2 25.8アップグレード後にテスト

はじめに

前提条件

要件

使用するコンポーネント

設定

ネットワーク図

コンフィギュレーション

確認

トラブルシュート

これは、エンジニアがASR9000でのトラフィックのドロップの問題をトラブルシューティングする方法を示すのに役立つ高度なトラブルシューティングガイドです。すべてのシナリオをカバーしているわけではありませんが、最も一般的なケースを一般化しようとしています。

ジャルゴン・バスター

- GDPlane :汎用データプレーン
- CEF:Cisco Express Forwarding(CEF)
- RFD受信フレームディスクリプタ
- PLU:Prefix Lookup Unit（プレフィックスルックアップユニット）
- PHU:PLUヒントユニット
- TBM:ツリービットマップ
- BUM:ブロードキャスト/不明なユニキャスト/L2マルチキャスト
- LC:Line Card（ラインカード）
    - Tomahawk ベースのラインカード

ASR 9000 シリーズの第 3 世代のイーサネットラインカードは、Tomahawk ベースのラインカードと呼ばれています。この呼び方は、これらのラインカードに使用されている NP に由来します。

    - Lightspeedベースのラインカード

ASR 9000シリーズイーサネットラインカードの第4世代は、Lightspeedベースのラインカードとも呼ばれます。この呼び方は、これらのラインカードに使用されている NP に由来します。これらはLSQと呼ばれることもあります。

    - Lightspeed-Plusベースのラインカード

ASR 9000シリーズイーサネットラインカードの第5世代は、Lightspeed-Plusベースのラインカードとも呼ばれます。この呼び方は、これらのラインカードに使用されている NP に由来します。これらはLSPと呼ばれることもあります。

ASR 9000シリーズラインカードのタイプの理解

- VNI:VxLANの特定
    - L2VNI:レイヤ2 Vxlan識別子
    - L3VNI:レイヤ3 Vxlan識別子
- フラッド：通常、ユニキャストパケットは1つの出力ポートだけに送信されます。ただし、スイッチがパケットの送信先を認識しない場合（MACの欠落が原因）、着信VLANのすべてのメンバーポートにパケットを送信します。それは洪水と呼ばれる。
- FGID:Fabric Group Identifier（ファブリックグループ識別子）
- MGID:マルチキャストグループID

はじめに

このドキュメントでは、さまざまなパケットドロップシナリオと、これらのケースのデバッグを進めるための手順ごとの方法をリストします。

R9K：パケットの寿命

入力機能順序

出力機能順序

パケット処理に関係するモジュール

「当社の」トラフィック

アプリケーションに応じて、「for us」パケットをLCまたはRSPに送信できます。

- LC CPUへのパント用

  ワイヤからのパケット → NP <->パントスイッチ<-> SPP(LC CPU) <-> Netio/Spioクライアント<->アプリケーション

- パントからRP CPUへ
  ワイヤからのパケット→NP <-> LC FIA <->クロスバー<-> RSP FIA <->パント/ダオ/チャFPGA <-> SPP (RSP CPU) <-> Netio/Spioクライアント

中継トラフィック

- ワイヤからのパケット→入力NP <-> LC FIA <->クロスバー<->出力NP →パケット出力はワイヤへ

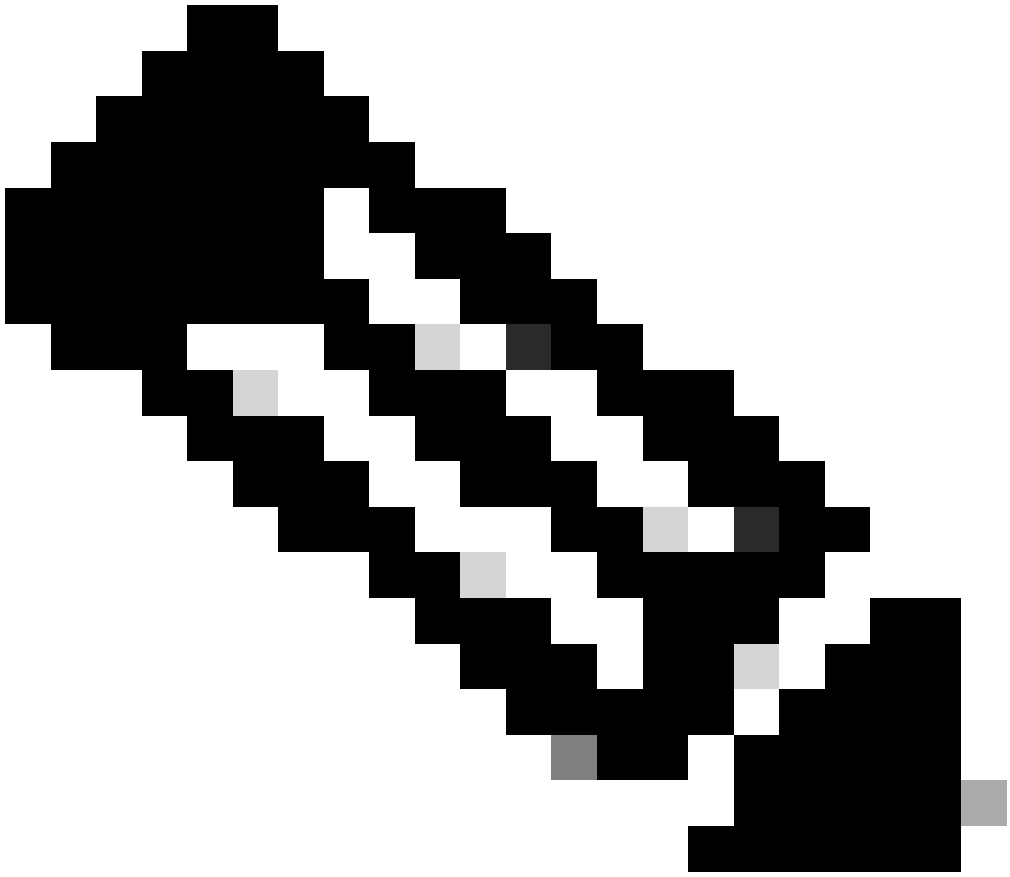
トラフィックの挿入

- LC CPUから
  - 出力インジェクト
    アプリケーション<-> Netio/Spioクライアント<-> SPP(LC CPU) <->パントスイッチ<->出力NP →パケット出力からワイヤ
  - 内向きに注射する
    アプリケーション<-> SRPM <->パントスイッチ<->入力NP <-> LC FIA <->クロスバー<->出力NP →パケット送信 (有線)
- RP CPUから
  - 出力インジェクト
    アプリケーション<-> Netio/Spioクライアント<-> SPP (RP CPU) <-> RSP FIA <->クロスバー<-> LC FIA <->出力NP → パケット送信 (有線)
- LC CPUからRSP CPU
  Netio/Spioクライアント<-> SPP (LC CPU) <->パントスイッチ<-> NP <-> LC Fia <->クロスバー<-> RSP Fia <->パント/ダオ/チャFPGA <-> SPP (RSP CPU) <-> Netio/Spioクライアント
- RSP CPUからLC CPU
  Netio/Spioクライアント<-> SPP (RSP CPU) <->パント/ダオ/チャFPGA <-> RSP Fia <->クロスバー<-> LC Fia <-> NP <->パントスイッチ<-> SPP (LC CPU) <-> Netioクライアント

