Risoluzione dei problemi di inoltro intra-fabric ACI - Cadute intermittenti

Sommario

Introduzione

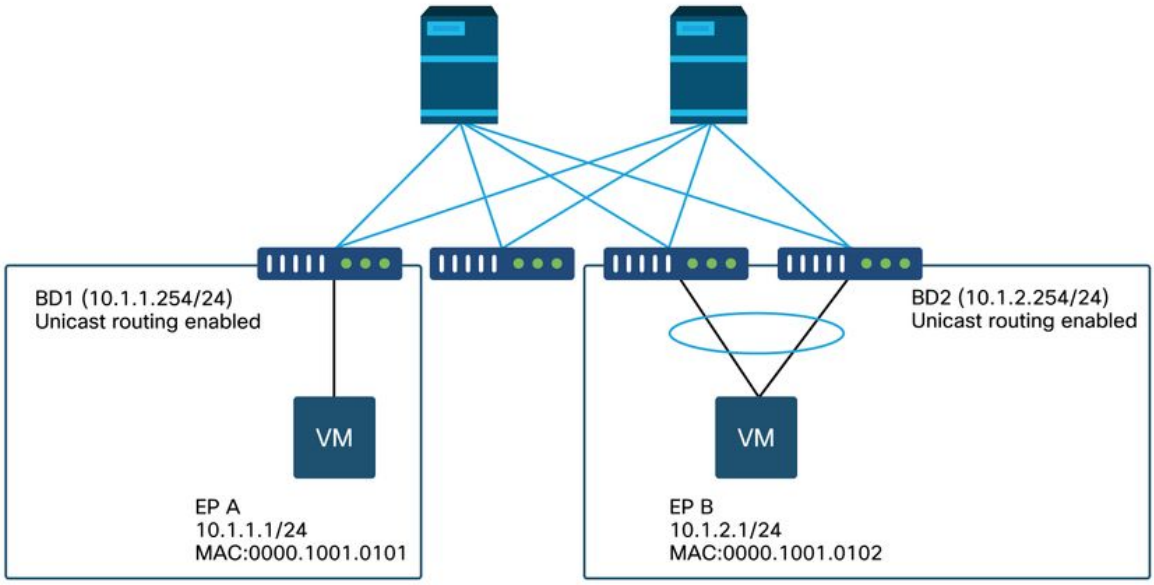
In questo documento viene descritto come risolvere i problemi relativi alle perdite intermittenti in ACI.

Premesse

Il materiale di questo documento è stato estratto dal libro Troubleshooting Cisco Application Centric Infrastructure, Second Edition, in particolare il capitolo **Intra-Fabric forward - Intermittent drops**.

Risoluzione dei problemi di inoltro intra-fabric ACI - Cadute intermittenti

Esempio di topologia



Nell'esempio, nel ping tra EP A (10.1.1.1) e EP B (10.1.2.1) si verificano cali intermittenti.

```
[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
```

Flusso di lavoro di risoluzione dei problemi

1. Determinare la direzione che causa le cadute intermittenti

Eseguire un'acquisizione pacchetto (tcpdump, Wireshark, ecc.) sull'host di destinazione (EP B). Per ICMP, focalizzare l'attenzione sul numero di sequenza per vedere che i pacchetti scartati in modo intermittente vengono osservati su 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
...
```

- Pattern 1: tutti i pacchetti vengono osservati durante l'acquisizione dei pacchetti EP B.

Le gocce devono essere in risposta echo ICMP (da EP B a EP A).

- Pattern 2 - Le gocce intermittenti vengono osservate nell'acquisizione dei pacchetti EP B.

Le gocce devono essere in modalità echo ICMP (da EP A a EP B).

2. Verificare se un altro protocollo con lo stesso indirizzo IP di origine/destinazione ha lo stesso problema

Se possibile, provare a verificare la connettività tra i due endpoint utilizzando un protocollo diverso consentito dal contratto tra di essi (ad esempio ssh, telnet, http,...)

- Pattern 1 - Altri protocolli hanno la stessa perdita intermittente.

Il problema potrebbe essere dovuto al flapping dell'endpoint o all'accodamento/buffering, come mostrato di seguito.

- Pattern 2 - Solo ICMP presenta una perdita intermittente.

Le tabelle di inoltro (ad esempio la tabella degli endpoint) non devono presentare problemi poiché l'inoltro è basato su MAC e IP. Anche l'accodamento/buffering non dovrebbe essere il motivo, in quanto ciò influirebbe su altri protocolli. L'unico motivo per cui ACI prenderebbe una decisione di inoltro diversa in base al protocollo è il caso di utilizzo del PBR.

Una possibilità è che uno dei nodi della spine abbia un problema. Quando un protocollo è diverso, il pacchetto con la stessa origine e destinazione può essere bilanciato dal carico su un'altra porta uplink/fabric (ad esempio un'altra spine) dalla foglia in entrata.

I contatori atomici possono essere utilizzati per garantire che i pacchetti non vengano scartati sui nodi della spine e raggiungano la foglia di uscita. Nel caso in cui i pacchetti non raggiungano la foglia di uscita, controllare la ELAM sulla foglia di entrata per vedere quale porta di fabric i pacchetti vengono inviati. Per isolare il problema su una spine specifica, è possibile chiudere gli uplink foglia per forzare il traffico verso un'altra spine.

3. Verificare se è correlato a un problema di apprendimento dell'endpoint

ACI utilizza una tabella di endpoint per inoltrare i pacchetti da un endpoint all'altro. Il flapping dell'endpoint può causare un problema di raggiungibilità intermittente perché informazioni inappropriate sull'endpoint causano l'invio del pacchetto a una destinazione errata o la perdita del contratto a causa della classificazione del pacchetto nell'EPG errato. Anche se la destinazione è un L3Out anziché un gruppo di endpoint, verificare che l'IP non venga appreso come endpoint nello stesso VRF su uno switch foglia.

Per ulteriori informazioni su come risolvere i problemi relativi al flapping degli endpoint, vedere la sezione secondaria "Flapping degli endpoint" in questa sezione.

4. Verificare se è correlato a problemi di buffer modificando la frequenza del traffico

Aumentare o ridurre l'intervallo del ping per verificare se il rapporto di rilascio cambia. La differenza di intervallo deve essere sufficientemente grande.

In Linux, l'opzione '-i' può essere utilizzata per modificare l'intervallo (sec):

