ACIイントラファブリックフォワーディングのトラブルシューティング：断続的なドロップ

内容

概要

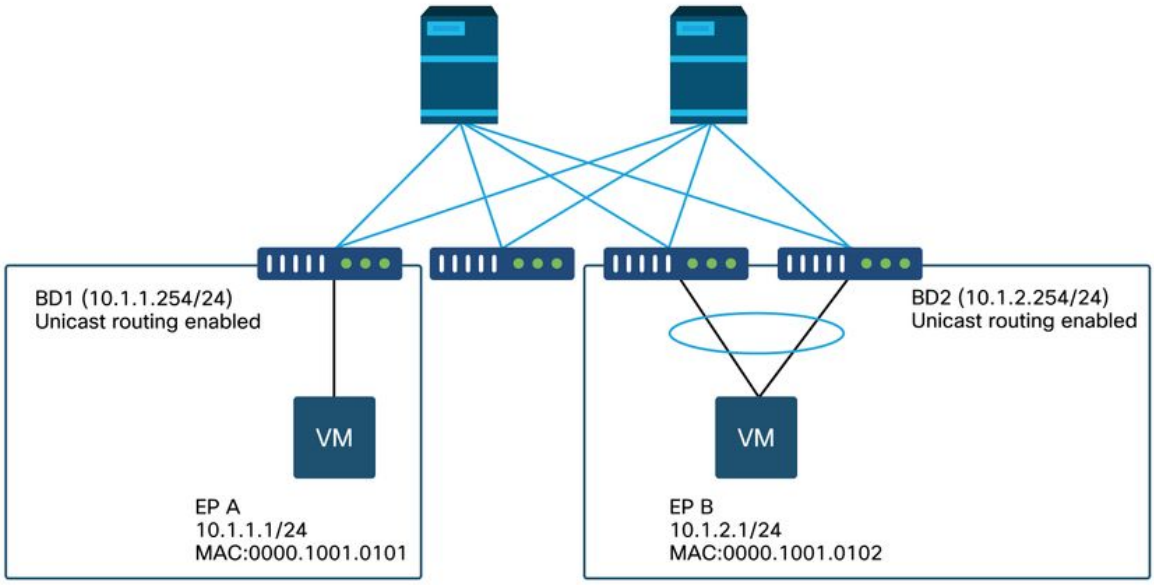
このドキュメントでは、ACIの断続的なドロップをトラブルシューティングする手順について説明します。

背景説明

このドキュメントの内容は、『Troubleshooting Cisco Application Centric Infrastructure, Second Edition』の書籍、特に「**Intra-Fabric forwarding - Intermittent drops**」の章から抜粋したものです。

ACIイントラファブリックフォワーディングのトラブルシューティング：断続的なドロップ

トポロジの例



この例では、EP A(10.1.1.1)からEP B(10.1.2.1)へのpingで断続的なドロップが発生しています。

```
[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
```

トラブルシューティングワークフロー

1.断続的なドロップの原因となっている方向を特定する

宛先ホスト(EP B)でパケットキャプチャ（tcpdump、Wiresharkなど）を実行します。 ICMPの場合は、シーケンス番号に注目して、断続的にドロップされるパケットがEP Bで観察されることを確認します。

```
[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
...
```

- パターン1：すべてのパケットがEP Bパケットキャプチャで観察されます。

ドロップはICMPエコー応答（EP BからEP A）である必要があります。

- パターン2:EP Bのパケットキャプチャで断続的なドロップが観察されます。

ドロップはICMPエコー(EP A ~ EP B)である必要があります。

2.同じ送信元/宛先IPを持つ別のプロトコルに同じ問題があるかどうかを確認する

可能であれば、2つのエンドポイント間の契約で許可されている別のプロトコル（ssh、telnet、httpなど）を使用して、2つのエンドポイント間の接続をテストします。

- パターン1：他のプロトコルにも同じ断続的な廃棄があります。

次に示すように、エンドポイントフラッピングまたはキューイング/バッファリングに問題がある可能性があります。

- パターン2：断続的な廃棄があるのはICMPだけです。

転送はMACとIPに基づいているため、転送テーブル（エンドポイントテーブルなど）に問題はありません。キューイング/バッファリングは他のプロトコルに影響を与えるため、この理由にはなりません。ACIがプロトコルに基づいて異なる転送を決定する唯一の理由は、PBRの使用例です。

可能性の1つは、スパインノードの1つに問題があることです。プロトコルが異なる場合、同じ送信元と宛先を持つパケットは、入力リーフによって別のアップリンク/ファブリックポート（つまり、別のスパイン）にロードバランシングされる可能性があります。

アトミックカウンタを使用すると、スパインノードでパケットがドロップされず、出力リーフに到達することを保証できます。パケットが出力リーフに到達しなかった場合は、入力リーフのELAMをチェックして、どのファブリックポートからパケットが送信されているかを確認します。問題を特定のスパインに切り分けるために、リーフアップリンクをシャットダウンして、トラフィックを別のスパインに向けることができます。

