ACI 패브릭 내 포워딩 문제 해결 - 간헐적 삭제

목차

소개

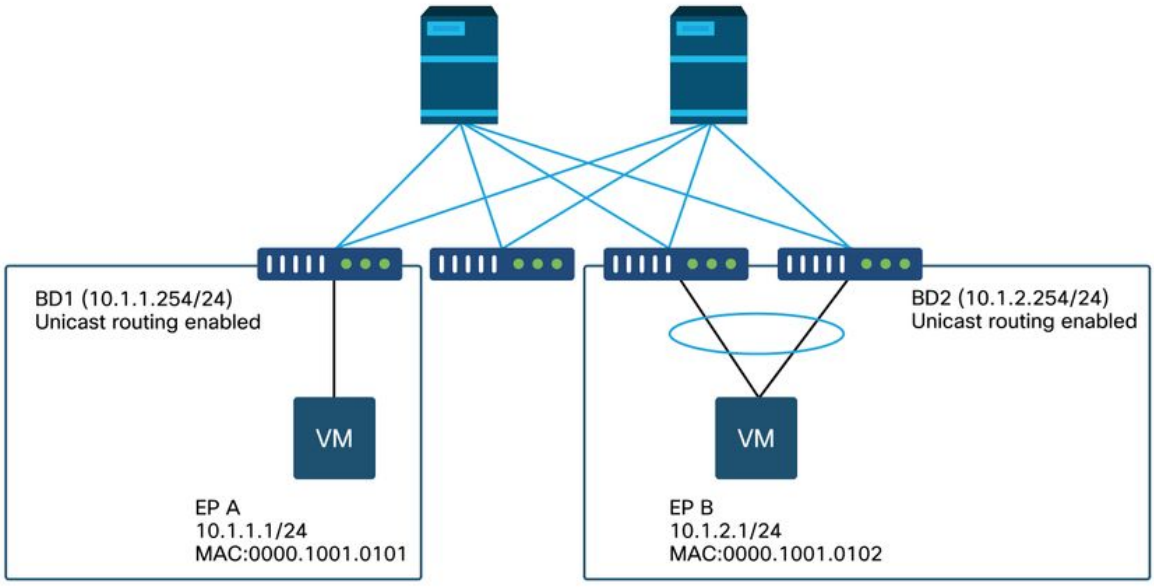
이 문서에서는 ACI의 간헐적 삭제 트러블슈팅 단계에 대해 설명합니다.

배경 정보

이 문서의 자료는 Troubleshooting Cisco Application Centric Infrastructure, Second Edition 책, 특히 Intra-**Fabric Fowarding - Intermittent drops 장에서** 추출되었습니다.

ACI Intra-Fabric Forwarding 문제 해결 - 간헐적 삭제

토폴로지 예



이 예에서는 EP A(10.1.1.1)에서 EP B(10.1.2.1)로 ping할 때 간헐적으로 감소합니다.

```
[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
```

문제 해결 워크플로

1. 간헐적으로 떨어지는 방향 확인

대상 호스트(EP B)에서 패킷 캡처(tcpdump, Wireshark 등)를 수행합니다. ICMP의 경우 시퀀스 번호에 초점을 맞춰 간헐적으로 삭제된 패킷이 EP B에서 관찰되는지 확인합니다.

```
[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
...
```

- 패턴 1 - 모든 패킷이 EP B 패킷 캡처에서 관찰됩니다.

삭제는 ICMP 에코 응답(EP B - EP A)에 있어야 합니다.

- 패턴 2 - EP B 패킷 캡처에서 간헐적인 드롭이 관찰됩니다.

삭제는 ICMP 에코(EP A - EP B)에 있어야 합니다.

2. 소스/대상 IP가 같은 다른 프로토콜의 문제가 동일한지 확인합니다

가능하면 두 엔드포인트 간의 계약에서 허용하는 다른 프로토콜(예: ssh, 텔넷, http 등)을 사용하여 두 엔드포인트 간의 연결을 테스트해 보십시오

- 패턴 1 - 다른 프로토콜의 경우 동일한 간헐적 드롭이 있습니다.

아래와 같이 엔드포인트 플래핑 또는 대기/버퍼링에 문제가 있을 수 있습니다.

- 패턴 2 - ICMP에만 간헐적 드롭이 있습니다.

포워딩은 MAC 및 IP를 기반으로 하므로 포워딩 테이블(예: 엔드포인트 테이블)에 문제가 없어야 합니다. 다른 프로토콜에도 영향을 미치므로 대기/버퍼링 역시 이유가 되어서는 안 됩니다. ACI가 프로토콜에 따라 다른 전달 결정을 내리는 유일한 이유는 PBR 활용 사례입니다.

스파인 노드 중 하나에 문제가 있을 수 있습니다. 프로토콜이 다른 경우, 동일한 소스 및 목적지의 패킷이 인그레스 리프에 의해 다른 업링크/패브릭 포트(즉, 다른 스파인)에 로드 밸런싱될 수 있습니다.

Atomic Counters를 사용하면 패킷이 스파인 노드에서 삭제되어 이그레스 리프에 도달하지 않도록 보장할 수 있습니다. 패킷이 이그레스 리프에 도달하지 않은 경우 인그레스 리프의 ELAM을 확인하여 패킷이 전송되는 패브릭 포트를 확인합니다. 특정 스파인에 문제를 격리하려면 리프 업링크를 종료하여 트래픽을 다른 스파인으로 강제 전달할 수 있습니다.