```
[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
```

Se il rapporto di rilascio aumenta quando l'intervallo diminuisce, è probabile che sia correlato all'accodamento o al buffering su endpoint o switch.

La percentuale di rilascio da considerare è (numero di pacchetti inviati/totale) anziché (numero di rilasci/tempo).

In questo scenario, verificare quanto segue.

1. Controllare se i contatori di rilascio sulle interfacce dello switch stanno aumentando insieme al ping. Per ulteriori informazioni, vedere la sezione "Interfaccia rilasciata" nel capitolo "Inoltro intra-fabric".
2. Verificare se il contatore Rx aumenta insieme ai pacchetti sull'endpoint di destinazione. Se il contatore Rx viene aumentato con lo stesso numero dei pacchetti trasmessi, è probabile che i pacchetti vengano scartati sull'endpoint stesso. Ciò potrebbe essere dovuto al buffering dell'endpoint sullo stack TCP/IP.

Ad esempio, se si inviano 100000 ping con l'intervallo più breve possibile, è possibile osservare il contatore Rx sull'endpoint in quanto aumenta di 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. Verificare se l'ACI sta inviando i pacchetti in uscita o se la destinazione li sta ricevendo

Eseguire un'acquisizione SPAN sulla porta di uscita dello switch foglia per eliminare il fabric ACI

dal percorso di risoluzione dei problemi.

I contatori Rx sulla destinazione possono essere utili anche per eliminare tutti gli switch di rete dal percorso di risoluzione dei problemi, come mostrato nei passaggi precedenti per il buffering.

Sfarfallio degli endpoint

Questa sezione spiega come verificare il flapping degli endpoint. Per ulteriori informazioni, consultare i seguenti documenti:

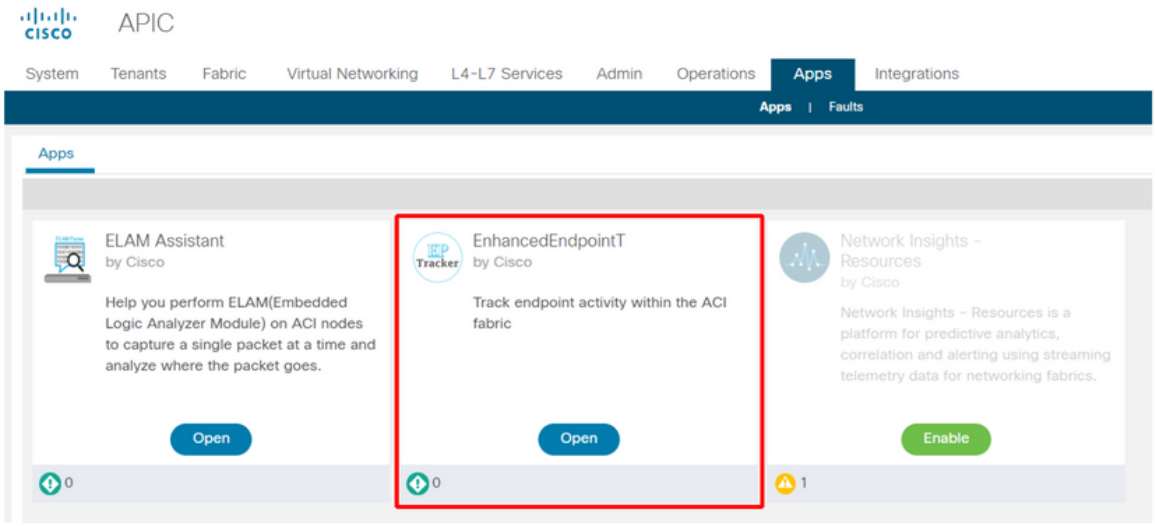
- "ACI Fabric Endpoint Learning Whitepaper" su www.cisco.com
- "Cisco Live BRKACI-2641 ACI - Risoluzione dei problemi: Endpoints" su www.ciscolive.com

Quando ACI apprende lo stesso indirizzo MAC o IP in più percorsi, sembrerà che l'endpoint sia stato spostato. Ciò può essere causato anche da un dispositivo di spoofing o da una configurazione errata. Tale comportamento è noto come flapping degli endpoint. In uno scenario di questo tipo, il traffico verso l'endpoint di spostamento/flapping (indirizzo MAC per il traffico con bridging, indirizzo IP per il traffico con routing) avrà errori in modo intermittente.