3.エンドポイントの学習問題に関連しているかどうかを確認する

ACIはエンドポイントテーブルを使用して、あるエンドポイントから別のエンドポイントにパケットを転送します。不適切なエンドポイント情報によって、パケットが誤った宛先に送信されたり、誤ったEPGに分類されてコントラクトがドロップされたりするため、エンドポイントのフラッピングによって断続的な到達可能性の問題が発生する可能性があります。宛先がエンドポイントグループではなくL3Outであると想定される場合でも、すべてのリーフスイッチ間で同じVRFのエンドポイントとしてIPが学習されていないことを確認します。

エンドポイントフラッピングのトラブルシューティング方法の詳細については、このセクションの「エンドポイントフラッピング」サブセクションを参照してください。

4.トラフィックの頻度を変更して、バッファリングの問題に関連しているかどうかを確認する

pingの間隔を増減して、ドロップ率が変化するかどうかを確認します。間隔の差は十分に大きくする必要があります。

Linuxでは、'-i'オプションを使って間隔（秒）を変更できます。

```
[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
```

インターバルが減少するとドロップ率が増加する場合、エンドポイントまたはスイッチでのキューイングまたはバッファリングに関連している可能性があります。

考慮すべき廃棄率は、（ドロップ数/時間）ではなく（ドロップ数/送信パケットの総数）です。

このようなシナリオでは、次の点を確認してください。

1. pingとともに、スイッチインターフェイスのドロップカウンタが増加しているかどうかを確認します。詳細については、「ファブリック内転送」の章の「インターフェイスドロップ」の項を参照してください。
2. 宛先エンドポイントのパケットとともにRxカウンタが増加しているかどうかを確認します。Rxカウンタが送信パケットと同じ数だけ増加している場合、パケットはエンドポイント自体でドロップされている可能性があります。これは、TCP/IPスタックでのエンドポイントバッファリングが原因である可能性があります。

