Dépannage du transfert intra-fabric ACI - Pertes intermittentes

Contenu

Introduction

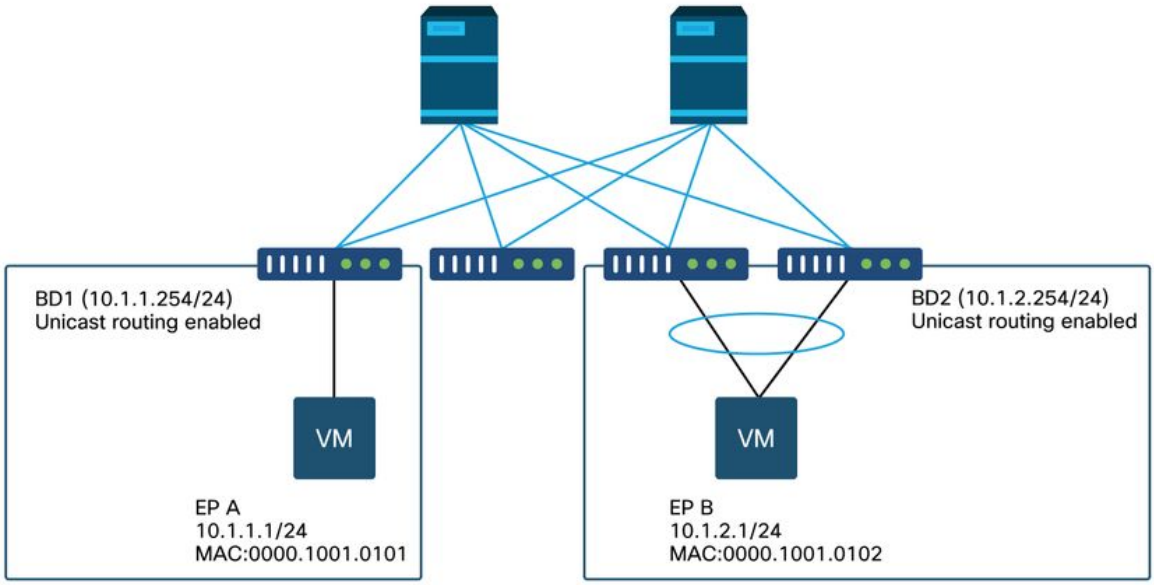
Ce document décrit les étapes pour dépanner les abandons intermittents dans l'ACI.

Informations générales

Le contenu de ce document a été extrait du livre Troubleshooting Cisco Application Centric Infrastructure, Second Edition, en particulier le chapitre **Intra-Fabric Forwarding - Intermittent Drops**.

Dépannage du transfert intra-fabric ACI - Pertes intermittentes

Exemple de topologie



Dans cet exemple, la requête ping envoyée depuis EP A (10.1.1.1) vers EP B (10.1.2.1) subit des pertes intermittentes.

```
[EP-A ~]$ ping 10.1.2.1 -c 10
PING 10.1.2.1 (10.1.2.1) 56(84) bytes of data.
64 bytes from 10.1.2.1: icmp_seq=1 ttl=231 time=142 ms
64 bytes from 10.1.2.1: icmp_seq=2 ttl=231 time=141 ms
                                <-- missing icmp_seq=3

64 bytes from 10.1.2.1: icmp_seq=4 ttl=231 time=141 ms
64 bytes from 10.1.2.1: icmp_seq=5 ttl=231 time=141 ms
64 bytes from 10.1.2.1: icmp_seq=6 ttl=231 time=141 ms
                                 <-- missing icmp_seq=7

64 bytes from 10.1.2.1: icmp_seq=8 ttl=231 time=176 ms
64 bytes from 10.1.2.1: icmp_seq=9 ttl=231 time=141 ms
64 bytes from 10.1.2.1: icmp_seq=10 ttl=231 time=141 ms
```

```
--- 10.1.2.1 ping statistics ---
10 packets transmitted, 8 received, 20% packet loss, time 9012ms
```

Workflow de dépannage

1. Déterminez la direction qui provoque les chutes intermittentes

Effectuez une capture de paquets (tcpdump, Wireshark, etc.) sur l'hôte de destination (EP B). Pour ICMP, concentrez-vous sur le numéro de séquence pour voir les paquets abandonnés par intermittence sont observés sur EP B.

```
[admin@EP-B ~]$ tcpdump -ni eth0 icmp
11:32:26.540957 IP 10.1.1.1 > 10.1.2.1: ICMP echo request, id 3569, seq 1, length 64
11:32:26.681981 IP 10.1.2.1 > 10.1.1.1: ICMP echo reply, id 3569, seq 1, length 64
11:32:27.542175 IP 10.1.1.1 > 10.1.2.1: ICMP echo request, id 3569, seq 2, length 64
11:32:27.683078 IP 10.1.2.1 > 10.1.1.1: ICMP echo reply, id 3569, seq 2, length 64
11:32:28.543173 IP 10.1.1.1 > 10.1.2.1: ICMP echo request, id 3569, seq 3, length 64   <---
11:32:28.683851 IP 10.1.2.1 > 10.1.1.1: ICMP echo reply, id 3569, seq 3, length 64     <---
11:32:29.544931 IP 10.1.1.1 > 10.1.2.1: ICMP echo request, id 3569, seq 4, length 64
11:32:29.685783 IP 10.1.2.1 > 10.1.1.1: ICMP echo reply, id 3569, seq 4, length 64
11:32:30.546860 IP 10.1.1.1 > 10.1.2.1: ICMP echo request, id 3569, seq 5, length 64
...
```

- Modèle 1 : tous les paquets sont observés lors de la capture de paquets EP B.

Les abandons doivent être dans la réponse d'écho ICMP (EP B à EP A).

- Modèle 2 : les pertes intermittentes sont observées lors de la capture de paquets EP B.

Les gouttes doivent être en écho ICMP (EP A à EP B).