3. 엔드포인트 학습 문제와 관련이 있는지 확인

ACI는 엔드포인트 테이블을 사용하여 한 엔드포인트에서 다른 엔드포인트로 패킷을 전달합니다. 부적절한 엔드포인트 정보로 인해 패킷이 잘못된 목적지로 보내지거나 잘못된 EPG로 분류되어 contract dropped될 수 있기 때문에 엔드포인트 flapping으로 인해 간헐적인 연결 문제가 발생할 수 있습니다. 대상이 엔드포인트 그룹 대신 L3Out이어야 하는 경우에도 IP가 리프 스위치에서 동일한 VRF의 엔드포인트로 학습되지 않도록 해야 합니다.

엔드포인트 플래핑 문제 해결 방법에 대한 자세한 내용은 이 섹션의 "엔드포인트 플래핑" 하위 섹션

을 참조하십시오.

4. 트래픽 주파수를 변경하여 버퍼링 문제와 관련이 있는지 확인합니다

삭제 비율이 변경되는지 확인하려면 ping 간격을 늘리거나 줄입니다. 간격 차이는 충분히 커야 합니다.

Linux에서는 '-i' 옵션을 사용하여 간격(초)을 변경할 수 있습니다.

```
[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
```

간격이 감소할 때 드롭 비율이 증가하면 엔드포인트 또는 스위치에서 대기하거나 버퍼링하는 것과 관련이 있을 수 있습니다.

고려할 삭제 비율은 (삭제 횟수/시간) 대신 (전송 된 총 패킷 수/삭제 횟수)입니다.

이러한 시나리오에서는 다음을 확인합니다.

1. 스위치 인터페이스의 삭제 카운터가 ping과 함께 증가하고 있는지 확인합니다. 자세한 내용은 "패브릭 내 포워딩" 장의 "인터페이스 삭제" 섹션을 참조하십시오.
2. Rx 카운터가 대상 엔드포인트의 패킷과 함께 증가하는지 확인합니다. Rx 카운터가 전송된 패킷과 같은 수로 증가하면 엔드포인트 자체에서 패킷이 삭제될 가능성이 높습니다. 이는 TCP/IP 스택에서 엔드포인트 버퍼링 때문일 수 있습니다.