たとえ100000、pingができるだけ短い間隔で送信される場合は、エンドポイントのRxカウンタが100ずつ増加する様子を観察でき100000す。

```
[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. ACIがパケットを送信しているか、または宛先がパケットを受信しているかを確認します

リーフスイッチの出力ポートでSPANキャプチャを実行し、ACIファブリックをトラブルシューティングパスから除外します。

宛先のRxカウンタも、前のバッファリングの手順で示したように、ネットワークスイッチ全体を

トラブルシューティングパスから除外するのに役立ちます。

エンドポイントフラッピング

このセクションでは、エンドポイントフラッピングをチェックする方法について説明します。詳細については、次のドキュメントを参照してください。

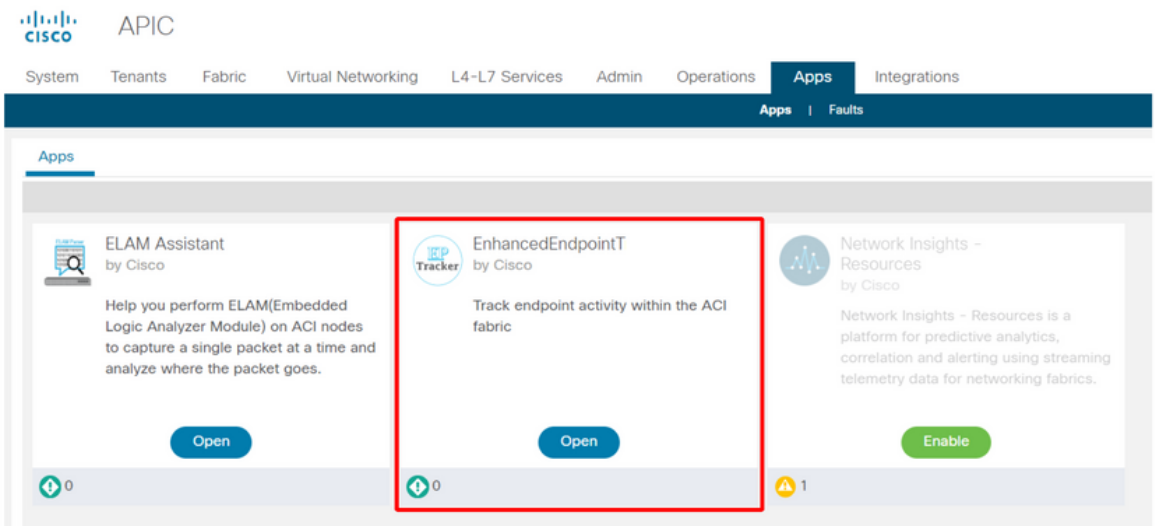
- 『ACI Fabric Endpoint Learning Whitepaper』(www.cisco.com)
- 「Cisco Live BRKACI-2641 ACIのトラブルシューティング：Endpoints」を参照してください。www.ciscolive.com

ACIが複数の場所で同じMACアドレスまたはIPアドレスを学習すると、エンドポイントが移動したように見えます。また、スプーフィングデバイスや設定ミスが原因で発生することもあります。このような動作は、エンドポイントフラッピングと呼ばれます。このようなシナリオでは、移動/フラッピングエンドポイントへのトラフィック（ブリッジドトラフィックのMACアドレス、ルーテッドトラフィックのIPアドレス）が断続的に失敗します。

エンドポイントフラッピングを検出する最も効果的な方法は、Enhanced Endpoint Trackerを使用することです。このアプリは、ACI AppCenterアプリとして、または外部サーバー上のスタンドアロンアプリとして実行できます。

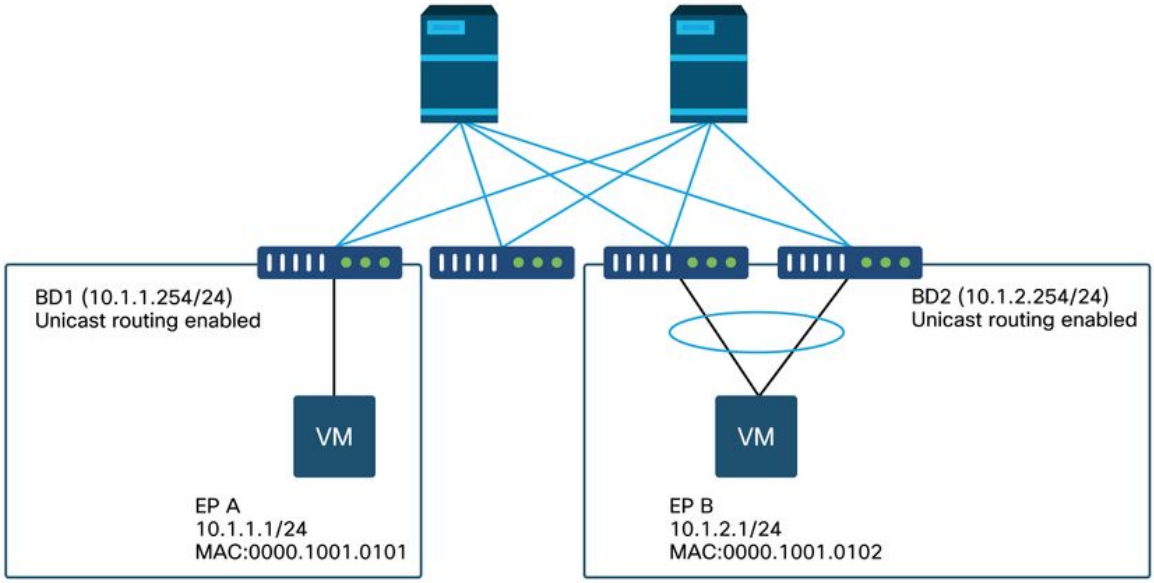
拡張エンドポイントトラッカー

廃止警告このガイドは4.2に書かれています。それ以来、Nexus Dashboard Insightsの機能を優先してEnhanced Endpoint Trackerアプリは廃止されました。詳細については、Cisco Bug ID CSCvz59365を参照してください。 .



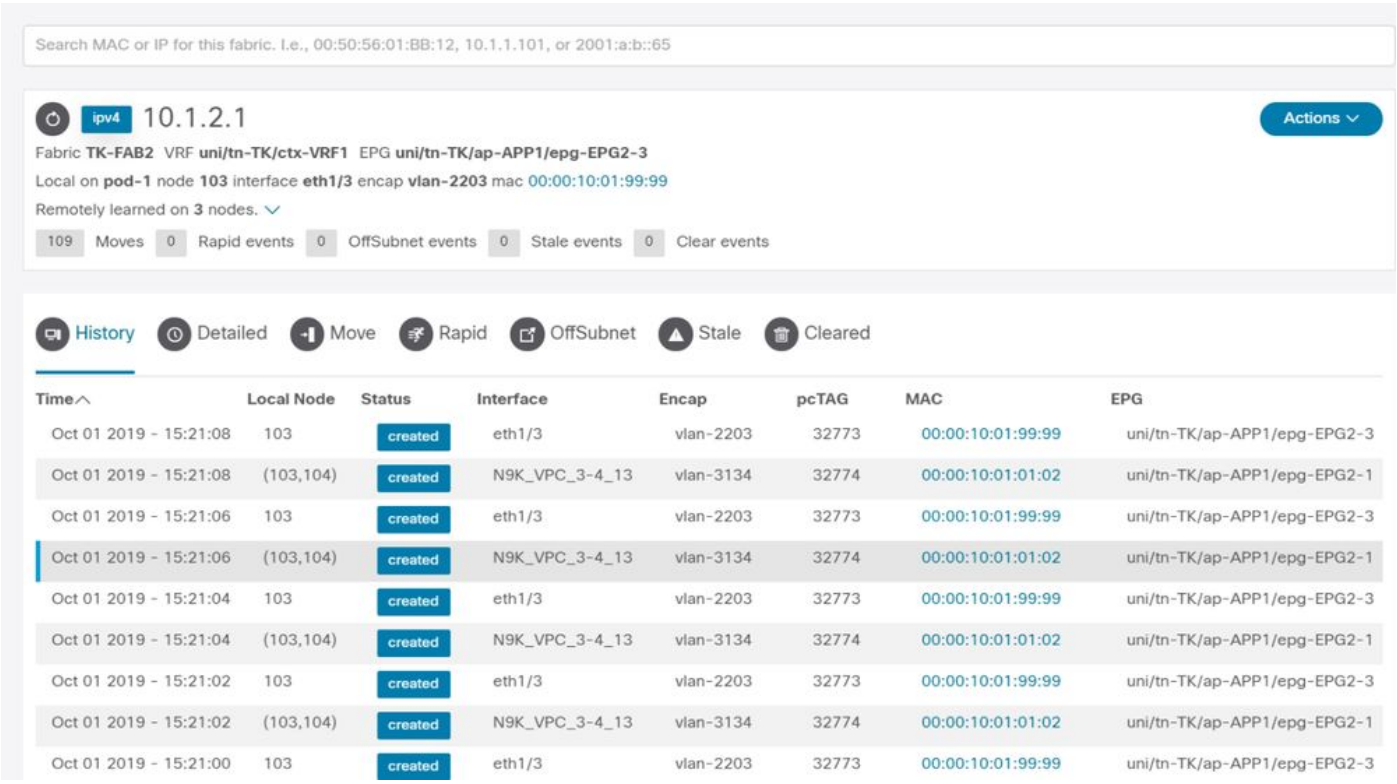
上の図は、AppCenterのEnhanced Endpoint Trackerを示しています。次に、Enhanced Endpoint Trackerを使用してフラッピングしているエンドポイントを検索する方法の例を示します。