問題のあるデバイスの特定：

1. トラフィック問題の分類
   問題のタイプを見つけます。完全ドロップ、部分的なパケットドロップ、サイレントドロップ、またはその他のシナリオであるかどうかを特定します。
2. トラフィックタイプを決定する
   L2/L3/ユニキャスト/BUM/マルチキャスト
3. 単一の被害フローの特定
   IXIAドリルダウンから可能な限り、さらにトリアージするために使用する1つのフローを見つけます
4. 単一のフローをトレースし、重複をドロップ/開始するデバイス (疑わしいデバイス) を絞

り込みます。



注：トポロジダイアグラムとshow interface countersを使用して、パケットが通過する実際のパスを導き出します

---

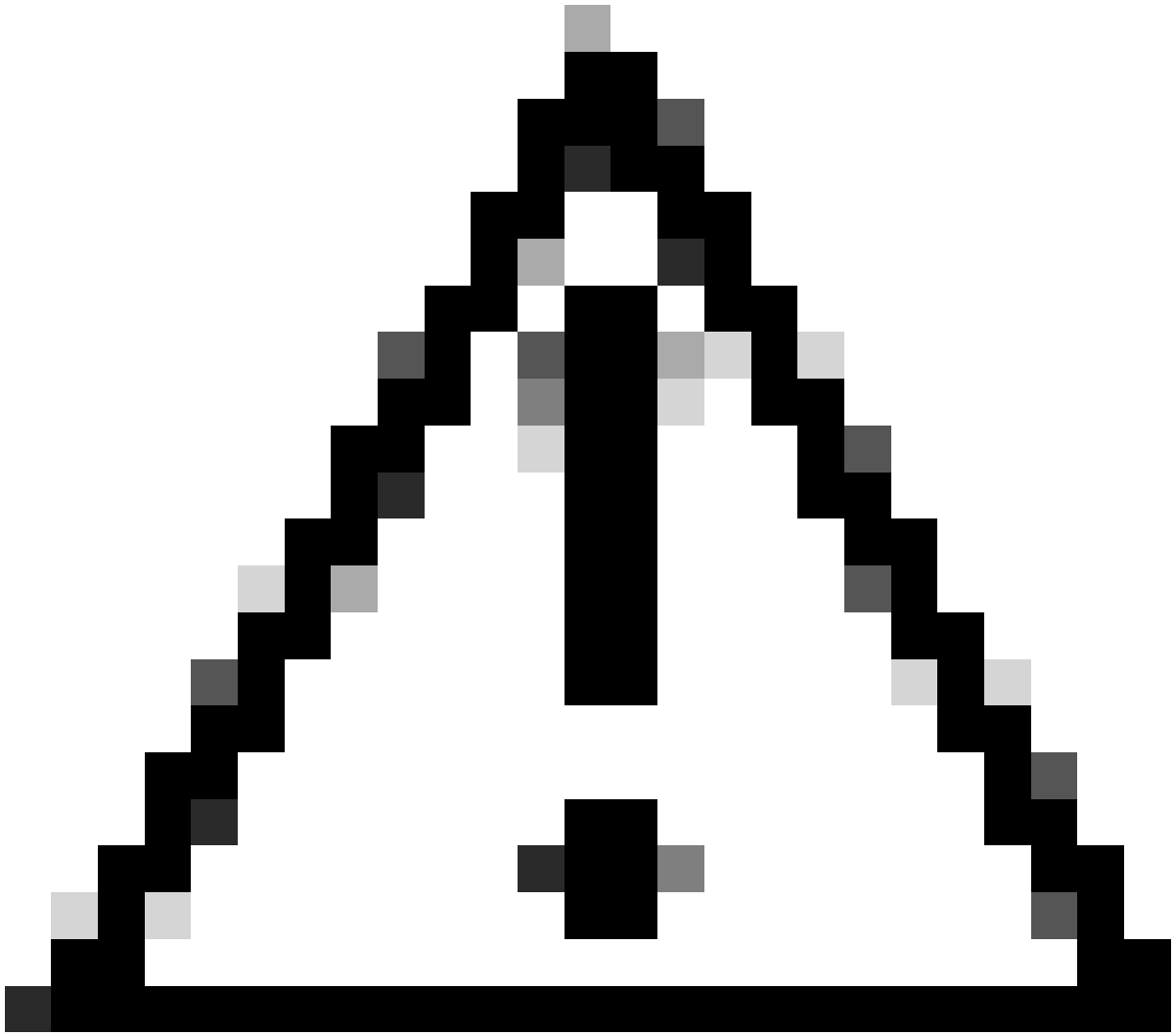
1. IXIAですべてのトラフィックを停止し、新しいトラフィックストリーム「DEBUG」を作成します。このトラフィックストリームには、ステップ2で選択した1つのフローがあり、トラフィックレートを高いレートに設定します（たとえば、データトラフィックの場合、ARP/その他のスーパーバイザ向けのコントロールプレーンでは、レートリミッタ/coppを通過する際に低いレートを維持します）
2. IXIAでは、新しいトラフィック項目のみを開始し、入力デバイスから「sh int counters brief」を使用して、問題が発生しているデバイス（ドロップ/複製）を特定します

5. フローの以下の詳細を取得し、簡単なトラブルシューティングのためにそれをメモします
    1. 送信元 MAC
    2. 宛先 MAC
    3. 送信元 IP
    4. 宛先 IP

5. 送信元Vlan
6. 宛先Vlan（ルーテッドトラフィックの場合）
7. 送信元と宛先のVRF情報（L3ルーテッドトラフィックの場合）
8. VNI情報
    1. L2トラフィックの場合はL2VNI
    2. L3VNI（L3ルーテッドトラフィックの場合）

6. フローを絞り込んだ後、次の方法を使用して問題のあるルータ/デバイスを特定します。
    1. Traceroute/Ping/MPLS Ping/イーサネットPing
    2. ACL – トラフィックがデバイスの入力ポートに実際に到達しているかどうかを確認します
    3. Interface Counters
    4. インターフェイスコントローラ統計情報
    5. ラベルスイッチング統計情報
7. 設定関連の問題がないことを確認します。
   一般的な設定ミスのセクションを参照してください。