Il metodo più efficace per rilevare lo sfarfallio degli endpoint consiste nell'utilizzare Enhanced Endpoint Tracker. Questa app può essere eseguita come app ACI AppCenter o come app autonoma su un server esterno nel caso in cui debba gestire un'infrastruttura molto più grande.

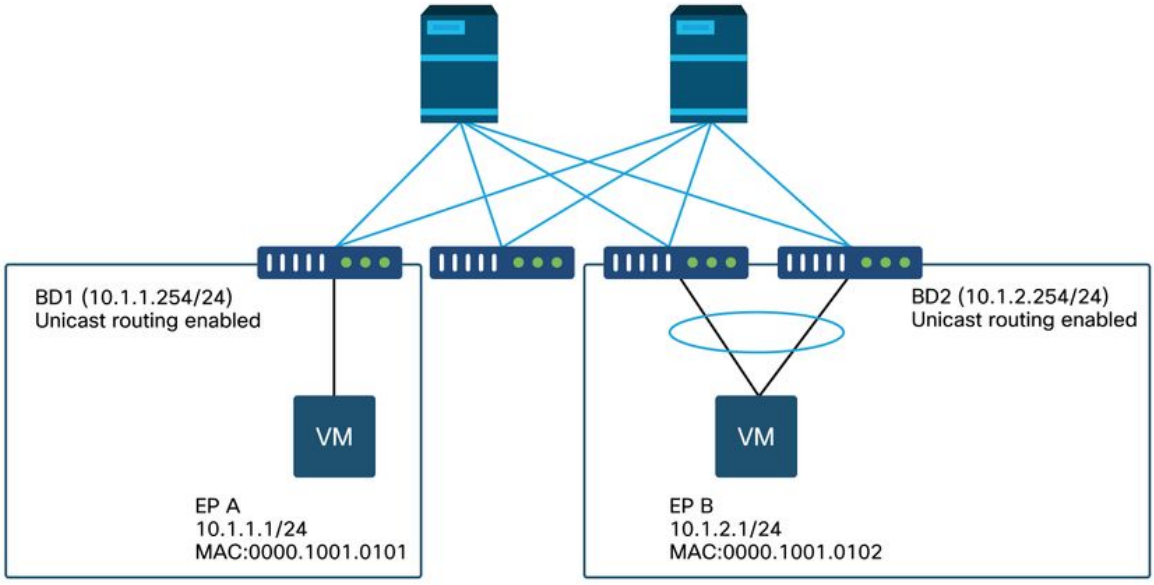
Enhanced Endpoint Tracker

AVVISO DEPRECAZIONE La guida è stata scritta il 4.2; da allora Enhanced Endpoint Tracker app è stato deprecato in favore della funzionalità su Nexus Dashboard Insights. Per ulteriori informazioni, vedere l'ID bug Cisco CSCvz59365 .



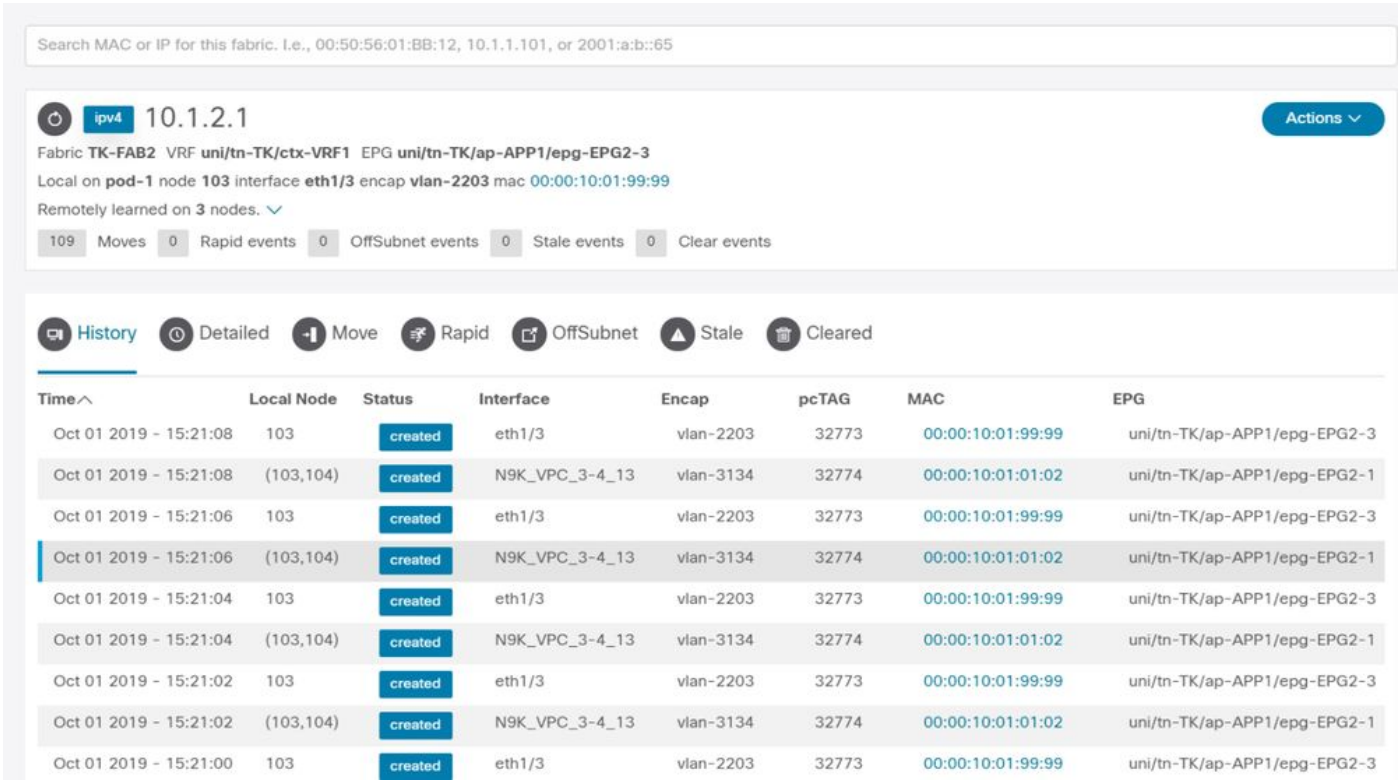
Nella figura precedente è illustrato Enhanced Endpoint Tracker in AppCenter. Nell'esempio seguente viene illustrato come trovare gli endpoint che si alternano con Enhanced Endpoint Tracker.

Esempio di flapping degli endpoint



Nell'esempio, IP 10.1.2.1 deve appartenere a EP B con MAC 0000.1001.0102. Tuttavia, anche un EP X con MAC 0000.1001.9999 sta inviando il traffico con IP 10.1.2.1 a causa di una configurazione errata o forse di uno spoofing IP.

Output Enhanced Endpoint Tracker - Movimenti

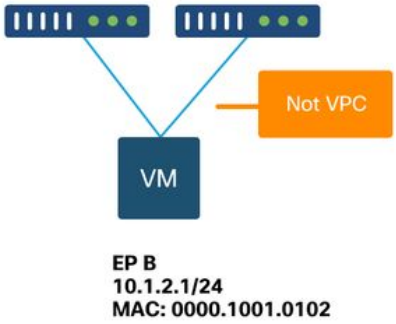


Enhanced Endpoint Tracker mostra quando e dove è stato appreso IP 10.1.2.1. Come mostrato nella schermata precedente, 10.1.2.1 lampeggia tra due endpoint con MAC 000.1001.0102 (previsto) e 0000.1001.9999 (imprevisto). Ciò causerà un problema di raggiungibilità verso IP 10.1.2.1 perché quando viene appreso sull'indirizzo MAC sbagliato, il pacchetto verrà inviato a un dispositivo sbagliato tramite l'interfaccia sbagliata. Per risolvere questo problema, eseguire le operazioni necessarie per impedire che la VM imprevista determini l'origine del traffico con un

indirizzo IP non appropriato.

Di seguito viene illustrato un tipico esempio di flapping dell'endpoint dovuto a una configurazione non appropriata.

Esempio di topologia che potrebbe causare il flapping dell'endpoint



Quando un server o una VM è collegata ai nodi foglia ACI tramite due interfacce senza VPC, il server deve utilizzare il raggruppamento NIC attivo/standby. In caso contrario, i pacchetti vengono bilanciati in base al carico su entrambi gli uplink e sembra che gli endpoint stiano lampeggiando tra due interfacce dalla prospettiva dello switch foglia ACI. In questo caso, è richiesta la modalità di raggruppamento NIC attiva/standby o equivalente o è sufficiente utilizzare un VPC sul lato ACI.

Interfaccia scartata

