Solução de problemas de encaminhamento entre estruturas da ACI - quedas intermitentes

Contents

Introduction

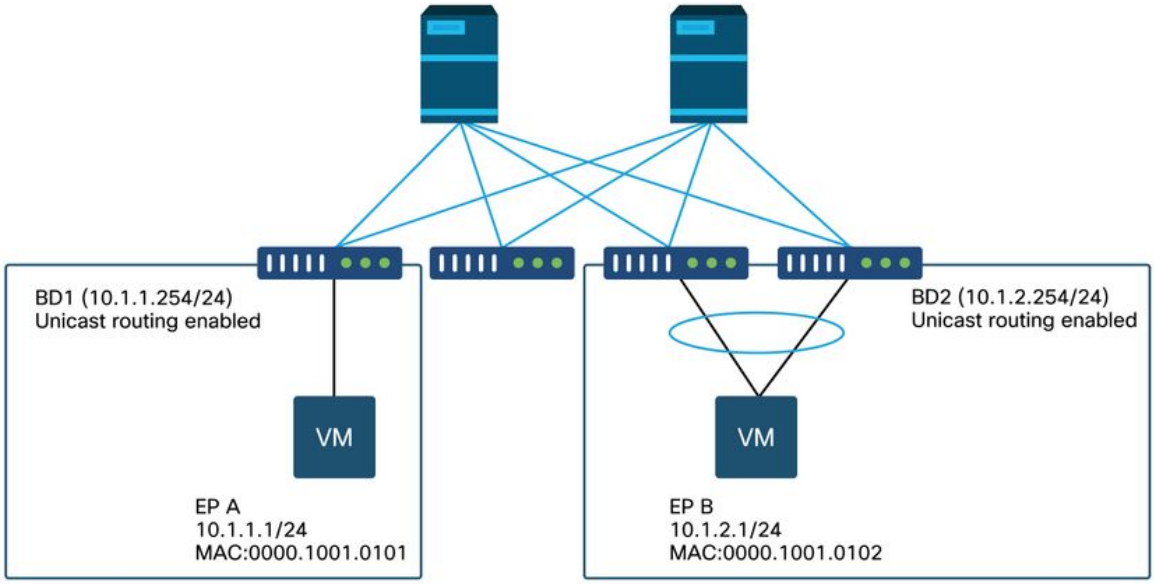
Este documento descreve as etapas para solucionar problemas de quedas intermitentes na ACI.

Informações de Apoio

O material deste documento foi extraído do livro Troubleshooting Cisco Application Centric Infrastructure, Second Edition, especificamente do capítulo **Encaminhamento intracorde - quedas intermitentes**.

Solução de problemas de encaminhamento de estrutura interna da ACI - quedas intermitentes

Exemplo de topologia



Neste exemplo, o ping do EP A (10.1.1.1) para o EP B (10.1.2.1) está experimentando quedas intermitentes.

```
[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
```

Troubleshooting de fluxo de trabalho

1. Determine em que direção as quedas intermitentes estão sendo causadas

Execute uma captura de pacote (tcpdump, Wireshark, etc.) no host de destino (EP B). Para o ICMP, concentre-se no número de sequência para ver se os pacotes descartados intermitentemente são observados no 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
...
```

- Padrão 1 - Todos os pacotes são observados na captura de pacotes EP B.

As quedas devem estar na resposta de eco ICMP (EP B para EP A).

- Padrão 2 - As quedas intermitentes são observadas na captura de pacote EP B.

As quedas devem estar no eco ICMP (EP A para EP B).

2. Verifique se outro protocolo com o mesmo IP de origem/destino tem o mesmo problema

Se possível, tente testar a conectividade entre os dois pontos finais usando um protocolo diferente permitido pelo contrato entre eles (como ssh, telnet, http,...)

- Padrão 1 - Outros protocolos têm a mesma queda intermitente.

O problema pode estar na oscilação de endpoint ou no enfileiramento/buffer, como mostrado abaixo.

- Padrão 2 - Somente o ICMP tem a queda intermitente.

As tabelas de encaminhamento (como a tabela de endpoint) não devem ter problema, pois o encaminhamento é baseado em MAC e IP. O enfileiramento/buffer também não deve ser o motivo, pois isso afetaria outros protocolos. O único motivo pelo qual a ACI tomaria uma decisão de encaminhamento diferente com base no protocolo seria o caso de uso do PBR.

Uma possibilidade é que um dos nós spine tenha um problema. Quando um protocolo é diferente, o pacote com a mesma origem e destino pode ter a carga balanceada para outra porta de uplink/estrutura (ou seja, outra coluna) pela folha de entrada.

Os contadores atômicos podem ser usados para garantir que os pacotes não sejam descartados em nós spine e cheguem à folha de saída. Caso os pacotes não cheguem à folha de saída, verifique o ELAM na folha de entrada para ver qual porta de estrutura os pacotes são enviados. Para isolar o problema em um spine específico, os uplinks leaf podem ser desativados para forçar o tráfego em direção a outro spine.

3. Verifique se está relacionado a um problema de aprendizagem de endpoint

A ACI usa uma tabela de endpoint para encaminhar pacotes de um endpoint para outro. Um problema de acessibilidade intermitente pode ser causado pela oscilação de endpoint porque informações inadequadas de endpoint farão com que o pacote seja enviado para um destino errado ou que seja descartado por contrato, pois está classificado no EPG errado. Mesmo que o destino deva ser uma L3Out em vez de um grupo de endpoint, certifique-se de que o IP não seja aprendido como um endpoint no mesmo VRF em todos os switches leaf.

Consulte a subseção "Flapping de endpoint" nesta seção para obter mais detalhes sobre como solucionar problemas de flapping de endpoint.

4. Verifique se está relacionado a problemas de buffer alterando a frequência de tráfego

Aumente ou diminua o intervalo do ping para ver se a taxa de queda muda. A diferença de intervalo deve ser grande o suficiente.

No Linux, a opção '-i' pode ser usada para alterar o intervalo (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
```