예를 들어 100000 ping이 최대한 짧은 간격으로 전송되는 경우 엔드포인트의 Rx 카운터는 100000 증가하면서 관찰될 수 있습니다.

```
[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. ACI에서 패킷을 보내고 있는지 아니면 대상에서 패킷을 받고 있는지 확인합니다

문제 해결 경로에서 ACI 패브릭을 제거하려면 리프 스위치의 이그레스 포트에 SPAN 캡처를 사용합니다.

또한 이전 버퍼링 단계에 나와 있는 것처럼 전체 네트워크 스위치를 문제 해결 경로에서 제거하는 데 대상의 Rx 카운터를 유용하게 사용할 수 있습니다.

엔드포인트 플래핑

이 섹션에서는 엔드포인트 플래핑을 확인하는 방법에 대해 설명합니다. 자세한 내용은 다음 문서에서 확인할 수 있습니다.

- "ACI Fabric Endpoint Learning 백서" on www.cisco.com
- "Cisco Live BRKACI-2641 ACI 트러블슈팅: Endpoints" on www.ciscolive.com

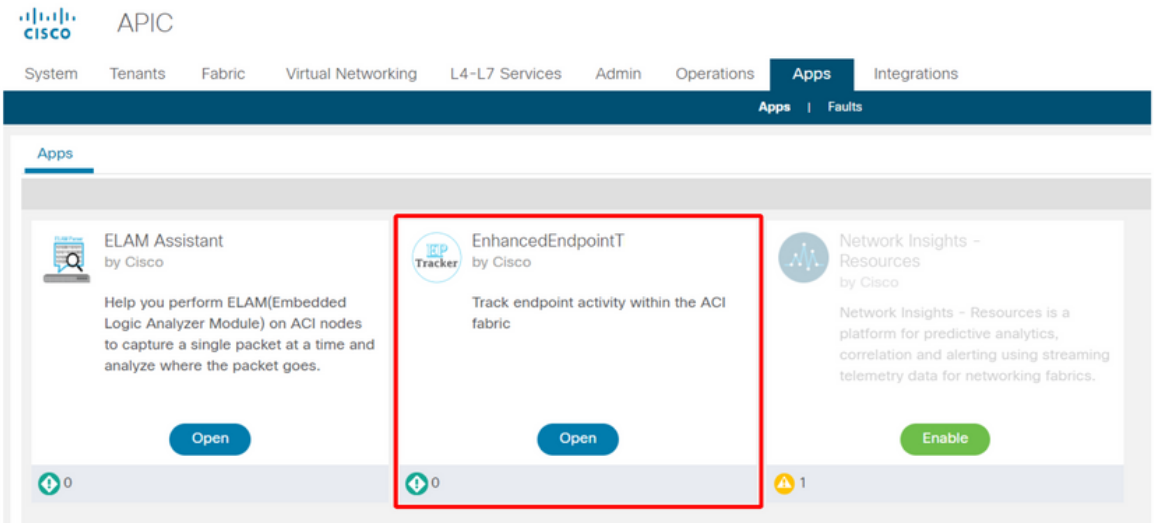
ACI가 여러 위치에서 동일한 MAC 또는 IP 주소를 학습하면 엔드포인트가 이동한 것처럼 보입니다.

이는 또한 스푸핑 디바이스 또는 잘못된 컨피그레이션에 의해 야기될 수 있다. 이러한 동작을 엔드포인트 플래핑이라고 합니다. 이러한 시나리오에서는 이동/플랩 엔드포인트(브리지 트래픽의 MAC 주소, 라우팅된 트래픽의 IP 주소)로 향하는 트래픽이 간헐적으로 실패합니다.

엔드포인트 플래핑을 탐지하는 가장 효과적인 방법은 고급 엔드포인트 추적기를 사용하는 것입니다. 이 앱은 훨씬 큰 패브릭을 관리해야 하는 경우 ACI AppCenter 앱으로 실행하거나 외부 서버에서 독립형 앱으로 실행할 수 있습니다.

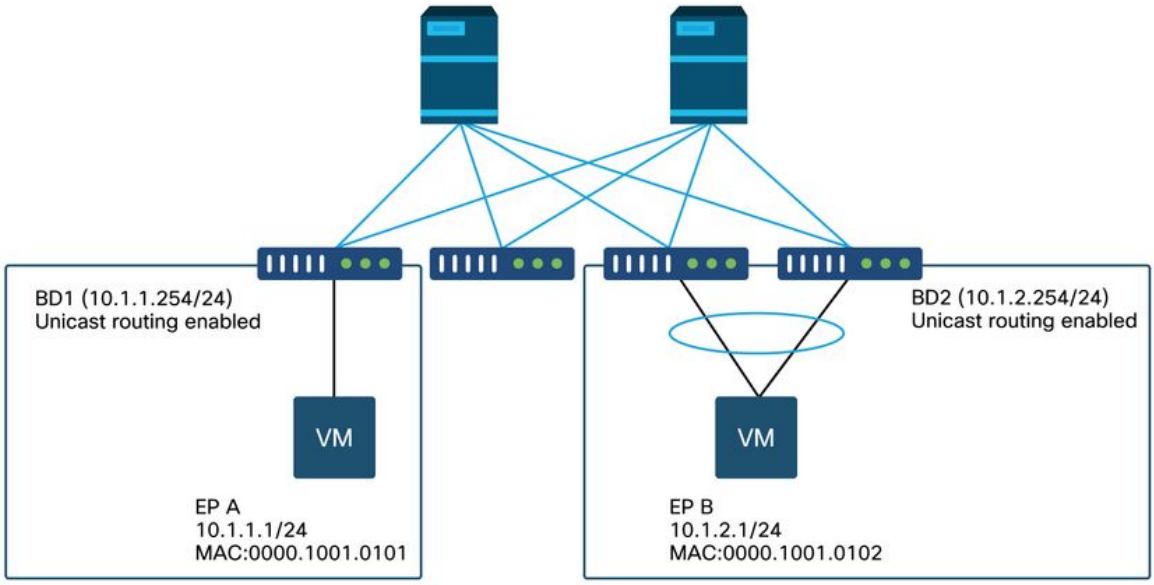
향상된 엔드포인트 추적기

경고! 이 가이드는 4.2에 작성되었습니다. 그 이후로 Enhanced Endpoint Tracker 앱은 더 이상 사용되지 않으며 Nexus Dashboard Insights의 기능을 더 많이 사용합니다. 자세한 내용은 Cisco 버그 ID CSCvz를 참조하십시오59365 .