エンドポイントフラッピングの例



この例では、IP 10.1.2.1はMAC 0000.1001.0102を持つEP Bに属している必要があります。ただし、MAC 0000.1001.9999を持つEP Xも、設定ミスやIPスプーフィングが原因で、IP 10.1.2.1を持つトラフィックをっています。

Enhanced Endpoint Tracker出力：Moves



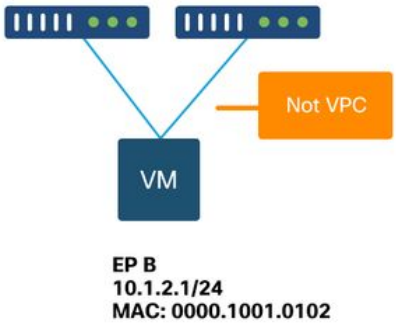
Time	Local Node	Status	Interface	Encap	pcTAG	MAC	EPG
Oct 01 2019 - 15:21:08	103	created	eth1/3	vlan-2203	32773	00:00:10:01:99:99	uni/tn-TK/ap-APP1/epg-EPG2-3
Oct 01 2019 - 15:21:08	(103,104)	created	N9K_VPC_3-4_13	vlan-3134	32774	00:00:10:01:01:02	uni/tn-TK/ap-APP1/epg-EPG2-1
Oct 01 2019 - 15:21:06	103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

Enhanced Endpoint Trackerには、IP 10.1.2.1が学習された時間と場所が表示されます。上のスクリーンショットに示されているように、MAC 0000.1001.0102（予定）と0000.1001.9999（予定なし）の2つのエンドポイント間で10.1.2.1がフラッピングしています。 これにより、IP 10.1.2.1に対する到達可能性の問題が発生します。これは、誤ったMACアドレスで学習されたパケットが、誤ったインターフェイスを介して誤ったデバイスに送信されるためです。この問題を解決するには、予期しないVMが不適切なIPアドレスを持つトラフィックを送信しないように対策

を講じます。

次に、不適切な設定によるエンドポイントのフラッピングの典型的な例を示します。

エンドポイントフラッピングを引き起こす可能性があるトポロジ例



サーバまたはVMがVPCのない2つのインターフェイスを介してACIリーフノードに接続されている場合、サーバはアクティブ/スタンバイNICチーミングを使用する必要があります。そうでない場合、パケットは両方のアップリンクにロードバランシングされ、ACIリーフスイッチの観点からは、エンドポイントが2つのインターフェイス間でフラッピングしているように見えます。この場合、アクティブ/スタンバイまたは同等のNICチーミングモードが必要です。または、ACI側でVPCを使用します。

