

Comprendre les erreurs de vérification de redondance cyclique sur les commutateurs Nexus

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Matériel applicable](#)

[Définition de CRC](#)

[Définition d'une erreur CRC](#)

[Symptômes courants des erreurs CRC](#)

[Erreurs reçues sur les hôtes Windows](#)

[Erreurs RX sur les hôtes Linux](#)

[Erreurs CRC sur les périphériques réseau](#)

[Erreurs d'entrée sur les périphériques réseau avec stockage et transfert](#)

[Erreurs d'entrée et de sortie sur les périphériques réseau Cut-Through](#)

[Suivre et isoler les erreurs CRC](#)

[Causes premières des erreurs CRC](#)

[Résoudre les erreurs CRC](#)

[Informations connexes](#)

Introduction

Ce document décrit les erreurs CRC (Cyclic Redundancy Check) observées sur les compteurs d'interface et les statistiques des commutateurs Cisco Nexus.

Conditions préalables

Exigences

Cisco vous recommande de comprendre les bases de la commutation Ethernet et de l'interface de commande en ligne Cisco NX-OS (CLI). Pour plus d'informations, consultez l'un des documents applicables suivants :

- [Guide de configuration de base NX-OS de Cisco Nexus 9000, version 10.2 \(x\)](#)
- [Guide de configuration de base NX-OS de Cisco Nexus série 9000, version 9.3 \(x\)](#)
- [Guide de configuration de base NX-OS de Cisco Nexus série 9000, version 9.2 \(x\)](#)

- [Guide de configuration de base NX-OS de Cisco Nexus série 9000, version 7.x](#)
- [Résolution de problèmes Ethernet](#)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Commutateurs de la gamme Nexus 9000, à partir de la version 9.3(8) du logiciel NX-OS
- Commutateurs de la gamme Nexus 3000, à partir de la version 9.3(8) du logiciel NX-OS

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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Ce document décrit en détail les erreurs de contrôle de redondance cyclique (CRC) observées sur les compteurs d'interface sur les commutateurs de la gamme Cisco Nexus. Ce document décrit ce qu'est un CRC, comment il est utilisé dans le champ Frame Check Sequence (FCS) des trames Ethernet, comment les erreurs CRC se manifestent sur les commutateurs Nexus, et comment les erreurs CRC interagissent dans la commutation Store-and-Forward. Cet article décrit également les scénarios de commutation cut-through, les causes premières les plus probables des erreurs CRC et la manière de dépanner et de résoudre les erreurs CRC.

Matériel applicable

Les renseignements contenus dans ce document s'appliquent à tous les commutateurs Cisco Nexus. Certaines informations contenues dans ce document peuvent également s'appliquer à d'autres plateformes de routage et de commutation de Cisco, telles que les routeurs et les commutateurs Cisco Catalyst.

Définition de CRC

Un CRC est un mécanisme de détection d'erreurs couramment utilisé dans les réseaux informatiques et de stockage pour identifier les données modifiées ou corrompues pendant la transmission. Lorsqu'un périphérique connecté au réseau doit transmettre des données, il exécute un algorithme de calcul basé sur des codes cycliques sur les données, ce qui donne un numéro de longueur fixe. Ce numéro de longueur fixe s'appelle la valeur CRC, mais familièrement, il est souvent appelé le CRC sous sa forme abrégée. Cette valeur CRC est ajoutée aux données et transmise par le réseau vers un autre périphérique. Ce périphérique distant exécute le même algorithme de code cyclique sur les données et compare la valeur obtenue avec le CRC ajouté aux données. Si les deux valeurs correspondent, le périphérique distant suppose que les données ont été transmises sur le réseau sans être endommagées. Si les valeurs ne

correspondent pas, le périphérique distant suppose que les données ont été endommagées lors de la transmission sur le réseau. Ces données corrompues ne sont pas fiables et sont rejetées.

Les contrôleurs CRC sont utilisés pour la détection d'erreurs dans plusieurs technologies de réseau informatique, comme Ethernet (versions filaires et sans fil), Token Ring, le mode de transfert asynchrone (ATM) et le relayage de trames. Les trames Ethernet comportent un champ FCS (Frame Check Sequence) de 32 bits à la fin de la trame (immédiatement après la charge utile de la trame) où une valeur CRC de 32 bits est insérée.

Par exemple, envisageons un scénario dans lequel deux hôtes nommés Host-A et Host-B sont directement connectés l'un à l'autre par leurs cartes d'interface réseau (NIC). Host-A doit envoyer la phrase « Ceci est un exemple » à Host-B sur le réseau. Host-A crée une trame Ethernet destinée à Host-B avec la charge utile « Ceci est un exemple » et calcule que la valeur CRC de la trame est une valeur hexadécimale de 0xABCD. L'hôte A insère la valeur CRC de 0xABCD dans le champ FCS de la trame Ethernet, puis transmet la trame Ethernet de la carte réseau de l'hôte A à l'hôte B.