In questo capitolo viene descritto come controllare i contatori principali relativi alla perdita di interfacce in entrata.

Tipi di contatori di rilascio hardware

Sugli switch Nexus 9000 in modalità ACI, sono disponibili tre contatori hardware principali sull'ACI per le perdite di interfaccia in entrata.

Avanti

I motivi principali sono:

- SECURITY_GROUP_DENY: Un calo dovuto a contratti mancanti per permettere la comunicazione.
- VLAN_XLATE_MISS: Caduta a causa di VLAN non appropriata. Ad esempio, un frame entra nella struttura con una VLAN 10 802.1Q. Se lo switch ha la VLAN 10 sulla porta, esaminerà i contenuti e prenderà una decisione di inoltro in base all'MAC di destinazione. Tuttavia, se la VLAN 10 non è consentita sulla porta, viene eliminata e etichettata come VLAN_XLATE_MISS.
- ACL_DROP: Una goccia a causa di SUP-TCAM. SUP-TCAM negli switch ACI contiene regole speciali da applicare oltre alla normale decisione di inoltro L2/L3. Le regole di SUP-TCAM sono incorporate e non configurabili dall'utente. L'obiettivo delle regole SUP-TCAM è

principalmente quello di gestire alcune eccezioni o un certo traffico di control plane e non è destinato ad essere controllato o monitorato dagli utenti. Quando un pacchetto raggiunge le regole SUP-TCAM e la regola è di scartare il pacchetto, il pacchetto scartato viene contato come ACL_DROP e incrementa il contatore di rilascio in avanti.

I pacchetti inoltrati sono essenzialmente pacchetti ignorati per un motivo noto valido. In genere possono essere ignorate e non causano penalità nelle prestazioni, a differenza di quanto accade con le reali riduzioni del traffico di dati.

Errore

Quando lo switch riceve un frame non valido, viene scartato come errore. Ad esempio, i frame con errori FCS o CRC. Per ulteriori informazioni, vedere la sezione successiva "CRC — FCS — cut-through switching".

Buffer

Quando uno switch riceve un frame e non sono disponibili buffer in entrata o in uscita, il frame viene scartato con 'Buffer'. Ciò suggerisce che in qualche punto della rete vi è congestione. Il collegamento che mostra l'errore potrebbe essere pieno o il collegamento contenente la destinazione potrebbe essere congestionato.

Raccolta dei contatori tramite l'API

Èimportante notare che sfruttando l'API e il modello a oggetti, l'utente può eseguire rapidamente query sul fabric per tutte le istanze di queste cadute (eseguirle da un 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"
```

