Probleemoplossing voor ACI-doorsturen in intra-fabric - intermitterende drop

Inhoud

Inleiding

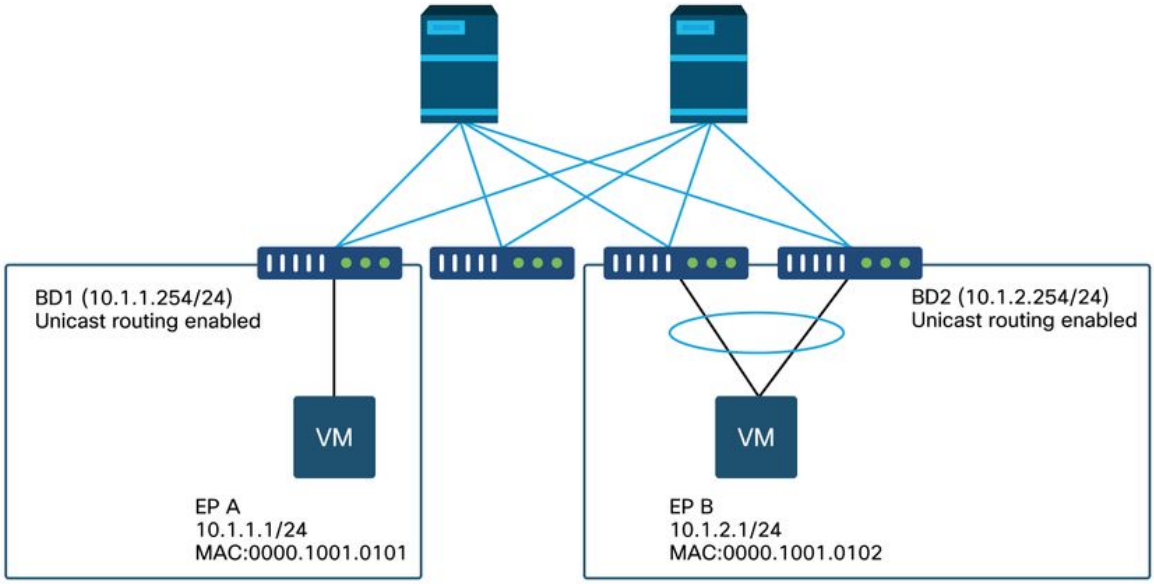
In dit document worden de stappen beschreven voor het oplossen van intermitterende drops in ACI.

Achtergrondinformatie

Het materiaal van dit document is afgeleid uit het boek Cisco Application Centric Infrastructure, Second Edition, met name het hoofdstuk **Intra-Fabric doorsturen - Intermittent drops**.

Probleemoplossing voor ACI Intra-Fabric Forwarding - onderbrekingen

Topologievoorbeeld



In dit voorbeeld ervaart ping van EP A (10.1.1.1) tot EP B (10.1.2.1) de intermitterende dalingen.

```
[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
```

Werkstroom voor probleemoplossing

1. Bepaal welke richting de intermitterende dalingen veroorzaakt

Voer een pakketopname (tcpdump, Wireshark, enzovoort) uit op de doelhost (EP-B). Voor ICMP, focus op het volgnummer om te zien de met tussenpozen gevallen pakketten worden waargenomen op 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
...
```

- Patroon 1 - Alle pakketten worden waargenomen op EP B-pakketopname.

De druppels moeten worden opgenomen in het ICMP echo antwoord (EP B naar EP A).

- Patroon 2 - De intermitterende dalingen worden waargenomen op EP B pakketopname.

De druppels moeten in ICMP echo (EP A tot EP B) worden geplaatst.

2. Controleer of een ander protocol met dezelfde bron/bestemming-IP hetzelfde probleem heeft

Indien mogelijk, probeer de connectiviteit tussen de twee eindpunten te testen met behulp van een ander protocol dat is toegestaan door het contract tussen hen (zoals ssh, telnet, http,..)

- Patroon 1 - Andere protocollen hebben dezelfde intermitterende daling.

Het probleem kan zijn in eindpunt flappen of wachtrij/buffering zoals hieronder weergegeven.

- Patroon 2 - Alleen ICMP heeft de intermitterende daling.

De tabellen doorsturen (zoals de endpointtabel) hoeft geen probleem te hebben omdat doorsturen gebaseerd is op MAC en IP. Wachtrijen/bufferen zou ook niet de reden moeten zijn, omdat dit andere protocollen zou beïnvloeden. De enige reden dat ACI een ander op protocol gebaseerd doorsturen besluit zou maken is de PBR use-case.

Eén mogelijkheid is dat één van de wervelkolomknooppunten een probleem heeft. Wanneer een protocol anders is, kan het pakket met dezelfde bron en bestemming worden geladen in een andere uplink/fabric-poort (d.w.z. een andere wervelkolom) door het toegangsblad.

Met behulp van atoomtellers kan ervoor worden gezorgd dat pakketten niet op wervelwervelknooppunten en bereik naar het uitgangsblad vallen. Als de pakjes niet bij het uitgangsblad kwamen, controleer dan de ELAM op het ingangsblad om te zien welke fabricpoort de pakjes worden verzonden. Om de kwestie aan een specifieke wervelkolom te isoleren, kunnen de bladopstraalverbindingen worden gesloten om het verkeer naar een andere wervelkolom te dwingen.

3. Controleer of het gerelateerd is aan een leerprobleem met endpoints

ACI gebruikt een endpointtabel om pakketten van het ene eindpunt naar een ander eindpunt te sturen. Een intermitterende bereikbaarheidskwestie kan door eindpunt worden veroorzaakt klapend omdat de ongepaste eindpuntinformatie zal veroorzaken dat het pakket wordt verzonden naar een verkeerde bestemming of om contract te zijn gelaten vallen zoals zijn geclassificeerd in verkeerde EPG. Zelfs als de bestemming een L3Out in plaats van een eindpuntgroep zou moeten zijn, zorg ervoor dat IP niet als eindpunt in zelfde VRF over om het even welke bladswitches wordt geleerd.

Zie de subsectie "Endpoint Flapping" in deze sectie voor meer informatie over het oplossen van problemen bij het flappen van eindpunten.

4. Controleer of dit verband houdt met buffering door de verkeersfrequentie te wijzigen

Verhoog of verlaag het interval van ping om te zien of de druppelverhouding verandert. Het interval moet groot genoeg zijn.

In Linux kan de optie '-i' worden gebruikt om het interval (sec) te wijzigen:

```
[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
```

Als de druppelverhouding toeneemt wanneer het interval wordt verlaagd, is dit waarschijnlijk gerelateerd aan wachtrijen of buffering op eindpunten of switches.

De druppelverhouding is (aantal druppels/totaal verzonden pakketten) in plaats van de (aantal druppels/tijd).

Controleer in dat geval het volgende.

1. Controleer of er bij de switch-interfaces meer druppeltellers komen, samen met de ping. Zie de sectie "Interface drops" in het hoofdstuk "Intra-Fabric Forwarding" voor meer informatie.
2. Controleer of de Rx-teller samen met de pakketten op het doeleindpunt toeneemt. Als de Rx-teller wordt verhoogd met hetzelfde nummer als de verzonden pakketten, worden pakketten waarschijnlijk op het eindpunt zelf gedropt. Dit kan het gevolg zijn van endpointbuffering op TCP/IP-stack.

Bijvoorbeeld, als 100000 met zo kort mogelijke interval worden verzonden, kan de Rx teller op het eindpunt worden waargenomen aangezien het door 100000 stijgt.

```
[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. Controleer of ACI de pakketten verstuurt of dat de bestemming de pakketten ontvangt

Neem een SPAN-opname op de uitgangspoort van de switch om ACI-stof te verwijderen uit het pad voor probleemoplossing.

Rx-tellers op de bestemming kunnen ook handig zijn om de gehele netwerk switches te elimineren van het pad voor probleemoplossing zoals in de vorige stappen voor buffering.

Endpoint flapping

In deze paragraaf wordt uitgelegd hoe u op flappen van eindpunten moet controleren. Deze documenten bevatten meer informatie:

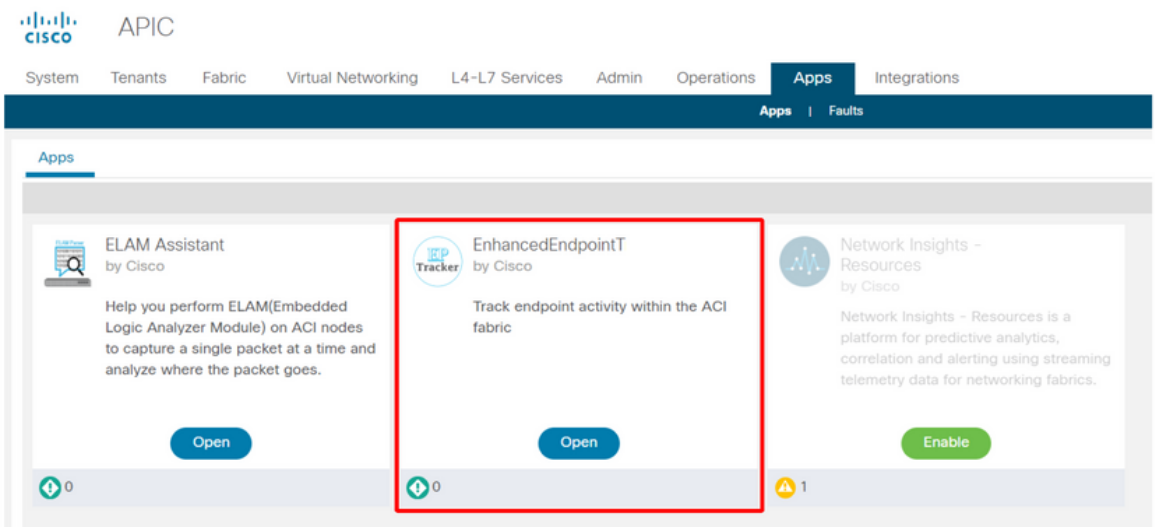
- "ACI Fabric Endpoint Learning Whitepaper" op www.cisco.com
- "Cisco Live ACI-2641 ACI voor probleemoplossing: Endpoints" op www.ciscolive.com

Wanneer ACI hetzelfde MAC- of IP-adres op meerdere locaties leert, ziet het eruit alsof het eindpunt is verplaatst. Dit kan ook worden veroorzaakt door een spoofingapparaat of een verkeerde configuratie. Dit gedrag wordt eindpuntflapping genoemd. In een dergelijk scenario zal verkeer naar het bewegende/flappende eindpunt (MAC-adres voor overbrugd verkeer, IP-adres voor routed verkeer) met tussenpozen falen.