Lorsque l'hôte B reçoit cette trame, il peut calculer la valeur CRC de la trame à l'aide du même algorithme que l'hôte A. Host-B calcule que la valeur CRC de la trame est une valeur hexadécimale de 0xABCD, ce qui indique à Host-B que la trame Ethernet n'a pas été corrompue lors de la transmission de la trame à Host-B.

Définition d'une erreur CRC

Une erreur CRC se produit lorsqu'un périphérique (un périphérique réseau ou un hôte connecté au réseau) reçoit une trame Ethernet avec une valeur CRC dans le champ FCS de la trame qui ne correspond pas à la valeur CRC calculée par le périphérique pour la trame.

Ce concept est mieux illustré par un exemple. Voici un scénario dans lequel deux hôtes nommés Host-A et Host-B sont directement connectés l'un à l'autre par leurs cartes d'interface réseau (NIC). Host-A doit envoyer la phrase « Ceci est un exemple » à Host-B sur le réseau. Host-A crée une trame Ethernet destinée à Host-B avec la charge utile « Ceci est un exemple » et calcule que la valeur CRC de la trame est la valeur hexadécimale 0xABCD. L'hôte A insère la valeur CRC de 0xABCD dans le champ FCS de la trame Ethernet, puis transmet la trame Ethernet de la carte réseau de l'hôte A à l'hôte B.

Cependant, les dommages sur le support physique connectant Host-A à Host-B corrompent le contenu du cadre de sorte que la phrase dans le cadre devient « Ceci était un exemple » au lieu de la charge utile souhaitée « Ceci est un exemple ».

Lorsque l'hôte B reçoit cette trame, il peut calculer la valeur CRC de la trame et inclure la charge utile corrompue dans le calcul. Host-B calcule que la valeur CRC de la trame est une valeur hexadécimale de 0xDEAD, qui est différente de la valeur CRC 0xABCD dans le champ FCS de la trame Ethernet. Cette différence de valeurs CRC indique à Host-B que la trame Ethernet a été corrompue lors de la transmission de la trame à Host-B. Par conséquent, l'hôte B ne peut pas faire confiance au contenu de cette trame Ethernet et peut donc la supprimer. L'hôte B peut également incrémenter un certain type de compteur d'erreurs sur sa carte réseau, par exemple les

compteurs d'« erreurs d'entrée », d'« erreurs CRC » ou d'« erreurs RX ».

Symptômes courants des erreurs CRC

Les erreurs CRC se manifestent généralement de l'une des deux manières suivantes :

1. Compteurs d'erreurs incrémentaux ou non nuls sur les interfaces des périphériques connectés au réseau.
2. Perte de paquets/trames pour le trafic qui traverse le réseau en raison de périphériques connectés au réseau qui abandonnent des trames corrompues.

Ces erreurs se manifestent de façons légèrement différentes en fonction du périphérique avec lequel vous travaillez à l'époque. Ces sous-sections détaillent chaque type d'appareil.

Erreurs reçues sur les hôtes Windows

Les erreurs CRC sur les hôtes Windows se manifestent généralement par un compteur d'erreurs reçues non nul dans la sortie de la commande `netstat -e` à partir de l'invite de commande. Voici un exemple de compteur d'erreurs reçues non nul à partir de l'invite de commande d'un hôte Windows :

```
<#root>
```

```
>
```

```
netstat -e
```

```
Interface Statistics
```

```
Received
```

| | Sent | |
|---------------------|--------------|------------|
| Bytes | 1116139893 | 3374201234 |
| Unicast packets | 101276400 | 49751195 |
| Non-unicast packets | 0 | 0 |
| Discards | 0 | 0 |
| Errors | 47294 | |
| | 0 | |
| Unknown protocols | 0 | |

La carte réseau et son pilote respectif doivent prendre en charge la gestion des erreurs CRC reçues par la carte réseau pour que le nombre d'erreurs reçues signalées par la commande `netstat -e` soit exact. La plupart des cartes réseau modernes et leurs pilotes respectifs prennent en charge la comptabilisation précise des erreurs CRC reçues par la carte réseau.

Erreurs RX sur les hôtes Linux

Les erreurs CRC sur les hôtes Linux se manifestent généralement par l'affichage d'un compteur d'erreurs RX non nul dans la sortie de la commande `ifconfig`. Voici un exemple de compteur d'erreurs RX non nul à partir d'un hôte Linux :

```
<#root>
$
ifconfig eth0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.0.2.10 netmask 255.255.255.128 broadcast 192.0.2.255
    inet6 fe80::10 prefixlen 64 scopeid 0x20<link>
    ether 08:62:66:be:48:9b txqueuelen 1000 (Ethernet)
    RX packets 591511682 bytes 214790684016 (200.0 GiB)

RX errors 478920

    dropped 0 overruns 0 frame 0
    TX packets 85495109 bytes 288004112030 (268.2 GiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Les erreurs CRC sur les hôtes Linux peuvent également se manifester par l'affichage d'un compteur d'erreurs RX non nul dans la sortie de la commande `ip -s link show`. Voici un exemple de compteur d'erreurs RX non nul à partir d'un hôte Linux :

```
<#root>
$
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 carte réseau et son pilote respectif doivent prendre en charge la gestion des erreurs CRC reçues par la carte réseau pour que le nombre d'erreurs RX signalées par les commandes `ifconfig` ou `ip -s link show` soit exact. La plupart des cartes réseau modernes et leurs pilotes respectifs prennent en charge la comptabilisation précise des erreurs CRC reçues par la carte réseau.