疑わしいデバイスからの実際のデバッグの開始



注意：問題の疑われるデバイスがトラフィックをドロップ/フラッディングしていますが

、これが原因で問題が発生しているわけではありません。場合によっては、疑わしいデバイスにトラフィックを送信したデバイスが原因である可能性があります。

トラフィックのドロップの場所/モジュール：

インターフェイスレベルのドロップ

- show interface <インターフェイス>

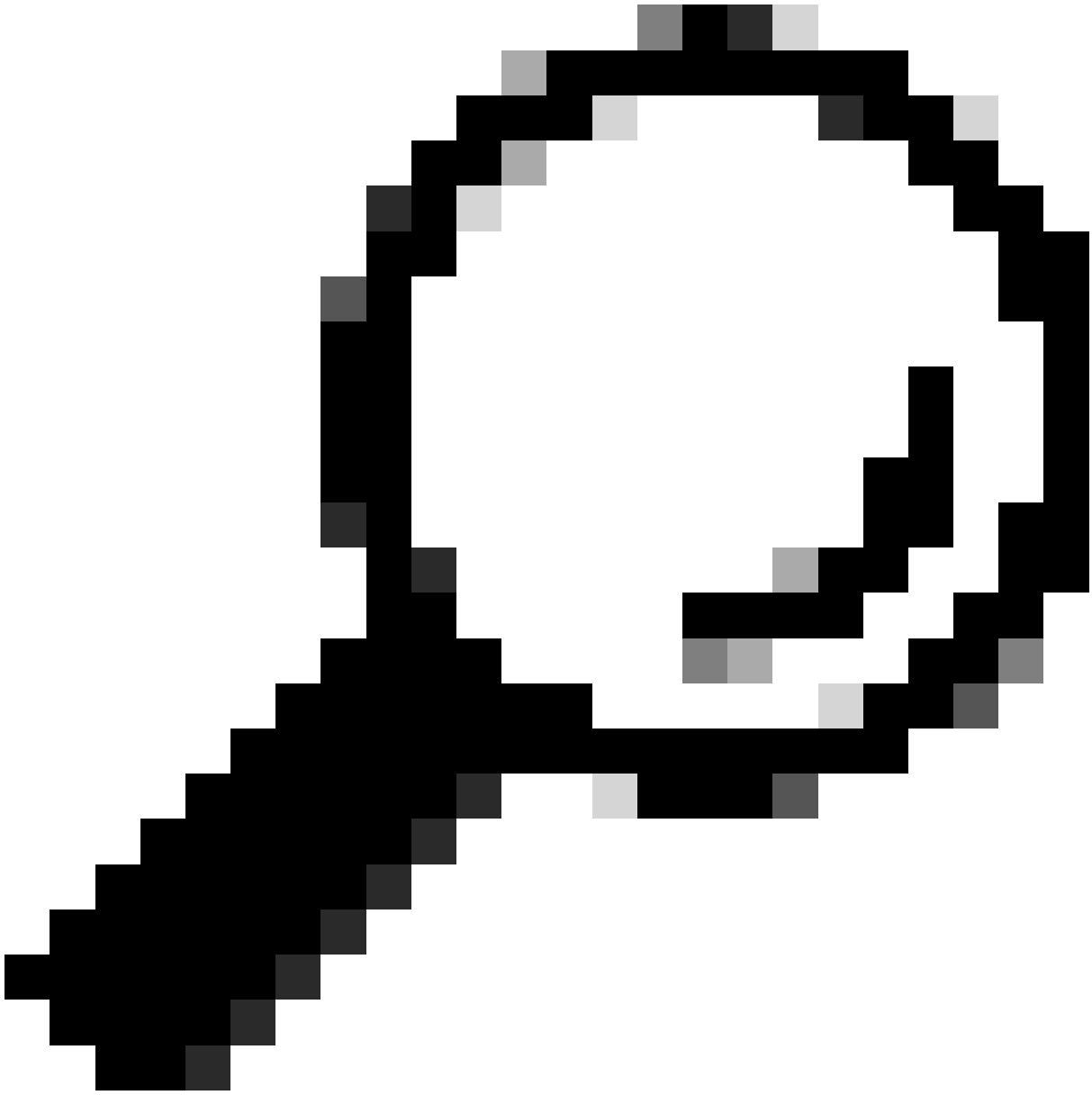
RP/0/RSP0/CPU0:YOG-CDCT-CN2-C9910# show interface Bundle-Ether602.3048 5月11日（木）13:16:40.091 WIB Bundle-Ether602.3048 is up, line protocol is upインターフェイス状態の遷移： 1 Dampening enabled: penalty, not suppressed half-life: 1 reuse: 755550: 750: 2 000 max-suppress-time: 4 restart-penalty: 0ハードウェアはVLANサブインターフェイス、アドレスはecce.13c9.d8c5説明： ABIS_MCBSC_CDC4_NSN_VLAN3048インターネットアドレスは10.17.191.179/28 MTU 9216バイト、BW 2000000 Kbit (最大：2000000 85212564 Kbit)信頼性255/255、txload 0/25、rxload/25 5 Encapsulation 802.1Q Virtual LAN, VLAN Id 3048, loopback not set, Last link flapped 36w1d ARP type ARPA, ARP timeout 04:00:00 Last input 00:00:00, output never Last clearing of "show interface" counters 135y46w 30 second input rate 4000 bits/sec, 9 packets/sec 30 output rate 0 bits input, 5396765891 2493252749入力ドロップの総数0未認識の上位レベルプロトコルのドロップ受信20089331ブロードキャストパケット、39963824マルチキャストパケット70999919503パケット出力、7186711514645バイト、0出力ドロップの総数出力309ブロードキャストパケット、57マルチキャストパケット

- show controllers <インターフェイス> stats

RP/0/RSP0/CPU0#show controller hundredGigE0/3/0/40 stats Wed Oct 18 16:54:04.904 WEST Statistics for interface HundredGigE0/3/0/40（キャッシュされた値）:Ingress: Input total bytes = 16850796039449085 Input good bytes = 16850796039449085 Input total packets = 13769166661248 Input 802.1Q frames = 0 Input pkts 64 bytes 257446881559 Input pkts 5 ~ 127バイト= 1285971034813入力パケット128 ~ 255バイト= 401173319511入力パケット256 ~ 511バイト= 261817914140入力パケット512 ~ 1023バイト= 323254550402入力パケット1024 ~ 1518バイト= 6444289537421入力パケット1519 ~ Maxバイト= 4795213423402入力正常パケット= 13769166661248入力ユニキャストパケット= 13769157512691入力マルチキャストパケット= 9147481入力ブロードキャストパケット= 1076入力オーバーラン= 0 abort = 0 Input drop invalid VLAN = 0 Input drop invalid DMAC = 0 Input drop invalid encap = 0 Input drop other = 0 Input error giant = 0 Input error runt = 0 Input error fragments = 0 Input error CRC = 0 Input error collisions = 0 Input error symbol = 0 Input error other = 0 Input MIB giant = 4795213423402 Input MIB jabber = 0 Input MIB CRC = 0 Egress: Output total = 3150799484820437 Output Good bytes = 3150799484820437 Output packets 5987194620610 8 02.1Qフレーム= 0出力pauseフレーム= 0出力pkts 64バイト= 59685948036出力pkts 65-127バイト= 3272599163757出力pkts 128-255バイト= 477536708073150420175953 191150155497 999535758139 836266711152 5987194446122 5987180721273 13724849 174488出力pkts 256-511バイト=☆出力pkts 512-1023バイト=´出力pkts 1024-1518バイト=´出力pkts 1519最大バイト= ¶ Output multicast pkts = ¶ Output broadcast pkts = 0出力ドロップアンダーラン= 0出力ドロップ中止= 0出力ドロップその他= 0出力エラーその他= ¶