Se a taxa de queda aumenta quando o intervalo é reduzido, é provável que esteja relacionada ao enfileiramento ou buffer em endpoints ou switches.

A taxa de queda a ser considerada é (número de quedas/total de pacotes enviados) em vez de (número de quedas/tempo).

Nesse cenário, verifique o seguinte.

1. Verifique se algum contador de queda nas interfaces do switch está aumentando junto com o ping. Consulte a seção "Quedas de interface" no capítulo "Encaminhamento dentro da estrutura" para obter detalhes.
2. Verifique se o contador Rx está aumentando junto com os pacotes no ponto final de destino. Se o contador Rx for aumentado com o mesmo número que os pacotes transmitidos, os pacotes provavelmente serão descartados no próprio ponto final. Isso pode ser devido ao armazenamento de ponto final na pilha TCP/IP.

Por exemplo, se 100000 pings forem enviados com o intervalo mais curto possível, o contador Rx no ponto final pode ser observado à medida que ele aumenta em 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. Verifique se a ACI está enviando os pacotes ou se o destino está recebendo os pacotes

Faça uma captura de SPAN na porta de saída do switch leaf para eliminar a estrutura da ACI do caminho de solução de problemas.

Os contadores Rx no destino também podem ser úteis para eliminar os switches de rede inteiros do caminho de solução de problemas, como mostrado nas etapas anteriores para armazenamento em buffer.

Não-sincronização de endpoint

Esta seção explica como verificar a oscilação do ponto final. Detalhes adicionais podem ser encontrados nestes documentos:

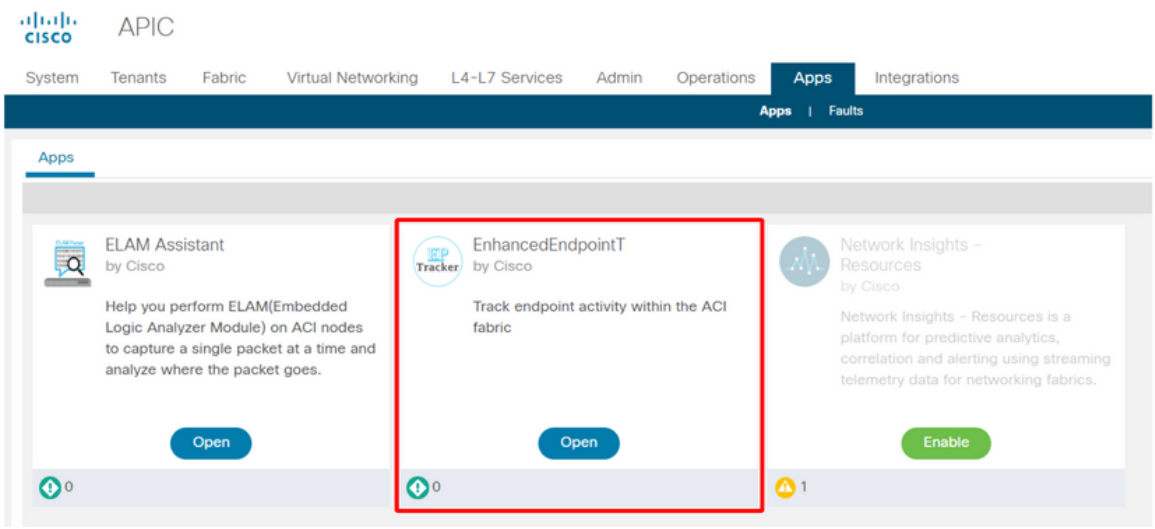
- "White paper de aprendizagem de endpoints de malha da ACI" em www.cisco.com
- "Solução de problemas do Cisco Live BRKACI-2641 ACI: endpoints" em www.ciscolive.com

Quando a ACI aprende o mesmo endereço MAC ou IP em vários locais, parece que o endpoint foi movido. Isso também pode ser causado por um dispositivo de falsificação ou uma configuração incorreta. Esse comportamento é conhecido como oscilação de ponto final. Nesse cenário, o tráfego em direção ao endpoint em movimento/oscilação (endereço MAC para tráfego em ponte, endereço IP para tráfego roteado) falhará intermitentemente.

