por um meio físico em boas condições do mesmo tipo.
2. Substitua o transceptor inserido na interface de um dispositivo por um transceptor em boas condições do mesmo modelo. Se isso não resolver os erros de CRC, substitua o transceptor inserido na interface do outro dispositivo por um transceptor em boas condições do mesmo modelo.
3. Se algum patch panel for usado como parte do link danificado, mova o link para uma porta em boas condições no patch panel. Como alternativa, elimine o patch panel como uma possível causa raiz conectando o link sem usar o patch panel, se possível.
4. Mova o link danificado para uma porta diferente em boas condições em cada dispositivo. Você precisará testar várias portas diferentes para isolar uma falha de MAC, ASIC ou placa de linha.
5. Se o link danificado envolver um host, mova o link para uma placa de rede diferente no host. Como alternativa, conecte o link danificado a um host em boas condições para isolar uma falha da placa de rede do host.

Se o componente defeituoso for um produto da Cisco (como um dispositivo de rede ou transceptor da Cisco) coberto por um contrato de suporte ativo, você poderá abrir um caso de suporte com o Cisco TAC detalhando sua solução de problemas para que o componente defeituoso seja substituído por meio de uma RMA (Return Material Authorization, Autorização de Devolução de Material).

Informações Relacionadas

- Procedimento de identificação e rastreamento de CRC do Nexus 9000 Cloud Scale
- Suporte Técnico e Documentação - Cisco Systems