Visualizzazione dello stato di rilascio nella CLI

Se si rilevano errori o è necessario controllare le perdite di pacchetti sulle interfacce usando la CLI, il modo migliore per farlo è visualizzare i contatori della piattaforma nell'hardware. Non tutti i contatori vengono visualizzati utilizzando 'show interface'. I tre motivi principali di rilascio possono essere visualizzati solo utilizzando i contatori della piattaforma. Per visualizzarli, procedere come segue:

Foglia

SSH sulla foglia ed eseguire questi comandi. Questo esempio è per 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
...
```

Dorso

Un dorso fisso (N9K-C9332C e N9K-C9364C) può essere controllato usando lo stesso metodo degli interruttori a foglia.

Per un dorso modulare (N9K-C9504, ecc.), è necessario collegare la scheda di linea prima di poter visualizzare i contatori della piattaforma. SSH sul dorso ed eseguire questi comandi. Questo esempio è per 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
...
```

I contatori di stato dell'accodamento vengono visualizzati tramite 'show queuing interface'. Questo esempio è per ethernet 1/5.

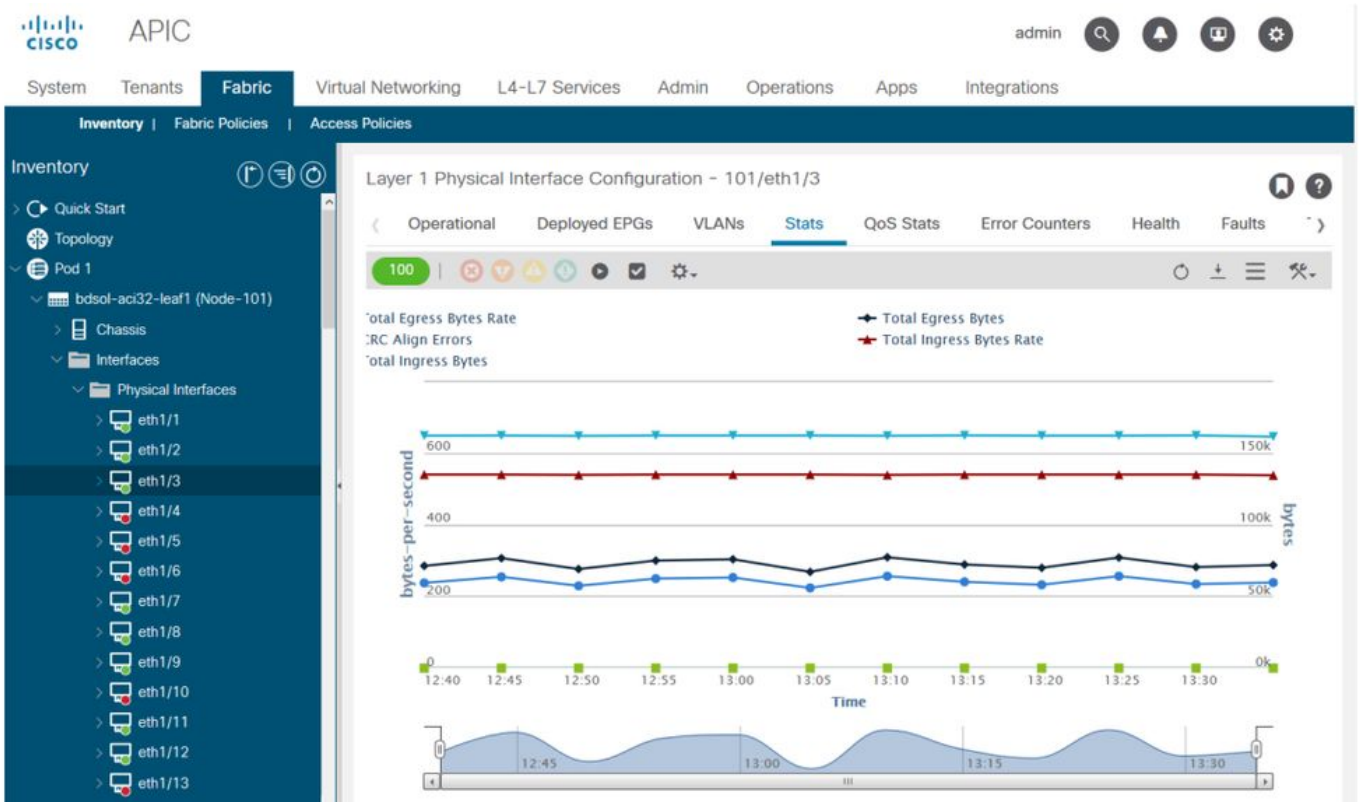
```
ACI-LEAF# show queuing interface ethernet 1/5
================================================================================
               Queuing stats for ethernet 1/5
================================================================================
================================================================================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

...
```