Erreurs CRC sur les périphériques réseau

Les périphériques réseau fonctionnent dans l'un des deux modes de transfert suivants :

- Mode de transfert Store-and-Forward
- Mode de transfert Cut-Through

La façon dont un périphérique réseau gère une erreur CRC reçue varie en fonction de ses modes de transmission. Les sous-sections ci-dessous décrivent le comportement spécifique de chaque mode de transmission.

Erreurs d'entrée sur les périphériques réseau avec stockage et transfert

Lorsqu'un périphérique réseau fonctionnant en mode de transfert Store-and-Forward reçoit une trame, il peut mettre en mémoire tampon la trame entière (« Store ») avant de valider la valeur CRC de la trame, de prendre une décision de transfert sur la trame et de transmettre la trame à partir d'une interface (« Forward »). Par conséquent, lorsqu'un périphérique réseau fonctionnant en mode de transfert Store-and-Forward reçoit une trame corrompue avec une valeur CRC incorrecte sur une interface spécifique, il peut abandonner la trame et incrémenter le compteur « Erreurs d'entrée » sur l'interface.

En d'autres termes, les trames Ethernet corrompues ne sont pas transférées par les périphériques réseau fonctionnant en mode de transfert Store-and-Forward; elles sont écartées à l'entrée.

Les commutateurs Cisco Nexus des séries 7000 et 7700 fonctionnent en mode de transfert Store-and-Forward. Voici un exemple d'un compteur d'erreurs d'entrée et de compteur CRC/FCS non nul pour un commutateur Nexus 7000 ou 7700 :

```
<#root>
```

```
switch#
```

```
show interface
```

```
<snip>
```

```
Ethernet1/1 is up
```

```
  RX
```

```
    241052345 unicast packets  5236252 multicast packets  5 broadcast packets
```

```
    245794858 input packets  17901276787 bytes
```

```
    0 jumbo packets  0 storm suppression packets
```

```
    0 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
```

Les erreurs CRC peuvent également se manifester sous la forme d'un compteur « FCS-Err » non nul dans la sortie des erreurs `show interface counters`. Le compteur "Rcv-Err" dans la sortie de cette commande peut également avoir une valeur non nulle, qui est la somme de toutes les erreurs d'entrée (CRC ou non) reçues par l'interface. Un exemple de ce processus est montré ici :

```
<#root>
```

```
switch#
```

```
show interface counters errors
```

```
<snip>
```

```
-----  
Port          Align-Err    FCS-Err    Xmit-Err    Rcv-Err    UnderSize  OutDiscards  
-----  
Eth1/1                0      579204          0      579204          0          0
```

Erreurs d'entrée et de sortie sur les périphériques réseau Cut-Through

Lorsqu'un périphérique réseau fonctionnant en mode de transmission « Cut-Through » commence à recevoir une trame, il peut prendre une décision de transmission sur l'en-tête de trame et commencer à transmettre la trame à partir d'une interface dès qu'il en reçoit suffisamment pour prendre une décision de transmission valide. Comme les en-têtes de trame et de paquet se trouvent au début de la trame, cette décision de transfert est généralement prise avant la réception des données utiles de la trame.

Le champ FCS d'une trame Ethernet se trouve à la fin de la trame, immédiatement après la charge utile de la trame. Par conséquent, un périphérique réseau fonctionnant en mode de transfert Cut-Through peut déjà avoir commencé à transmettre la trame à partir d'une autre interface au moment où il peut calculer le CRC de la trame. Si le CRC calculé par le périphérique réseau pour la trame ne correspond pas à la valeur CRC présente dans le champ FCS, cela signifie que le périphérique réseau a transmis une trame corrompue à travers le réseau. Dans ce cas, le périphérique réseau peut incrémenter deux compteurs :

1. Le compteur « Erreurs d'entrée » sur l'interface où la trame corrompue a été reçue à l'origine.
2. Le compteur « Erreurs de sortie » sur toutes les interfaces où la trame corrompue a été transmise. Pour le trafic de monodiffusion, il peut généralement s'agir d'une seule interface. Toutefois, pour le trafic de diffusion, de multidiffusion ou de monodiffusion inconnue, il peut s'agir d'une ou de plusieurs interfaces.