2. Vérifiez si un autre protocole avec la même adresse IP source/de destination présente le même problème

Si possible, essayez de tester la connectivité entre les deux points d'extrémité à l'aide d'un protocole différent autorisé par le contrat entre eux (tel que ssh, telnet, http,...)

- Modèle 1 : les autres protocoles présentent la même baisse intermittente.

Le problème peut être lié au battement des terminaux ou à la mise en file d'attente/en mémoire tampon, comme indiqué ci-dessous.

- Modèle 2 - Seul le protocole ICMP présente une baisse intermittente.

Les tables de transfert (telles que la table de terminaux) ne doivent pas poser de problème, car le transfert est basé sur MAC et IP. La mise en file d'attente/en mémoire tampon ne devrait pas non plus être la raison, car cela affecterait d'autres protocoles. La seule raison pour laquelle l'ACI prendrait une décision de transfert différente basée sur le protocole serait l'exemple d'utilisation PBR.

Une possibilité est que l'un des noeuds spine a un problème. Lorsqu'un protocole est différent, le paquet ayant la même source et la même destination peut être équilibré en charge vers un autre port de matrice/liaison ascendante (c'est-à-dire un autre spine) par le leaf d'entrée.

Les compteurs atomiques peuvent être utilisés pour s'assurer que les paquets ne sont pas abandonnés sur les noeuds spine et qu'ils n'atteignent pas le leaf de sortie. Si les paquets n'ont pas atteint la feuille de sortie, vérifiez l'ELAM sur la feuille d'entrée pour voir quel port de fabric les

paquets sont envoyés. Pour isoler le problème d'un spine spécifique, les liaisons ascendantes leaf peuvent être arrêtées pour forcer le trafic vers un autre spine.

3. Vérifiez si cela est lié à un problème d'apprentissage des terminaux

L'ACI utilise une table de terminaux pour transférer les paquets d'un terminal à un autre. Un problème d'accessibilité intermittent peut être causé par le battement du point d'extrémité, car des informations inappropriées sur le point d'extrémité entraîneront l'envoi du paquet vers une destination incorrecte ou l'abandon du contrat comme son classement dans le mauvais EPG. Même si la destination est supposée être une L3Out au lieu d'un groupe de terminaux, assurez-vous que l'IP n'est pas apprise en tant que terminal dans le même VRF sur tous les commutateurs Leaf.

Reportez-vous à la sous-section « Fluctuation des points de terminaison » de cette section pour plus d'informations sur la façon de dépanner le battement des points de terminaison.

4. Vérifiez si elle est liée à des problèmes de mise en mémoire tampon en modifiant la fréquence du trafic

Augmentez ou diminuez l'intervalle de la requête ping pour voir si le taux de perte change. La différence d'intervalle doit être suffisamment importante.

Sous Linux, l'option -i peut être utilisée pour modifier l'intervalle (s) :

```
[EP-A ~]$ ping 10.1.2.1 -c 10 -i 5     -- Increase it to 5 sec
[EP-A ~]$ ping 10.1.2.1 -c 10 -i 0.2   -- Decrease it to 0.2 msec
```

Si le taux d'abandon augmente lorsque l'intervalle diminue, il est probablement lié à la mise en file d'attente ou à la mise en mémoire tampon sur les terminaux ou les commutateurs.

Le taux de perte à prendre en compte est (nombre de pertes/nombre total de paquets envoyés) au lieu de (nombre de pertes/temps).

Dans un tel scénario, vérifiez les points suivants.

1. Vérifiez si des compteurs de suppression sur les interfaces de commutateur augmentent avec la requête ping. Pour plus d'informations, reportez-vous à la section relative aux suppressions d'interface du chapitre « Transfert intra-fabric ».
2. Vérifiez si le compteur Rx augmente avec les paquets sur le point d'extrémité de destination. Si le compteur Rx est augmenté avec le même nombre que les paquets transmis, les paquets sont probablement abandonnés sur le point d'extrémité lui-même. Cela peut être dû à la mise en mémoire tampon des terminaux sur la pile TCP/IP.