早期ファストドロップ

EFDがパケットをドロップしていることを確認する方法



ヒント：トマホークのEFDドロップは「show controller np counters <>」コマンドの出力にも「show drops」コマンドの出力にも表示されないことに注意してください。新しい機能拡張要求がオープンされ、「show drops」コマンドにEFDドロップが追加されました。WLC の管理ユーザを認証するために TACACS+ を設定する方法を理解するには、

RP/0/RP0/CPU0:asr9k-1# sh controllers np fast-drop np0 location 0/0/CPU0 Fri Jan 27 12:17:57.333 PST Node: 0/0/CPU0: ---------- ---------- NP 0のすべてのファーストドロップカウンタ： TenGigE0/0/0/1/0-TenGigE0/0/1_9:[Priority1] 0 TenGigE0/0/0/0/1 0-TenGigE0/0/0/1_9:[Priority2] 0 TenGigE0/0/0/1/0-TenGigE0/0/0/1_9:[Priority3] 0 HundredGigE0/0/0/0-TenGigE0/0/0/0-TenGigE0/0/1_9:[Priority2] 0 GigE0/0/0/0-TenGigE0/0/0_1_9:[Priority3] 123532779 <=== Priority 3 packets dropped ---------- RP/0/RP0/CPU0:asr9k-1#

収集するデータ

ASR9000トマホークおよびLightspeedラインカード上の「np_perf」機能によるNP高速廃棄のト

ラブルシューティング

NPドロップ

1. 入力ポート情報に基づいて、関連するNPを特定します。次のコマンドを使用すると、NPを識別できます

show controllers np portmap all location < >

```
RP/0/RSP0/CPU0:SRv6-R5# show controllers np portmap all location 0/1/CPU0 5月17日（水
）05:30:40.389 EDT Node: 0/1/CPU0: ----------------------------------------------------------
-------- Show Port Map for NP: 0, and RX Unicast Ports phy port num interface desc
uiMappedSourcePort 0 HundredGigE0_1_0 1_0 10 100000000000000000 1_0_1 10 20
HundredGigE0_1_0_2 20 30 HundredGigE0_1_0_3 30ポートマップNP: 1およびRXユニキャストポートphy
port num interface desc uiMappedSourcePort 0 HundredGigE0_1_0_4 0 10 10 TenGigE0_1_0_5_0
10 11 TenGigE0_1_0_5_1_1 2 TenGigE0_1_0_5_2 257 （バンドル） 13 TenGigE0_1_0_5_3 13 20
HundredGigE0_1_0_6 20 30 TenGigE0_1_0_7_0 30 31 TenGigE0_1_0_7_1 31 32
TenGigE0_1_0_7_256 （バンドル） 3 GigE0_1_0_7_3 33 RP/0/RSP0/CPU0:SRv6-R5#
```

2. ステップ(a)で特定されたNPのnpカウンタの統計情報を確認します。

show controller np counters <npnum>/all > location < >

RP/0/RSP0/CPU0:SRv6-R5# show controller np counters all location 0/3/CPU0 Wed Oct 18 16:54:46.557 WEST Node: 0/3/CPU0: ---------- Show global stats counters for NP0, revision v0このNPのカウンタの最後のクリアリング： 2543:27:1 Read 0 non-zero NP counters: Offset Counter Value Rate (pps) ---------- 10 4 BFD discriminator zero packet 2 0 158 IPv4 PIM all routers detected 31878304 3 170 IPv6 LL hash lookup miss on egress 1 0 192 L2 MAC learning source MAC lookup miss 53 0 193 L2 MAC move on egress NP 55 0 194 L2 MAC notify delete 15 0 195 L2 MAC notify delete no entry 2 0 198 L2 MAC NOTIFY COMPLETE notify complete 2520170 0 2 00 L2 MAC notify received 21518947 3 201 L2 MAC notify reflection filtered 113082 0 202 L2 MAC notify refresh complete 18885133 3 205 L2 MAC notify update with bridge domain flush 366 0 206 L2 MAC notify update with port flush 30 0 208 L2 MAC update via reverse MAC notify skipped 2 0 220 L2 aging scan delete from BD key mismatch 108 0 221 L2 scan delete from XID 3 0 223 L2 AGING SCAN DELETE FROM ENTRY AGING OUT 2516745 0 227 L2 EGRESS MAC modify 18885584 3 246 L2 ingress MAC bridge domain flush 2 0 250 L2 ingress MAC learn 53 0 251 L2 ingress MAC modify 113027 0 253 L2 ingress MAC move 2 0 256 L2 ingress MAC refresh 113025 0 266 L2 on demand scan delete from BD key mismatch 3060 26 L2オンデマンドスキャンdelete from XID invalid 49 0 292 MAPT - TBPG Event 1562667425 171 349 TBPG L2メールボックスイベント1376253865 150 350 TBPG MACスキャンイベント22942615 351 TBPG stat events 88080247335 9620 361 VPLS egress MAC lock retry 607 0 363 VPLS egress MAC notify entry lock retry 176 72 VPLS ingress entry lock not acquired 4758 0 373 VPLS ingress entry lock retry 1362180 0 400 DMAC mismatch MY_MAC or MCAST_MAC for L3 intf 1 0 420 GRE IPv4 decap qualification failed 34389 0 431 GRE IPv6 decap qualification failed 34 0 460 IPマルチキャストルートドロップフラグ enabled 10985 0 463 IP BFD TTL minor 2705 0 464 IPv4 BFD SH packet invalid size 2294 0 486 IPv4マルチキャスト出力no route 1363073 0 488 IPv4マルチキャスト失敗RPF drop 222733 0 550 L2 VNI info no hash entry drop 7 0 562 L2 egress VLAN tag missing drop 97 0 576 L2 ingress LAG no match 172286 592 L2 flood GID NULL FINGRESS FINGRESS NULL drop 62617 4577940 27398 60273 67132 22229 1502161 984281239 4472288 18133144 3293512 2412441 281239 406582755 199262152 295962479 101423 3512168 13281 65599 27441792 152495 173434294 213116 466671481 413684 2230163 152501 152559 78667597 9155455 9760672 1673465 516895376 64643796 26014 9143978 13053 339606 29024842290654 3235969 29024410231530 3235922 23530268012585 2664187 23530333637629 2664266 605997250 980248296 1081176162 1081176162