O método mais eficaz para detectar oscilação de endpoint é usar o Controlador de Endpoint Avançado. Esse aplicativo pode ser executado como um aplicativo ACI AppCenter ou como um aplicativo autônomo em um servidor externo, caso precise gerenciar uma malha muito maior.

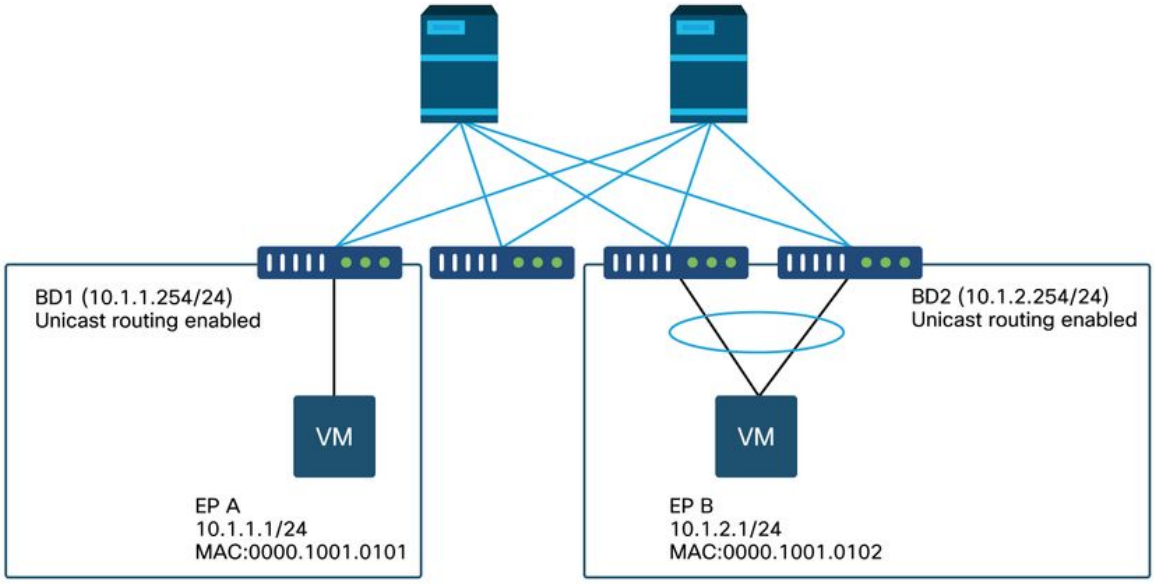
Controlador de endpoint avançado

AVISO DE REPROVAÇÃO! Este guia foi escrito em 4.2; desde então, o aplicativo Enhanced Endpoint Tracker foi substituído em favor da funcionalidade no Nexus Dashboard Insights. Para obter mais informações, consulte o bug da Cisco ID CSCvz59365 .



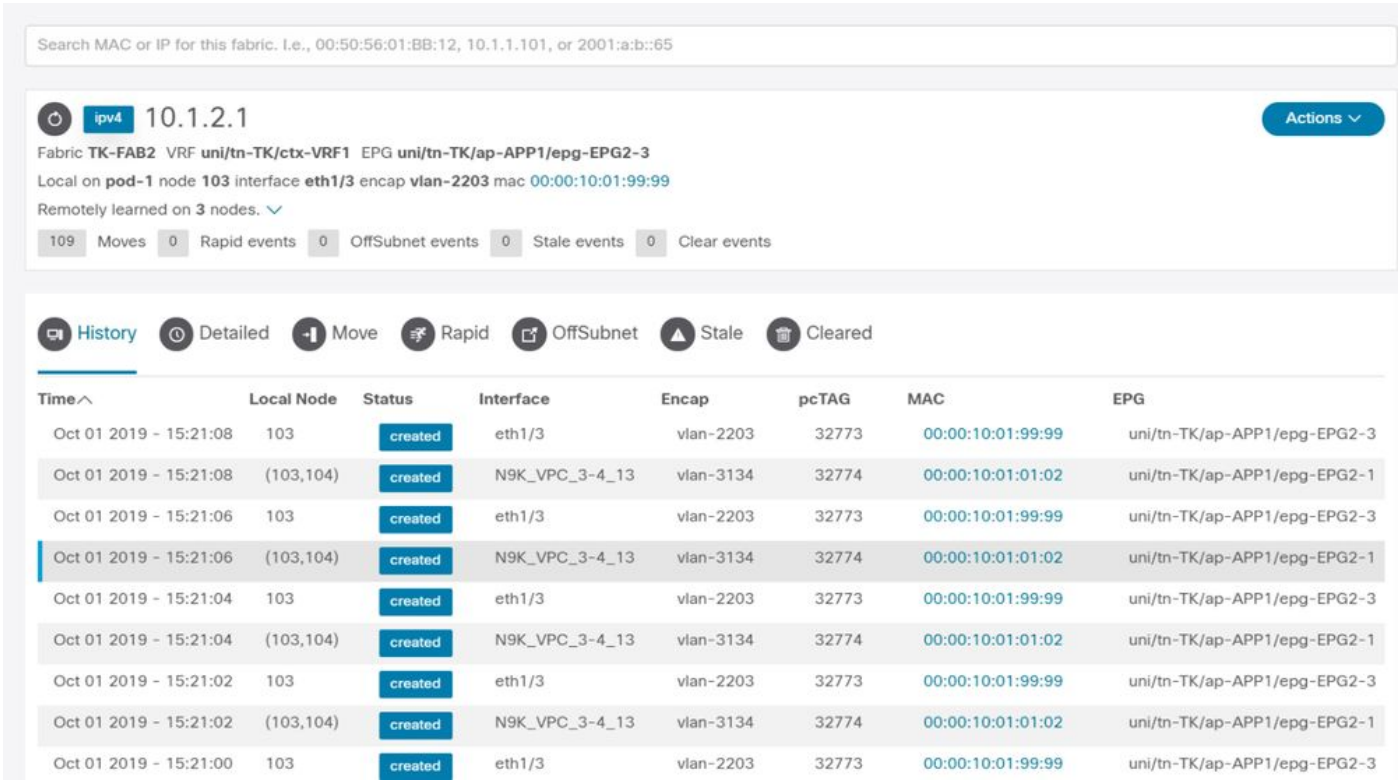
A figura acima mostra o Controlador de endpoint aprimorado no AppCenter. Veja a seguir um exemplo de como encontrar pontos finais oscilantes com o Controlador de ponto final aprimorado.