Par exemple, si 100000 requêtes ping sont envoyées avec un intervalle aussi court que possible, le compteur Rx sur le point d'extrémité peut être observé lorsqu'il augmente de 100000.

```
[EP-B ~]$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 10.1.2.1  netmask 255.255.255.0  broadcast 10.1.2.255
      ether 00:00:10:01:01:02  txqueuelen 1000  (Ethernet)
      RX packets 101105  bytes 1829041
      RX errors 0  dropped 18926930  overruns 0  frame 0
```

```
TX packets 2057  bytes 926192
TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

5. Vérifiez si l'ACI envoie les paquets ou si la destination les reçoit

Effectuez une capture SPAN sur le port de sortie du commutateur Leaf pour éliminer le fabric ACI du chemin de dépannage.

Les compteurs Rx sur la destination peuvent également être utiles pour éliminer l'ensemble des commutateurs réseau du chemin de dépannage, comme indiqué dans les étapes précédentes pour la mise en mémoire tampon.

Fluctuation des extrémités

Cette section explique comment vérifier l'instabilité des terminaux. Vous trouverez des détails supplémentaires dans les documents suivants :

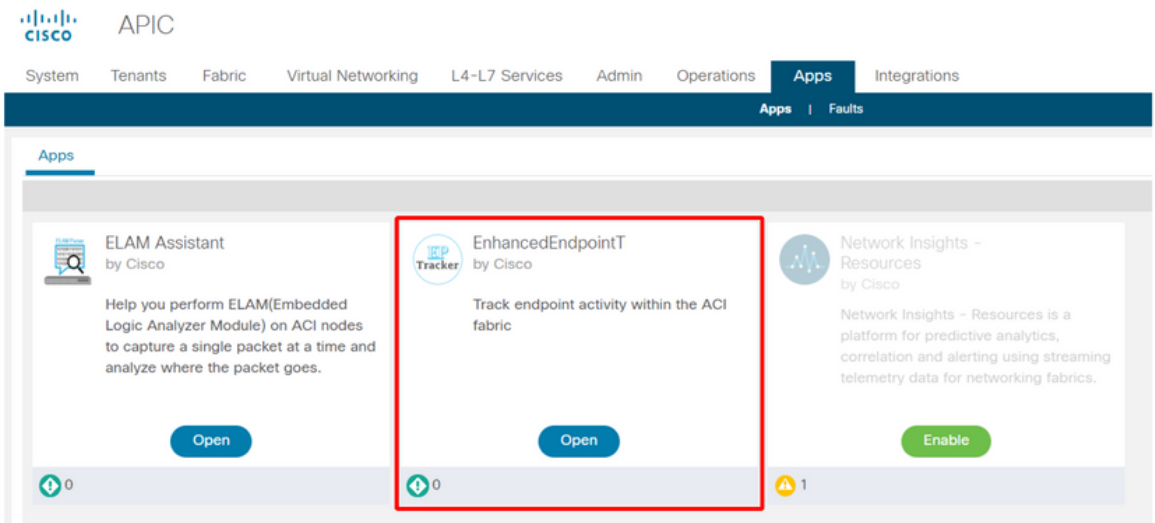
- «Livre blanc ACI Fabric Endpoint Learning » sur www.cisco.com
- «Dépannage de l'ACI Cisco Live BRKACI-2641 : Endpoints" sur www.ciscolive.com

Lorsque l'ACI apprend la même adresse MAC ou IP à plusieurs endroits, il semble que le terminal a été déplacé. Cela peut également être dû à un dispositif d'usurpation ou à une configuration incorrecte. Ce comportement est appelé battement de point d'extrémité. Dans un tel scénario, le trafic vers le point d'extrémité mobile/instable (adresse MAC pour le trafic ponté, adresse IP pour le trafic routé) échoue par intermittence.

La méthode la plus efficace pour détecter le battement des points d'extrémité consiste à utiliser Enhanced Endpoint Tracker. Cette application peut s'exécuter en tant qu'application ACI AppCenter ou en tant qu'application autonome sur un serveur externe au cas où elle aurait besoin de gérer un fabric beaucoup plus étendu.

Enhanced Endpoint Tracker

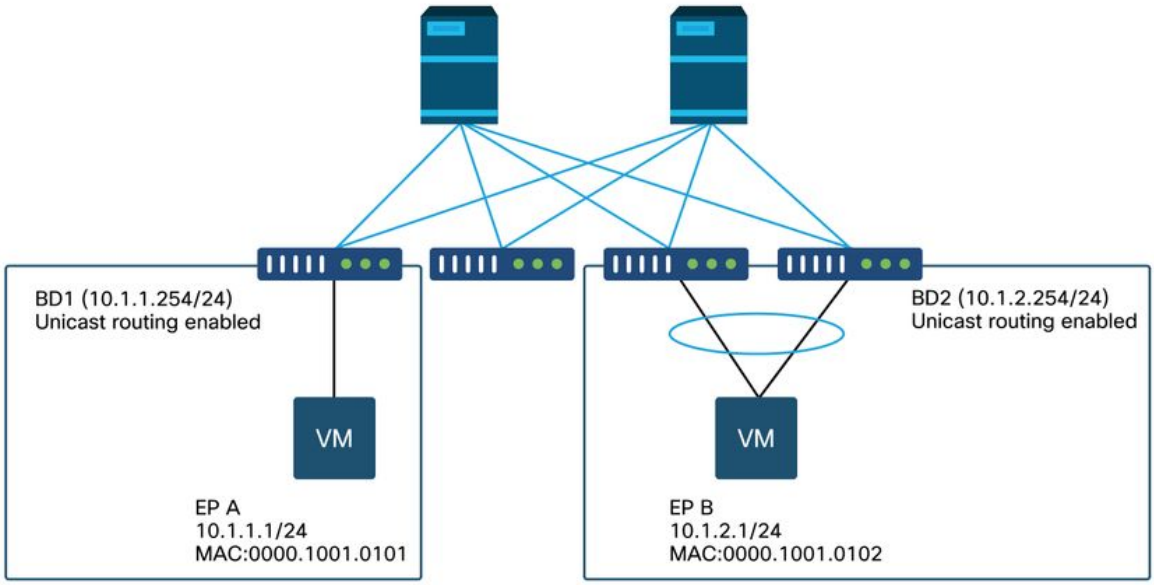
AVERTISSEMENT DE DÉPRÉCIATION ! Ce guide a été rédigé en 4.2. depuis lors, l'application Enhanced Endpoint Tracker a été dépréciée en faveur de la fonctionnalité sur Nexus Dashboard Insights. Pour plus d'informations, consultez l'ID de bogue Cisco CSCvz59365 .



L'image ci-dessus montre le dispositif Enhanced Endpoint Tracker dans AppCenter. L'exemple suivant montre comment rechercher des points d'extrémité instables à l'aide de Enhanced

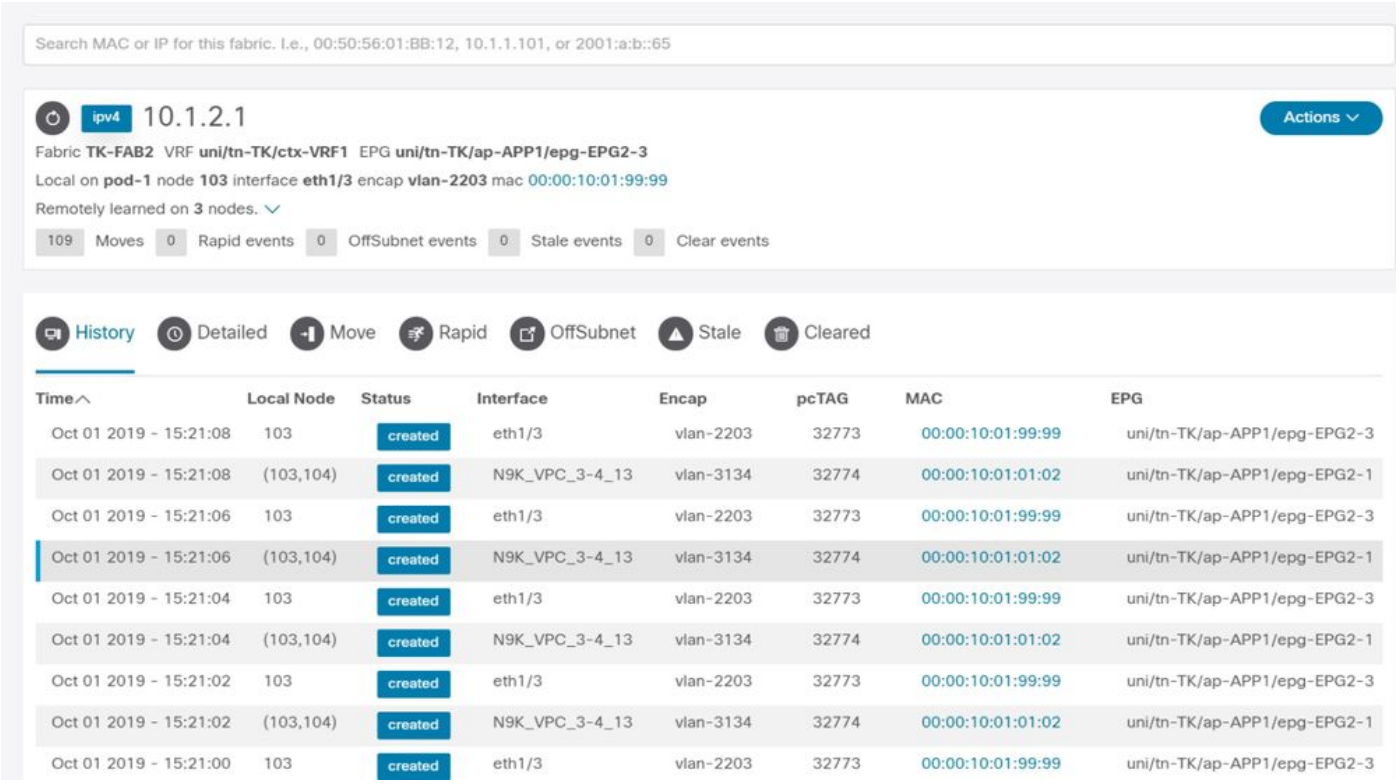
Endpoint Tracker.

Exemple de battement de terminal



Dans cet exemple, IP 10.1.2.1 devrait appartenir à EP B avec MAC 0000.1001.0102. Cependant, un EP X avec MAC 0000.1001.9999 fournit également du trafic avec IP 10.1.2.1 en raison d'une mauvaise configuration ou peut-être d'une usurpation IP.

Résultats de Enhanced Endpoint Tracker — Déplacements

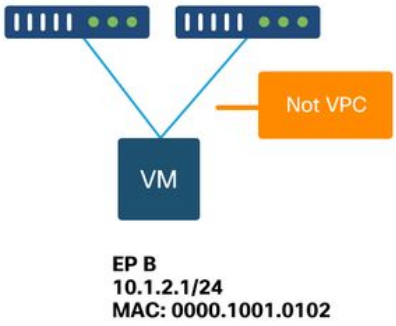


Le dispositif Enhanced Endpoint Tracker indique quand et où IP 10.1.2.1 a été appris. Comme l'illustre la capture d'écran ci-dessus, 10.1.2.1 oscille entre deux points d'extrémité avec les

adresses MAC 0000.1001.0102 (prévues) et 0000.1001.9999 (non prévues). Cela entraînera un problème d'accessibilité vers IP 10.1.2.1, car lorsqu'il est appris sur la mauvaise adresse MAC, le paquet sera envoyé à un mauvais périphérique via la mauvaise interface. Pour résoudre ce problème, prenez des mesures pour empêcher la machine virtuelle inattendue d'approvisionner le trafic avec une adresse IP inappropriée.