1081176162 23531332324079 2664493 23531313885879 2664491 18438204 18438204 214940487672 23474 0 602 L2 on L3 ingress unknown protocol 0 617 LAC subscribers L2TP version mismatch drop 404 0 623 LSM dropped due to egress drop flag on label 3 0 635 MPLS over UDP decap is disabled 5 0 650 P2MP tries more than two labelsラベル0 652 P2MP with invalid v4 or v6 explicit label 0 671 Tail drops due to queue limit to queue limit 0 7228入力DXID no match drop 5 0 729 WREDカーブ確率ドロップ数0 734 CLNSファブリックプレルートからのマルチキャスト0 0 738ファブリックプレルートからのIPv4 206 739ファブリックプレルートからのIPv4内向き0 740 IPv4内向き2 742ファブリックプレルートからのIPv4マルチキャスト0 745 IPv6ファブリックプレルート7からのリンク 49ファブリックプレルートからのIPv6マルチキャスト529 0 753ファブリックへのインジェクトMSG 151 754ポートへのインジェクトMSG 106 755 MPLS from fabric0 759プレルートパント要求0 1410無効なテーブルコンテンツによるドロップ9 0 1418 IPv4出力ヌルルート1 0 1423 IPv4の無効な長入力210 144444 MPLS バイト exceeded ¶ 0 1466 MPLS invalid payload when disposition all labels 85 0 1468 MPLS leaf with no control flags set設定0 1470 MPLS receive adjacency 1 0 1503 ARP 0 1518 Bundle protocol 3 1524 Diags 0 1572 IPv4 options 188 0 1587 ICMP generation needed 33 159 TTL exceeded 216 0パントポリサー： TTL exceeded 7506 0 1602 IPv4 fragmentation needed IPv4 BFD 1288 0 1611 IFIB 157 1612パントポリサー： IFIB 0 1632 IPv6 hop-by-hop 1285 0 1635 IPv6 TTL error 95診断RSPアクティブ0 1698診断RSPスタンバイ0 1701 NetIO RPからLC CPU 8 1716 SyncE 1 1749 MPLS fragmentation needed 16 0 1752 MPLS TTL exceeded 194 0 1755 IPv4 adjacency null route 0 1756 punt policer: IPv4 adjacency null 0 1809 PTP ethernet☆56 1899 DHCP broadcast 891 0 1995 IPv4 incomplete Rx adjacency・6 1996 Punt policer: IPv4 incomplete Rx adjacency・0 1998 IPv4 incomplete Tx adjacency・0 1999 Punt policer: IPv4 Tx adjacency・0 2013 IPv6 Tx・adjacency・2 06 0 2022 MPLS inject Tx adjacency不完全Tx adjacency0 0 2028 Remote punt BFD 31 0 HW Received from LineファブリックへHW TransmitファブリックへHW Received from FabricファブリックへHW Transmit to LineへHW Inject受信したHW Inject25 HW Host Punt25 HW Local Loopback受信iGTR Þ 309 HW Local Loopback Received at Egress 309 HW Transmit to TM from eGTR☆HW Transmit to L2☆HW Received from Service Loopback 2HW Transmit to Service Loopback 2HW Internal generated by PDMA☆で生成されるハードウェア

a.L3固有のカウンタ

ドロップについては、以下のWikiで理由を調べてください。L3カテゴリに該当するかどうかを確認します。

L3カテゴリの場合は、フローに関連するすべてのL3関連の出力を取得してください。
L3 CEFチェーンの出力と他のshowコマンド

show cef [ipv4 | ipv6 | mpls] hardware [ingress | egress] detail location <LC>

show mpls forwarding labels <ラベル> hardware egress detail location <LC>

show cef vrf <vrf> <IP> internal location <LC>

show cef vrf <vrf> <IP> hardware [ingres | egress] location <LC>

show cef mpls local-label <LABEL> EOS

show cef mpls local-label <LABEL> non-eos location <LC>

show mpls forwarding labels <LABEL> det hardware [ingres | egress] location <LC>（mpls転送ラベル<ラベル> det hardware [ingres | egress] location <LC>）

インターフェイスレベルの出力に関連するshowコマンド[Sub-interface, Bundles and its members..]

インターフェイスに関連するuidb imデータベースとそのチェーンを表示します。

show bundle <> relatedコマンド（バンドルが呼び出された場合）

sh controllers pm vqi location <LC

PIコマンド：

sh cef <IP> internal location <LC>

sh cef <IP> detail location <LC>

show cef unresolved loc <>

show cef adjacency loc <>（CEF隣接関係ロケーションの表示）

show cef [drops | exception] loc <>

show cef [misc | summary] loc <>

show cef [ipv4 | ipv6 | mpls] trace [error | eve | table] loc <>

show cef interface <> loc <>

show mpls forwarding [..] loc <>（mpls転送の例）

b. L2専用カウンタ

ドロップについては、以下のWikiで理由を調べてください。L2カテゴリに該当するかどうかを確認します。
LSPのすべてのカウンタの詳細
L2カテゴリの場合は、フローに関連するすべてのL2関連の出力を取得してください。
L2VPNチェーンの出力と他のshowコマンド

show l2vpn forwarding hardware ingress detail location <LC>

show l2vpn forwarding hardware egress detail location <LC>（l2vpn転送ハードウェア出力詳細ロケーションを表示する）

show l2vpn forwarding bridge-domain <BD Group: BD Name> hardware ingress detail location <LC>

show l2vpn forwarding bridge-domain <BD Group: BD Name> hardware egress detail location <LC>

show l2vpn forwarding bridge-domain mac-address hardware ingress

location <LC>

show l2vpn forwarding interface pw-ether <PW> hard detail location <LC>

show l2vpn xconnect interface pw-ether <PW> detail

show l2vpn forwarding main-port pwhe interface pw-ether600 hardware ingress detail location <LC>

show l2vpn mstp port msti 0

show l2vpn mstp port msti 1

インターフェイスレベルの出力に関連するshowコマンド[Sub-interface, Bundles and its members..]

インターフェイスに関連するuidb imデータベースとそのチェーンを表示します。

show bundle <> relatedコマンド（バンドルが呼び出された場合）

sh controllers pm vqi location < >

show l2vpn forwarding bridge-domain mac-address internal private first 1000 location 0/RP0/CPU0

show evpn internal-label private location 0/RP0/CPU0

show evpn internal-label path-list private location 0/RP0/CPU0

show evpn internal-id private location 0/RP0/CPU0

show l2vpn forwarding bridge-domain mac-address internal private first 1000 location 0/RP1/CPU0

show evpn internal-label private location 0/RP1/CPU0

show evpn internal-label path-list private location 0/RP1/CPU0

3. ドロップカウンタのモニタnpカウンタをキャプチャします。

例：カウンタ<DROP_COUNTER_NAME>を監視するには、次のコマンドを実行します。

monitor np counter <DROP_COUNTER_NAME> <np> location <LC>

RP/0/RP0/CPU0:agg03.rjo# monitor np counter PARSE_DROP_IPV4_CHECKSUM_ERROR np0 location 0/1/cpu0 Tue Oct 5 10:49:30.349 BRA NPモニタの使用は、シスコ社内での使用にのみ推奨されます。代わりに、NPでのパケットドロップのトラブルシューティングには「show controllers np capture」を、（サブ）インターフェイスカウンタごとのモニタリングには「monitor np interface」を使用してください。警告：キャプチャされたすべてのパケットがドロップされます。「count」オプションを使用して複数のプロトコルパケットをキャプチャすると、プロトコルセッション（例、OSPFセッションフラップ）が中断される可能性があります。 したがって、プロトコルパケ