Visualizzazione delle statistiche nella GUI

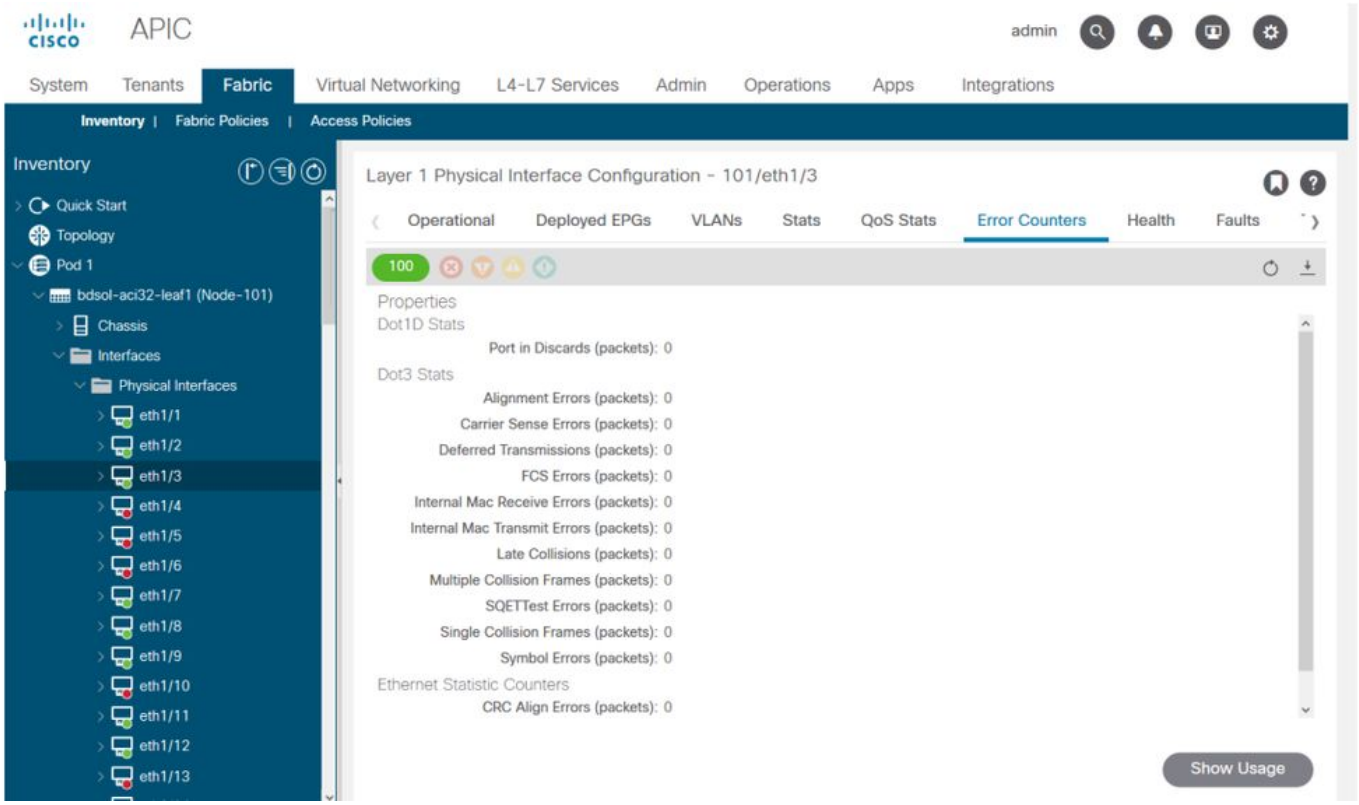
Il percorso è 'Fabric > Inventory > Leaf/Spine > Physical interface > Stats'.