L'exemple suivant illustre un exemple typique de battement de point d'extrémité dû à une configuration inappropriée.

Exemple de topologie pouvant provoquer un basculement des terminaux



Lorsqu'un serveur ou une machine virtuelle est connecté à des noeuds leaf ACI via deux interfaces sans VPC, le serveur doit utiliser l'association de cartes réseau actives/en veille. Sinon, la charge des paquets est équilibrée sur les deux liaisons ascendantes et il semblerait que les points d'extrémité battent entre deux interfaces du point de vue du commutateur leaf ACI. Dans ce cas, le mode d'association actif/veille ou un mode d'association de carte réseau équivalent est requis ou utilisez simplement un VPC côté ACI.

Abandons d'interface

Ce chapitre décrit comment vérifier les principaux compteurs liés à l'abandon de l'interface d'entrée.

Types de compteurs de branchement matériels

Sur les commutateurs Nexus 9000 s'exécutant en mode ACI, l'ACI comporte trois compteurs matériels principaux pour les abandons d'interface d'entrée.

Transférer

Les principales raisons des chutes sont :

- SECURITY_GROUP_DENY : Abandon en raison de contrats manquants pour autoriser la communication.
- VLAN_XLATE_MISS : Une perte en raison d'un VLAN inapproprié. Par exemple, une trame entre dans le fabric avec un VLAN 10 802.1Q. Si le commutateur a le VLAN 10 sur le port, il inspecte le contenu et prend une décision de transmission basée sur l'adresse MAC de destination. Cependant, si VLAN 10 n'est pas autorisé sur le port, il le supprime et l'étiquette

comme VLAN_XLATE_MISS.
- ACL_DROP : Une baisse due à SUP-TCAM. La SUP-TCAM des commutateurs ACI contient des règles spéciales à appliquer en plus de la décision de transfert L2/L3 normale. Les règles de SUP-TCAM sont intégrées et ne sont pas configurables par l'utilisateur. L'objectif des règles SUP-TCAM est principalement de traiter certaines exceptions ou certains trafics de plan de contrôle et non destinés à être contrôlés ou surveillés par les utilisateurs. Lorsqu'un paquet entre en contact avec les règles SUP-TCAM et que la règle est d'abandonner le paquet, le paquet abandonné est compté comme ACL_DROP et il incrémente le compteur d'abandon de transmission.

Les abandons de transmission sont essentiellement des paquets abandonnés pour une raison connue valide. Ils peuvent généralement être ignorés et ne provoqueront pas de pénalités de performances, contrairement aux pertes de trafic de données réelles.

Erreur

Lorsque le commutateur reçoit une trame non valide, elle est abandonnée en tant qu'erreur. Les trames avec des erreurs FCS ou CRC en sont des exemples. Reportez-vous à la section ultérieure « CRC — FCS — cut-through switching » pour plus de détails.

Tampon

Lorsqu'un commutateur reçoit une trame et qu'aucune mémoire tampon n'est disponible pour l'entrée ou la sortie, la trame est abandonnée avec « Mémoire tampon ». Cela indique généralement une congestion quelque part dans le réseau. La liaison qui affiche la panne peut être pleine ou la liaison contenant la destination est encombrée.

Collecte des compteurs via l'API

Il est intéressant de noter qu'en exploitant l'API et le modèle objet, l'utilisateur peut rapidement interroger le fabric pour toutes les instances de ces abandons (exécutez-les à partir d'une apic).