Un exemple est illustré ici, où la sortie de la commande `show interface` indique que plusieurs trames corrompues ont été reçues sur l'Ethernet1/1 du périphérique réseau et transmises depuis l'Ethernet1/2 en raison du mode de transfert Cut-Through de l'appareil réseau :

```
<#root>
```

```
switch#
```

```
show interface
```

```
<snip>
```

```
Ethernet1/1 is up
```

```
RX
```

```
46739903 unicast packets 29596632 multicast packets 0 broadcast packets  
76336535 input packets 6743810714 bytes
```

```
15 jumbo packets 0 storm suppression bytes
0 runs 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
```

Les erreurs CRC peuvent également se manifester par un compteur « FCS-Err » non nul sur l'interface d'entrée et par des compteurs « Xmit-Err » non nuls sur les interfaces de sortie dans la sortie des erreurs `show interface counters errors`. Le compteur "Rcv-Err" sur l'interface d'entrée dans la sortie de cette commande peut également avoir une valeur non nulle, qui est la somme de toutes les erreurs d'entrée (CRC ou non) reçues par l'interface. Un exemple de ce processus est montré ici :

<#root>

switch#

`show interface counters errors`

<snip>

Port Align-Err

FCS-Err

Xmit-Err

Rcv-Err

UnderSize OutDiscards

Eth1/1

0

47294

0

47294

0

0

Eth1/2

0 0
47294
0 0 0

Le périphérique réseau peut également modifier la valeur CRC dans le champ FCS de la trame d'une manière spécifique qui indique aux périphériques réseau en amont que cette trame est endommagée. On parle alors de « piétinement » du CRC. La manière précise dont le CRC est modifié varie d'une plate-forme à l'autre, mais généralement, il calcule la valeur CRC de la trame corrompue, puis inverse cette valeur et l'insère dans le champ FCS de la trame. Voici un exemple de ceci :

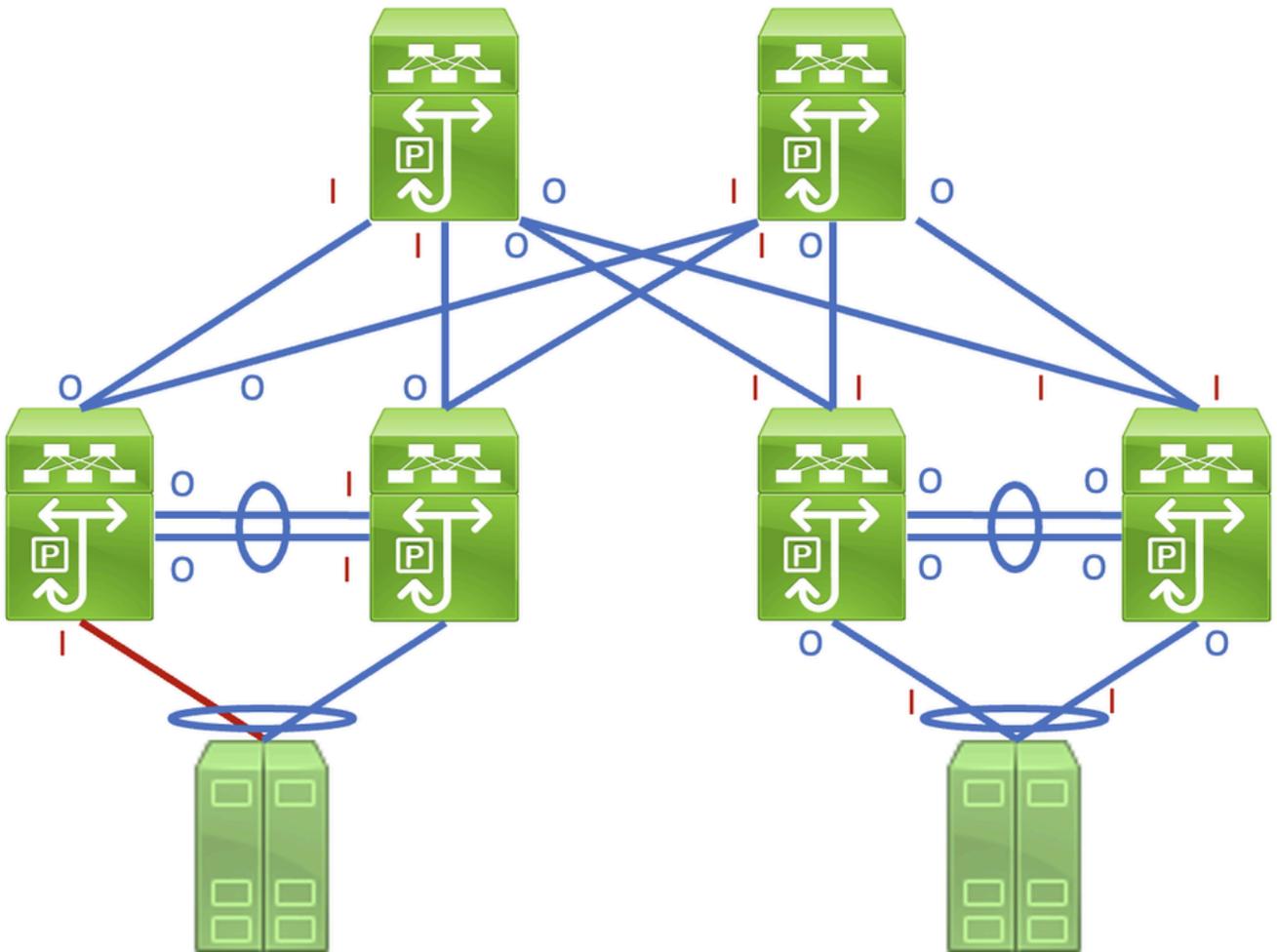
```
Original Frame's CRC: 0xABCD (1010101111001101)
Corrupted Frame's CRC: 0xDEAD (1101111010101101)
Corrupted Frame's Stomped CRC: 0x2152 (0010000101010010)
```