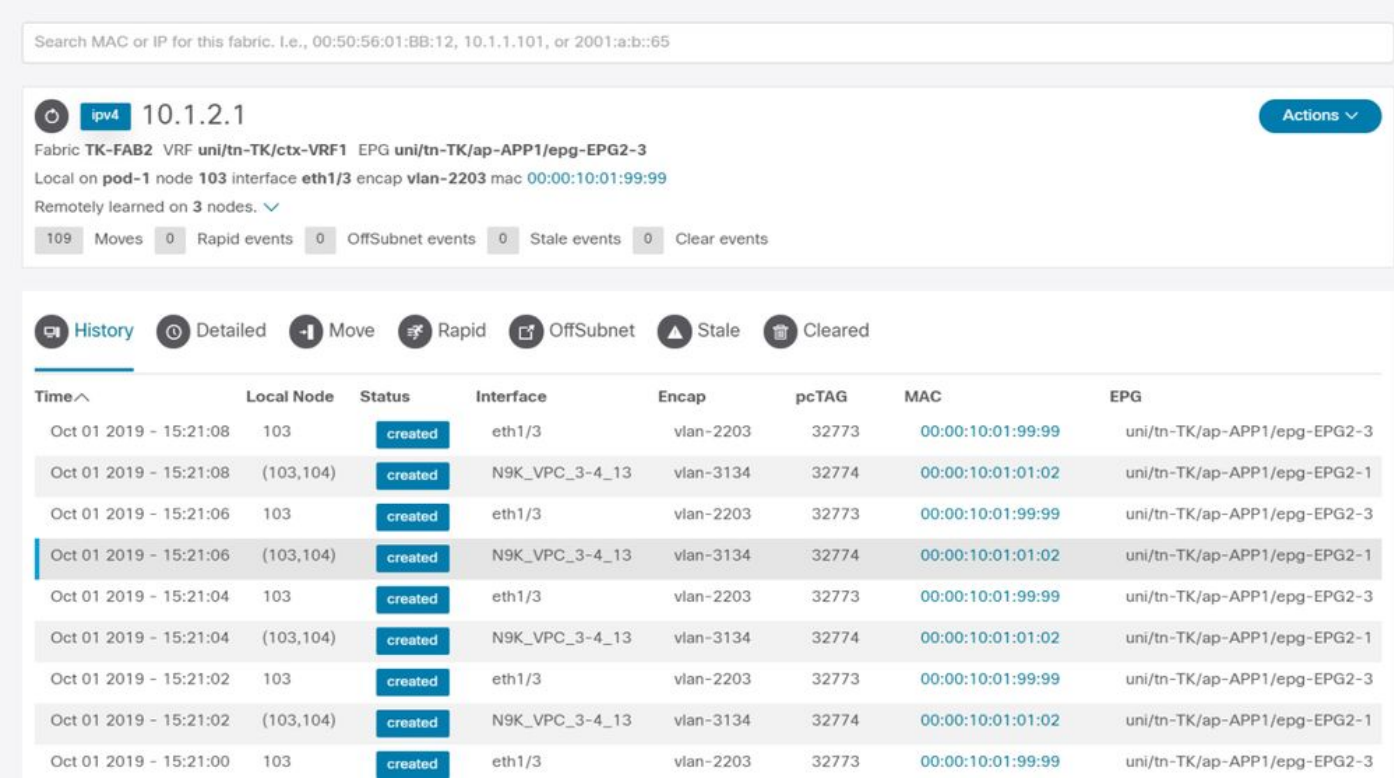
위 그림에는 AppCenter의 Enhanced Endpoint Tracker가 나와 있습니다. 다음은 Enhanced Endpoint Tracker를 사용하여 플래핑 엔드포인트를 찾는 방법의 예입니다.

엔드포인트 플래핑 예



이 예에서 IP 10.1.2.1은 MAC 0000.1001.0102의 EP B에 속해야 합니다. 그러나 MAC 0000.1001.9999의 EP X도 잘못 구성되거나 IP 스푸핑으로 인해 IP 10.1.2.1로 트래픽을 소싱하고 있습니다.

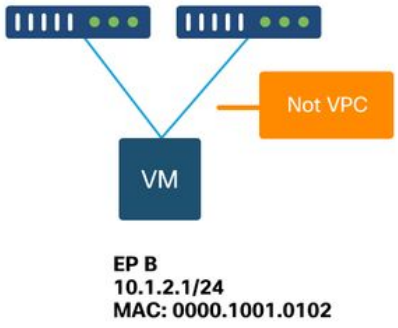
향상된 엔드포인트 추적기 출력 - 이동



Enhanced Endpoint Tracker(고급 엔드포인트 추적기)는 IP 10.1.2.1을 학습한 시기와 위치를 표시합니다. 위 스크린샷에 나와 있는 것처럼 MAC 0000.1001.0102(예상) 및 0000.1001.9999(예상 안 됨)를 사용하는 두 엔드포인트 간에 10.1.2.1이 펄럭입니다. 그러면 IP 10.1.2.1에 대한 연결 문제가 발생합니다. 잘못된 MAC 주소를 학습하면 패킷이 잘못된 인터페이스를 통해 잘못된 디바이스로 전송되기 때문입니다. 이 문제를 해결하려면 예기치 않은 VM이 부적절한 IP 주소로 트래픽을 소싱하지 않도록 조치를 취하십시오.

다음은 부적절한 컨피그레이션으로 인한 엔드포인트 플래핑의 일반적인 예입니다.

엔드포인트 플래핑을 일으킬 수 있는 토폴로지 예



서버 또는 VM이 VPC 없이 두 인터페이스를 통해 ACI 리프 노드에 연결된 경우, 서버는 액티브/스탠바이 NIC 티밍을 사용해야 합니다. 그렇지 않으면 패킷이 두 업링크에 모두 로드 밸런싱되며, ACI

리프 스위치 관점에서 보면 엔드포인트가 두 인터페이스 간에 플래핑하는 것처럼 보입니다. 이 경우 액티브/스탠바이 또는 동급의 NIC 티밍 모드가 필요하거나 ACI 측에서 VPC를 사용해야 합니다.

인터페이스 삭제

이 장에서는 인그레스 인터페이스 삭제와 관련된 주요 카운터를 확인하는 방법에 대해 설명합니다.

하드웨어 폐기 카운터 유형