インターフェイスの廃棄

この章では、入力インターフェイスのドロップに関連する主要なカウンタをチェックする方法について説明します。

ハードウェア ドロップ カウンタのタイプ

ACIモードで動作するNexus 9000スイッチには、入力インターフェイスドロップ用のACI上の3つの主要なハードウェアカウンタがあります。

[転送（Forward）]

ドロップの主な理由は次のとおりです。

- SECURITY_GROUP_DENY:通信を許可す契約の欠如が原因のドロップ。
- VLAN_XLATE_MISS:不適切な VLAN によるドロップ。たとえば、フレームが802.1Q VLAN 10を持つファブリックに入ったとします。スイッチのポートにVLAN 10が設定されている場合、スイッチはその内容を検査し、宛先MACに基づいて転送を決定します。ただし、VLAN 10がポートで許可されていない場合は、VLAN 10をドロップし、VLAN_XLATE_MISSとしてラベル付けします。
- ACL_DROP:sup-tcam によるドロップ。ACIスイッチのSUP-TCAMには、通常のL2/L3転送の決定に加えて適用される特別なルールが含まれています。sup-tcam ルールは組み込み型でユーザ設定はできません。SUP-TCAMルールの目的は主に、一部の例外または一部のコントロールプレーントラフィックを処理することであり、ユーザによるチェックや監視を意図した

ものではありません。パケットがSUP-TCAMルールにヒットし、そのルールがパケットをドロップする場合、ドロップされたパケットはACL_DROPとしてカウントされ、転送ドロップカウンタが増加します。

転送ドロップは、基本的に、既知の有効な理由でドロップされたパケットです。一般に無視することができ、実際のデータトラフィックのドロップとは異なり、パフォーマンスのペナルティは発生しません。

エラー

スイッチが無効なフレームを受信すると、エラーとしてドロップされます。この例として、FCS や CRC エラーのフレームなどがあります。詳細については、後述の「CRC — FCS – カットスルースイッチング」の項を参照してください。

バッファ

スイッチがフレームを受信し、入力または出力に使用できるバッファがない場合、フレームは「Buffer」とともにドロップされます。 これは、ネットワークのどこかで輻輳が発生していることを示唆しています。障害を示しているリンクがいっぱいであるか、宛先を含むリンクが輻輳している可能性があります。

APIを使用したカウンタの収集

APIとオブジェクトモデルを活用することで、ユーザはファブリックに対して、これらのドロップのすべてのインスタンスを迅速に問い合わせることができます (これらはapicから実行されます) 。