```
# FCS Errors (non-stomped CRC errors)
moquery -c rmonDot3Stats -f 'rmon.Dot3Stats.fCSErrors>="1"' | egrep "dn|fCSErrors"

# FCS + Stomped CRC Errors
moquery -c rmonEtherStats -f 'rmon.EtherStats.cRCAlignErrors>="1"' | egrep "dn|cRCAlignErrors"

# Output Buffer Drops
moquery -c rmonEgrCounters -f 'rmon.EgrCounters.bufferdroppkts>="1"' | egrep "dn|bufferdroppkts"

# Output Errors
moquery -c rmonIfOut -f 'rmon.IfOut.errors>="1"' | egrep "dn|errors"
```

Affichage des statistiques de suppression dans CLI

Si des défaillances sont signalées ou s'il est nécessaire de vérifier les abandons de paquets sur les interfaces à l'aide de l'interface de ligne de commande, la meilleure façon d'y parvenir consiste à afficher les compteurs de plate-forme dans le matériel. Tous les compteurs ne sont pas affichés avec « show interface ». Les trois principales raisons de perte ne peuvent être visualisées qu'à l'aide des compteurs de plate-forme. Pour les afficher, procédez comme suit :

Feuille

Établissez une connexion SSH avec le leaf et exécutez ces commandes. Cet exemple concerne Ethernet 1/31.

```
ACI-LEAF# vsh_lc
module-1# show platform internal counters port 31
Stats for port 31
(note: forward drops includes sup redirected packets too)
IF          LPort                    Input                        Output
                                Packets       Bytes          Packets    Bytes
eth-1/31    31  Total          400719   286628225      2302918    463380330
                  Unicast     306610   269471065       453831     40294786
                  Multicast        0           0      1849091    423087288
                  Flood        56783     8427482            0            0
               Total Drops     37327                        0
                  Buffer           0                        0
                  Error            0                        0
                  Forward      37327
                  LB               0
                  AFD RED                                   0
...
```

Une colonne vertébrale fixe (N9K-C9332C et N9K-C9364C) peut être vérifiée en utilisant la même méthode que les commutateurs Leaf.

Pour une colonne vertébrale modulaire (N9K-C9504, etc.), la carte de ligne doit être attachée avant que les compteurs de la plate-forme puissent être affichés. Envoyez une requête SSH à la colonne vertébrale et exécutez ces commandes. Cet exemple concerne Ethernet 2/1.

