Comprender los errores de verificación de redundancia cíclica en los switches Nexus

Contenido

Introducción

Este documento describe los detalles sobre los errores de Verificación por redundancia cíclica (CRC) observados en los contadores de interfaz y las estadísticas de los switches Cisco Nexus.

Prerequisites

Requirements

Cisco recomienda que comprenda los conceptos básicos de switching Ethernet y la interfaz de línea de comandos (CLI) de Cisco NX-OS. Para obtener más información, consulte uno de estos documentos aplicables:

- Guía de configuración de los fundamentos de Cisco Nexus 9000 NX-OS, versión 10.2(x)
- Guía de configuración de los fundamentos de Cisco Nexus serie 9000 NX-OS, versión 9.3(x)
- Guía de configuración de los fundamentos de Cisco Nexus serie 9000 NX-OS, versión 9.2(x)
- Guía de configuración de los fundamentos de Cisco Nexus serie 9000 NX-OS, versión 7.x

- Resolución de problemas de Ethernet

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Switches Nexus serie 9000 a partir de la versión 9.3(8) del software NX-OS
- Switches Nexus serie 3000 a partir de la versión 9.3(8) del software NX-OS

La información de este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier 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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Este documento describe los detalles relacionados con los errores de Verificación por redundancia cíclica (CRC) observados en los contadores de interfaces en los switches de la serie Cisco Nexus. Este documento describe qué es un CRC, cómo se utiliza en el campo Secuencia de verificación de tramas (FCS) de las tramas Ethernet, cómo se manifiestan los errores CRC en los switches Nexus, cómo interactúan los errores CRC en los escenarios de conmutación de almacenamiento y reenvío y de conmutación de corte, las causas principales más probables de los errores CRC, y cómo solucionar y resolver los errores CRC.

Hardware aplicable

La información de este documento es aplicable a todos los switches Nexus de Cisco. Parte de la información de este documento también puede aplicarse a otras plataformas de routing y switching de Cisco, como routers y switches Cisco Catalyst.

Definición CRC

Un CRC es un mecanismo de detección de errores que se utiliza comúnmente en las redes informáticas y de almacenamiento para identificar los datos cambiados o dañados durante la transmisión. Cuando un dispositivo conectado a la red necesita transmitir datos, el dispositivo ejecuta un algoritmo de cálculo basado en códigos cíclicos contra los datos que resultan en un número de longitud fija. Este número de longitud fija se denomina valor CRC, pero coloquialmente, a menudo se denomina CRC para abreviar. Este valor CRC se agrega a los datos y se transmite a través de la red hacia otro dispositivo. Este dispositivo remoto ejecuta el mismo algoritmo de código cíclico con respecto a los datos y compara el valor resultante con el CRC agregado a los datos. Si ambos valores coinciden, el dispositivo remoto asume que los datos se transmitieron a través de la red sin estar dañados. Si los valores no coinciden, el dispositivo remoto asume que los datos se dañaron durante la transmisión a través de la red. Estos datos dañados no se pueden confiar y se descartan.

Los CRC se utilizan para la detección de errores en varias tecnologías de redes informáticas, como Ethernet (ambas variantes, por cable e inalámbricas), Token Ring, Asynchronous Transfer

Mode (ATM) y Frame Relay. Las tramas Ethernet tienen un campo de Secuencia de verificación de tramas (FCS) de 32 bits al final de la trama (inmediatamente después de la carga útil de la trama) donde se inserta un valor CRC de 32 bits.

Por ejemplo, considere un escenario en el que dos hosts denominados Host-A y Host-B estén directamente conectados entre sí a través de sus Tarjetas de Interfaz de Red (NIC). El Host A necesita enviar la frase "Este es un ejemplo" al Host-B a través de la red. El Host A crea una trama Ethernet destinada al Host-B con una carga útil de "Esto es un ejemplo" y calcula que el valor CRC de la trama es un valor hexadecimal de 0xABCD. Host-A inserta el valor CRC de 0xABCD en el campo FCS de la trama Ethernet y luego transmite la trama Ethernet fuera de la NIC del Host-A hacia el Host-B.

