Comprensione degli errori del controllo di ridondanza ciclico sugli switch Nexus

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Premesse](#)
[Dispositivi interessati](#)
[Definizione CRC](#)
[Definizione errore CRC](#)
[Sintomi comuni degli errori CRC](#)
[Errori ricevuti su host Windows](#)
[Errori RX su host Linux](#)
[Errori CRC su dispositivi di rete](#)
[Errori di input nei dispositivi di rete Store-and-Forward](#)
[Errori di input e output su dispositivi di rete cut-through](#)
[Individuazione e isolamento degli errori CRC](#)
[Cause principali degli errori CRC](#)
[Risolvi errori CRC](#)
[Informazioni correlate](#)

Introduzione

Questo documento descrive i dettagli relativi agli errori CRC (Cyclic Redundancy Check) osservati sui contatori di interfaccia e le statistiche degli switch Cisco Nexus.

Prerequisiti

Requisiti

Cisco consiglia di comprendere le nozioni di base dello switching Ethernet e dell'interfaccia della riga di comando (CLI) di Cisco NX-OS. Per ulteriori informazioni, fare riferimento a uno dei seguenti documenti applicabili:

- Guida alla configurazione delle nozioni fondamentali di Cisco Nexus 9000 NX-OS, versione 10.2(x)
- Guida alla configurazione delle nozioni fondamentali di Cisco Nexus serie 9000 NX-OS, versione 9.3(x)
- Guida alla configurazione delle nozioni fondamentali di Cisco Nexus serie 9000 NX-OS, versione 9.2(x)
- Guida alla configurazione delle nozioni fondamentali di Cisco Nexus serie 9000 NX-OS,

versione 7.x

- Risoluzione dei problemi Ethernet

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Switch Nexus serie 9000 a partire dal software NX-OS versione 9.3(8)
- Switch Nexus serie 3000 a partire dal software NX-OS versione 9.3(8)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Questo documento descrive i dettagli relativi agli errori CRC (Cyclic Redundancy Check) osservati sui contatori di interfaccia sugli switch Cisco serie Nexus. Questo documento descrive cos'è un CRC, come viene usato nel campo Frame Check Sequence (FCS) dei frame Ethernet, come gli errori CRC si manifestano sugli switch Nexus, come gli errori CRC interagiscono negli scenari di switching Store-and-Forward e switching Cut-Through, le cause principali più probabili degli errori CRC e come risolvere e risolvere gli errori CRC.

Dispositivi interessati

Le informazioni discusse in questo documento sono valide per tutti gli switch Cisco serie Nexus. Alcune informazioni discusse in questo documento possono essere valide anche per altre piattaforme di routing e switching Cisco, quali router e switch Cisco Catalyst.

Definizione CRC

Un CRC è un meccanismo di rilevamento degli errori comunemente utilizzato nelle reti di computer e di archiviazione per identificare i dati modificati o danneggiati durante la trasmissione. Quando un dispositivo connesso alla rete deve trasmettere dati, il dispositivo esegue un algoritmo di calcolo basato su codici ciclici rispetto ai dati che danno come risultato un numero a lunghezza fissa. Questo numero a lunghezza fissa è chiamato valore CRC, ma colloquialmente è spesso chiamato CRC per abbreviazione. Questo valore CRC viene aggiunto ai dati e trasmesso attraverso la rete a un altro dispositivo. Questo dispositivo remoto esegue lo stesso algoritmo di codice ciclico in base ai dati e confronta il valore risultante con il CRC aggiunto ai dati. Se entrambi i valori corrispondono, la periferica remota presuppone che i dati siano stati trasmessi in rete senza essere danneggiati. Se i valori non corrispondono, il dispositivo remoto presume che i

dati siano stati danneggiati durante la trasmissione attraverso la rete. I dati danneggiati non possono essere considerati attendibili e vengono eliminati.