En raison de ce comportement, les périphériques réseau fonctionnant en mode de transfert Cut-Through peuvent propager une trame corrompue à travers tout le réseau. Si un réseau se compose de plusieurs périphériques réseau fonctionnant en mode de transfert Cut-Through, une seule trame corrompue peut entraîner l'incrémentation des compteurs d'erreurs d'entrée et de sortie sur plusieurs périphériques réseau de votre réseau.

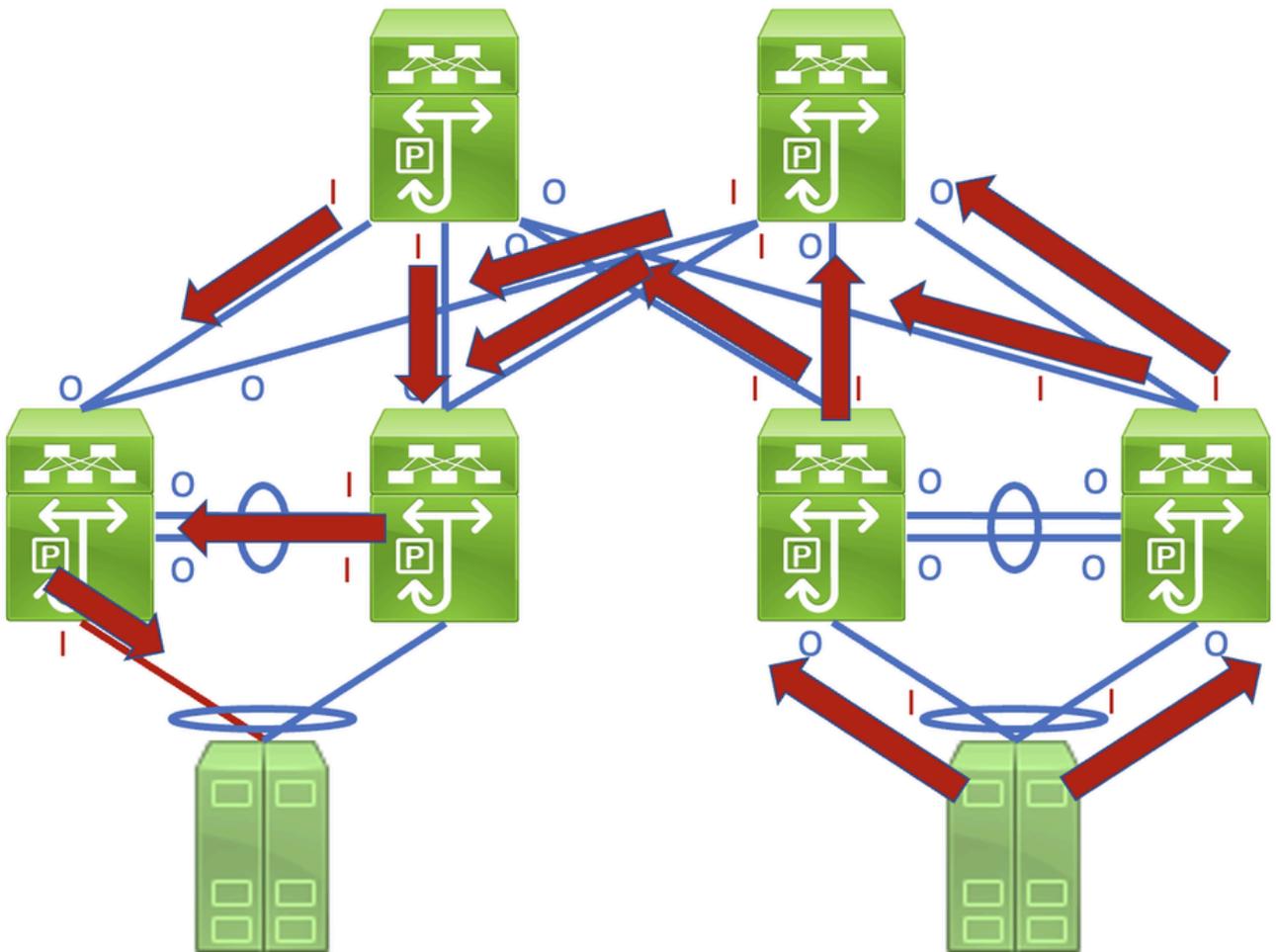
Suivre et isoler les erreurs CRC

La première étape pour identifier et résoudre la cause première des erreurs CRC consiste à isoler la source des erreurs CRC sur une liaison spécifique entre deux périphériques de votre réseau. Un périphérique connecté à cette liaison peut avoir un compteur d'erreurs de sortie d'interface avec une valeur de zéro ou n'est pas incrémentant, tandis que l'autre périphérique connecté à cette liaison peut avoir un compteur d'erreurs d'entrée d'interface non nul ou incrémentant. Ceci suggère que le trafic sort de l'interface d'un périphérique intact est corrompu au moment de la transmission au périphérique distant et est compté comme une erreur d'entrée par l'interface d'entrée de l'autre périphérique sur la liaison.

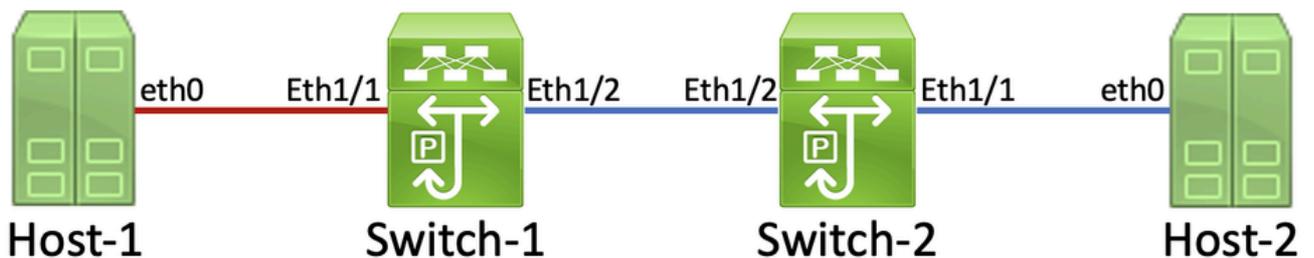
L'identification de cette liaison dans un réseau constitué de périphériques réseau fonctionnant en mode de transfert Store and Forward est une tâche simple. Cependant, si vous identifiez cette liaison dans un réseau constitué de périphériques réseau fonctionnant en mode Cut-Through forwarding, cela est plus difficile, car de nombreux périphériques réseau peuvent avoir des compteurs d'erreurs d'entrée et de sortie différents de zéro. Un exemple de ce phénomène peut être vu dans la topologie ici, où la liaison surlignée en rouge est endommagée de sorte que le trafic traversant la liaison est corrompu. Les interfaces étiquetées d'un « I » rouge indiquent des interfaces qui pourraient avoir des erreurs d'entrée non nulles, tandis que les interfaces étiquetées d'un « O » bleu indiquent des interfaces qui pourraient avoir des erreurs de sortie non nulles.