De meest effectieve methode om eindpunt flapping te detecteren is om de Enhanced Endpoint Tracker te gebruiken. Deze app kan worden uitgevoerd als een ACI AppCenter-app of als een standalone-app op een externe server voor het geval er een veel grotere verbinding moet worden beheerd.

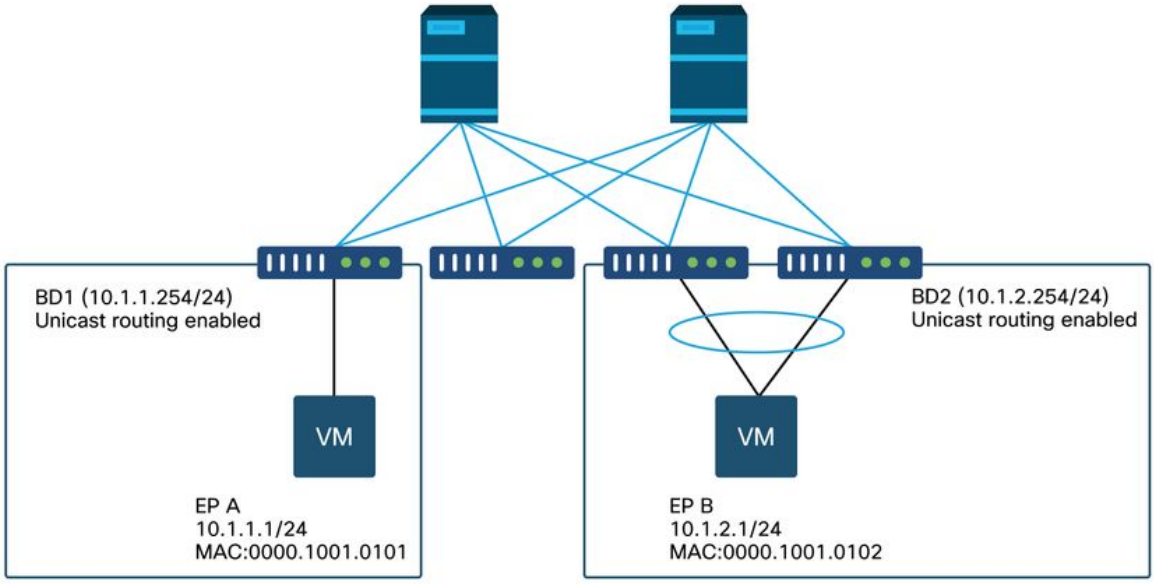
Enhanced Endpoint Tracker

WAARSCHUWING VOOR VOORBEDACHTEN RADE! Deze gids is geschreven op 4.2; sindsdien is de Enhanced Endpoint Tracker-app afgekeurd ten gunste van functionaliteit op Nexus Dashboard Insights. Zie Cisco bug-id CSCvz voor meer informatie59365 .



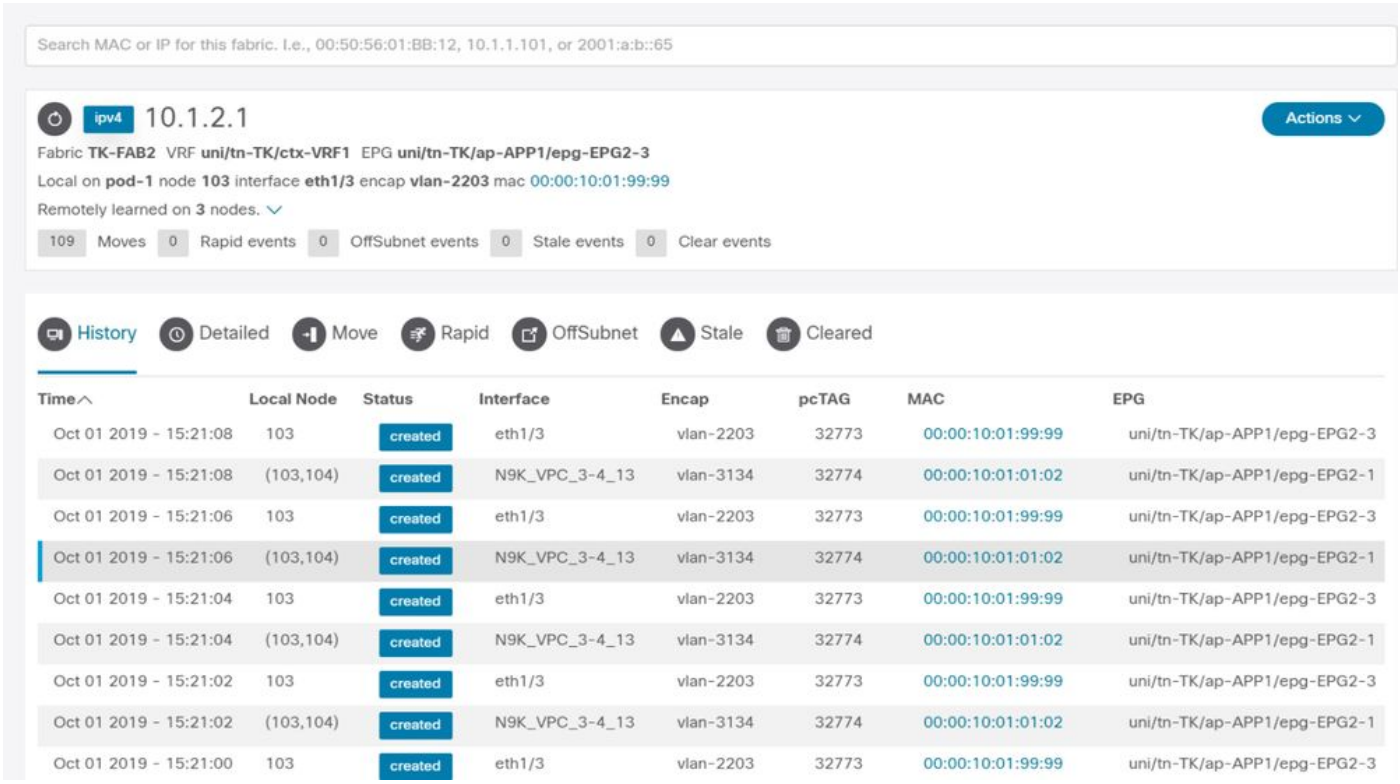
Het bovenstaande beeld toont de Enhanced Endpoint Tracker in AppCenter. Hieronder ziet u een voorbeeld van hoe u flappende eindpunten kunt vinden met de Enhanced Endpoint Tracker.