```
ACI-SPINE# vsh
ACI-SPINE# attach module 2
module-2# show platform internal counters port 1
Stats for port 1
(note: forward drops include sup redirected packets too)
IF          LPort                    Input                        Output
                                Packets       Bytes          Packets    Bytes
eth-2/1      1  Total        85632884  32811563575     126611414   25868913406
                  Unicast   81449096  32273734109     104024872   23037696345
                  Multicast  3759719   487617769     22586542   2831217061
                  Flood            0           0            0            0
               Total Drops         0                        0
                  Buffer           0                        0
                  Error            0                        0
                  Forward          0
                  LB               0
                  AFD RED                                   0
...
```

Les compteurs d'état de mise en file d'attente sont affichés en utilisant « show queuing interface ». Cet exemple concerne Ethernet 1/5.

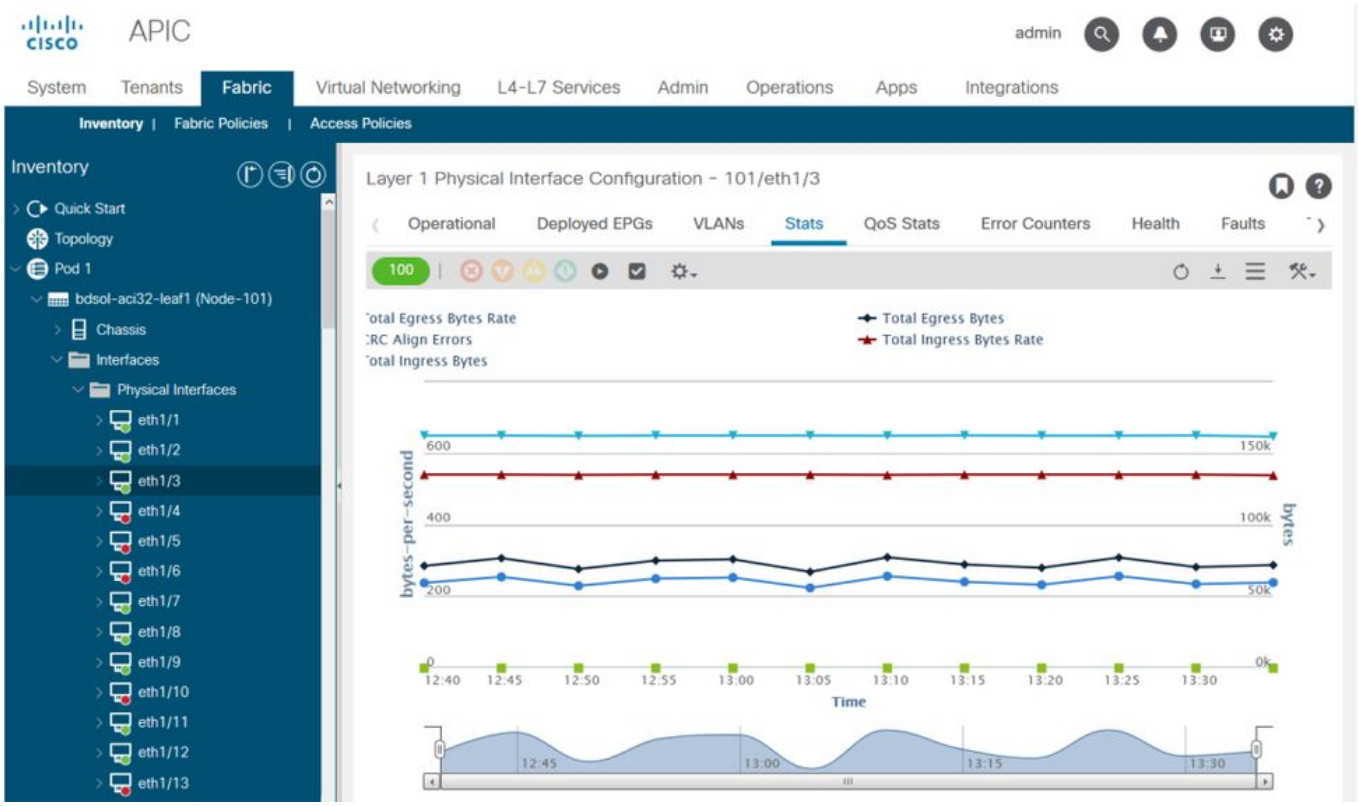
```
ACI-LEAF# show queuing interface ethernet 1/5
================================================================================
               Queuing stats for ethernet 1/5
```

```
================================================================================
================================================================================
                Qos Class level1
================================================================================
Rx Admit Pkts :  0                      Tx Admit Pkts :  0
Rx Admit Bytes:  0                      Tx Admit Bytes:  0
Rx Drop Pkts  :  0                      Tx Drop Pkts  :  0
Rx Drop Bytes :  0                      Tx Drop Bytes :  0

================================================================================
                Qos Class level2
================================================================================
Rx Admit Pkts :  0                      Tx Admit Pkts :  0
Rx Admit Bytes:  0                      Tx Admit Bytes:  0
Rx Drop Pkts  :  0                      Tx Drop Pkts  :  0
Rx Drop Bytes :  0                      Tx Drop Bytes :  0

================================================================================
                Qos Class level3
================================================================================
Rx Admit Pkts :  1756121                Tx Admit Pkts :  904909
Rx Admit Bytes:  186146554              Tx Admit Bytes:  80417455
Rx Drop Pkts  :  0                      Tx Drop Pkts  :  22
Rx Drop Bytes :  0                      Tx Drop Bytes :  3776