Ce document décrit les erreurs CRC (Cyclic Redundancy Check) observées sur les compteurs d'interface et les statistiques des commutateurs Cisco Nexus.



Un exemple illustre parfaitement un processus détaillé de suivi et d'identification d'une liaison endommagée. Examinez la topologie suivante :



Dans cette topologie, l'interface Ethernet1/1 d'un commutateur Nexus nommé Switch-1 est connectée à un hôte nommé Host-1 par l'intermédiaire de la carte d'interface réseau (NIC) eth0 de Host-1. L'interface Ethernet1/2 de Switch-1 est connectée à un deuxième commutateur Nexus, nommé Switch-2, par l'interface Ethernet1/2 de Switch-2. L'interface Ethernet1/1 du commutateur 2 est connectée à un hôte nommé Hôte-2 via la carte réseau Hôte-2 eth0.

La liaison entre l'hôte 1 et le commutateur 1 via l'interface Ethernet1/1 du commutateur 1 est endommagée et entraîne l'altération intermittente du trafic qui traverse la liaison. Cependant, on ne sait pas à ce stade si la liaison est endommagée. Vous devez suivre le chemin que les trames corrompues laissent dans le réseau via des compteurs d'erreurs d'entrée et de sortie non nuls ou incréments pour localiser la liaison endommagée dans ce réseau.

Dans cet exemple, la carte réseau de l'hôte 2 signale qu'elle reçoit des erreurs CRC.

```
<#root>
```

```
Host-2$
```

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

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DEFAULT group default qlen 1000  
    link/ether 00:50:56:84:8f:6d brd ff:ff:ff:ff:ff:ff
```

```
RX:
```

```
bytes  packets
```

```
errors
```

```
dropped overrun mcast
```

```
32246366102 444908978
```

```
478920
```

```
647      0      419445867
```

```
TX: bytes  packets  errors  dropped carrier collsns
```

```
3352693923 30185715 0        0        0        0
```

```
altname enp11s0
```

Vous savez que la carte réseau de l'hôte 2 se connecte au commutateur 2 via l'interface Ethernet1/1. Vous pouvez vérifier que l'interface Ethernet1/1 a un compteur d'erreurs de sortie non nul avec la commande show interface.