Voorbeeld van flappen voor endpoints



In dit voorbeeld zou IP 10.1.2.1 moeten behoren tot EP B met MAC 0000.1001.0102. Een EP X met MAC 0000.1001.9999 is echter ook bezig met het inkopen van verkeer met IP 10.1.2.1 vanwege een misconfiguratie of misschien IP-spoofing.

Uitgebreide Endpoint Tracker-uitvoer — Bewegingen



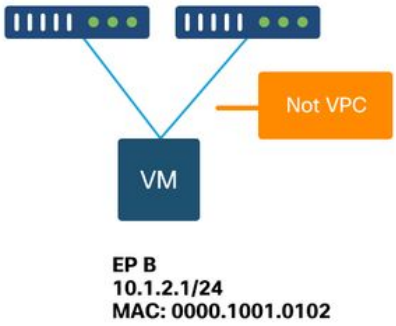
Time	Local Node	Status	Interface	Encap	pcTAG	MAC	EPG
Oct 01 2019 - 15:21:08	103	created	eth1/3	vlan-2203	32773	00:00:10:01:99:99	uni/tn-TK/ap-APP1/epg-EPG2-3
Oct 01 2019 - 15:21:08	(103,104)	created	N9K_VPC_3-4_13	vlan-3134	32774	00:00:10:01:01:02	uni/tn-TK/ap-APP1/epg-EPG2-1
Oct 01 2019 - 15:21:06	103	created	eth1/3	vlan-2203	32773	00:00:10:01:99:99	uni/tn-TK/ap-APP1/epg-EPG2-3
Oct 01 2019 - 15:21:06	(103,104)	created	N9K_VPC_3-4_13	vlan-3134	32774	00:00:10:01:01:02	uni/tn-TK/ap-APP1/epg-EPG2-1
Oct 01 2019 - 15:21:04	103	created	eth1/3	vlan-2203	32773	00:00:10:01:99:99	uni/tn-TK/ap-APP1/epg-EPG2-3
Oct 01 2019 - 15:21:04	(103,104)	created	N9K_VPC_3-4_13	vlan-3134	32774	00:00:10:01:01:02	uni/tn-TK/ap-APP1/epg-EPG2-1
Oct 01 2019 - 15:21:02	103	created	eth1/3	vlan-2203	32773	00:00:10:01:99:99	uni/tn-TK/ap-APP1/epg-EPG2-3
Oct 01 2019 - 15:21:02	(103,104)	created	N9K_VPC_3-4_13	vlan-3134	32774	00:00:10:01:01:02	uni/tn-TK/ap-APP1/epg-EPG2-1
Oct 01 2019 - 15:21:00	103	created	eth1/3	vlan-2203	32773	00:00:10:01:99:99	uni/tn-TK/ap-APP1/epg-EPG2-3

De Enhanced Endpoint Tracker toont wanneer en waar IP 10.1.2.1 is geleerd. Zoals in de screenshot hierboven wordt getoond, knippert 10.1.2.1 tussen twee eindpunten met MAC 0000.1001.0102 (verwacht) en 0000.1001.9999 (niet verwacht). Dit zal een bereikbaarheidsprobleem naar IP 10.1.2.1 veroorzaken omdat wanneer het op het verkeerde adres van MAC wordt geleerd, het pakket naar een verkeerd apparaat via de verkeerde interface zal worden verzonden. Om dit op te lossen, moet u stappen ondernemen om te voorkomen dat de

onverwachte VM verkeer met een ongeschikt IP-adres gaat kopen.

Hieronder ziet u een typisch voorbeeld van flappen op eindpunten door een onjuiste configuratie.

Topologievoorbeeld dat eindpunt flapping kan veroorzaken



Wanneer een server of VM via twee interfaces zonder VPC is verbonden met ACI-bladknooppunten, moet de server Active/Standby NIC-teaming gebruiken. Anders worden de pakketten met beide uplinks gebalanceerd en ziet het eruit alsof de eindpunten tussen twee interfaces knipperen vanuit het perspectief van de ACI-switch. In dit geval is de Active/Standby- of equivalente NIC-teammodus vereist of gebruik alleen een VPC aan de ACI-zijde.