Statistiche interfaccia GUI



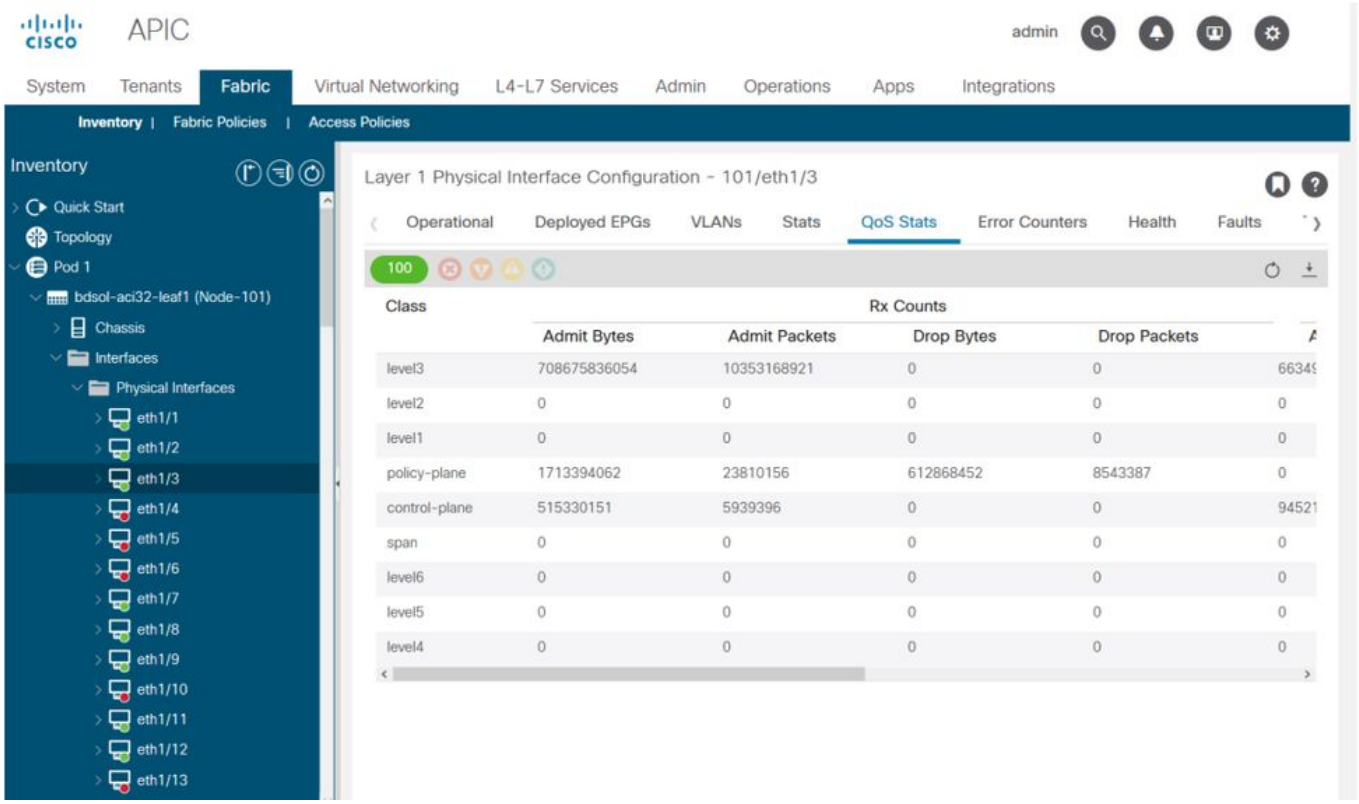
Le statistiche degli errori possono essere visualizzate nella stessa posizione:

Errori interfaccia GUI



Infine, la GUI può visualizzare le statistiche QoS per interfaccia:

Contatori QoS interfaccia GUI



CRC — FCS — cut-through switching

Che cos'è il controllo di ridondanza ciclico (CRC)?

CRC è una funzione polinomiale sul frame che restituisce un numero 4B in Ethernet. Rileva tutti gli errori di bit singolo e una buona percentuale di errori di bit doppio. In tal modo si intende garantire che il telaio non sia stato danneggiato durante la trasmissione. Se il contatore di errore CRC aumenta, significa che quando l'hardware esegue la funzione polinomiale sul fotogramma, il risultato è un numero 4B che differisce dal numero 4B trovato sul fotogramma stesso. I frame possono danneggiarsi a causa di diverse cause, ad esempio una mancata corrispondenza del duplex, un errore nel cablaggio e la rottura dell'hardware. Tuttavia, ci si dovrebbe aspettare un certo livello di errori CRC e lo standard permette una frequenza di errore fino a 10-12 bit su Ethernet (1 bit su 1012 può invertire).

Switching store-and-forward e cut-through

Gli switch di layer 2 store-and-forward e cut-through basano le decisioni di inoltro sull'indirizzo MAC di destinazione dei pacchetti dati. Imparano anche gli indirizzi MAC mentre esaminano i campi MAC di origine (SMAC) dei pacchetti mentre le stazioni comunicano con gli altri nodi della rete.