...
```

Affichage des statistiques dans la GUI

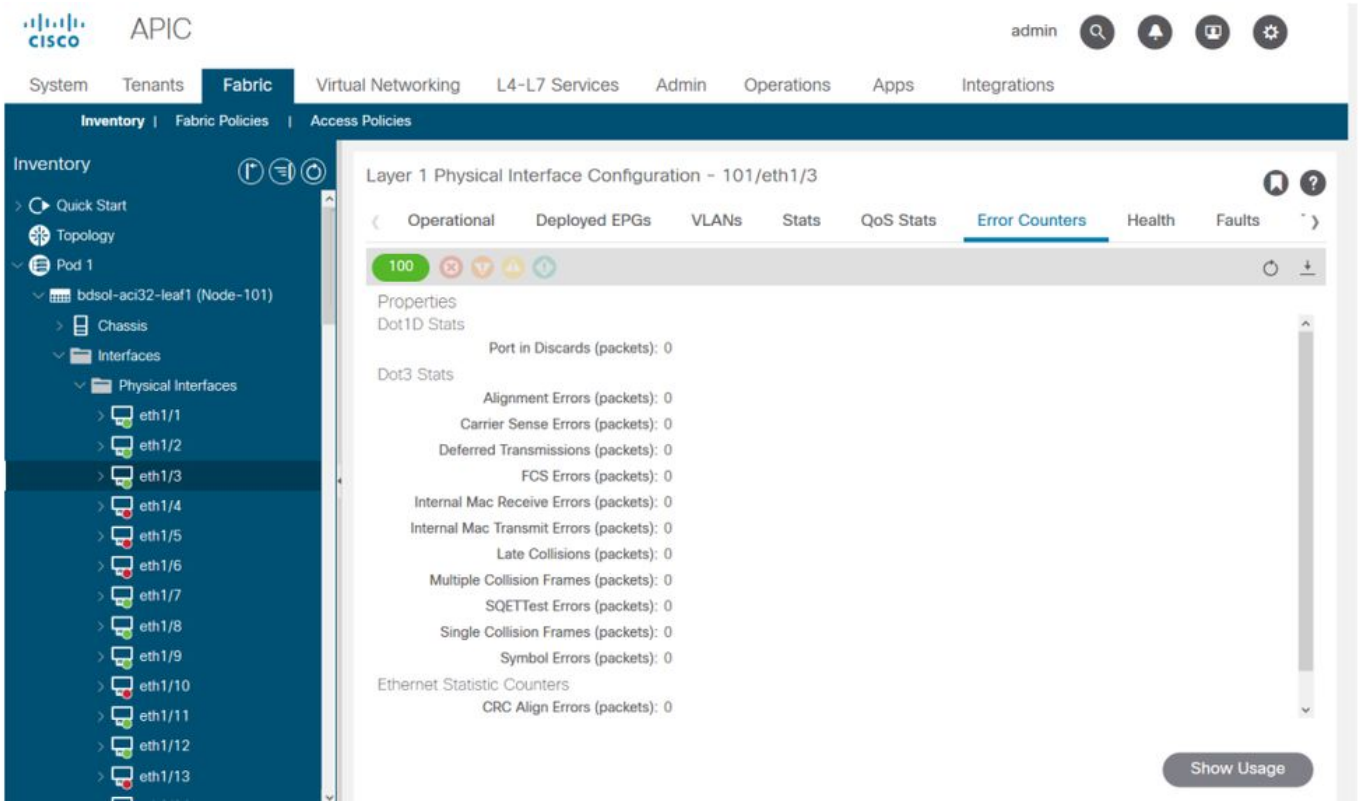
L'emplacement est 'Fabric > Inventory > Leaf/Spine > Physical interface > Stats'.

Statistiques d'interface GUI



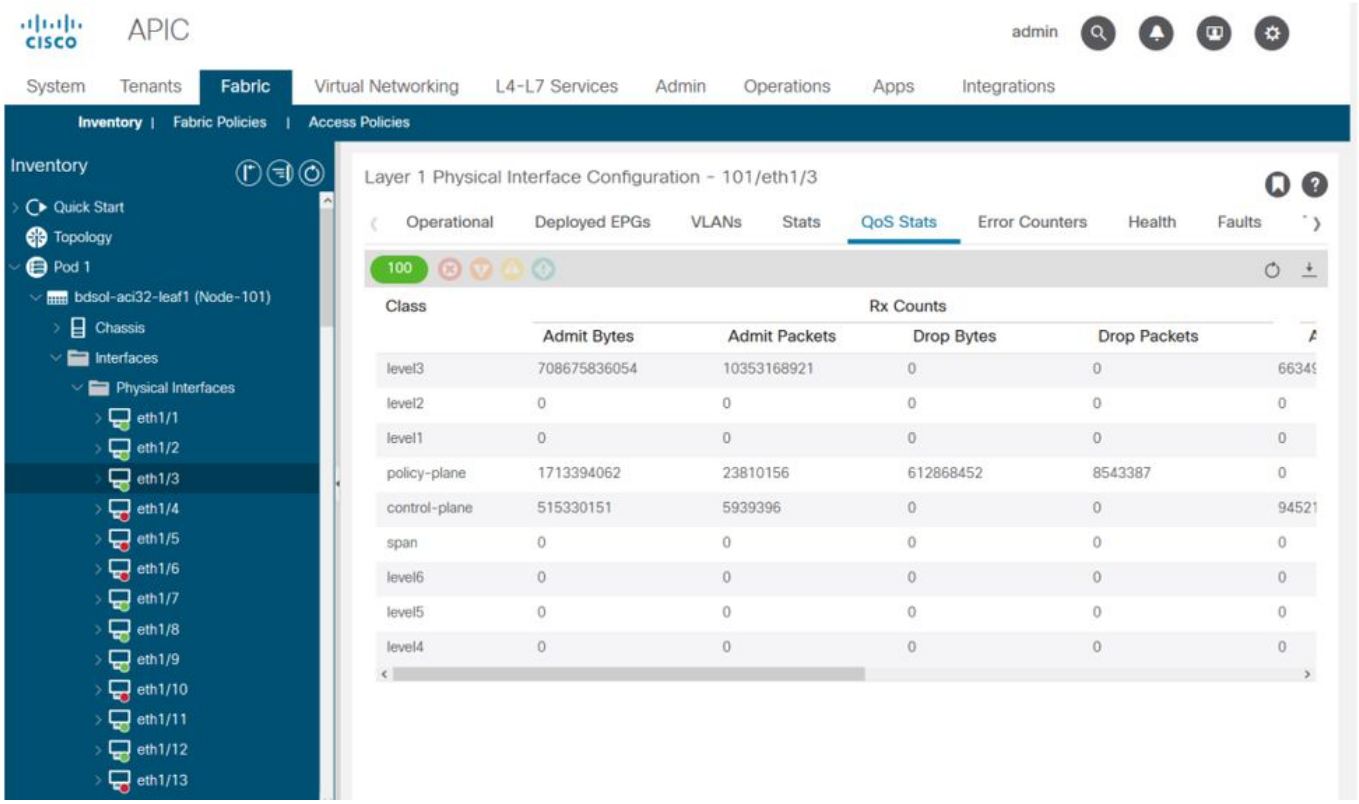
Les statistiques d'erreur sont visibles au même endroit :

Erreurs d'interface GUI



Enfin, l'interface utilisateur graphique peut afficher les statistiques QoS par interface :

Interface GUI - Compteurs QoS



CRC — FCS — commutation cut-through

Qu'est-ce que le contrôle par redondance cyclique (CRC) ?

CRC est une fonction polynomiale sur la trame qui renvoie un nombre 4B dans Ethernet. Il détecte toutes les erreurs de bits simples et un bon pourcentage d'erreurs de bits doubles. Il est donc destiné à assurer que la trame n'a pas été corrompue en transit. Si le compteur d'erreurs CRC augmente, cela signifie que lorsque le matériel a exécuté la fonction polynomiale sur la trame, le résultat était un nombre 4B qui différait du nombre 4B trouvé sur la trame elle-même. Les trames peuvent être corrompues pour plusieurs raisons, telles qu'une non-correspondance de mode duplex, un câblage défectueux et un matériel défectueux. Cependant, un certain niveau d'erreurs CRC doit être attendu et la norme autorise un taux d'erreurs allant jusqu'à 10-12 bits sur Ethernet (1 bit sur 1012 peut basculer).

Commutation « Store and Forward » et « Cut-through »

Les commutateurs de couche 2 « Store and Forward » et « Cut-through » basent leurs décisions de transmission sur l'adresse MAC de destination des paquets de données. Ils apprennent également les adresses MAC en examinant les champs MAC source (SMAC) des paquets lorsque les stations communiquent avec d'autres noeuds du réseau.

Un commutateur Store and Forward prend une décision de transmission sur un paquet de données après avoir reçu la trame entière et vérifié son intégrité. Un commutateur cut-through s'engage dans le processus de transmission peu après avoir examiné l'adresse MAC de destination (DMAC) d'une trame entrante. Cependant, un commutateur cut-through doit attendre d'avoir consulté l'intégralité du paquet avant d'effectuer la vérification CRC. Cela signifie qu'au moment de la validation du CRC, le paquet a déjà été transféré et ne peut pas être abandonné en cas d'échec de la vérification.

Traditionnellement, la plupart des périphériques réseau fonctionnaient en mode Store and Forward. Les technologies de commutation cut-through tendent à être utilisées dans les réseaux à haut débit qui exigent un transfert à faible latence.

En particulier, en ce qui concerne le matériel ACI de génération 2 et ultérieure, la commutation cut-through est effectuée si l'interface d'entrée est à une vitesse supérieure et l'interface de sortie est à la même vitesse ou à une vitesse inférieure. La commutation Store and Forward est effectuée si la vitesse de l'interface d'entrée est inférieure à celle de l'interface de sortie.

Martelage