Interfacedalingen

In dit hoofdstuk wordt beschreven hoe u de belangrijkste tellers met betrekking tot de indringingsinterface kunt controleren.

Hardware drop-tellers

Op Nexus 9000 switches die in ACI-modus draaien, zijn er drie belangrijke hardwaretellers op de ACI voor ingress-interfacedalingen.

Doorsturen

Belangrijke redenen voor druppels zijn:

- SECURITY_GROUP_DENY: Een daling vanwege ontbrekende contracten om de communicatie toe te staan.
- VLAN_XLATE_MISS: Een daling wegens ongepast VLAN. Een frame gaat bijvoorbeeld de stof in met een 802.1Q VLAN 10. Als de switch VLAN 10 op de poort heeft, zal het de inhoud inspecteren en een doorsturen besluit maken op basis van de bestemmings-MAC. Als VLAN 10 echter niet is toegestaan op de poort, zal het het laten vallen en labelen als VLAN_XLATE_MISS.
- ACL_DROP: Een druppel vanwege SUP-TCAM. SUP-TCAM in ACI-switches bevat speciale regels die moeten worden toegepast bovenop de normale L2/L3-doorsturen. Regels in SUP-TCAM zijn ingebouwd en kunnen niet door de gebruiker worden geconfigureerd. Het doel van de SUP-TCAM-regels is voornamelijk om bepaalde uitzonderingen of een bepaald verkeer

van besturingsplanten aan te pakken en niet bedoeld om te worden gecontroleerd of gecontroleerd door gebruikers. Wanneer een pakket op SUP-TCAM regels drukt en de regel is om het pakket te laten vallen, wordt het gedropte pakket geteld als ACL_DROP en het zal de voorwaartse drop teller verhogen.

Voorwaartse druppels zijn in wezen pakketten die om een geldige bekende reden worden gedropt. Zij kunnen over het algemeen worden genegeerd en zullen geen prestatiesstraffen veroorzaken, in tegenstelling tot echt gegevensverkeer daalt.

Fout

Wanneer de switch een ongeldig frame ontvangt, wordt dit als een fout weergegeven. Voorbeelden hiervan zijn frames met FCS- of CRC-fouten. Zie de laatste sectie "CRC — FCS — cut-through switching" voor meer informatie.

buffer

Wanneer een switch een frame ontvangt en er geen buffers beschikbaar zijn voor in- of uitgangen, wordt het frame met 'Buffer' gedropt. Dit duidt doorgaans op congestie ergens in het netwerk. De link die de fout toont kan vol zijn, of de link met de bestemming is verstopt.

Verzameltellers met behulp van de API

Het is de moeite waard om op te merken dat door het hefboomeffect van de API en het objectmodel, de gebruiker snel kan vragen de stof voor alle instanties van deze druppels (voer deze uit een 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"
```

Dropstatistieken bekijken in CLI

Als er fouten worden opgemerkt, of als er een noodzaak is om pakketdalingen op interfaces te controleren met de CLI, is de beste manier om dit te doen door de platformtellers in hardware te bekijken. Niet alle tellers worden weergegeven met 'show interface'. De drie belangrijkste redenen kunnen alleen worden bekeken met behulp van de platformtellers. Voer de volgende stappen uit om deze te bekijken:

Blad

SSH naar het blad en voer deze opdrachten uit. Dit voorbeeld is voor 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
...
```

Een vaste ruggengraat (N9K-C933C en N9K-C9364C) kan worden gecontroleerd met dezelfde methode als de switches.