```
<#root>
```

```
Switch-2#
```

```
show interface
```

```
<snip>
```

```
Ethernet1/1 is up
```

```
admin state is up, Dedicated Interface
```

```
  RX
```

```
    30184570 unicast packets  872 multicast packets  273 broadcast packets
```

```
    30185715 input packets  3352693923 bytes
```

```
    0 jumbo packets  0 storm suppression bytes
```

```
    0 runs  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
```

Comme le compteur d'erreurs de sortie de l'interface Ethernet1/1 est non nul, il y a très probablement une autre interface de Switch-2 qui a un compteur d'erreurs d'entrée non nul. Vous pouvez utiliser la commande `show interface counters errors non-zero` afin de déterminer si des interfaces de Switch-2 ont un compteur d'erreurs d'entrée différent de zéro.

```
<#root>
```

```
Switch-2#
```

```
show interface counters errors non-zero
```

```
<snip>
```

```
-----
```

| Port | Align-Err | FCS-Err | Xmit-Err | Rcv-Err | UnderSize | OutDiscards |
|--------|-----------|---------|----------|---------|-----------|-------------|
| Eth1/1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 478920 | | | | | | |
| Eth1/2 | 0 | 0 | 0 | 0 | 0 | 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 |
|------|------------|
| | |

```
-----
```

Vous pouvez voir que l'Ethernet1/2 de Switch-2 a un compteur d'erreurs d'entrée non nul. Cela suggère que Switch-2 reçoit un trafic corrompu sur cette interface. Vous pouvez confirmer quel périphérique est connecté à l'Ethernet1/2 de Switch-2 grâce aux fonctionnalités du protocole de découverte Cisco (CDP) ou du protocole de découverte locale Link (LLDP). Un exemple est

illustré ici avec la commande show cdp neighbors.

```
<#root>
```

```
Switch-2#
```

```
show cdp neighbors
```

```
<snip>
```

```
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge  
S - Switch, H - Host, I - IGMP, r - Repeater,  
V - VoIP-Phone, D - Remotely-Managed-Device,  
s - Supports-STP-Dispute
```

```
Device-ID          Local Intrfce  Hldtme Capability Platform      Port ID
```

```
Switch-1
```

```
(FD012345678)
```

```
Eth1/2
```

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

```
Eth1/2
```

Vous savez maintenant que le commutateur Switch-2 reçoit du trafic corrompu sur son interface Ethernet1/2 à partir de l'interface Ethernet1/2 du commutateur Switch-1, mais vous ne savez pas encore si la liaison entre l'Ethernet1/2 du commutateur Switch-1 et l'Ethernet1/2 du commutateur Switch-2 est endommagée et provoque la corruption, ou si le commutateur Switch-1 est un commutateur cut-through qui transfère du trafic corrompu qu'il reçoit. Vous devez vous connecter à Switch-1 pour le vérifier.

Vous pouvez confirmer que l'interface Ethernet1/2 de Switch-1 a un compteur d'erreurs de sortie non nul à l'aide de la commande show interfaces.