ACI 모드로 실행되는 Nexus 9000 스위치에서는 인그레스 인터페이스 삭제를 위한 ACI의 세 가지 주요 하드웨어 카운터가 있습니다.

앞으로

삭제의 주요 원인은 다음과 같습니다.

- 보안_그룹_거부: 커뮤니케이션을 허용할 계약이 누락되었기 때문에 누락되었습니다.
- VLAN_XLATE_MISS: 부적절한 VLAN으로 인한 삭제 예를 들어, 프레임이 802.1Q VLAN 10이 있는 패브릭에 들어갑니다. 스위치에 포트에 VLAN 10이 있으면 내용을 검사하고 대상 MAC을 기준으로 포워딩 결정을 내립니다. 그러나 VLAN 10이 포트에서 허용되지 않을 경우 이를 삭제하고 VLAN_XLATE_MISS로 레이블링합니다.
- ACL_DROP: SUP-TCAM으로 인한 하락입니다. ACI 스위치의 SUP-TCAM에는 일반적인 L2/L3 포워딩 결정에 우선하여 적용되는 특수 규칙이 포함되어 있습니다. SUP-TCAM의 규칙은 기본적으로 제공되며 사용자가 구성할 수 없습니다. SUP-TCAM 규칙의 목적은 주로 일부 예외 또는 일부 컨트롤 플레인 트래픽을 처리하기 위한 것이며 사용자가 확인하거나 모니터링하기 위한 것이 아닙니다. 패킷이 SUP-TCAM 규칙에 도달하고 규칙이 패킷을 삭제하는 경우, 삭제된 패킷은 ACL_DROP으로 계산되고 포워드 드랍 카운터가 증가합니다.

전달 삭제는 기본적으로 유효한 알려진 이유로 인해 삭제된 패킷입니다. 실제 데이터 트래픽 감소와 달리, 이러한 현상은 일반적으로 무시될 수 있으며 성능 저하 문제가 발생하지 않습니다.

오류

스위치에서 유효하지 않은 프레임을 수신하면 오류로 인해 삭제됩니다. 이것의 예는 FCS 또는 CRC 오류가 있는 프레임을 포함한다. 자세한 내용은 "CRC — FCS — 컷스루 스위칭" 뒷부분의 내용을 참조하십시오.

버퍼

스위치에서 프레임을 수신했는데 인그레스 또는 이그레스에 사용할 수 있는 버퍼가 없는 경우, 프레임은 'Buffer'로 삭제됩니다. 이는 일반적으로 네트워크의 어딘가에서 혼잡함을 암시합니다. 결함을 표시하는 링크가 꽉 찼거나 대상을 포함하는 링크가 혼잡할 수 있습니다.

API를 사용하여 카운터를 모으고 있습니다.

API와 객체 모델을 활용하여 사용자가 패브릭에 이러한 삭제의 모든 인스턴스를 빠르게 쿼리할 수 있다는 점에 유의하십시오(apic에서 실행).