Voor een modulaire wervelkolom (N9K-C9504 etc.), moet de lijnkaart worden bevestigd alvorens de platformtellers kunnen worden bekeken. SSH naar de wervelkolom en voer deze opdrachten uit. Dit voorbeeld is voor 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
...
```

De statstellers van wachtrijen worden weergegeven met behulp van 'show wachtrij interface'. Dit voorbeeld is voor Ethernet 1/5.

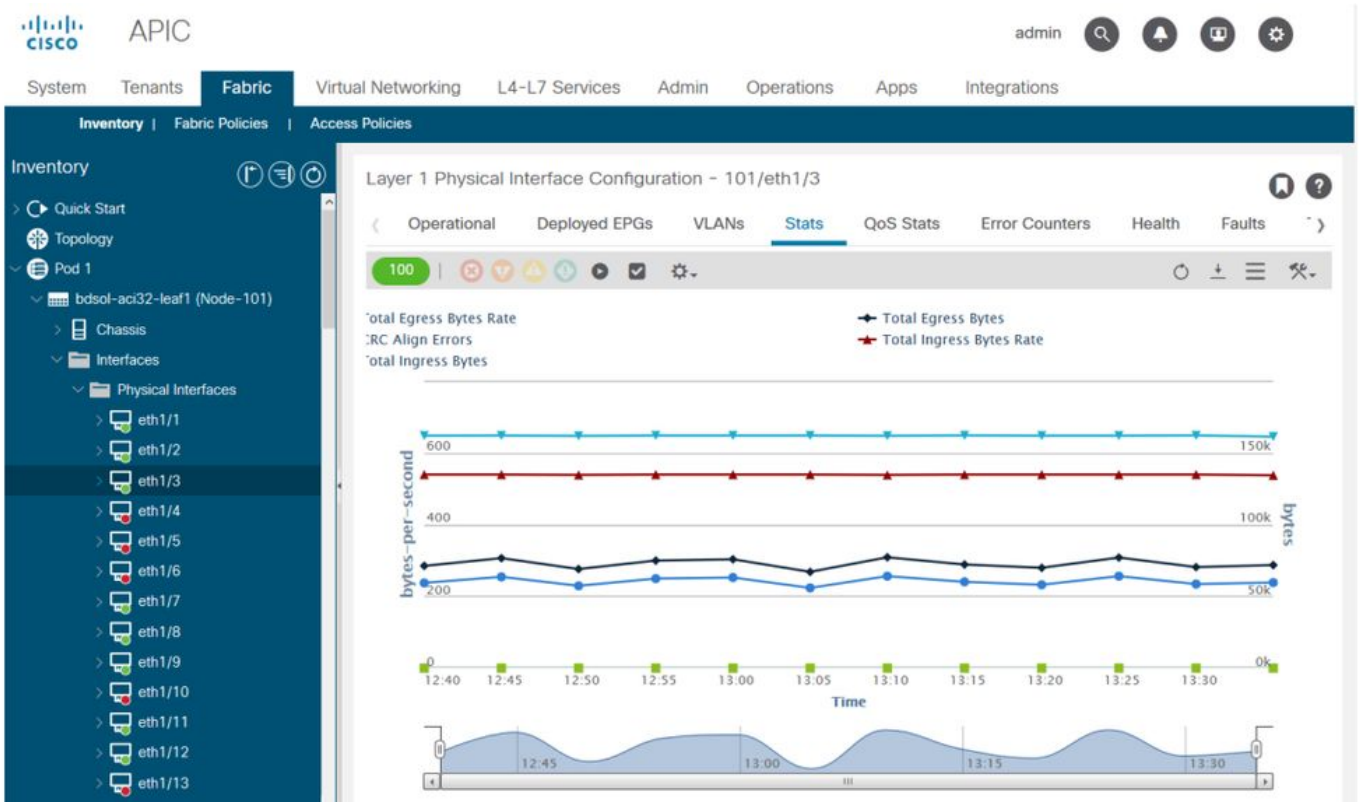
```
ACI-LEAF# show queuing interface ethernet 1/5
================================================================================
               Queuing stats for ethernet 1/5
================================================================================
================================================================================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