I CRC vengono utilizzati per il rilevamento degli errori in più tecnologie di rete, ad esempio Ethernet (varianti cablate e wireless), Token Ring, ATM (Asynchronous Transfer Mode) e Frame Relay. I frame Ethernet hanno un campo Frame Check Sequence (FCS) a 32 bit alla fine del frame (immediatamente dopo il payload del frame) in cui è inserito un valore CRC a 32 bit.

Ad esempio, si consideri uno scenario in cui due host denominati Host-A e Host-B sono direttamente connessi tra loro tramite le schede di interfaccia di rete (NIC, Network Interface Card). L'host-A deve inviare la frase "Questo è un esempio" all'host-B attraverso la rete. L'host A crea un frame Ethernet destinato all'host B con un payload di "Questo è un esempio" e calcola che il valore CRC del frame sia un valore esadecimale di 0xABCD. L'host A inserisce il valore CRC di 0xABCD nel campo FCS del frame Ethernet, quindi trasmette il frame Ethernet dalla scheda NIC dell'host A all'host B.

Quando l'host B riceve questo frame, calcola il valore CRC del frame utilizzando lo stesso algoritmo dell'host A. Host-B calcola che il valore CRC del frame è un valore esadecimale di 0xABCD, che indica all'host-B che il frame Ethernet non è stato danneggiato durante la trasmissione del frame all'host-B.

Definizione errore CRC

Un errore CRC si verifica quando un dispositivo (un dispositivo di rete o un host connesso alla rete) riceve un frame Ethernet con un valore CRC nel campo FCS del frame che non corrisponde al valore CRC calcolato dal dispositivo per il frame.

Questo concetto può essere dimostrato attraverso un esempio. Si consideri uno scenario in cui due host denominati Host-A e Host-B sono collegati direttamente tra loro tramite le schede di interfaccia di rete (NIC, Network Interface Card). L'host A deve inviare la frase "Questo è un esempio" all'host B attraverso la rete. L'host A crea un frame Ethernet destinato all'host B con un payload di "Questo è un esempio" e calcola che il valore CRC del frame sia il valore esadecimale 0xABCD. L'host A inserisce il valore CRC di 0xABCD nel campo FCS del frame Ethernet, quindi trasmette il frame Ethernet dalla scheda NIC dell'host A all'host B.

Tuttavia, un danno sul supporto fisico che collega l'host A all'host B danneggia il contenuto del frame in modo che la frase all'interno del frame cambia in "Questo era un esempio" invece del payload desiderato di "Questo è un esempio".

Quando l'host B riceve questo frame, calcola il valore CRC del frame incluso il payload danneggiato. Host-B calcola che il valore CRC del frame è un valore esadecimale di 0xDEAD, che è diverso dal valore 0xABCD CRC nel campo FCS del frame Ethernet. Questa differenza nei valori CRC indica all'host-B che il frame Ethernet è stato danneggiato durante la trasmissione del frame all'host-B. Di conseguenza, l'host-B non può considerare attendibile il contenuto del frame Ethernet, pertanto verrà eliminato. L'host B in genere incrementa alcuni tipi di contatori di errori sulla scheda di interfaccia di rete (NIC, Network Interface Card), ad esempio i contatori "errori di input", "errori CRC" o "errori RX".

Sintomi comuni degli errori CRC

Gli errori CRC si manifestano in genere in uno dei due modi seguenti:

1. Incrementare o non azzerare i contatori di errori sulle interfacce dei dispositivi connessi alla rete.
2. Perdita di pacchetti/frame per il traffico che attraversa la rete a causa della perdita di frame danneggiati da parte dei dispositivi connessi alla rete.

Questi errori si manifestano in modi leggermente diversi a seconda del dispositivo utilizzato. Le sezioni secondarie illustrano nel dettaglio i singoli tipi di dispositivi.