Exemplo de oscilação de endpoint



Neste exemplo, o IP 10.1.2.1 deve pertencer ao EP B com MAC 0000.1001.0102. No entanto, um EP X com MAC 0000.1001.9999 também está originando o tráfego com IP 10.1.2.1 devido a uma configuração incorreta ou talvez a falsificação de IP.

Resultado avançado do rastreador de endpoint — mudanças

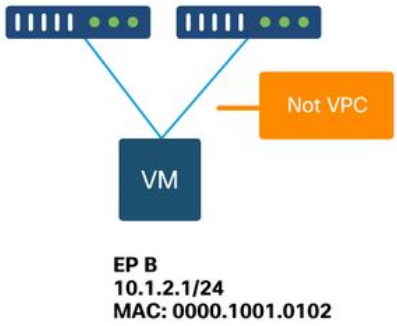


Time	Local Node	Status	Interface	Encap	pcTAG	MAC	EPG
Oct 01 2019 - 15:21:08	103	created	eth1/3	vlan-2203	32773	00:00:10:01:99:99	uni/tn-TK/ap-APP1/epg-EPG2-3
Oct 01 2019 - 15:21:08	(103,104)	created	N9K_VPC_3-4_13	vlan-3134	32774	00:00:10:01:01:02	uni/tn-TK/ap-APP1/epg-EPG2-1
Oct 01 2019 - 15:21:06	103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

O Enhanced Endpoint Tracker mostra quando e onde o IP 10.1.2.1 foi aprendido. Como mostrado na captura de tela acima, 10.1.2.1 está oscilando entre dois endpoints com MAC 0000.1001.0102 (esperado) e 0000.1001.9999 (não esperado). Isso causará um problema de acessibilidade em relação ao IP 10.1.2.1, pois quando ele for aprendido no endereço MAC errado, o pacote será enviado a um dispositivo errado através da interface errada. Para resolver isso, tome medidas para impedir que a VM inesperada forneça tráfego com um endereço IP inadequado.

A seguir, um exemplo típico de oscilação de endpoint devido a uma configuração inadequada.

Exemplo de topologia que poderia causar oscilação de ponto final



Quando um servidor ou uma VM é conectada a nós leaf da ACI por meio de duas interfaces sem um VPC, o servidor precisa usar o agrupamento de NICs Ativo/Standby. Caso contrário, os pacotes terão a carga balanceada para ambos os uplinks e pareceria que os endpoints estão oscilando entre duas interfaces da perspectiva do switch de leaf da ACI. Nesse caso, é necessário o modo de agrupamento Ativo/Em espera ou equivalente da placa de rede ou apenas usar um VPC no lado da ACI.

Desconexão de interfaces

Este capítulo descreve como verificar os principais contadores relacionados à queda da interface de entrada.

Tipos de contador de queda de hardware

Nos switches Nexus 9000 executados no modo ACI, há três contadores de hardware principais na ACI para quedas de interface de entrada.