...
```

Statistieken in GUI bekijken

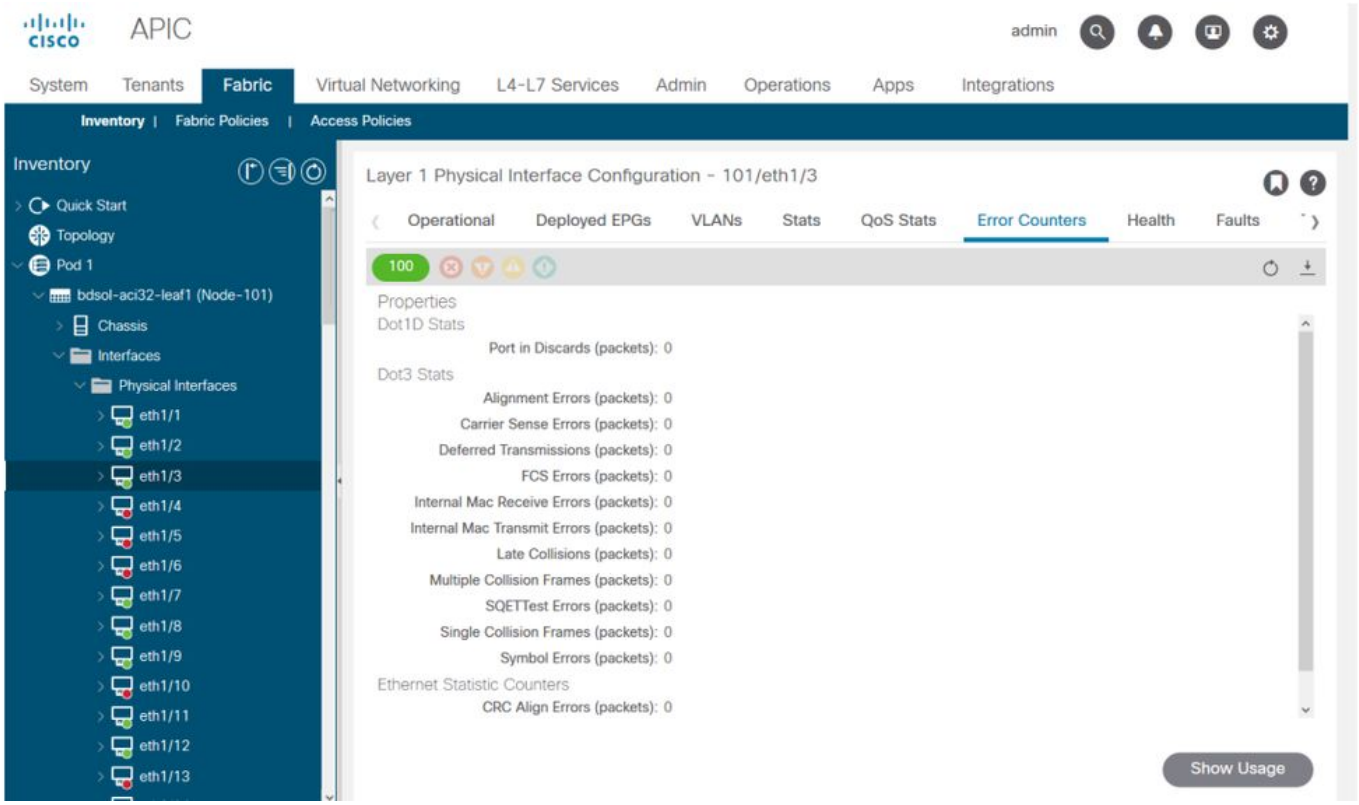
De locatie is 'Stof > Inventaris > Leaf/Spine > Fysieke interface > Stats'.

GUI-interfacestatistieken



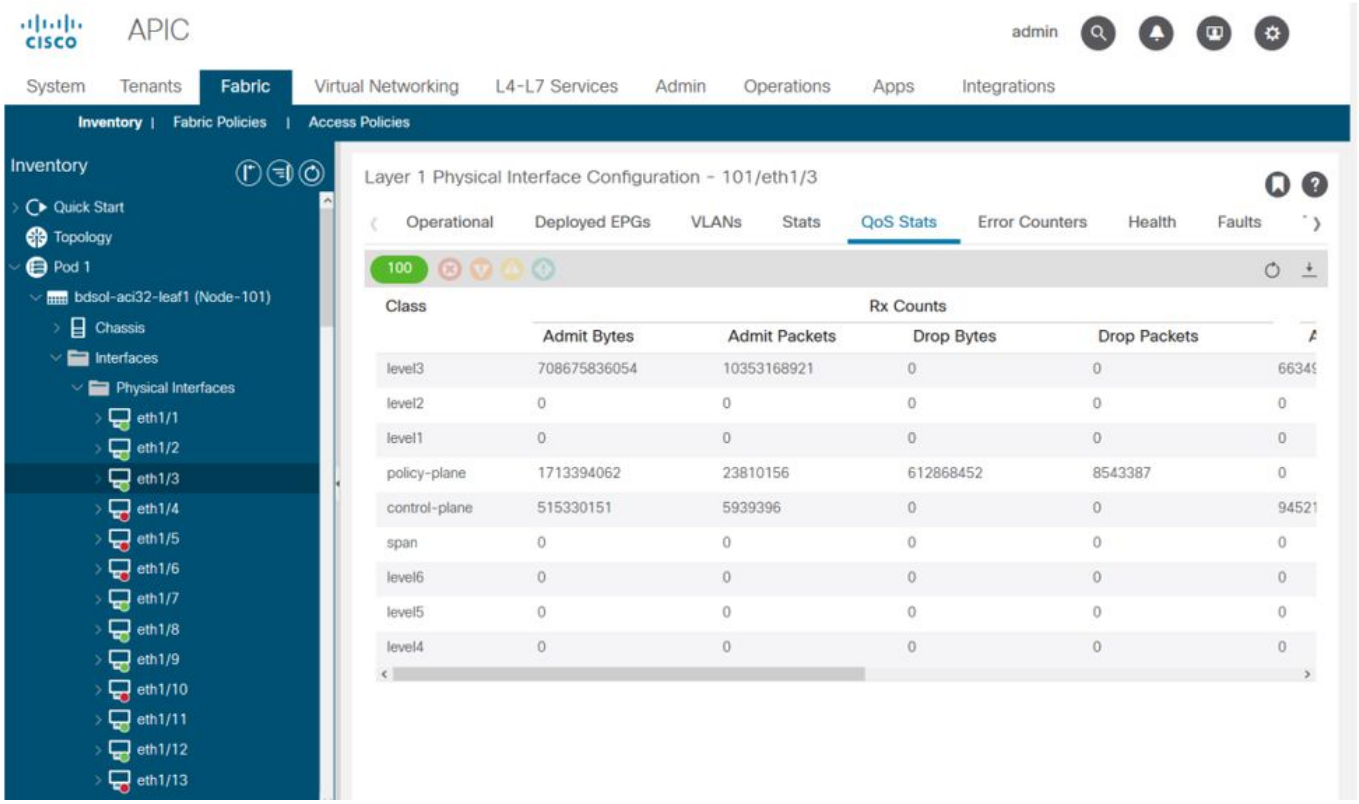
De foutstatistieken kunnen op dezelfde plaats worden bekeken:

GUI-interfacefouten



Tot slot kan de GUI QoS-stats per interface weergeven:

QoS-tellers voor GUI-interface



CRC — FCS — doorgesneden switching

Wat is cyclische redundantiecontrole (CRC)?

CRC is een polynomiale functie op het frame die een 4B nummer in Ethernet retourneert. Het vangt alle single bit fouten en een goed percentage double bit fouten. Het is dus bedoeld om ervoor te zorgen dat het frame tijdens het transport niet beschadigd is. Als de CRC-foutteller toeneemt, betekent dit dat wanneer de hardware de polynomiale functie op het frame uitvoerde, het resultaat een 4B-nummer was dat verschilde van het 4B-nummer op het frame zelf. Frames kunnen beschadigd raken door verschillende redenen, zoals duplex mismatch, defecte bekabeling en kapotte hardware. Er moeten echter CRC-fouten van een bepaald niveau worden verwacht en de standaard maakt een foutpercentage van maximaal 10-12 bits op Ethernet mogelijk (1 bit van de 1012 kan worden gespiegeld).

Store-and-forward vs doorgesneden switching

Zowel store-and-forward als cut-through Layer 2 switches baseren hun doorsturen beslissingen op het doeladres van MAC van gegevenspakketten. Ze leren ook MAC-adressen wanneer ze de bronMAC (SMAC) velden van pakketten onderzoeken, omdat stations communiceren met andere knooppunten op het netwerk.

Een store-and-forward switch neemt een doorsturen besluit over een gegevenspakket nadat het het gehele frame heeft ontvangen en de integriteit ervan heeft gecontroleerd. Een cut-through switch neemt deel aan het doorsturen proces snel nadat het het bestemmingsMAC (DMAC) adres van een inkomend kader heeft onderzocht. Een cut-through switch moet echter wachten tot hij het gehele pakket heeft bekeken voordat hij de CRC-controle uitvoert. Dat betekent dat tegen de tijd dat CRC wordt bevestigd, het pakket reeds door:sturen en kan niet worden gelaten vallen als het de controle ontbreekt.

Traditioneel werken de meeste netwerkapparaten op basis van store-and-forward. Snij-door omschakelingstechnologieën neigen om in hoge snelheidsnetwerken gebruikt te worden die lage latentie het door:sturen vereisen.

Met name voor de ACI-hardware van de tweede generatie en de latere generatie wordt de doorgesneden omschakeling uitgevoerd als de toegangsinterface een hogere snelheid heeft en de uitgangsinterface dezelfde snelheid of een lagere snelheid heeft. Store-and-forward switching wordt uitgevoerd als de snelheid van de toegangsinterface lager is dan de uitgangsinterface.