```
# 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"
```

CLI에서 삭제 통계 보기

결함이 발견되거나 CLI를 사용하여 인터페이스의 패킷 삭제를 확인해야 하는 경우, 이를 수행하는 가장 좋은 방법은 하드웨어에서 플랫폼 카운터를 보는 것입니다. 일부 카운터는 'show interface'를 사용하여 표시되지 않습니다. 세 가지 주요 삭제 이유는 플랫폼 카운터를 통해서만 볼 수 있습니다. 이를 보려면 다음 단계를 수행하십시오.

리프

SSH를 leaf에 연결하고 이 명령을 실행합니다. 이 예는 이더넷 1/31에 대한 것입니다.

```
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
...
```

스파인(Spine)

리프 스위치와 동일한 방법으로 고정 스파인(N9K-C9332C 및 N9K-C9364C)을 확인할 수 있습니다 .

모듈형 스파인(N9K-C9504 등)의 경우 플랫폼 카운터를 보려면 먼저 라인 카드를 연결해야 합니다. spine에 SSH를 적용하고 이 명령을 실행합니다. 이 예는 이더넷 2/1에 대한 것입니다.

```
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
...
```

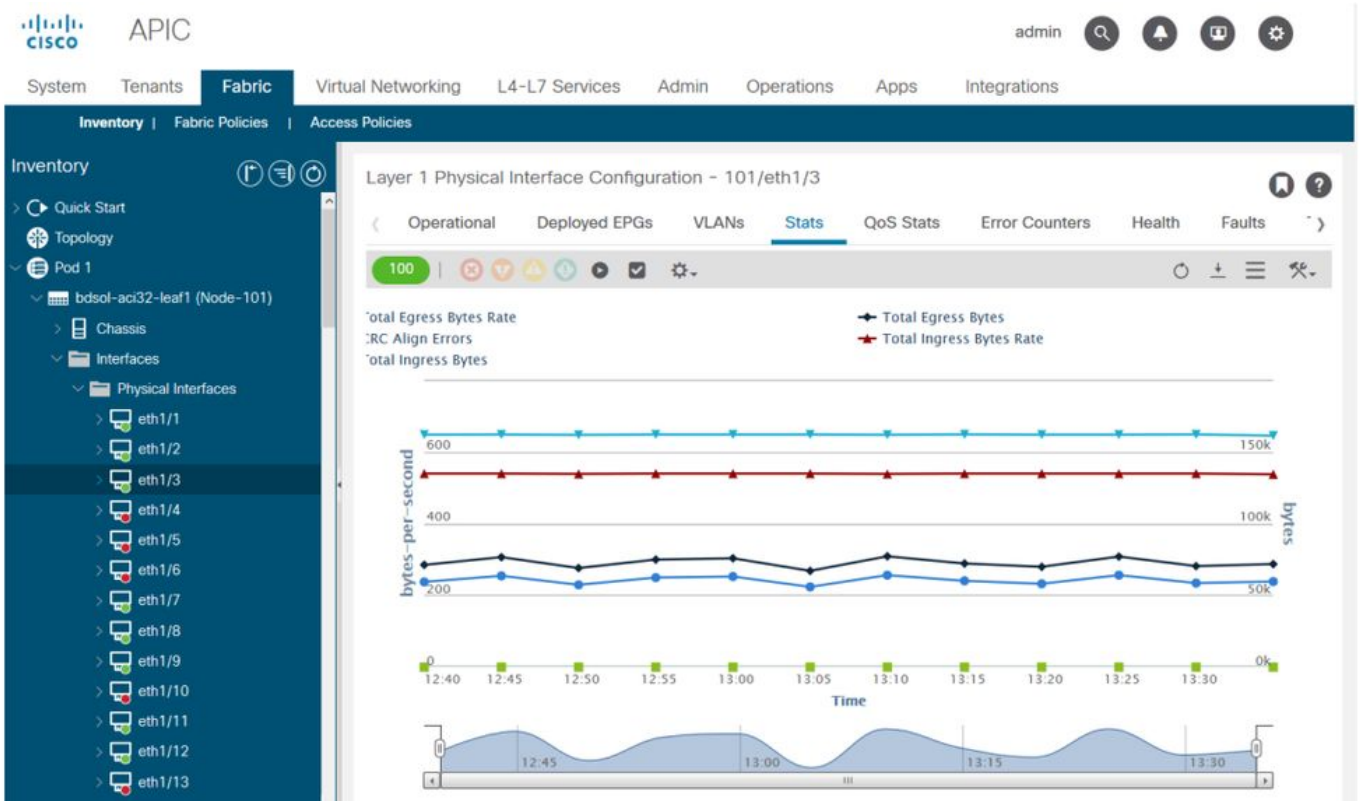
대기열 통계 카운터는 'show queuing interface'를 사용하여 표시됩니다. 이 예는 이더넷 1/5에 대한 것입니다.