Encaminhar

Os principais motivos para descartes são:

- SECURITY_GROUP_DENY: Uma queda devido à falta de contratos para permitir a comunicação.
- VLAN_XLATE_MISS: Uma queda devido a uma VLAN inadequada. Por exemplo, um quadro entra na estrutura com uma VLAN 10 802.1Q. Se o switch tiver a VLAN 10 na porta, ele inspecionará o conteúdo e tomará uma decisão de encaminhamento com base no MAC destino. No entanto, se a VLAN 10 não for permitida na porta, ela será descartada e rotulada como VLAN_XLATE_MISS.
- ACL_DROP: Uma queda devido a SUP-TCAM. O SUP-TCAM em switches ACI contém regras especiais a serem aplicadas sobre a decisão normal de encaminhamento L2/L3. As regras em SUP-TCAM são incorporadas e não configuráveis pelo usuário. O objetivo das regras SUP-TCAM é principalmente lidar com algumas exceções ou algum tráfego de plano de controle e não se destina a ser verificado ou monitorado pelos usuários. Quando um

pacote está atingindo as regras SUP-TCAM e a regra é descartar o pacote, o pacote descartado é contado como ACL_DROP e incrementará o contador de queda de encaminhamento.

Quedas de encaminhamento são essencialmente pacotes descartados por uma razão conhecida válida. Eles geralmente podem ser ignorados e não causarão penalidades de desempenho, ao contrário de quedas de tráfego de dados reais.

Erro

Quando o switch recebe um quadro inválido, ele é descartado como um erro. Exemplos disso incluem quadros com erros de FCS ou CRC. Consulte a seção posterior "CRC — FCS — switching cut-through" para obter mais detalhes.

Buffer

Quando um switch recebe um quadro e não há buffers disponíveis para entrada ou saída, o quadro é descartado com 'Buffer'. Isso geralmente sugere um congestionamento em algum lugar da rede. O link que está mostrando a falha pode estar cheio ou o link que contém o destino está congestionado.

Coletando contadores usando a API

Vale observar que, aproveitando a API e o modelo de objeto, o usuário pode consultar rapidamente a estrutura para todas as instâncias desses descartes (executá-los a partir de uma 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"
```

Exibição de estatísticas de queda na CLI

Se forem observadas falhas ou se houver necessidade de verificar descartes de pacotes nas interfaces usando o CLI, a melhor maneira de fazer isso é visualizando os contadores da plataforma no hardware. Nem todos os contadores são mostrados usando-se 'show interface'. Os três motivos principais de queda só podem ser visualizados usando os contadores da plataforma. Para visualizá-los, execute estas etapas:

Folha

Use SSH para a folha e execute esses comandos. Este exemplo é para a 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
...
```

Coluna

Uma coluna fixa (N9K-C9332C e N9K-C9364C) pode ser verificada usando o mesmo método que os switches leaf.

Para uma lombada modular (N9K-C9504 etc.), a placa de linha deve ser conectada antes que os contadores da plataforma possam ser visualizados. Use SSH para o spine e execute esses comandos. Este exemplo é para a 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
...
```

Os contadores de estatísticas de enfileiramento são mostrados usando 'show queuing interface'. Este exemplo é para a Ethernet 1/5.

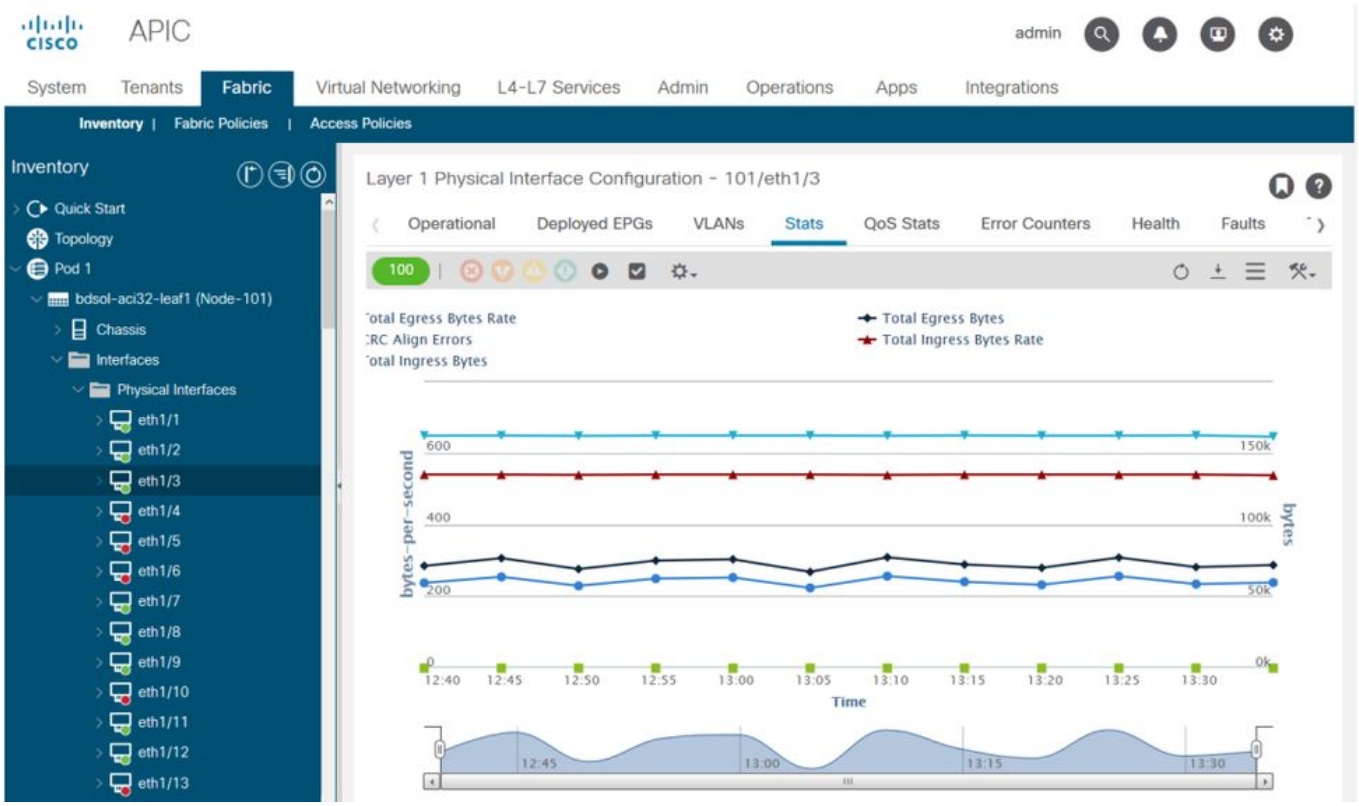
```
ACI-LEAF# show queuing interface ethernet 1/5
================================================================================
               Queuing stats for ethernet 1/5
================================================================================
================================================================================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