ットをキャプチャする場合は、一度に1つだけキャプチャします。警告：モニタの後にNPのリセットが必須で実行され、クリーンアップされます。これにより、約150ミリ秒のトラフィック停止が発生します。リンクはアップしたままになります。Proceed y/n [y] > y Monitor PARSE_DROP_IPV4_CHECKSUM_ERROR on NP0 ... (Ctrl-C to quit) Tue Oct 5 10:49:33 2021 — NP0 packet From HundredGigE0_1_0_0: 86 packet 0000: b0 26 80 67 3c bc 165 5e 2c 0480 40 0&.g<=<.e^,...E. 0010: 00 48 cb b9 40 00 38 11 53 7f b3 e8 5e 74 08 08 .HK9@.8.S.3h^t..0020: 08 08 b5 a6 00 35 00 34 e5 22 d0 01 00 00 01 ..5&.5.4e"Pp.... 000 00 00 00 00 00 00 00 0e 6e 72 64 70 35 31 2d 61 70 .....nrdp51-ap 0040: 70 62 6f 74 7 6e 65 74 66 6c 69 78 03 63 6f pboot.netflix.co 0050: 6d 00 00 01 00 01 m.....

monitor np counter <DROP_COUNTER_NAME> <np> detail location <LC>

RP/0/RP0/CPU0:PE23#monitor np counter 12 np3 detail location 0/0/CPU0 Mon Mar 11 18:20:49.180 IST NP monitorの使用は、シスコ社内でのみ推奨されます。警告：モニタを使用すると、短時間のトラフィック損失が2回発生し、セットアップとテイクダウンが行われます。それぞれの停止は、？ミリ秒を超える可能性があります。パケットが監視されると、通常の処理（転送、パント、ドロップなど）が再開されます。 トラフィック停止の準備はできていますか？[enter] Monitoring NP3 for NP counter 12 [Invalid stats pointer 12] ... (Ctrl-C to quit) Mon Mar 11 18:21:25 2024 — NP3パケット150バイト---------- ---------- NPU 03:Cluster 11: PPE 15: Thread 00 Ptrace 00 Received from : Fabric GPM Pkt Dump Contents: 004 08 0C 114 118 c G 000: 70e42225 e554f86b d9a39247 88470057 80049000 0054004a 00000000 00000000 G 020: 00000000 9424118c 05000400 000000a6 c024400f 00000001 248c80c1000004 G 040: 000186a0 000186a0 00000000 dad4994e 00200000 20c80318ba 00010100060296 64001700 000001 00034 00000000 801318 044420 00000020 00000000 040401 82000201 190080 00000004 053942 20048 810003 08004500 00640000 21764 00010800 79520000 00000000 40000256 009609 00000000 00000000 0000010 05000172 40000000 00000000 00000000 810003 00000000 70000000 01004 64000300 00000000 02000000 00000000 0000000 000992 00000000 00000000 00000000 01800000 00000000 0000000 00000000 00711 00000046 41800000 01000001 64000 00064 39247 00009003 00000000 00000000 00000000 00000000 0000000 00018 00000000 00000076 00000000 39247 00009003 00000000 00000000 00000000 00000000 83211001 00000000 94001 000001 00000000 28010100 00000000 00000000 0000004 0000000 00000000 00002000 0000004 90004031 800019 00000000 00000000 00000004 00000004 01000000 000000 8008810 01010003 00000000 00000000 00000000 00000000 00000000 010423 80000000 00000008 00021000 00008008 000001 083961 000011 00000172 00000000 0000000 00000000 000210 000210 00000084 000210 00009000 800019 000210 00000000 02000000 00000000 00680 20000 000000 02000000 05800010 00040004 00000000 00020390 04441100 044422 800980 00000001 0000000 0000000 084204 00000032 18000004 04442200 044421 00000008 00000003 000210 00000004 00000001 00000001 80119 04442170 000210 000210 000000 80125 04442140 000210 000210 00000001 00000001 00500000 000210 000210 000210 000210 00000001 084204 00000004 000000 00000001 00000032 00000001 00500000 18000004 00000001 80125 800980 04442200 80119 04442140 00000001 044421 04442170 0000000 00000008 000210 0000000 00000003 0000001 0000008 00000003 00040250 00000001 00020330 00000000 00095 0000008 732982 00020390 00000000 00000000 00000000 00000000 00000034 00095 0000008 00000001 000003 00000000 000003 00000000 60411000 15000 08000000 08000000 00000000 00000000 19382747 00000003 00000000 00000008 00000000 0000000 00000000 00000003 00000007 00060330 00000000 00000000 00000000 800034 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 8000000 04441400 00000001 00000000 000000 00000000 ba G60: 011bef8c00ec8 03e83cff 064eddff 45c G 080: ~e5~b0 0000fc00~ ~a0000ff80~0000fd0~g0a0: ~d000000e00000~e000000000000: 003bbbff 0001f86b d9a3923f e9 000ff01 8bdG 0e0: 00fe1764 b4ee1a25 00000:00fe1764 abcd1a25 0000:abcdabcdabcdabcdabcdabcdabcdabcdAbcdGG 1220: abcd abcd abcd abcd49d6 Content: 00 04 08 0C 14 18 1C 000：~c0 ~デッドビーフデッドビーフ020：f e9 ~e9 ~e004c49040：~c1ba06 ~f100 80: 000f0109...06d035fb ...ed1 0a0: 8200f86b d9a.....

8200f86b d9a 1e01f25f☆100:☆0d b 0992a096 07aa60a2 1e000fa0 1c 120:deadbeef deadbeef deadbeef debeef debeef deadbeef 140: deadbeef deadbeef deadbeef deadbeef deadbeef 160: deadbeef deadbeef deadbeef deadbeef deadbeef deadbeef deadbeef deadbeef deadbeef deadbeef deadbeef deadbeef deadbeef deadbeef 180: deadbeef deadbeef deadbeef deadbeef 1a0: deadbeef deadbeef deadbeef 1c0: deadbeef deadbeef deadbeef . . . . . .

. . . . . .

.....