Stompen

Pakketten met een CRC fout vereisen een daling. Als het kader in een besnoeiingsweg wordt geschakeld, gebeurt de bevestiging CRC nadat het pakket reeds door:sturen. Als zodanig is de enige optie de Ethernet Frame Check Sequence (FCS) te stoppen. Bij het **stompen van een frame moet de FCS worden ingesteld op een bekende waarde die geen CRC-controle doorgeeft**. Hierdoor kan één slecht frame dat CRC faalt als CRC op elke interface die het doorkruist, tot het een store-and-forward switch bereikt die het zal laten vallen.

ACI en CRC: op zoek naar defecte interfaces

- Als een blad CRC fouten op een downlink poort ziet, is het meestal een probleem op de downlink SFP of met componenten op het externe apparaat/netwerk.
- Als een wervelkolom CRC-fouten ziet, is het meestal een probleem op die lokale poort, SFP, Fibre of Neighbor SFP. CRC falende pakjes van bladeren downlinks worden niet gestompt aan de stekels. Alsof de headers leesbaar zijn, is het VXLAN ingekapseld en wordt er een nieuwe CRC berekend. Als de kopregels niet leesbaar waren van framecorruptie, zou het

pakket worden gedropt.
- Als een blad CRC-fouten ziet in stoffen links, kan het: Een probleem bij het lokale glasvezel/SFP-paar, de ingangsvezel van de wervelkolom of het SFP-paar.Een gestompt frame op weg door de stof.

Stomen: problemen oplossen bij stompen

- Zoek interfaces met FCS-fouten in de stof. Aangezien FCS lokaal in een poort voorkomt, is het waarschijnlijk dat de glasvezel of SFP aan beide uiteinden aanwezig is.
- CRC-fouten in uitvoer 'interface weergeven' geven de totale FCS+Stomp-waarde weer.\

Bekijk een voorbeeld:

Controleer een poort met de opdracht

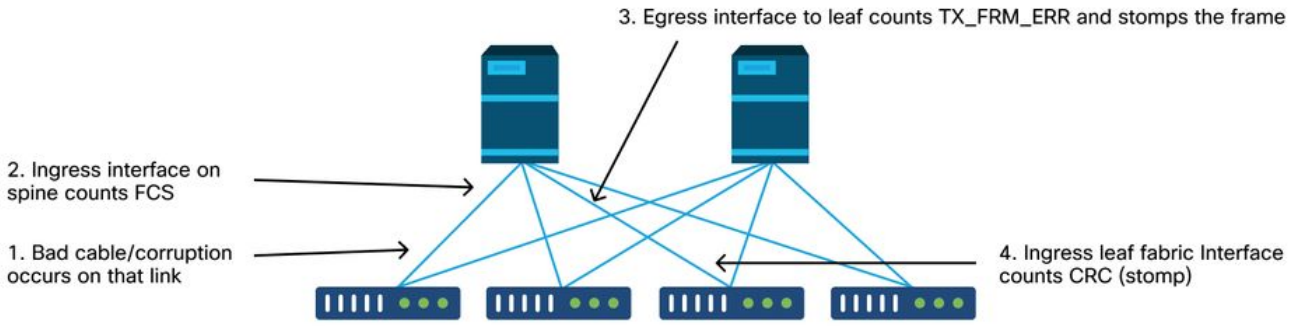
```
vsh_lc: 'show platform internal counter port <X>'
```

In deze opdracht zijn 3 waarden belangrijk:

- RX_FCS_ERR - FCS-fout.
- RX_CRCERR - Ontvangen stomped CRC foutframe.
- TX_FRM_ERROR - Verzonden stomped CRC foutframe.

```
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
```

CRC-stomp probleemoplossing



Als een beschadigde link een groot aantal beschadigde frames genereert, kunnen die frames overstroomd worden naar alle andere bladknooppunten en is het zeer mogelijk om CRC te vinden op de toegang van stoffen uplinks van de meeste bladknooppunten in de stof. Die zouden waarschijnlijk allemaal afkomstig zijn van één enkele corrupte schakel.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.