Cuando el Host B recibe esta trama, calculará el valor CRC de la trama con el uso del mismo algoritmo exacto que el Host-A. Host-B calcula que el valor CRC de la trama es un valor hexadecimal de 0xABCD, lo que indica al Host-B que la trama Ethernet no estaba dañada mientras la trama se transmitía al Host-B.

Definición de error CRC

Un error CRC ocurre cuando un dispositivo (ya sea un dispositivo de red o un host conectado a la red) recibe una trama Ethernet con un valor CRC en el campo FCS de la trama que no coincide con el valor CRC calculado por el dispositivo para la trama.

La mejor manera de demostrar este concepto es a través de un ejemplo. Considere un escenario en el que dos hosts denominados Host-A y Host-B se conectan directamente entre sí a través de sus tarjetas de interfaz de red (NIC). El Host A necesita enviar la frase "Este es un ejemplo" al Host-B a través de la red. El Host A crea una trama Ethernet destinada al Host-B con una carga útil de "Esto es un ejemplo" y calcula que el valor CRC de la trama es el valor hexadecimal 0xABCD. Host-A inserta el valor CRC de 0xABCD en el campo FCS de la trama Ethernet y luego transmite la trama Ethernet fuera de la NIC del Host-A hacia el Host-B.

Sin embargo, el daño en los medios físicos que conectan al Host A al Host B corrompe el contenido de la trama de modo que la frase dentro de la trama cambie a "Este fue un ejemplo" en lugar de la carga útil deseada de "Este es un ejemplo".

Cuando el Host B recibe esta trama, calcula el valor CRC de la trama, incluida la carga útil dañada. Host-B calcula que el valor CRC de la trama es un valor hexadecimal de 0xDEAD, que es diferente del valor CRC 0xABCD dentro del campo FCS de la trama Ethernet. Esta diferencia en los valores CRC indica al Host-B que la trama Ethernet estaba dañada mientras la trama se transmitía al Host-B. Como resultado, el Host-B no puede confiar en el contenido de esta trama Ethernet, por lo que la descartará. El host B normalmente incrementará también algún tipo de contador de errores en su tarjeta de interfaz de red (NIC), como los contadores de "errores de entrada", "errores CRC" o "errores RX".

Síntomas comunes de errores CRC

Los errores CRC normalmente se manifiestan de dos maneras:

1. Incrementar o no los contadores de errores en las interfaces de los dispositivos conectados a la red.
2. Pérdida de paquetes/tramas para el tráfico que atraviesa la red debido a que los dispositivos

conectados a la red descartan tramas dañadas.

Estos errores se manifiestan de maneras ligeramente diferentes dependiendo del dispositivo con el que esté trabajando. Estas subsecciones se detallan para cada tipo de dispositivo.

Errores recibidos en hosts de Windows

Los errores CRC en los hosts de Windows se manifiestan normalmente como un contador **de errores recibidos** distinto de cero que se muestra en la salida del comando **netstat -e** del símbolo del sistema. A continuación se muestra un ejemplo de un contador de errores recibidos que no es cero desde el símbolo del sistema de un host de Windows:

```
>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
```

La NIC y su controlador respectivo deben soportar la contabilización de los errores CRC recibidos por la NIC para que el número de errores recibidos reportados por el **comando netstat -e** sea preciso. La mayoría de los NIC modernos y sus respectivos controladores admiten una contabilidad precisa de los errores CRC recibidos por el NIC.

Errores RX en hosts Linux

Los errores CRC en los hosts Linux se manifiestan normalmente como un contador de "errores RX" distinto de cero que se muestra en la salida del **comando ifconfig**. Un ejemplo de un contador de errores RX no cero de un host Linux está aquí:

```
$ 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
```

Los errores CRC en los hosts Linux también pueden manifestarse como un contador de "errores RX" no cero que se muestra en la salida del comando **ip -s link show**. Un ejemplo de un contador de errores RX no cero de un host Linux está aquí:

```
$ 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
```

La NIC y su controlador respectivo deben soportar la contabilización de los errores CRC recibidos por la NIC para que el número de errores RX informados por los comandos **ifconfig** o **ip -s link show** sea preciso. La mayoría de los NIC modernos y sus respectivos controladores admiten una contabilidad precisa de los errores CRC recibidos por el NIC.