```
# 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"
```

CLI でのドロップ状態表示

障害が指摘された場合、またはCLIを使用してインターフェイス上のパケットドロップを確認する必要がある場合は、ハードウェアのプラットフォームカウンタを表示するのが最善の方法です。すべてのカウンタが「show interface」を使用して表示されるわけではありません。 3つの主なドロップの理由は、プラットフォームカウンタを使用してのみ表示できます。これらを表示するには、次の手順を実行します。

リーフ

リーフに SSH 接続し、次のコマンドを実行します。この例は、イーサネット1/31用です。

```
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
...
```

スパイン

固定スパイン（N9K-C9332CおよびN9K-C9364C）は、リーフスイッチと同じ方法でチェックできます。

モジュラスパイン（N9K-C9504など）の場合は、プラットフォームカウンタを表示する前に、ラインカードを接続する必要があります。スパインにSSH接続し、次のコマンドを実行します。この例は、ethernet 2/1用です。

```
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
...
```

キューイング統計情報カウンタは、「show queuing interface」を使用して表示されます。 この例は、イーサネット1/5用です。

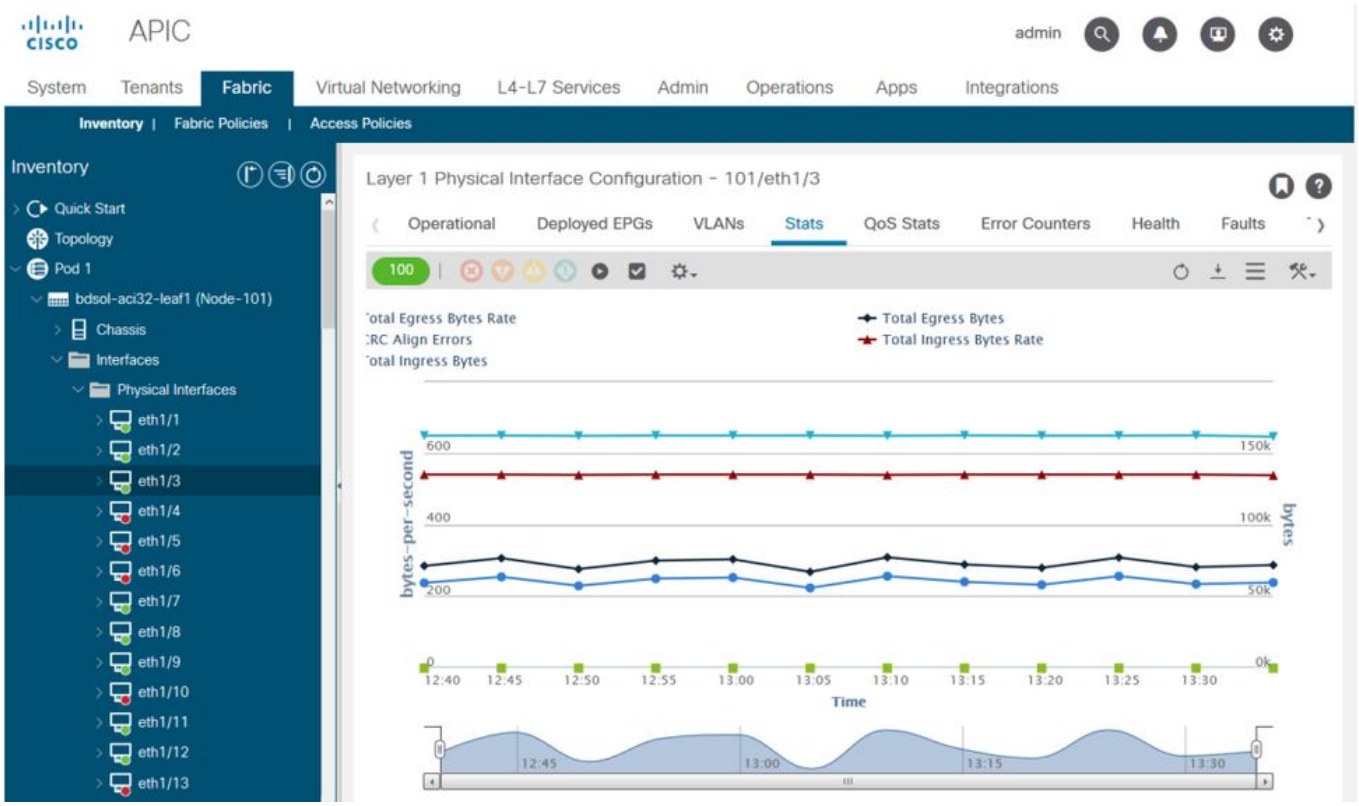
```
ACI-LEAF# show queuing interface ethernet 1/5
================================================================================
               Queuing stats for ethernet 1/5
================================================================================
================================================================================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