デッドビーフデッドビーフデッドビーフデッドビーフデッドビーフデッドビーフデッドビーフ280：デッドビーフデッドビーフデッドビーフデッドビーフデッドビーフ2a0：デッドビーフデッドビーフデッドビーフデッドビーフデッドビーフ2c0: 000f0108 004aea60デッドビーフデッドビーフ001e003°デッドビーフ2e0：デッドビーフデッドビーフデッドビーフデッドビーフデッドビーフデッドビーフデッドビーフデッドビーフ30000090:09299 004 04fc49ef deadbeef deadbeef deadbeef☆ef deadbeef deadbeef 320: ef 03e83cff 061adff deadbeef deadbeef 340: deadbeef deadbeef c0000ec8☆ef deadbeef☆30000beefビーフeec0 a2961b030deadbeef0 e83cffデッドビーフdeadbeef001f250 3a0: ~ d3 ~ a0デッドビーフdeadbeefだデッドビーフ00ffbeef00 ~ efデッドビーフ3e0: ~ a395f8feだc0登録内容： ~ r00 ~ a9060 ~ a03c0 ~ a08 : þd0☆a0☆a0☆a a0☆a a0☆a a1111100 fffff000000000000000000ffffffff r24:☆a0000fc0000000000000000000000000000040004000000400000 a0 | a16 004aea60 | a24 A0 a01 | a09 | a17 3ca☆a25 a02☆ff | a10☆a26 ~ a03 00ffffff | a11»a19 | a27 a04faf | a09 | a22a20fafa9 | a2 | a28☆bab a05 } | a13☆a21»d0 | a29☆a06 0000fc00 | a14 °c | a22☆a30 0000fc00 a07 | a15 °c| a23 }a31 fffff000レジスタ： sar = window_a_start base =☆epc =☆exccause =☆a (SycallCause) ps = sse_cop_errorcode = sse_cop_errorcode = deb4cf17 h3tb = deadbf03 h3tc = deadbef7 h3tr = 2609d946 timestamp_high_1 =☆a09 timestamp_low_1 = 19f84b99 cycle_high_1 = ccycle_low_1 = 1ppe_6d60idue b_ext0 = 3195f8fe uidb_ext1 =☆uidb_ext3 =☆uidb_ext4 = }uidb_ext5 = }softerr_misc = 19f8609a cycle count_2 = }c732ae8 =ciスレッド=}aストップスレッド=}a8_stop_2 = memctrl = softerr_dmem0 = 67fsofterr_dmem1 = 67fcodec_segment0 =☆code_segment1 =¯ l1t_data_sbe_log = random_1 = random_control = φ1t_tag_parity_log = 6bc60d7e random_2 = 697de1cb depc = timeout_control = rtb0 = rtb1 = rtb1 invalidate = 6tlu_cmd60d = 6e t_enables = þ l1t_replacement_way = þ l1t_data_mbe_log =☆l1t_mshr_mbe_log = sse_cop_seedh = 356c9b sse_cop_tlu_cnt1_rw = sse_cop_lock = 7 sse_cop_tlu_perr = sse_cop_tlu_cnte1_rw = sse_cop_tps_tps_parity = ssse_cop_tps_spt_log = sse_cop_tmu_parity_log_rw = sse_cop_tmu_sram_mbe_log_rw = sse_cop_tmu_sram_sbe_log_rw = sse_cop_tlu_cnte0_rw = sse_cop_tlu_cntp_rw = sse_cop_tlu_cntp_rw = sse_cop_tlrw u_cnt0_rw = rtc rtt_index =☆rtt_data0 =☆rtt_data1 =☆rtt_data1 =☆ppe_lock =☆c stack_limit =☆stack_limit_enable =☆sse_cop_dma_mem_access =☆sse_cop_dma_mem_data =☆a0 error_code =（エラーなし）

4.HWプログラミングの詳細 – 以下を使用して、フォワーディングHW構造体のプログラミングの詳細を収集できます。（NPチームがさらにデバッグする際に役立ちます）

L3

show controller np struct R-LDI unsafe det all location <LC>（すべてのロケーションに対するshow controller np struct R-LDIの安全性が低い、デフォルトの安全性が低い、など）
show controller np struct NR-LDI unsafe det all location <LC>（すべてのロケーションに対するshow controller np struct NR-LDIの安全でないデフォルト）

show controller np struct TE-NH-ADJ unsafe det all location <LC>

show controller np struct RX-ADJ unsafe det all location <LC>

show controller np struct TX-ADJ unsafe det all location <LC>

show controller np struct NHINDEX unsafe det all location <LC>

show controller np struct LAG unsafe det all location <LC>（すべての口ケーションに対するshow controller np struct LAGの安全性が低い、デフォルトの安全性が低い、など）

show controller np struct LAG-Info unsafe det all location <LC>

L2

show controller np struct UIDB-EGR-EXT unsafe det all location <LC>

show controller np struct UIDB-Ext unsafe det all location <LC>

show controller np struct UIDB-ING-EXT unsafe det all location <LC>

show controller np struct EGR-UIDB unsafe det all location <LC>

show controller np struct XID unsafe det all location <LC>（すべての口ケーションに対するshow controller np struct XIDの安全でない検出を実行します）

show controller np struct XID-EXT unsafe det all location <LC>

show controller np struct BD unsafe det all location <LC>（すべての口ケーションに対するshow controller np struct BDの安全でない検出の実行）

show controller np struct BD-EXT unsafe det all location <LC>

show controller np struct BD-LEARN-COUNT unsafe det all location <LC>

show controller np struct L2-BRGMEM unsafe det all location <LC>

show controller np struct l2-fib unsafe det all location <LC>
LSP:ssh lc0_xr /pkg/bin/show_l2ufib <Collect in all active LCs>を実行します。

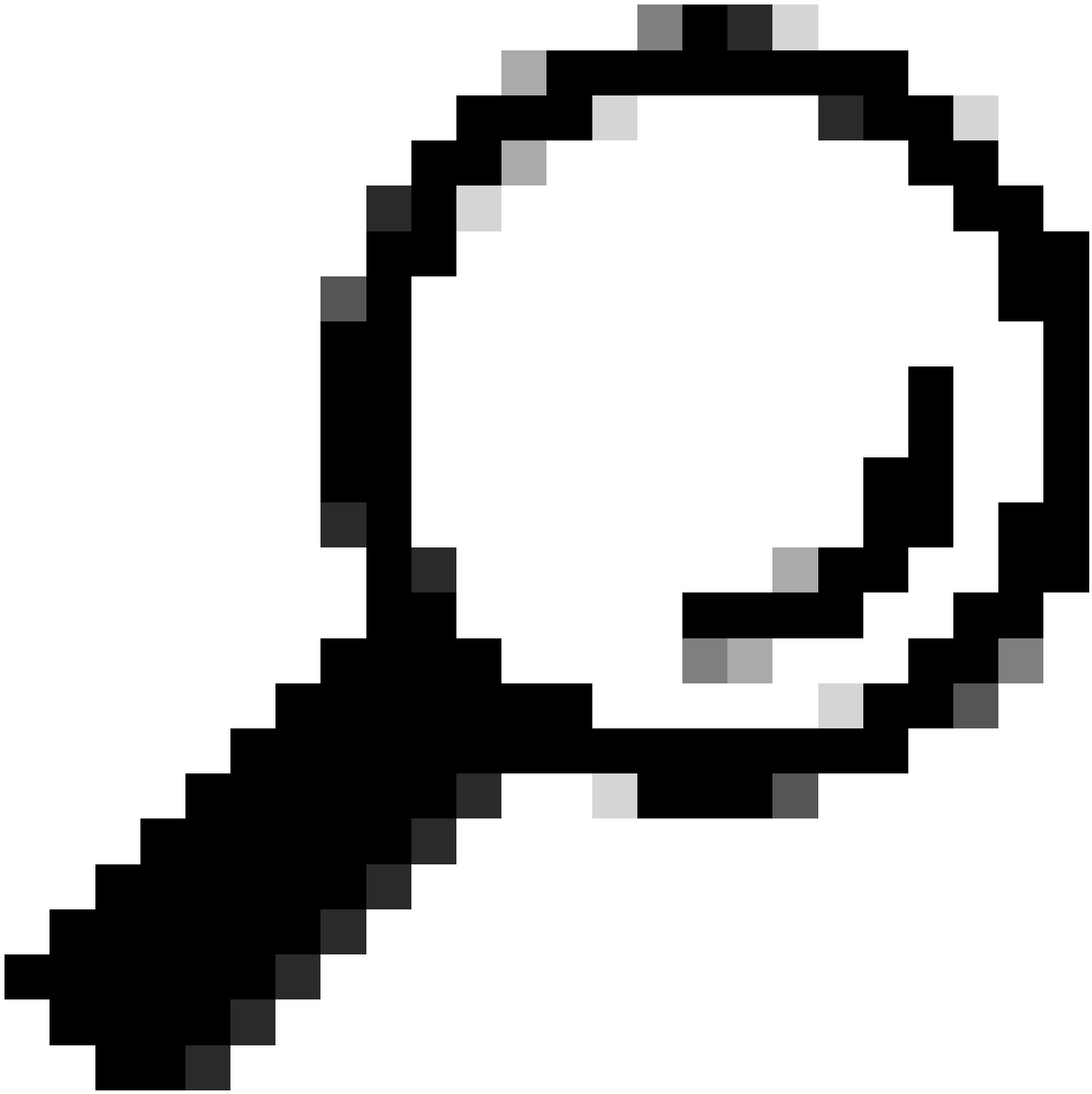
show controller np struct L2-MAILBOX unsafe det all location <LC>