Lo switch store-and-forward decide l'inoltro di un pacchetto dati dopo aver ricevuto l'intero frame e averne controllato l'integrità. Uno switch cut-through inizia il processo di inoltro subito dopo aver esaminato l'indirizzo MAC di destinazione (DMAC) di un frame in ingresso. Tuttavia, prima di eseguire il controllo CRC, uno switch cut-through deve attendere di aver visualizzato l'intero pacchetto. Ciò significa che al momento della convalida del CRC, il pacchetto è già stato inoltrato e non può essere scartato se non supera il controllo.

Tradizionalmente, la maggior parte dei dispositivi di rete operava in base al "store-and-forward". Le tecnologie di switching cut-through tendono ad essere utilizzate nelle reti ad alta velocità che richiedono l'inoltro a bassa latenza.

In particolare, per quanto riguarda l'hardware ACI di seconda e successiva generazione, la commutazione cut-through viene eseguita se l'interfaccia in entrata ha una velocità superiore e l'interfaccia in uscita ha la stessa velocità o una velocità inferiore. La commutazione store-and-forward viene eseguita se la velocità dell'interfaccia in entrata è inferiore a quella dell'interfaccia in uscita.

Stomping

I pacchetti con un errore CRC richiedono un rilascio. Se il frame viene commutato in un percorso cut-through, la convalida CRC viene eseguita dopo l'inoltro del pacchetto. Per questo motivo, l'unica opzione è quella di interrompere la sequenza di controllo del frame Ethernet (FCS). **Lo stomping di un frame implica l'impostazione del FCS su un valore noto che non superi un controllo CRC**. Per questo motivo, un frame danneggiato che non funziona può apparire come CRC su ogni interfaccia attraversata, finché non raggiunge un commutatore store-and-forward che lo rifiuta.

ACI e CRC: cerca interfacce guaste

- Se in una foglia vengono rilevati errori CRC su una porta di downlink, si tratta principalmente di un problema nell'SFP di downlink o con i componenti sulla periferica o sulla rete esterna.
- Se un dorso rileva errori CRC, è principalmente un problema su quella porta locale, SFP, Fiber o Neighbor SFP. I pacchetti CRC con errori provenienti da collegamenti in downlink foglia non vengono inviati automaticamente al dorso. Come se le relative intestazioni fossero leggibili, è incapsulato in VXLAN e verrà calcolato un nuovo CRC. Se le intestazioni non

fossero leggibili dal danneggiamento dei frame, il pacchetto verrebbe scartato.
- Se in una foglia vengono rilevati errori CRC nei collegamenti della struttura, è possibile che si tratti di: Un problema relativo alla coppia SFP/fibra locale, alla fibra in entrata della spina dorsale o alla coppia SFP.Un telaio a gradino che attraversa il tessuto.

Stomping: risoluzione dei problemi relativi alla riduzione

- Cercare le interfacce con errori FCS sulla struttura. Poiché FCS è presente in locale su una porta, è molto probabile che si tratti della fibra o dell'SFP su entrambe le estremità.
- Gli errori CRC nell'output 'show interface' riflettono il valore FCS+Stomp totale.\

Ecco un esempio:

Controllare una porta con il comando

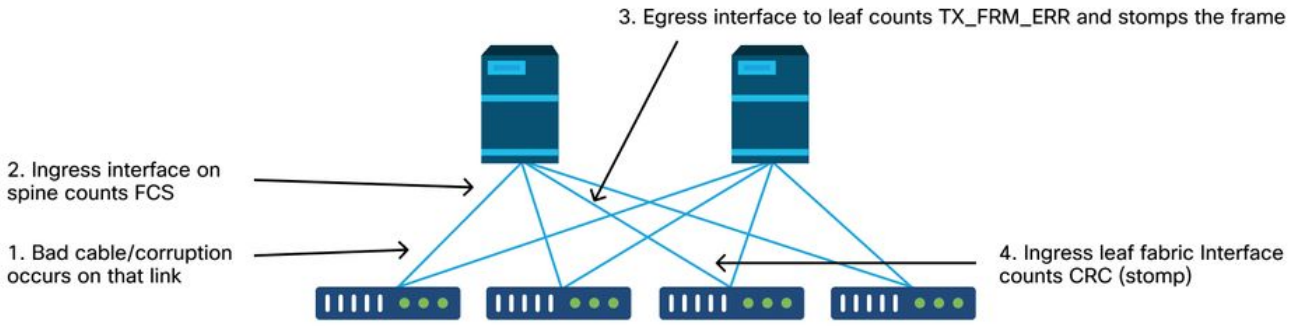
```
vsh_lc: 'show platform internal counter port <X>'
```

In questo comando 3 valori sono importanti:

- RX_FCS_ERR - Errore FCS.
- RX_CRCERR - Ricevuto frame di errore CRC di tipo stagnato.
- TX_FRM_ERROR: frame di errore CRC stagnato trasmesso.

```
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
```

Scenario di risoluzione dei problemi dello stomp CRC



Se un collegamento danneggiato genera un gran numero di frame danneggiati, questi frame potrebbero essere inondati a tutti gli altri nodi foglia ed è molto possibile trovare CRC sull'entrata degli uplink fabric della maggior parte dei nodi foglia nel tessuto. Quelli probabilmente verrebbero tutti da un unico legame corrotto.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).