...
```

Exibindo estatísticas na GUI

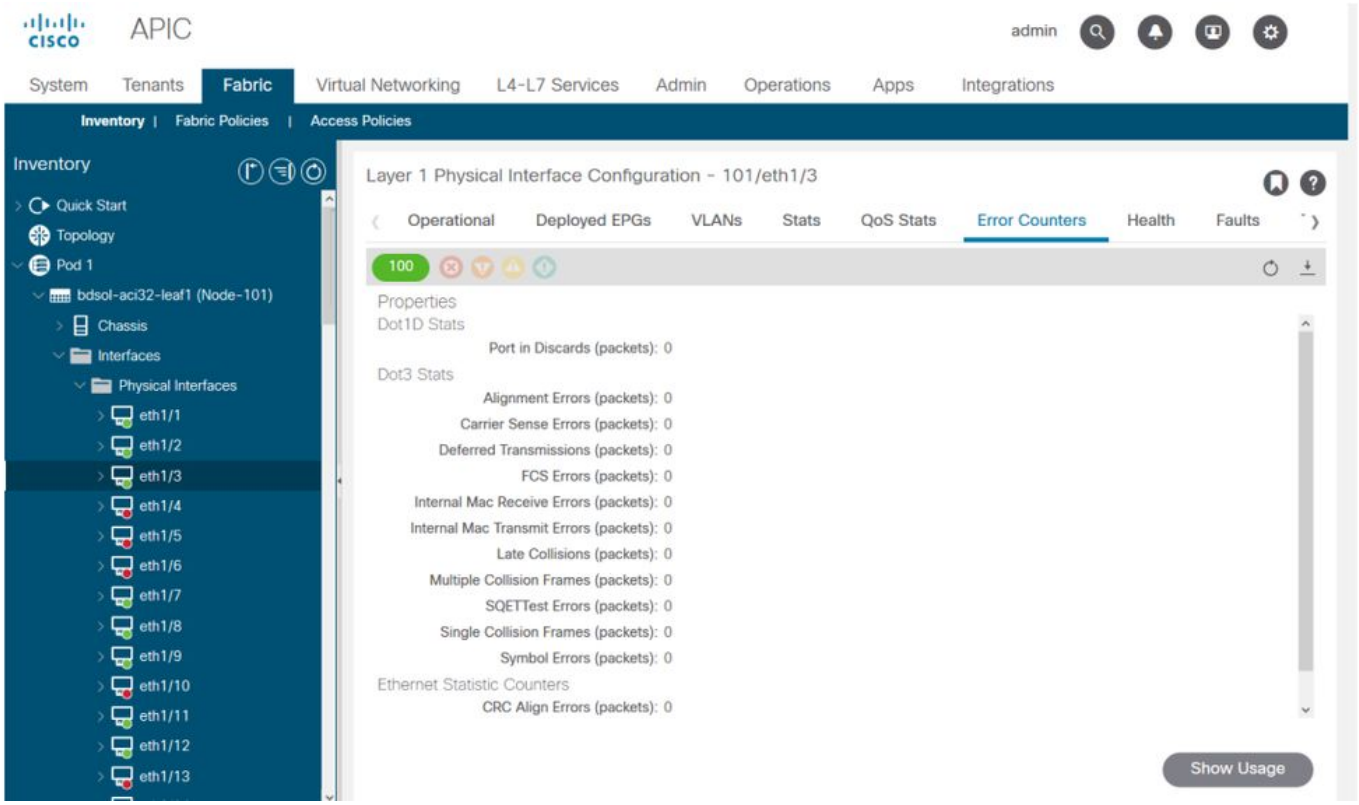
O local é 'Fabric > Inventory > Leaf/Spine > Physical interface > Stats'.

estatísticas da interface GUI



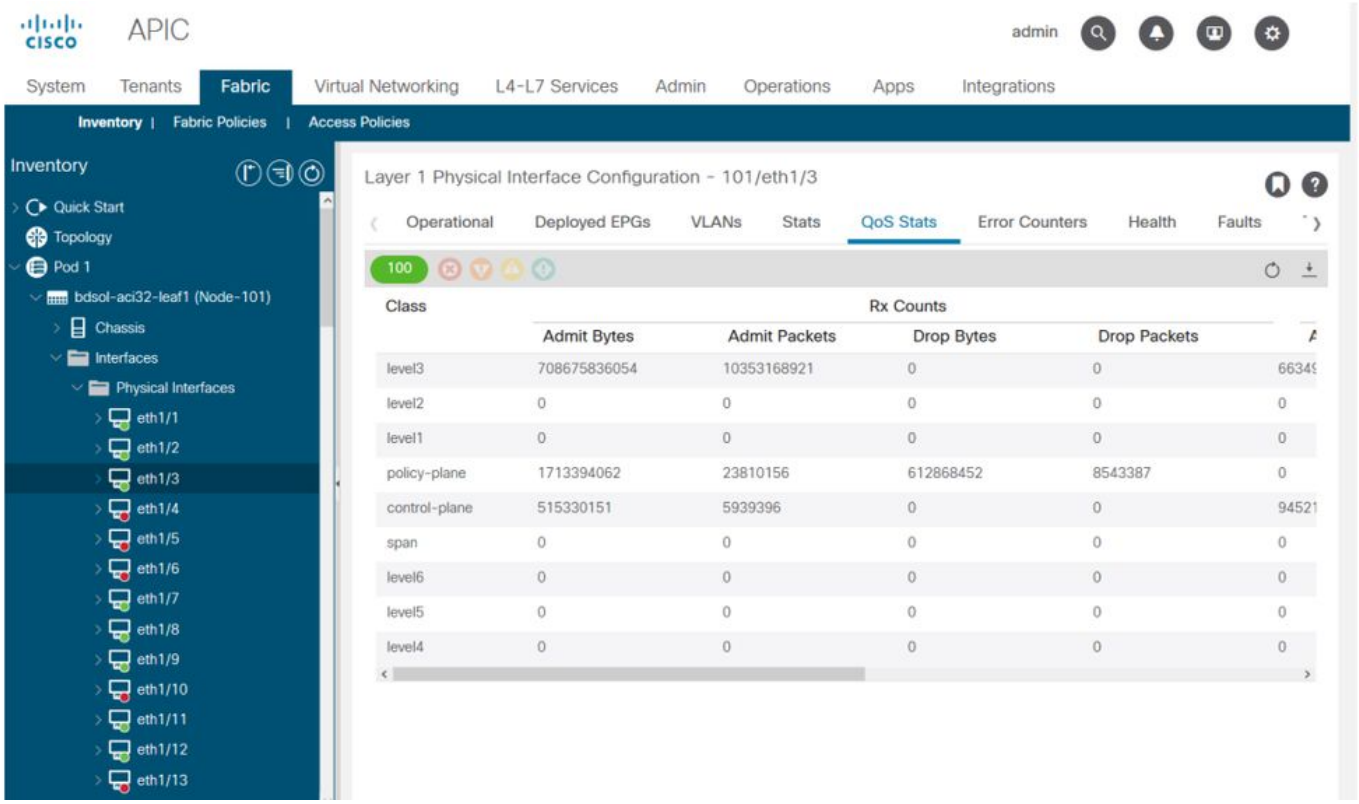
As estatísticas de erro podem ser vistas no mesmo local:

Erros de interface GUI



Por fim, a GUI pode exibir estatísticas de QoS por interface:

Contadores de QoS da interface GUI



CRC — FCS — switching cut-through

O que é verificação de redundância cíclica (CRC)?

O CRC é uma função polinomial no quadro que retorna um número 4B na Ethernet. Ele detectará todos os erros de bit único e uma boa porcentagem dos erros de bit duplo. Assim, ele serve para garantir que o quadro não seja corrompido em trânsito. Se o contador de erro CRC estiver aumentando, significa que quando o hardware executou a função polinomial no quadro, o resultado foi um número 4B que diferia do número 4B encontrado no próprio quadro. Os quadros podem ser corrompidos devido a vários motivos, como incompatibilidade duplex, cabeamento defeituoso e hardware quebrado. No entanto, deve-se esperar algum nível de erros de CRC e o padrão permite uma taxa de erros de até 10-12 bits na Ethernet (1 bit de 1012 pode virar).

Comutação store-and-forward vs cut-through

Os switches de Camada 2 store-and-forward e cut-through baseiam suas decisões de encaminhamento no endereço MAC destino dos pacotes de dados. Eles também aprendem os endereços MAC quando examinam os campos MAC origem (SMAC) dos pacotes quando as estações se comunicam com outros nós na rede.