Errori ricevuti su host Windows

Gli errori CRC negli host Windows in genere si manifestano come un contatore degli **errori ricevuti** diverso da zero visualizzato nell'output del comando **netstat -e** dal prompt dei comandi. Di seguito è riportato un esempio di contatore degli errori ricevuti diverso da zero dal prompt dei comandi di un host 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
```

Affinché il numero di errori ricevuti segnalati dal comando **netstat -e** sia accurato, la scheda NIC e il rispettivo driver devono supportare la contabilità degli errori CRC ricevuti dalla scheda NIC. La maggior parte delle schede NIC moderne e i relativi driver supportano la contabilizzazione accurata degli errori CRC ricevuti dalla scheda NIC.

Errori RX su host Linux

Gli errori CRC sugli host Linux in genere si manifestano come contatori di "errori RX" diversi da zero visualizzati nell'output del comando **ifconfig**. Di seguito è riportato un esempio di contatore degli errori RX diversi da zero da un host Linux:

```
$ 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
```

Gli errori CRC sugli host Linux possono anche essere visualizzati come contatori di "errori RX" diversi da zero visualizzati nell'output del comando **ip -s link show**. Di seguito è riportato un esempio di contatore degli errori RX diversi da zero da un host Linux:

```
$ 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 scheda NIC e il relativo driver devono supportare la contabilizzazione degli errori CRC ricevuti dalla scheda NIC in modo che il numero di errori RX segnalati dal **collegamento ifconfig** o **ip -s show** sia accurato. La maggior parte delle schede NIC moderne e i relativi driver supportano la contabilizzazione accurata degli errori CRC ricevuti dalla scheda NIC.

Errori CRC su dispositivi di rete

I dispositivi di rete funzionano in due modalità di inoltro: modalità di inoltro store-and-forward e modalità di inoltro cut-through. Il modo in cui un dispositivo di rete gestisce un errore CRC ricevuto varia a seconda delle modalità di inoltro. Nelle sottosezioni seguenti viene descritto il comportamento specifico di ciascuna modalità di inoltro.

Errori di input nei dispositivi di rete Store-and-Forward

Quando un dispositivo di rete che opera in modalità di inoltro "Store-and-Forward" riceve un frame, il dispositivo di rete memorizza l'intero frame ("Store") prima che il valore CRC del frame venga convalidato, prenda una decisione di inoltro sul frame e trasmetta il frame fuori da un'interfaccia ("Forward"). Pertanto, quando un dispositivo di rete che opera in modalità di inoltro Store-and-Forward riceve un frame danneggiato con un valore CRC errato su un'interfaccia specifica, lo scarta e incrementa il contatore "Errori di input" sull'interfaccia.

In altre parole, i frame Ethernet danneggiati non vengono inoltrati dai dispositivi di rete che operano in modalità di inoltro Store-and-Forward; vengono lasciati in entrata.

Gli switch Cisco Nexus serie 7000 e 7700 funzionano in modalità di inoltro Store-and-Forward. Di seguito è riportato un esempio di contatore degli errori di input diverso da zero e di contatore CRC/FCS diverso da zero relativo a uno 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
```

Gli errori CRC possono anche rivelarsi come contatori "FCS-Err" diversi da zero nell'output degli errori **show interface counters**. Il contatore "Rcv-Err" nell'output di questo comando avrà anche un valore diverso da zero, che è la somma di tutti gli errori di input (CRC o altro) ricevuti dall'interfaccia. Di seguito è riportato un esempio:

```
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
```

Errori di input e output su dispositivi di rete cut-through

Quando un dispositivo di rete che opera in modalità di inoltro Cut-Through inizia a ricevere un frame, il dispositivo di rete prende una decisione di inoltro sull'intestazione del frame e inizia a trasmettere il frame da un'interfaccia non appena riceve una quantità di frame sufficiente per prendere una decisione di inoltro valida. Poiché le intestazioni di frame e di pacchetto si trovano all'inizio del frame, questa decisione di inoltro viene in genere presa prima di ricevere il payload del frame.

Il campo FCS di un frame Ethernet si trova alla fine del frame, subito dopo il payload del frame. Pertanto, un dispositivo di rete che opera in modalità di inoltro Cut-Through avrà già iniziato a trasmettere il frame da un'altra interfaccia nel momento in cui può calcolare il CRC del frame. Se il CRC calcolato dal dispositivo di rete per il frame non corrisponde al valore CRC presente nel campo FCS, significa che il dispositivo di rete ha inoltrato un frame danneggiato alla rete. In questo caso, il dispositivo di rete incrementa due contatori:

1. Contatore "Errori di input" sull'interfaccia in cui è stato originariamente ricevuto il frame danneggiato.
2. Il contatore "Errori di output" su tutte le interfacce in cui è stato trasmesso il frame danneggiato. Per il traffico unicast, si tratta in genere di un'interfaccia singola. Tuttavia, per il traffico broadcast, multicast o unicast sconosciuto, si tratta di una o più interfacce.

Di seguito è riportato un esempio di questo problema, in cui l'output del comando **show interface** indica che sono stati ricevuti più frame danneggiati sulla rete Ethernet 1/1 del dispositivo di rete e trasmessi al di fuori della rete Ethernet 1/2 a causa della modalità di inoltro Cut-through del dispositivo di rete:

```
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
```

Gli errori CRC possono anche rivelarsi come contatori "FCS-Err" diversi da zero sull'interfaccia in entrata e contatori "Xmit-Err" diversi da zero sulle interfacce in uscita nell'output degli errori **show interface**. Il contatore "Rcv-Err" sull'interfaccia in entrata nell'output di questo comando avrà anche un valore diverso da zero, che è la somma di tutti gli errori di input (CRC o altro) ricevuti

dall'interfaccia. Di seguito è riportato un esempio:

```
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
```

Il dispositivo di rete modificherà inoltre il valore CRC nel campo FCS del frame in un modo specifico che indica ai dispositivi di rete upstream che il frame è danneggiato. Questo comportamento è noto come "calmare" il CRC. Il modo preciso in cui il CRC viene modificato varia da una piattaforma all'altra, ma in genere comporta l'inversione del valore CRC corrente presente nel campo FCS del frame. Ecco un esempio:

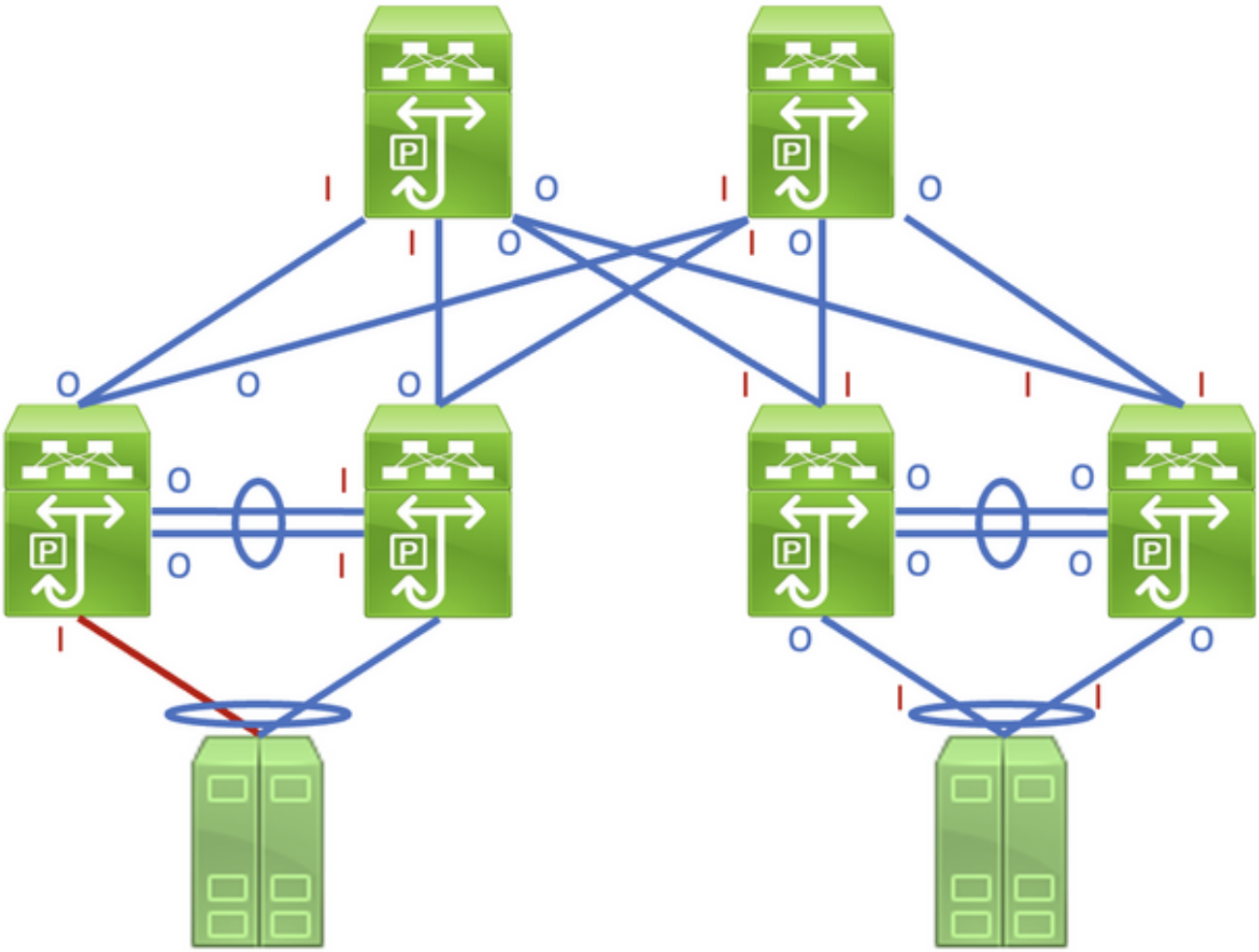
```
Original CRC: 0xABCD (1010101111001101)
Stomped CRC:  0x5432 (0101010000110010)
```

Come risultato di questo comportamento, i dispositivi di rete che operano in modalità di inoltro Cut-Through possono propagare un frame danneggiato in tutta la rete. Se una rete è costituita da più dispositivi di rete che operano in modalità di inoltro Cut-Through, un singolo frame danneggiato può causare l'incremento dei contatori degli errori di input e output su più dispositivi di rete all'interno della rete.

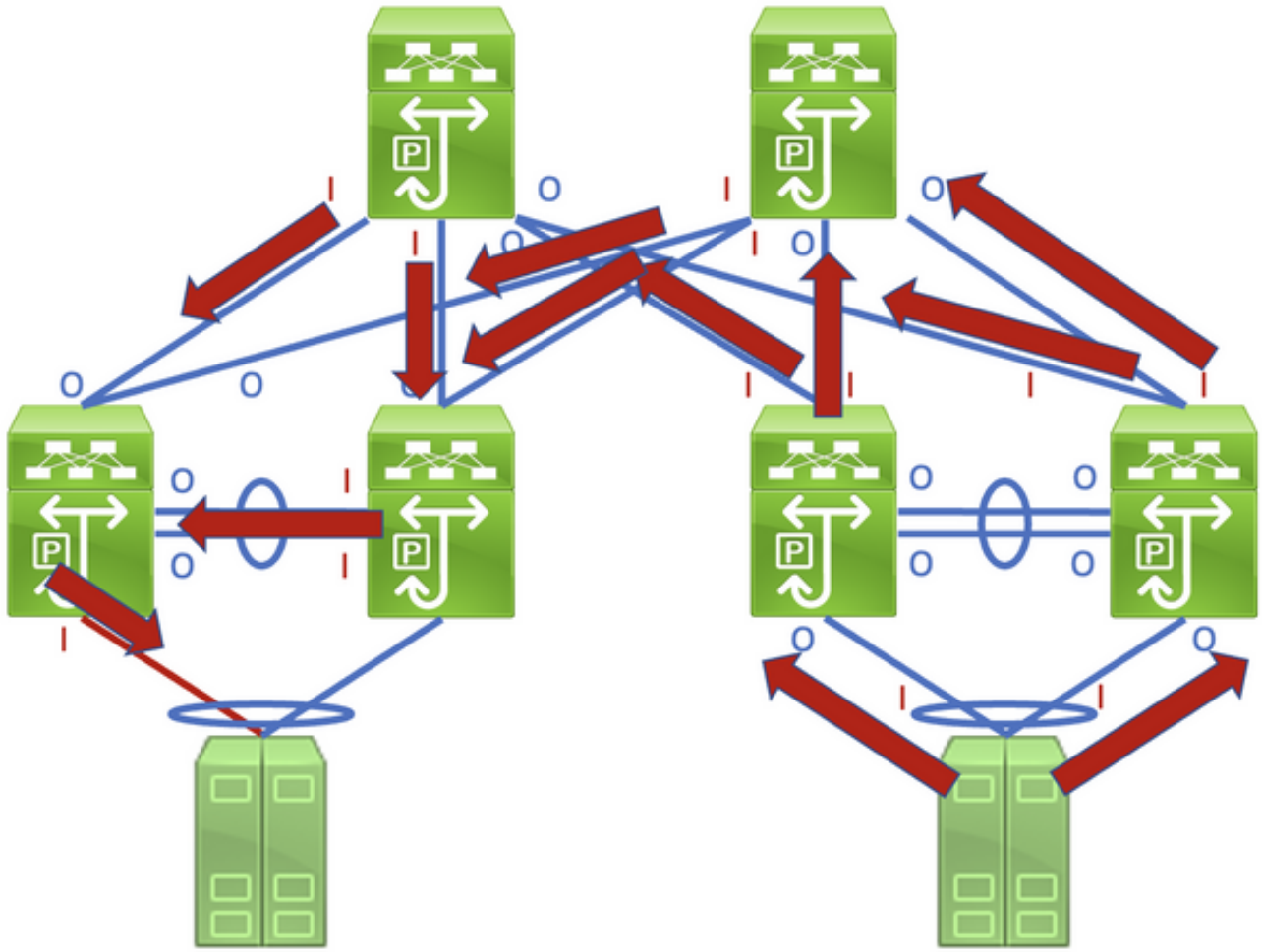
Individuazione e isolamento degli errori CRC

Il primo passaggio per identificare e risolvere la causa principale degli errori CRC è isolare l'origine degli errori CRC su un collegamento specifico tra due dispositivi della rete. Un dispositivo connesso a questo collegamento disporrà di un contatore degli errori di output dell'interfaccia con valore zero o non incrementale, mentre l'altro dispositivo connesso a questo collegamento disporrà di un contatore degli errori di input dell'interfaccia diverso da zero o incrementale. Ciò suggerisce che il traffico in uscita dall'interfaccia di un dispositivo intatto sia danneggiato al momento della trasmissione al dispositivo remoto e che venga conteggiato come un errore di input dall'interfaccia in entrata dell'altro dispositivo sul collegamento.