Errores CRC en dispositivos de red

Los dispositivos de red funcionan en uno de los dos modos de reenvío: modo de reenvío de almacenamiento y reenvío y modo de reenvío de corte. La forma en que un dispositivo de red maneja un error CRC recibido varía según sus modos de reenvío. Las subsecciones aquí describirán el comportamiento específico para cada modo de reenvío.

Errores de entrada en dispositivos de red de almacenamiento y reenvío

Cuando un dispositivo de red que funciona en modo de reenvío de almacenamiento y reenvío recibe una trama, el dispositivo de red almacenará la trama completa ("Almacenar") antes de validar el valor CRC de la trama, tomará una decisión de reenvío en la trama y transmitirá la trama fuera de una interfaz ("Reenviar"). Por lo tanto, cuando un dispositivo de red que opera en un modo de reenvío de almacenamiento y reenvío recibe una trama dañada con un valor CRC incorrecto en una interfaz específica, descartará la trama e incrementará el contador "Errores de entrada" en la interfaz.

En otras palabras, los dispositivos de red que funcionan en modo de reenvío Store-and-Forward no reenvían tramas Ethernet dañadas; se suprimen al ingreso.

Los switches Nexus de Cisco serie 7000 y 7700 funcionan en modo de reenvío de almacenamiento y reenvío. A continuación se muestra un ejemplo de un contador de errores de entrada distinto de cero y un contador CRC/FCS distinto de cero de un switch Nexus serie 7000 o 7700:

```
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
```

Los errores CRC también pueden manifestarse como un contador "FCS-Err" distinto de cero en la salida de errores **show interface counters**. El contador "Rcv-Err" en la salida de este comando también tendrá un valor distinto de cero, que es la suma de todos los errores de entrada (CRC o de otro tipo) recibidos por la interfaz. Aquí se muestra un ejemplo de esto:

```
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
```

Errores de entrada y salida en dispositivos de red cortados

Cuando un dispositivo de red que funciona en modo de reenvío de conexión directa comienza a recibir una trama, el dispositivo de red tomará una decisión de reenvío en el encabezado de la trama y comenzará a transmitir la trama desde una interfaz tan pronto como reciba suficiente de la trama para tomar una decisión de reenvío válida. Como los encabezados de trama y de paquete están al principio de la trama, esta decisión de reenvío se toma generalmente antes de que se reciba la carga útil de la trama.

El campo FCS de una trama Ethernet se encuentra al final de la trama, inmediatamente después de la carga útil de la trama. Por lo tanto, un dispositivo de red que opera en un modo de reenvío por corte ya habrá comenzado a transmitir la trama fuera de otra interfaz para el momento en que pueda calcular el CRC de la trama. Si el CRC calculado por el dispositivo de red para la trama no coincide con el valor CRC presente en el campo FCS, significa que el dispositivo de red reenvió una trama dañada a la red. Cuando esto sucede, el dispositivo de red incrementará dos contadores:

1. El contador "Errores de entrada" en la interfaz donde se recibió originalmente la trama dañada.
2. El contador "Errores de salida" en todas las interfaces donde se transmitió la trama dañada. Para el tráfico de unidifusión, ésta será normalmente una única interfaz; sin embargo, para el tráfico de difusión, multidifusión o unidifusión desconocida, podría ser una o más interfaces.

Aquí se muestra un ejemplo de esto, donde la salida del comando **show interface** indica que se recibieron varias tramas dañadas en Ethernet1/1 del dispositivo de red y se transmitieron desde Ethernet1/2 debido al modo de reenvío por corte del dispositivo de red:

```
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
```

Los errores CRC también pueden manifestarse como un contador "FCS-Err" distinto de cero en la interfaz de ingreso y contadores "Xmit-Err" no nulos en las interfaces de salida en la salida de errores **show interface counters**. El contador "Rcv-Err" en la interfaz de ingreso en la salida de este comando también tendrá un valor distinto de cero, que es la suma de todos los errores de entrada (CRC o de otro tipo) recibidos por la interfaz. Aquí se muestra un ejemplo de esto:

```
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
```

El dispositivo de red también modificará el valor CRC en el campo FCS de la trama de una manera específica que significa para los dispositivos de red ascendentes que esta trama está dañada. Este comportamiento se conoce como "pisotear" el CRC. La forma precisa en que se modifica el CRC varía de una plataforma a otra, pero generalmente implica invertir el valor actual de CRC presente en el campo FCS de la trama. Un ejemplo de esto es aquí:

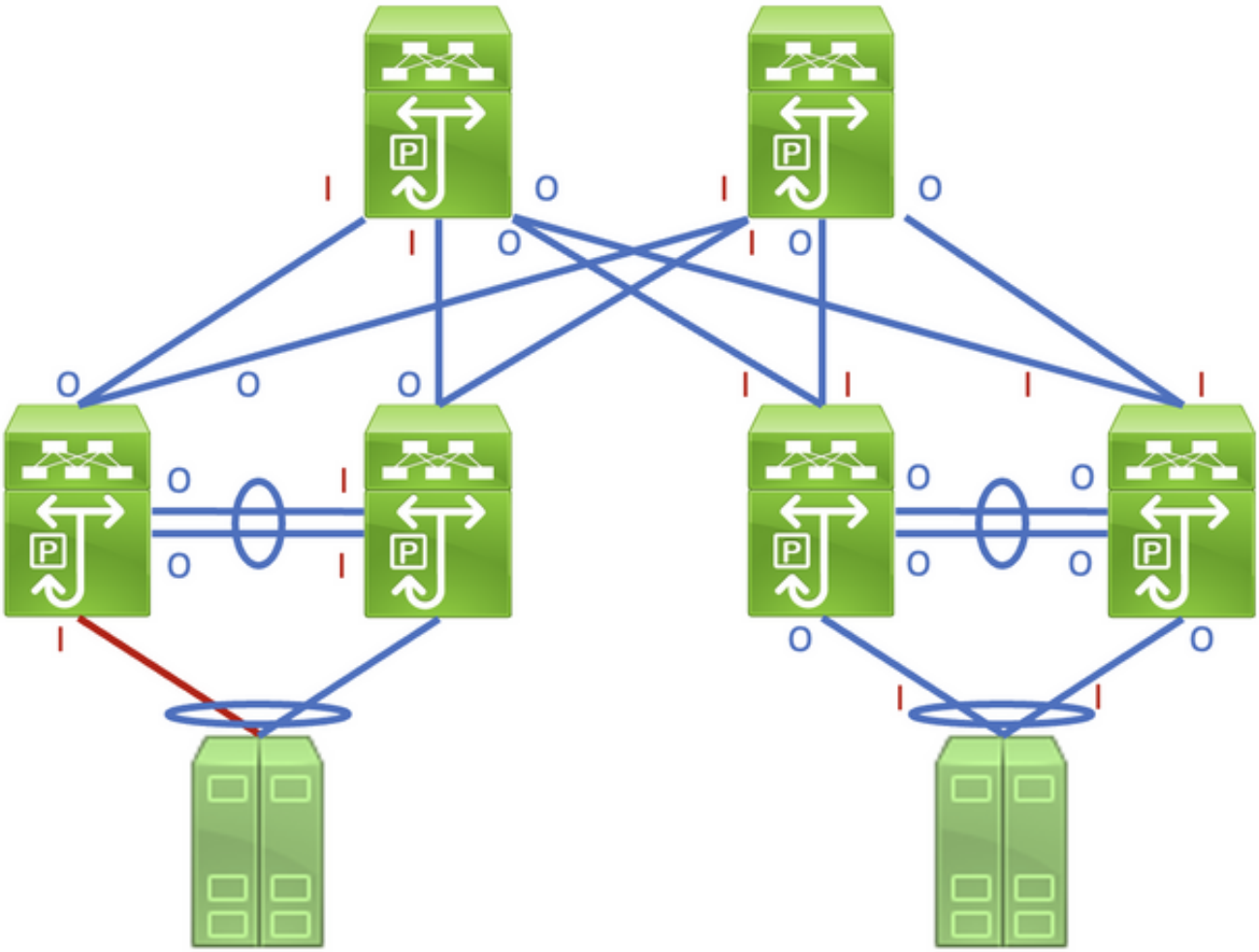
```
Original CRC: 0xABCD (1010101111001101)
Stomped CRC:  0x5432 (0101010000110010)
```

Como resultado de este comportamiento, los dispositivos de red que funcionan en un modo de reenvío de conexión directa pueden propagar una trama dañada a través de una red. Si una red consta de varios dispositivos de red que funcionan en modo de reenvío de conexión directa, una única trama dañada puede provocar que los contadores de errores de entrada y de salida aumenten en varios dispositivos de red dentro de la red.