...
```

GUIでの統計情報の表示

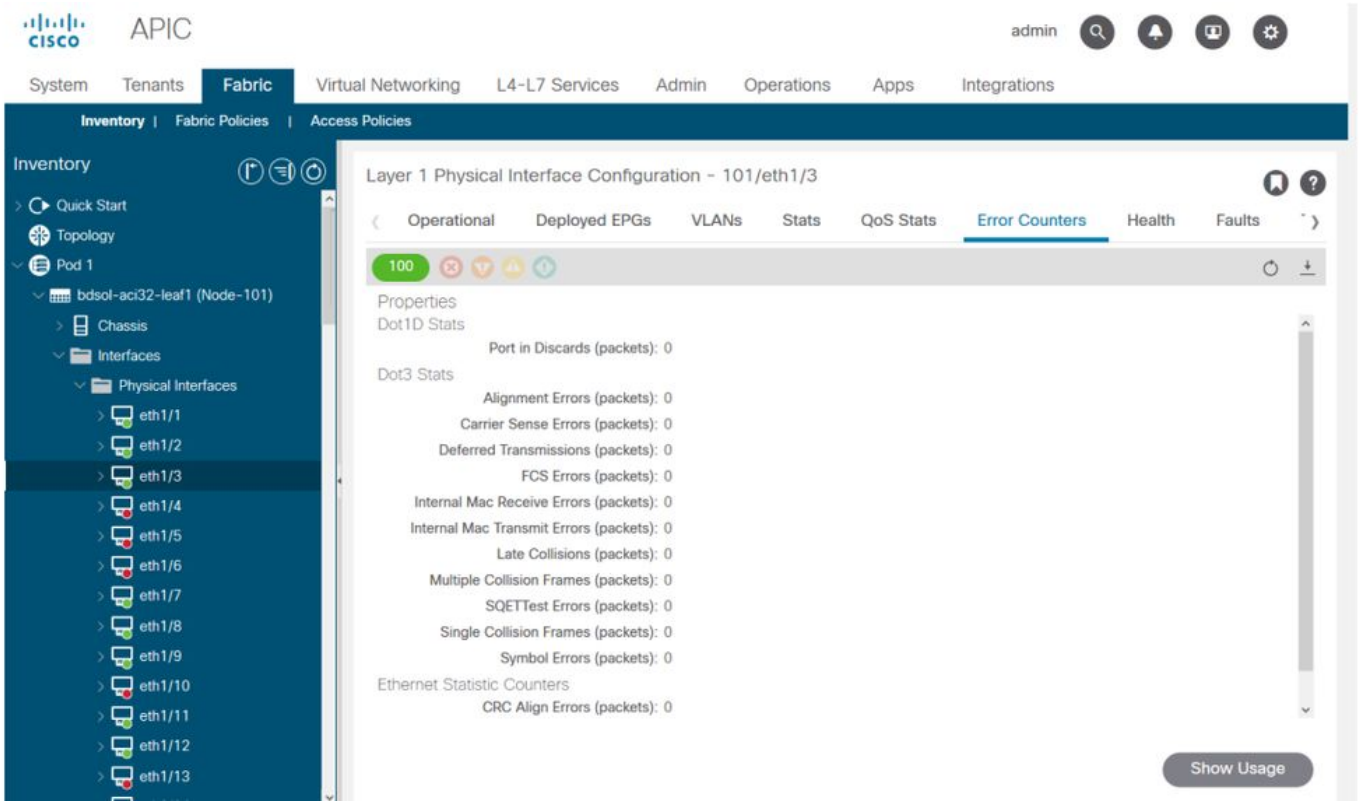
場所は、[Fabric] > [Inventory] > [Leaf/Spine] > [Physical interface] > [Stats]です。

GUIインターフェイス統計情報



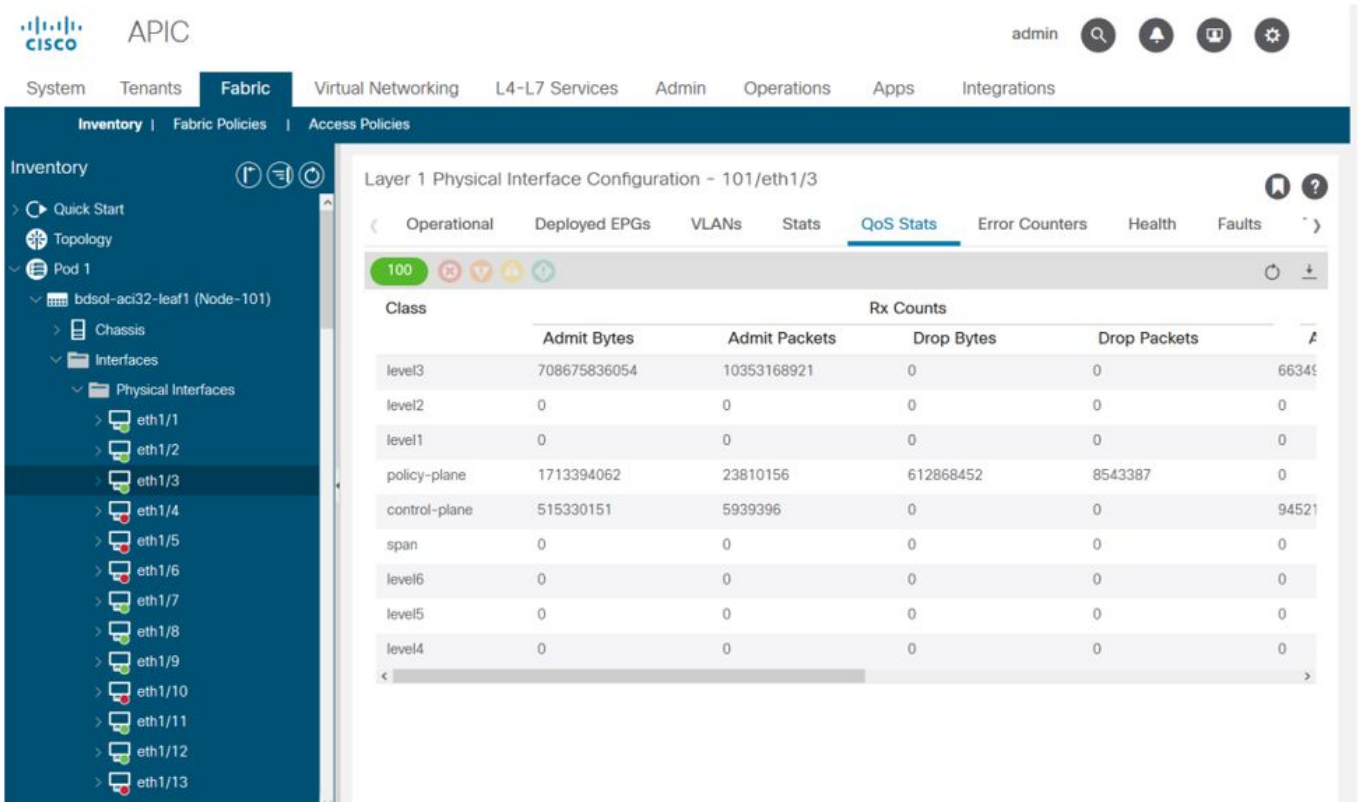
エラー統計情報は同じ場所で確認できます。

GUIインターフェイスエラー



最後に、GUIではインターフェイスごとにQoS統計情報を表示できます。

GUIインターフェイスQoSカウンタ



CRC:FCS：カットスルースイッチング

巡回冗長検査(CRC)とは何ですか。

CRCは、イーサネットで4Bの数値を返すフレームの多項式関数です。すべてのシングルビットエラーと、かなりの割合のダブルビットエラーが検出されます。したがって、フレームが送信中に破損していないことを保証することを目的としています。CRC工ラーカウンタが増加している場合は、ハードウェアがフレーム上で多項式関数を実行したときに、結果がフレーム自体にある4B番号とは異なる4B番号であったことを意味します。デュプレックスのミスマッチ、ケーブル配線の障害、ハードウェアの破損など、いくつかの理由でフレームが破損することがあります。ただし、ある程度のCRC工ラーが予想され、この規格ではイーサネットで最大10-12ビット工ラーレートが許容されます（1012ビットのうち1ビットが反転する可能性があります）。

ストアアンドフォワードスイッチングとカットスルースイッチング

ストアアンドフォワードスイッチとカットスルーレイヤ2スイッチは、どちらもデータパケットの宛先MACアドレスに基づいて転送を決定します。また、ステーションがネットワーク上の他のノードと通信するときに、パケットの送信元MAC(SMAC)フィールドを調べることで、MACアドレスを学習します。

ストアアンドフォワードスイッチは、フレーム全体を受信し、その完全性をチェックした後、データパケットに対して転送の決定を行います。カットスルースイッチは、着信フレームの宛先MAC(DMAC)アドレスを確認した直後に転送プロセスを開始します。ただし、カットスルースイッチは、CRCチェックを実行する前に、パケット全体を確認するまで待機する必要があります。つまり、CRCが検証される時点で、パケットはすでに転送されており、チェックに失敗したパケットは廃棄できません。

従来、ほとんどのネットワークデバイスはストアアンドフォワードに基づいて動作していました。カットスルースイッチングテクノロジーは、低遅延の転送を必要とする高速ネットワークで使用される傾向があります。

具体的には、Generation 2以降のACIハードウェアでは、入力インターフェイスの速度が高く、出力インターフェイスの速度が同じかそれよりも低い場合に、カットスルースイッチングが行われます。ストアアンドフォワードスイッチングは、入力インターフェイスの速度が出力インターフェイスよりも低い場合に実行されます。

踏み込み