Identificare questo collegamento in una rete costituita da dispositivi di rete che operano in modalità di inoltro Store-and-Forward è un'operazione semplice. Tuttavia, identificare questo collegamento in una rete costituita da dispositivi di rete che operano in modalità di inoltro Cut-Through è più difficile, in quanto molti dispositivi di rete avranno contatori di errori di input e output diversi da zero. Un esempio di questo fenomeno può essere visto nella topologia qui, dove il link evidenziato in rosso è danneggiato in modo che il traffico che attraversa il link sia danneggiato. Le interfacce contrassegnate con una "I" rossa indicano interfacce che potrebbero avere errori di input diversi da zero, mentre le interfacce contrassegnate con una "O" blu indicano interfacce che potrebbero avere errori di output diversi da zero.



L'identificazione del collegamento difettoso richiede di tracciare in modo ricorsivo il "percorso" che seguono i frame danneggiati nella rete tramite contatori di errori di input e output diversi da zero, con errori di input diversi da zero che puntano a monte verso il collegamento danneggiato nella rete. Come si vede nel grafico qui.



Èconsigliabile eseguire un processo dettagliato per rintracciare e identificare un collegamento danneggiato attraverso un esempio. Supponiamo di avere questa topologia:

In questa topologia, l'interfaccia Ethernet1/1 di uno switch Nexus denominato Switch-1 è collegata a un host denominato Host-1 tramite la scheda di interfaccia di rete (NIC) eth0 dell'host-1. L'interfaccia Ethernet1/2 dello switch-1 è collegata a un secondo switch Nexus, denominato Switch-2, tramite l'interfaccia Ethernet1/2 dello switch-2. L'interfaccia Ethernet1/1 dello switch-2 è collegata a un host denominato Host-2 tramite la scheda di interfaccia di rete eth0 dell'host-2.

Il collegamento tra l'host 1 e lo switch 1 tramite l'interfaccia Ethernet1/1 dello switch 1 è danneggiato, pertanto il traffico che attraversa il collegamento è danneggiato in modo intermittente. Tuttavia, non sappiamo ancora che questo collegamento sia danneggiato. Per individuare il collegamento danneggiato nella rete, è necessario tracciare il percorso dei frame danneggiati lasciati nella rete tramite contatori di errori di input e output diversi da zero o incrementali.

In questo esempio, la scheda di interfaccia di rete dell'host 2 segnala la ricezione di errori 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
```