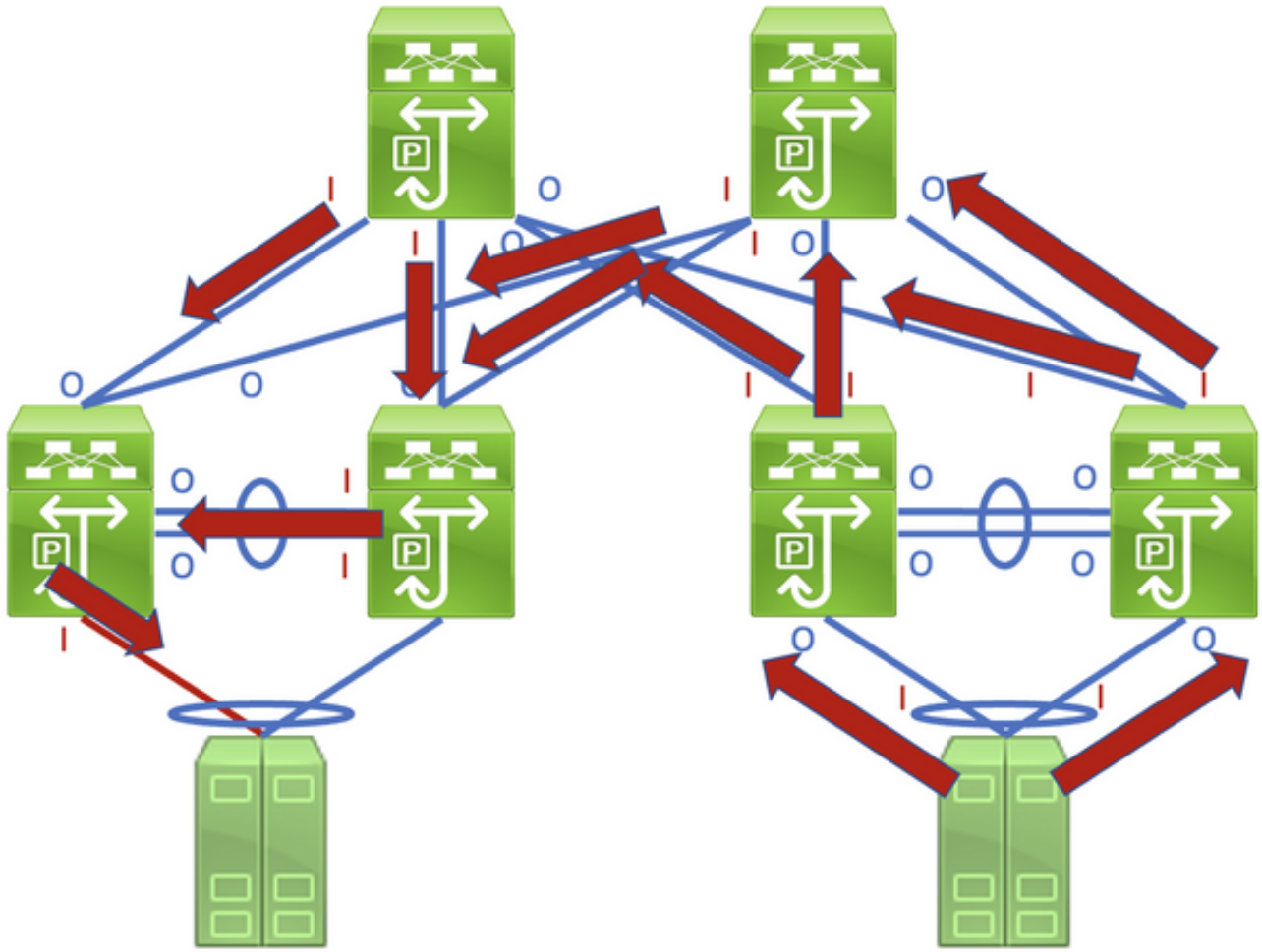
Seguimiento y aislamiento de errores CRC

El primer paso para identificar y resolver la causa raíz de los errores CRC es aislar el origen de los errores CRC a un link específico entre dos dispositivos dentro de su red. Un dispositivo conectado a este link tendrá un contador de errores de salida de interfaz con un valor de cero o no está aumentando, mientras que el otro dispositivo conectado a este link tendrá un contador de errores de entrada de interfaz que no sea cero o que aumentará. Esto sugiere que el tráfico que sale de la interfaz de un dispositivo intacto se daña en el momento de la transmisión al dispositivo remoto y se cuenta como un error de entrada por la interfaz de ingreso del otro dispositivo en el link.