CRC工ラーのあるパケットは廃棄が必要です。フレームがカットスルーパスでスイッチングされている場合、パケットがすでに転送された後にCRC検証が行われます。したがって、唯一のオプションは、イーサネットフレームチェックシーケンス(FCS)をストンプすることです。**フレームをストンプするには、FCSをCRCチェックを通過しない既知の値に設定する必要があります**。このため、CRCに失敗した1つの不良フレームは、通過するすべてのインターフェイス上でCRCとして表示される可能性があり、これをドロップするストアアンドフォワードスイッチに到達します。

ACIおよびCRC:障害のあるインターフェイスを探す

- リーフがダウンリンクポートでCRC工ラーを検出した場合、ダウンリンクSFPまたは外部デバイス/ネットワーク上のコンポーネントに関する問題が主な原因です。
- スパインでCRC工ラーが発生する場合、そのローカルポート、SFP、ファイバ、またはネイバーSFPの問題が主です。リーフダウンリンクからのCRC失敗パケットは、スパインにストンプされません。ヘッダーが読み取り可能であるかのように、VXLANカプセル化され、新しいCRCが計算されます。ヘッダーがフレーム破損から読み取れない場合、パケットはドロッ

プされます。
- リーフがファブリックリンクでCRCエラーを検出した場合は、次のいずれかの状態になります。 ローカルファイバ/SFPペア、スパインの入力ファイバ、またはSFPペアの問題。生地を突き破って進む踏み込んだフレーム。

踏み込み：踏み込みのトラブルシューティング

- ファブリック上でFCSエラーのあるインターフェイスを探します。FCSはポートに対してローカルに発生するため、ファイバまたはSFPのどちら側に存在する可能性が高くなります。
- 「show interface」の出力のCRCエラーは、FCS+Stomp値の合計を反映しています。\

次に例を示します。

次のコマンドを使用してポートをチェックします。

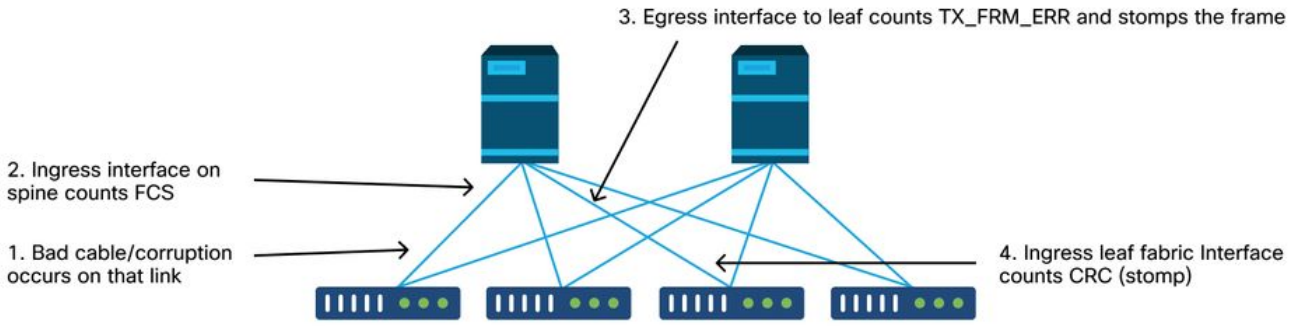
```
vsh_lc: 'show platform internal counter port <X>'
```

このコマンドでは、3つの値が重要です。

- RX_FCS_ERR:FCS障害。
- RX_CRCERR：ストンプされたCRCエラーフレームを受信しました。
- TX_FRM_ERROR：送信されたストンプされたCRCエラーフレーム。

```
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ストンプのトラブルシューティングシナリオ



破損したリンクによって大量の破損フレームが生成されると、そのフレームは他のすべてのリーフノードにフラッディングされる可能性があり、ファブリック内のほとんどのリーフノードのファブリックアップリンクの入力でCRCを検出する可能性が非常に高くなります。これらはすべて、単一の破損したリンクから発生する可能性があります。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。