Ènoto che la scheda NIC dell'host 2 si connette allo switch 2 tramite l'interfaccia Ethernet1/1. È possibile verificare che l'interfaccia Ethernet1/1 abbia un contatore degli errori di output diverso da zero con il 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
```

Poiché il contatore degli errori di output dell'interfaccia Ethernet1/1 è diverso da zero, è molto probabile che esista un'altra interfaccia dello switch 2 con un contatore degli errori di input diverso da zero. È possibile utilizzare il comando **show interface counters errors diverso da zero** per verificare se sulle interfacce dello switch 2 è presente un contatore degli errori di input diverso da 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
```

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

Si noti che Ethernet1/2 dello switch-2 ha un contatore di errori di input diverso da zero. Ciò suggerisce che lo switch 2 riceve traffico danneggiato su questa interfaccia. È possibile verificare quale periferica è collegata a Ethernet1/2 dello switch-2 tramite le funzionalità Cisco Discovery Protocol (CDP) o Link Local Discovery Protocol (LLDP). Di seguito è riportato un esempio con il 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
```

A questo punto, è possibile sapere che lo switch 2 riceve traffico danneggiato sull'interfaccia Ethernet 1/2 dello switch 1 dall'interfaccia Ethernet 1/2 dello switch 1, ma non si sa ancora se il collegamento tra l'interfaccia Ethernet 1/2 dello switch 1 e l'interfaccia Ethernet 1/2 dello switch 2 è danneggiato e causa il danneggiamento oppure se lo switch 1 è uno switch cut-through che inoltra il traffico danneggiato che riceve. Per verificare questa condizione, è necessario accedere allo switch 1.

Per verificare che l'interfaccia Ethernet 1/2 dello switch 1 abbia un contatore degli errori di output diverso da zero, usare il 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
```

Si noti che Ethernet1/2 dello switch-1 ha un contatore degli errori di output diverso da zero. Ciò suggerisce che il collegamento tra l'interfaccia Ethernet1/2 dello switch 1 e l'interfaccia Ethernet1/2 dello switch 2 non sia danneggiato - lo switch 1 è invece un traffico di inoltro switch cut-through danneggiato che riceve su un'altra interfaccia. Come mostrato in precedenza con lo switch 2, è possibile usare il comando **show interface counters errors diverso da zero** per

verificare se su alcune interfacce dello switch 1 è presente un contatore degli errori di input diverso da 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
--------------------------------------------------------------------------------
```

Si noti che Ethernet1/1 dello switch-1 ha un contatore degli errori di input diverso da zero. Ciò suggerisce che lo switch 1 riceve traffico danneggiato su questa interfaccia. È noto che questa interfaccia si connette alla scheda NIC eth0 dell'host 1. È possibile esaminare le statistiche dell'interfaccia NIC eth0 dell'host 1 per verificare se l'host 1 invia frame danneggiati da questa interfaccia.