Identificar este link en una red que consta de dispositivos de red que funcionan en modo de reenvío de almacenamiento y reenvío es una tarea sencilla. Sin embargo, es más difícil identificar este link en una red que consta de dispositivos de red que funcionan en modo de reenvío de conexión directa, ya que muchos dispositivos de red tendrán contadores de errores de entrada y salida distintos de cero. Un ejemplo de este fenómeno se puede ver en la topología aquí, donde el link resaltado en rojo se daña de tal manera que el tráfico que atraviesa el link está dañado. Las interfaces etiquetadas con una "I" roja indican interfaces que podrían tener errores de entrada distintos de cero, mientras que las interfaces etiquetadas con una "O" azul indican interfaces que podrían tener errores de salida distintos de cero.



La identificación del link defectuoso requiere que realice un seguimiento recursivo de las tramas dañadas de "trayectoria" que siguen en la red a través de contadores de errores de entrada y salida no nulos, con errores de entrada no nulos que apuntan hacia el link dañado en la red. Esto se demuestra en el diagrama aquí.



La mejor manera de demostrar a través de un ejemplo es un proceso detallado para rastrear e identificar un link dañado. Considere la topología aquí:

En esta topología, la interfaz Ethernet1/1 de un switch Nexus denominado Switch-1 se conecta a un host denominado Host-1 a través de la Tarjeta de interfaz de red (NIC) eth0 del host-1. La interfaz Ethernet1/2 del Switch-1 está conectada a un segundo switch Nexus, denominado Switch-2, a través de la interfaz Ethernet1/2 del Switch-2. La interfaz Ethernet1/1 del Switch-2 está conectada a un host denominado Host-2 a través de la NIC eth0 del Host-2.

El link entre el Host-1 y el Switch-1 a través de la interfaz Ethernet1/1 del Switch-1 está dañado, lo que causa que el tráfico que atraviesa el link se dañe intermitentemente. Sin embargo, todavía no sabemos que este link esté dañado. Debemos rastrear la trayectoria que dejan las tramas dañadas en la red a través de contadores de errores de entrada y salida no nulos o incrementando los contadores de errores de entrada y salida para localizar el link dañado en esta red.

En este ejemplo, la NIC del host 2 informa que está recibiendo errores 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
```

Usted sabe que la NIC del Host 2 se conecta al Switch-2 a través de la interfaz Ethernet1/1. Puede confirmar que la interfaz Ethernet1/1 tiene un contador de errores de salida distinto de cero con el 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
```

Dado que el contador de errores de salida de la interfaz Ethernet1/1 no es cero, es muy probable que haya otra interfaz del Switch-2 que tenga un contador de errores de entrada distinto de cero. Puede utilizar el comando **show interface counters errors non-zero** para identificar si alguna interfaz del Switch-2 tiene un contador de errores de entrada distinto de cero.

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

Puede ver que Ethernet1/2 del Switch-2 tiene un contador de errores de entrada distinto de cero. Esto sugiere que el Switch-2 recibe tráfico dañado en esta interfaz. Puede confirmar qué dispositivo está conectado a Ethernet1/2 del switch 2 a través de las funciones de protocolo de detección de Cisco (CDP) o protocolo de detección local de enlaces (LLDP). Aquí se muestra un ejemplo de esto con el 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
```

Ahora sabe que el Switch-2 está recibiendo tráfico dañado en su interfaz Ethernet1/2 de la interfaz Ethernet1/2 del Switch-1, pero todavía no sabe si el link entre Ethernet1/2 del Switch-1 y Ethernet1/2 del Switch-2 está dañado y causa la corrupción, o si el Switch-1 es un switch de conexión directa que reenvía el tráfico dañado que recibe. Debe iniciar sesión en el Switch-1 para verificar esto.

Puede confirmar que la interfaz Ethernet1/2 del Switch 1 tiene un contador de errores de salida distinto de cero con el 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
```