Um switch store-and-forward toma uma decisão de encaminhamento em um pacote de dados depois de receber o quadro inteiro e verificar sua integridade. Um switch cut-through inicia o processo de encaminhamento logo depois de examinar o endereço MAC de destino (DMAC) de um quadro de entrada. No entanto, um switch cut-through deve aguardar até que tenha visualizado o pacote inteiro antes de executar a verificação de CRC. Isso significa que quando o CRC for validado, o pacote já terá sido encaminhado e não poderá ser descartado se falhar na verificação.

Tradicionalmente, a maioria dos dispositivos de rede costumava operar com base no store-and-forward. As tecnologias de switching cut-through tendem a ser usadas em redes de alta velocidade que exigem encaminhamento de baixa latência.

Especificamente, com relação ao hardware da ACI de geração 2 e posterior, a comutação cut-through é realizada se a interface de entrada for de velocidade mais alta e a interface de saída for da mesma velocidade ou de velocidade mais baixa. O switching store-and-forward é feito se a velocidade da interface de entrada for menor que a da interface de saída.

Esmagamento

Pacotes com um erro de CRC necessitam de uma queda. Se o quadro estiver sendo comutado em um caminho cut-through, a validação de CRC acontece depois que o pacote já é encaminhado. Como tal, a única opção é pisar a FCS (Ethernet Frame Check Sequence). **O estancamento de um quadro envolve a definição da FCS para um valor conhecido que não passa uma verificação de CRC**. Por causa disso, um quadro defeituoso que falha no CRC pode aparecer como um CRC em cada interface atravessada, até alcançar um switch store-and-forward que o descartará.

ACI e CRC: procurar interfaces defeituosas

- Se uma folha vê erros de CRC em uma porta de downlink, é principalmente um problema no SFP de downlink ou com componentes no dispositivo/rede externo.