```
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

...
```

GUI에서 통계 보기

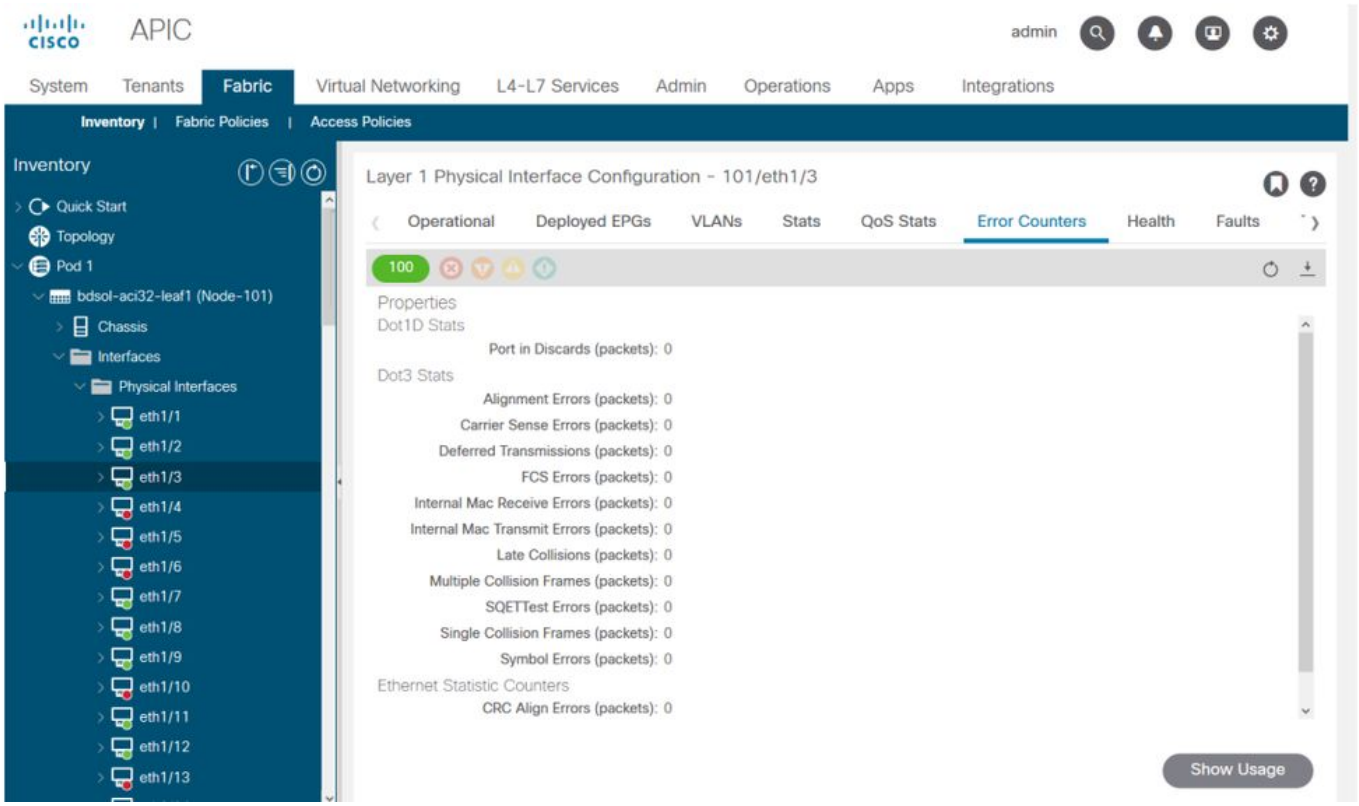
위치는 '패브릭 > 인벤토리 > 리프/스파인 > 물리적 인터페이스 > 통계'입니다.

GUI 인터페이스 통계



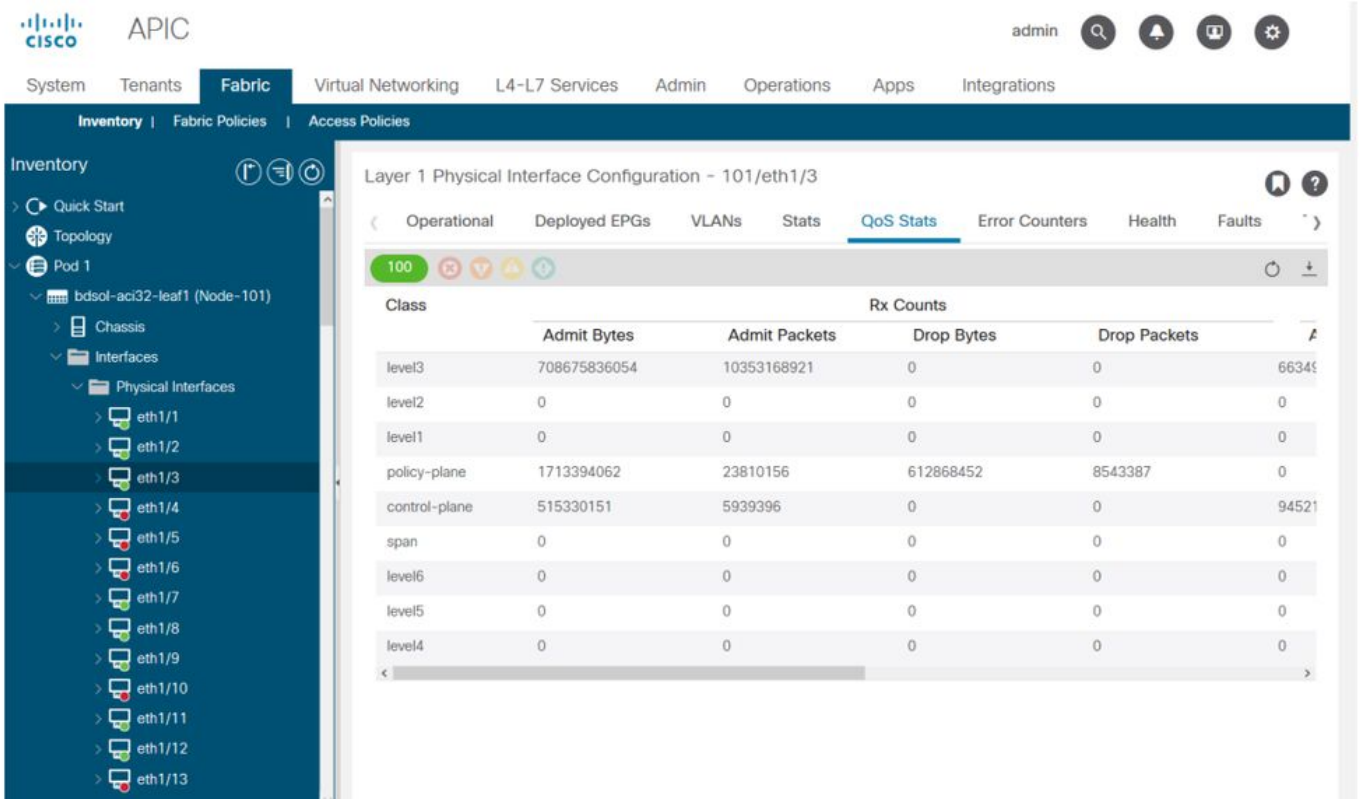
오류 통계는 동일한 위치에서 볼 수 있습니다.

GUI 인터페이스 오류



마지막으로, GUI에서는 인터페이스당 QoS 통계를 표시할 수 있습니다.

GUI 인터페이스 QoS 카운터



CRC — FCS — 컷스루 스위칭

CRC(Cyclic Redundancy Check)란 무엇입니까?

CRC는 이더넷에서 4B 숫자를 반환하는 프레임의 다항식 함수이다. 모든 단일 비트 오류와 높은 비율의 이중 비트 오류를 잡아냅니다. 따라서 프레임이 전송 중에 손상되지 않았음을 확인하기 위한 것입니다. CRC 오류 카운터가 증가하는 경우 하드웨어에서 프레임 상에서 다항식 함수를 실행할 때 프레임 자체에서 발견된 4B 번호와 다른 4B 번호가 생성되었음을 의미합니다. 이중 불일치, 케이블 오류, 하드웨어 고장과 같은 여러 가지 이유로 프레임이 손상될 수 있습니다. 그러나 일부 수준의 CRC 오류가 예상되어야 하며 표준에서는 이더넷에서 최대 10-12비트 오류 속도를 허용합니다(1012비트 중 1비트는 플립될 수 있음).

Store-and-forward와 cut-through 스위칭

저장-전달 및 컷스루 레이어 2 스위치는 모두 데이터 패킷의 대상 MAC 주소를 기준으로 전달 결정을 내립니다. 또한 스테이션이 네트워크의 다른 노드와 통신할 때 패킷의 소스 MAC(SMAC) 필드를 검사할 때 MAC 주소를 학습합니다.

저장-전달 스위치는 전체 프레임을 수신하고 무결성을 확인한 후 데이터 패킷에 대한 전달 결정을 내립니다. 컷스루 스위치는 수신 프레임의 목적지 MAC(DMAC) 주소를 검사한 직후 포워딩 프로세스에 참여합니다. 그러나 컷스루 스위치는 CRC 검사를 수행하기 전에 전체 패킷을 볼 때까지 기다려야 합니다. 즉, CRC가 검증될 때까지 패킷이 이미 전달되었으며 검사에 실패할 경우 삭제할 수 없습니다.

전통적으로 대부분의 네트워크 디바이스는 저장 후 전달을 기반으로 작동했습니다. 컷스루 스위칭 기술은 짧은 지연 시간의 포워딩이 필요한 고속 네트워크에서 사용되는 경향이 있습니다.

특히, 2세대 이상 ACI 하드웨어의 경우, 인그레스 인터페이스가 더 빠른 속도이고 이그레스 인터페이스가 같은 속도이거나 속도가 더 느린 경우 컷스루 스위칭이 수행됩니다. 저장 후 전달 스위칭은 인그레스 인터페이스 속도가 이그레스 인터페이스보다 낮은 경우 수행됩니다.