Puede ver que Ethernet1/2 del Switch-1 tiene un contador de errores de salida distinto de cero. Esto sugiere que el link entre Ethernet1/2 del Switch-1 y Ethernet1/2 del Switch-2 no está dañado; en cambio, el Switch-1 es un switch de conexión directa que reenvía el tráfico dañado que recibe en alguna otra interfaz. Como se demostró anteriormente con el Switch-2, puede utilizar el comando **show interface counters errors non-zero** para identificar si alguna interfaz del Switch-1 tiene un contador de errores de entrada distinto de cero.

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

Puede ver que Ethernet1/1 del Switch-1 tiene un contador de errores de entrada distinto de cero. Esto sugiere que el Switch-1 está recibiendo tráfico dañado en esta interfaz. Sabemos que esta interfaz se conecta con la NIC eth0 del Host 1. Podemos revisar las estadísticas de la interfaz NIC eth0 del Host-1 para confirmar si el Host-1 envía tramas dañadas fuera de esta interfaz.

```
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
```

Las estadísticas de la NIC eth0 del Host-1 sugieren que el host no está transmitiendo tráfico dañado. Esto sugiere que el link entre el eth0 del Host 1 y Ethernet1/1 del Switch-1 está dañado y es la fuente de esta corrupción del tráfico. Será necesario realizar más troubleshooting en este link para identificar el componente defectuoso que causa esta corrupción y reemplazarlo.

Causas principales de errores CRC

La causa principal más común de los errores CRC es un componente dañado o en mal funcionamiento de un link físico entre dos dispositivos. Algunos ejemplos son:

- Medio físico defectuoso o dañado (cobre o fibra) o cables de conexión directa (DAC).
- Transceptores/ópticos defectuosos o dañados.
- Puertos del panel de conexión defectuosos o dañados.
- Hardware de dispositivos de red defectuosos (incluidos puertos específicos, circuitos integrados específicos de la aplicación [ASIC], controles de acceso a medios [MAC], módulos de fabric, etc.),
- Tarjeta de interfaz de red que funciona mal insertada en un host.

También es posible que uno o más dispositivos mal configurados provoquen errores CRC inadvertidamente dentro de una red. Un ejemplo de esto es una discordancia de configuración de

la unidad máxima de transmisión (MTU) entre dos o más dispositivos dentro de la red, lo que hace que los paquetes grandes se trunquen incorrectamente. La identificación y resolución de este problema de configuración también puede corregir los errores CRC dentro de una red.

Resolver errores CRC

Puede identificar el componente específico del mal funcionamiento a través de un proceso de eliminación:

1. Reemplace el medio físico (ya sea de cobre o fibra) o DAC por un medio físico conocido del mismo tipo.
2. Sustituya el transceptor insertado en la interfaz de un dispositivo por un transceptor que se sepa que es correcto del mismo modelo. Si esto no resuelve los errores CRC, reemplace el transceiver insertado en la interfaz del otro dispositivo por un transceptor del mismo modelo que se sepa que es correcto.
3. Si se utiliza algún panel de conexión como parte del link dañado, mueva el link a un puerto que se sepa que es correcto en el panel de conexión. Alternativamente, elimine el panel de parches como causa raíz potencial conectando el link sin utilizar el panel de parches si es posible.
4. Mueva el link dañado a un puerto diferente, que se sepa que es correcto en cada dispositivo. Deberá probar varios puertos diferentes para aislar una falla de MAC, ASIC o tarjeta de línea.
5. Si el link dañado implica un host, mueva el link a una NIC diferente en el host. Alternativamente, conecte el link dañado a un host que se sabe que es correcto para aislar una falla de la NIC del host.

Si el componente que falla es un producto de Cisco (como un dispositivo de red o transceptor de Cisco) que está cubierto por un contrato de soporte activo, puede abrir un caso de soporte con el TAC de Cisco detallando su solución de problemas para que el componente que falla sea reemplazado a través de una Autorización de devolución de mercancía (RMA).

Información Relacionada

- Procedimiento de identificación y seguimiento de CRC de Nexus 9000 Cloud Scale ASIC
- Soporte Técnico y Documentación - Cisco Systems