- Se um spine vê erros de CRC, é principalmente um problema nessa porta local, SFP, Fibre ou SFP vizinho. Pacotes com falha de CRC a partir de downlinks de folha não são pisados nas colunas. Como se seus cabeçalhos fossem legíveis, ele é encapsulado por VXLAN e o novo CRC será computado. Se os cabeçalhos não fossem legíveis a partir da corrupção de

quadros, o pacote seria descartado.
- Se uma folha vê erros de CRC em links de estrutura, pode ser: Um problema no par de fibra local/SFP, na fibra de ingresso da coluna ou no par SFP.Uma moldura pisada atravessando o tecido.

Esvaziamento: solucionar problemas de stomping

- Procure interfaces com erros FCS na estrutura. Como o FCS ocorre no local de uma porta, é mais provável que seja a fibra ou o SFP em cada extremidade.
- Erros de CRC na saída de 'show interface' refletem o valor total de FCS+Stomp.\

Veja um exemplo:

Verifique uma porta com o comando

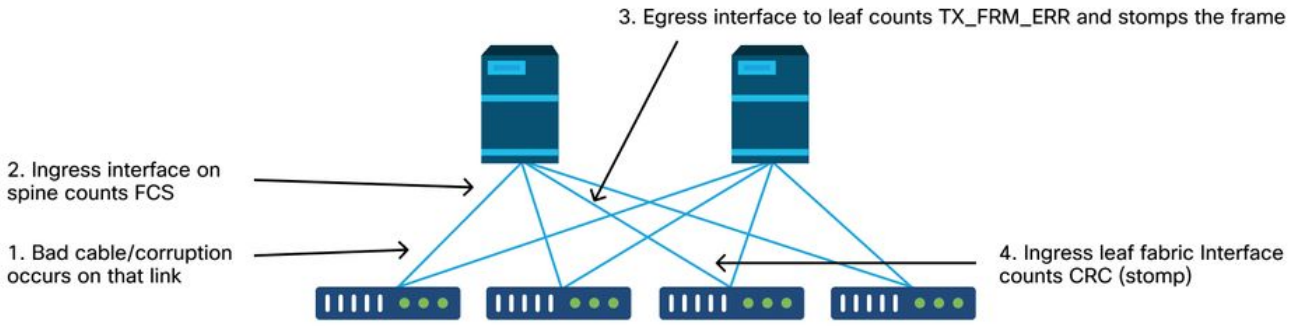
```
vsh_lc: 'show platform internal counter port <X>'
```

Neste comando, 3 valores são importantes:

- RX_FCS_ERR - Falha de FCS.
- RX_CRCERR - Quadro de erro CRC estombado recebido.
- TX_FRM_ERROR - Quadro de erro CRC estombado transmitido.

```
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
```

cenário de Troubleshooting de CRC stomp



Se um link corrompido gerar um grande número de quadros corrompidos, esses quadros podem ser inundados para todos os outros nós de folha e é muito possível encontrar o CRC no ingresso de uplinks de estrutura da maioria dos nós de folha na estrutura. Provavelmente, todos vêm de um único link corrompido.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.