Les paquets avec une erreur CRC nécessitent une suppression. Si la trame est commutée dans un chemin cut-through, la validation CRC se produit après que le paquet a déjà été transféré. En tant que telle, la seule option consiste à écraser la séquence de contrôle de trame Ethernet. L'**écrasement d'une trame implique de définir la séquence de contrôle de trame sur une valeur connue qui ne passe pas un contrôle CRC**. De ce fait, une trame défectueuse qui échoue le CRC peut apparaître comme CRC sur chaque interface qu'elle traverse, jusqu'à ce qu'elle atteigne un commutateur Store and Forward qui l'abandonne.

ACI et CRC : rechercher les interfaces défectueuses

- Si un leaf voit des erreurs CRC sur un port de liaison descendante, il s'agit principalement d'un problème sur le SFP de liaison descendante ou avec des composants sur le périphérique/réseau externe.

- Si une colonne vertébrale détecte des erreurs CRC, il s'agit principalement d'un problème sur ce port local, SFP, Fibre ou SFP voisin. Les paquets CRC défaillants des liaisons descendantes de feuille ne sont pas piétinés aux spines. Comme si ses en-têtes étaient lisibles, il est encapsulé VXLAN et le nouveau CRC sera calculé. Si les en-têtes n'étaient pas lisibles à partir d'une trame endommagée, le paquet serait abandonné.
- Si un noeud terminal détecte des erreurs CRC sur les liaisons de fabric, il peut être : Problème sur la paire fibre locale/SFP, la fibre d'entrée de la colonne vertébrale ou la paire SFP.Un cadre estampé fait son chemin à travers le tissu.

Stomping : dépannage du piétinement

- Recherchez les interfaces présentant des erreurs FCS sur le fabric. Comme la séquence de contrôle de trame est locale à un port, il s'agit très probablement de la fibre optique ou du module SFP à chaque extrémité.
- Les erreurs CRC sur la sortie « show interface » reflètent la valeur FCS+Stomp totale.\

Regardez un exemple :

Vérifiez un port à l'aide de la commande

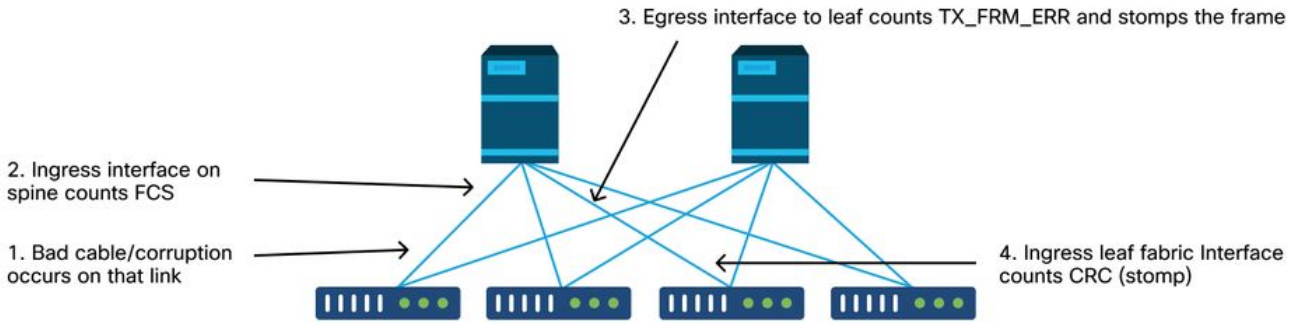
```
vsh_lc: 'show platform internal counter port <X>'
```

Dans cette commande, 3 valeurs sont importantes :

- RX_FCS_ERR - Échec FCS.
- RX_CRCERR - Trame d'erreur CRC estompée reçue.
- TX_FRM_ERROR - Trame d'erreur CRC tronquée transmise.

```
module-1# show platform internal counters port 1 | egrep ERR
       RX_FCS_ERR           0     ---- Real error local between the devices and its direct
neighbor
       RX_CRCERR            0     ---- Stomped frame --- so likely stomped by underlying devices
and generated further down the network
       TX_FRM_ERROR         0     ---- Packet received from another interface that was stomp on
Tx direction
```

Scénario de dépannage CRC Stop



Si une liaison corrompue génère un grand nombre de trames corrompues, ces trames peuvent être diffusées à tous les autres noeuds leaf et il est très possible de trouver CRC à l'entrée des liaisons ascendantes de fabric de la plupart des noeuds leaf du fabric. Ceux-ci proviendraient

probablement tous d'une seule liaison corrompue.

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.