```
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
```

Le statistiche eth0 NIC dell'host-1 suggeriscono che l'host non sta trasmettendo traffico danneggiato. Ciò suggerisce che il collegamento tra l'endpoint0 dell'host 1 e l'Ethernet1/1 dello switch 1 è danneggiato e che è la causa del danneggiamento del traffico. È necessario eseguire ulteriori operazioni di risoluzione dei problemi su questo collegamento per identificare il componente difettoso che causa il danneggiamento e sostituirlo.

Cause principali degli errori CRC

La causa principale più comune degli errori CRC è un componente danneggiato o che non funziona correttamente di un collegamento fisico tra due dispositivi. Alcuni esempi:

- Supporto fisico guasto o danneggiato (rame o fibra) o cavi DAC (Direct Attach Cables).
- Ricetrasmettitori/ottici guasti o danneggiati.
- Porte del pannello patch guaste o danneggiate.
- guasto hardware del dispositivo di rete (comprese porte specifiche, schede di linea, circuiti integrati specifici dell'applicazione [ASIC], controlli di accesso ai supporti [MAC], moduli fabric,

ecc.),

- Scheda di interfaccia di rete inserita in un host non funzionante.

Èinoltre possibile che uno o più dispositivi non configurati correttamente causino inavvertitamente errori CRC all'interno di una rete. Un esempio di ciò è la mancata corrispondenza della configurazione della MTU (Maximum Transmission Unit) tra due o più dispositivi nella rete che causa il troncamento errato di pacchetti di grandi dimensioni. L'identificazione e la risoluzione di questo problema di configurazione può correggere gli errori CRC anche all'interno di una rete.

Risolvi errori CRC

Èpossibile identificare il componente malfunzionante specifico mediante un processo di eliminazione:

1. Sostituire il mezzo fisico (rame o fibra) o il DAC con un mezzo fisico riconosciuto valido dello stesso tipo.
2. Sostituire il ricetrasmettitore inserito nell'interfaccia di un dispositivo con un ricetrasmettitore funzionante dello stesso modello. Se l'operazione non risolve gli errori CRC, sostituire il ricetrasmettitore inserito nell'interfaccia dell'altro dispositivo con un ricetrasmettitore funzionante dello stesso modello.
3. Se come parte del collegamento danneggiato vengono utilizzati pannelli di patch, spostare il collegamento su una porta riconosciuta valida sul pannello di patch. In alternativa, eliminate il pannello patch come potenziale causa principale collegando il collegamento senza usare il pannello patch, se possibile.
4. Spostare il collegamento danneggiato su una porta diversa riconosciuta valida su ciascun dispositivo. È necessario eseguire il test di più porte diverse per isolare un errore MAC, ASIC o di scheda di linea.
5. Se il collegamento danneggiato interessa un host, spostare il collegamento su una scheda NIC diversa sull'host. In alternativa, collegare il collegamento danneggiato a un host riconosciuto valido per isolare un guasto della scheda NIC dell'host.

Se il componente malfunzionante è un prodotto Cisco (ad esempio un dispositivo di rete o un ricetrasmettitore Cisco) coperto da un contratto di assistenza attivo, è possibile aprire una richiesta di assistenza in cui Cisco TAC fornisce dettagli sulla risoluzione dei problemi per sostituire il componente malfunzionante tramite un'autorizzazione restituzione materiale (RMA).

Informazioni correlate

- Procedura di identificazione e traccia CRC ASIC Scale Nexus 9000
- Documentazione e supporto tecnico – Cisco Systems