```
<#root>
```

```
Switch-1#
```

```
show interface
```

```
<snip>
```

```
Ethernet1/2 is up
```

```
admin state is up, Dedicated Interface
```

```
RX
```

```
30581666 unicast packets 178 multicast packets 931 broadcast packets
```

```
30582775 input packets 3352693923 bytes
```

```
0 jumbo packets 0 storm suppression bytes
```

```
0 runts 0 giants 0 CRC 0 no buffer
```

```
0 input error 0 short frame 0 overrun 0 underrun 0 ignored
```

```
0 watchdog 0 bad etype drop 0 bad proto drop 0 if down drop
```

```
0 input with dribble 0 input discard
```

```
0 Rx pause
```

TX

454301132 unicast packets 734 multicast packets 72 broadcast packets
454301938 output packets 32246366102 bytes
0 jumbo packets

478920 output error

0 collision 0 deferred 0 late collision
0 lost carrier 0 no carrier 0 babble 0 output discard
0 Tx pause

Vous pouvez voir que l'Ethernet1/2 de Switch-1 a un compteur d'erreurs de sortie non nul. Cela suggère que la liaison entre l'Ethernet1/2 du commutateur 1 et l'Ethernet1/2 du commutateur 2 n'est pas endommagée ; au lieu de cela, le commutateur 1 est un commutateur cut-through qui transfère le trafic corrompu qu'il reçoit sur une autre interface. Comme démontré précédemment avec le commutateur Comm2, vous pouvez utiliser la commande `show interface counters errors non-zero` afin d'identifier si des interfaces du commutateur Comm1 ont un compteur d'erreurs d'entrée différent de zéro.

<#root>

Switch-1#

show interface counters errors non-zero

<snip>

Port Align-Err

FCS-Err

Xmit-Err

Rcv-Err

UnderSize OutDiscards

Eth1/1 0

478920

0

478920

0

0

0

Eth1/2

0

0

478920

0

0

0

| Port | Single-Co1 | Multi-Co1 | Late-Co1 | Exces-Co1 | Carri-Sen | Runts |
|-------|------------|-------------|-------------|-------------|-------------|------------|
| ----- | | | | | | |
| Port | Giants | SQETest-Err | Deferred-Tx | IntMacTx-Er | IntMacRx-Er | Symbol-Err |
| ----- | | | | | | |
| Port | InDiscards | | | | | |
| ----- | | | | | | |

Vous pouvez voir que l'Ethernet1/1 de Switch-1 a un compteur d'erreurs d'entrée non nul. Cela suggère que Switch-1 reçoit un trafic corrompu sur cette interface. Vous savez que cette interface se connecte à la carte réseau eth0 de l'hôte 1. Vous pouvez examiner les statistiques de l'interface de la carte réseau eth0 de l'hôte 1 pour vérifier si l'hôte 1 envoie des trames endommagées à partir de cette interface.

<#root>

Host-1\$

`ip -s link show eth0`

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DEFAULT group default qlen 1000
    link/ether 00:50:56:84:8f:6d brd ff:ff:ff:ff:ff:ff
    RX: bytes  packets  errors  dropped  overrun  mcast
         73146816142  423112898  0        0        0        437368817
```

TX:

bytes packets

errors

dropped carrier collsns
3312398924 37942624

0

0 0 0
altname enp11s0

Les statistiques de la carte réseau eth0 de l'hôte 1 indiquent que l'hôte ne transmet pas de trafic corrompu. Cela laisse supposer que la liaison entre eth0 de Host-1 et l'Ethernet1/1 de Switch-1 est endommagée et que c'est la source de la corruption du trafic. Vous devez dépanner ce lien pour identifier le composant défectueux à l'origine de cette corruption et le remplacer.

Causes premières des erreurs CRC

La cause la plus courante des erreurs CRC est un composant endommagé ou défectueux d'un lien physique entre deux périphériques. Exemples :

- Support physique (cuivre ou fibre) défaillant ou endommagé ou câbles à connexion directe (DAC).
- Émetteurs-récepteurs ou éléments optiques défaillants ou endommagés.
- Ports du tableau de connexions défaillants ou endommagés.
- Matériel de périphérique réseau défectueux (ports spécifiques, cartes de ligne, circuits intégrés ASIC [Application-Specific Integrated Circuits], MAC [Media Access Controls], modules de fabric, etc.).

- Carte d'interface réseau défectueuse insérée dans un hôte.

Il est également possible qu'un ou plusieurs périphériques mal configurés provoquent par inadvertance des erreurs CRC au sein d'un réseau. Par exemple, la non-concordance de la configuration de l'unité de transmission maximale (MTU) entre deux périphériques ou plus du réseau entraîne une troncature incorrecte des paquets volumineux. Lorsque vous identifiez et résolvez ce problème de configuration, il peut également corriger les erreurs CRC au sein d'un réseau.

Résoudre les erreurs CRC

Vous pouvez identifier le composant défectueux par un processus d'élimination :

1. Remplacez le support physique (en cuivre ou en fibre optique) ou le DAC par un support physique en bon état du même type.
2. Remplacez l'émetteur-récepteur inséré dans une interface de périphérique par un émetteur-récepteur du même modèle, dont le fonctionnement a été vérifié. Si cela ne résout pas les erreurs CRC, remplacez l'émetteur-récepteur inséré dans l'interface de l'autre périphérique par un émetteur-récepteur du même modèle, dont le fonctionnement a été vérifié.
3. Si des tableaux de connexions sont utilisés dans le cadre du lien endommagé, déplacez-le vers un port en bon état sur le tableau de connexions. Vous pouvez également éliminer le panneau de brassage comme cause première potentielle en connectant la liaison sans le panneau de brassage, si possible.
4. Déplacez le lien endommagé vers un port différent en état de fonctionnement sur chaque périphérique. Vous pouvez avoir besoin de tester plusieurs ports différents pour isoler une défaillance MAC, ASIC ou de carte de ligne.
5. Si le lien endommagé implique un hôte, déplacez le lien vers une autre NIC sur l'hôte. Vous pouvez également connecter la liaison endommagée à un hôte dont le fonctionnement a été vérifié afin d'isoler une défaillance de la carte réseau de l'hôte.

Si le composant défectueux est un produit Cisco (tel qu'un périphérique réseau ou un émetteur-récepteur Cisco) couvert par un contrat d'assistance actif, vous pouvez [ouvrir un dossier d'assistance auprès du TAC Cisco](#), inclure les détails de votre problème et faire remplacer le composant défectueux par une autorisation de retour de matériel (RMA).

Informations connexes

- [Procédure d'identification et de traçage des ASIC CRC pour Nexus 9000 Cloud Scale](#)

- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.