쿵쿵

CRC 오류가 있는 패킷은 삭제해야 합니다. 프레임이 컷스루 경로에서 전환되는 경우 패킷이 이미 전달된 후 CRC 검증이 수행됩니다. 따라서 유일한 옵션은 FCS(Ethernet Frame Check Sequence)를 중단하는 것입니다. 프레임을 중단하려면 FCS**를 CRC 검사를 통과하지 않는 알려진 값으로 설정해야 합니다**. 이 때문에 CRC에 실패한 불량 프레임 하나가 드롭할 저장 및 전달 스위치에 도달할 때까지 통과하는 모든 인터페이스에 CRC로 표시될 수 있습니다.

ACI 및 CRC: 결함이 있는 인터페이스를 찾습니다.

- Leaf에서 다운링크 포트의 CRC 오류를 발견하면 대개 다운링크 SFP 또는 외부 디바이스/네트워크의 구성 요소에 문제가 발생합니다.
- 스파인에 CRC 오류가 표시되면 해당 로컬 포트, SFP, 파이버 또는 네이버 SFP에서 주로 문제가 발생합니다. 리프 다운링크에서 CRC 실패 패킷은 스핀으로 스탬프되지 않습니다. 헤더를 읽을 수 있는 것처럼 VXLAN이 캡슐화되고 새 CRC가 계산됩니다. 프레임 손상으로 헤더를 읽을 수 없는 경우 패킷이 삭제됩니다.
- leaf에서 패브릭 링크에 CRC 오류가 표시되는 경우 다음 중 하나가 될 수 있습니다. 로컬 파이버/SFP 쌍, 스파인의 인그레스 파이버 또는 SFP 쌍에 문제가 있습니다.직물을 통해 나아가고 있는 접은 프레임.

멈춤: 쿵쾅거리는 문제 해결

- 패브릭에서 FCS 오류가 있는 인터페이스를 찾습니다. FCS는 포트에서 로컬로 발생하므로 양쪽 끝에 파이버 또는 SFP가 있을 가능성이 높습니다.
- 'show interface' 출력의 CRC 오류는 총 FCS+Stomp 값을 반영합니다.\

예를 들어

명령을 사용하여 포트 확인

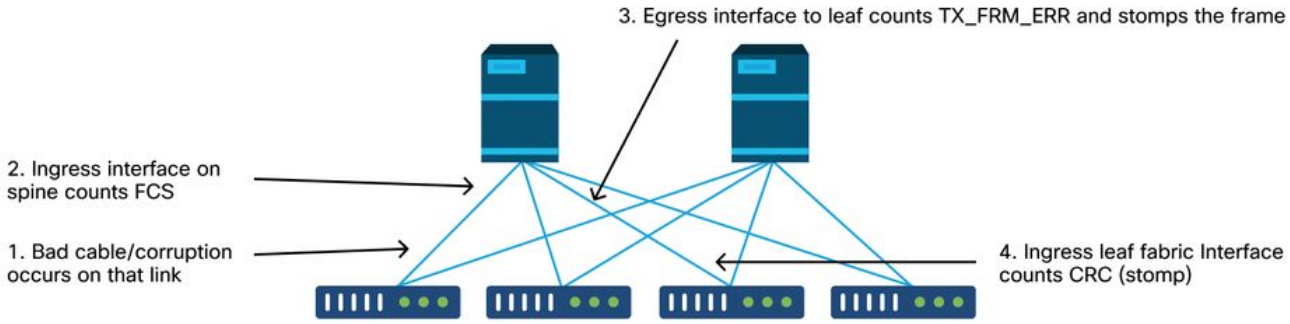
```
vsh_lc: 'show platform internal counter port <X>'
```

이 명령에서는 3개의 값이 중요합니다.

- RX_FCS_ERR - FCS 오류입니다.
- RX_CRCERR - 압축된 CRC 오류 프레임을 받았습니다.
- TX_FRM_ERROR - 전송된 압축 CRC 오류 프레임입니다.

```
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 멈춤 문제 해결 시나리오



손상된 링크가 손상된 프레임을 많이 생성할 경우, 해당 프레임은 다른 모든 리프 노드에 플러딩될 수 있으며 패브릭에서 대부분의 리프 노드의 패브릭 업링크 인그레스(ingress)에서 CRC를 찾을 수 있습니다. 이러한 모든 것은 손상된 단일 링크에서 발생할 수 있습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.