show controller np struct L2-MBX-HOST-TO-NP unsafe det all location <LC>（すべての口ケーションに対するshow controller np struct L2-MBX-HOST-TO-NPの安全でない検出の実行）

show controller np struct L2-MBX-NP-TO-HOST unsafe det all location <LC>（すべての口ケーションに対してshow controller np struct L2-MBX-NP-TO-HOSTの安全でないデットを実行する）

SPP

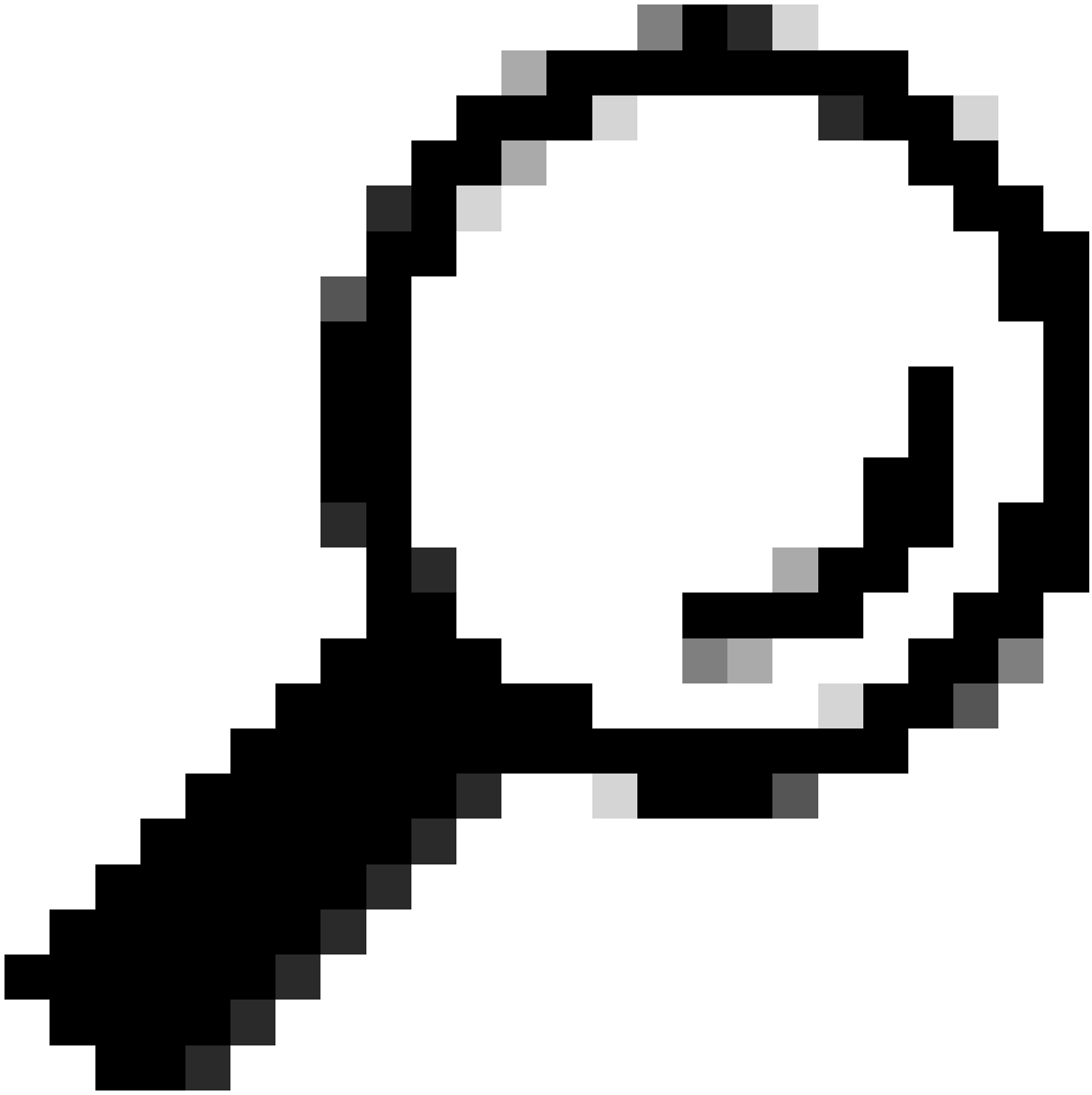
show spp sids stats location < > (隠しコマンド)
show spp node-counters location < >



ヒント:SPPでパケットをキャプチャ/フィルタリングする方法WLC の管理ユーザを認証するために TACACS+ を設定する方法を理解するには、

NETIO

show netio drops location < > (ネットワークのドロップの場所を表示します)



ヒント:

SRPM

ip maddr show eth-srpm（インターフェイスのマルチキャストエントリをチェックするため）

ip maddr show eth-srpm.1283（インターフェイスのマルチキャストエントリをチェックするため）

ifconfig（RXとTXが正しく行われているかどうかを確認するために、インターフェイスのパケット統計情報をチェックします）

[xr-vm_node0_0_CPU0: ~]$ip maddr show eth-srpm.1283 9: eth-srpm.1283 link 33:33:00:00:00:01 users 2 link

01:00:5e:01 0:00:01 users 2 link 33:33:ff:50:4e:52 users 2 link 01:56:47:50:4e:30 users 2 static link 33:33:00:01:00:03 users 2 inet 224.0.0.1 inet6 ff02::1:3 inet6 ff02::1:ff50:4e52 inet6 ff02::1 inet6 ff01::1 [xr-vm_node0_0_CPU0: ~]$ifconfig eth-srpm.1283: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9700 metric 1 inet6 fe80::54 b:47ff:fe50:4e52 prefixlen 64 scopeid 0x20<link> ether 56:4b:47:50:4e:52 txqueuelen 1000 (Ethernet) RXパケット0/バイト0 (0.0 B) RXエラー0ドロップ0オーバーラン0フレーム0 TXパケット828560/バイト138041161 (131.6 MiB) TXエラー0ドロップ0オーバーラン0キャリア0コリジョン

LPTS

- show lpts pifib hardware entry statistics loc <>
- show lpts pifib hard police loc <>
- show lpts pifib hardware static-police loc <>
- show lpts pifib ha entry stats location <>

ファブリック

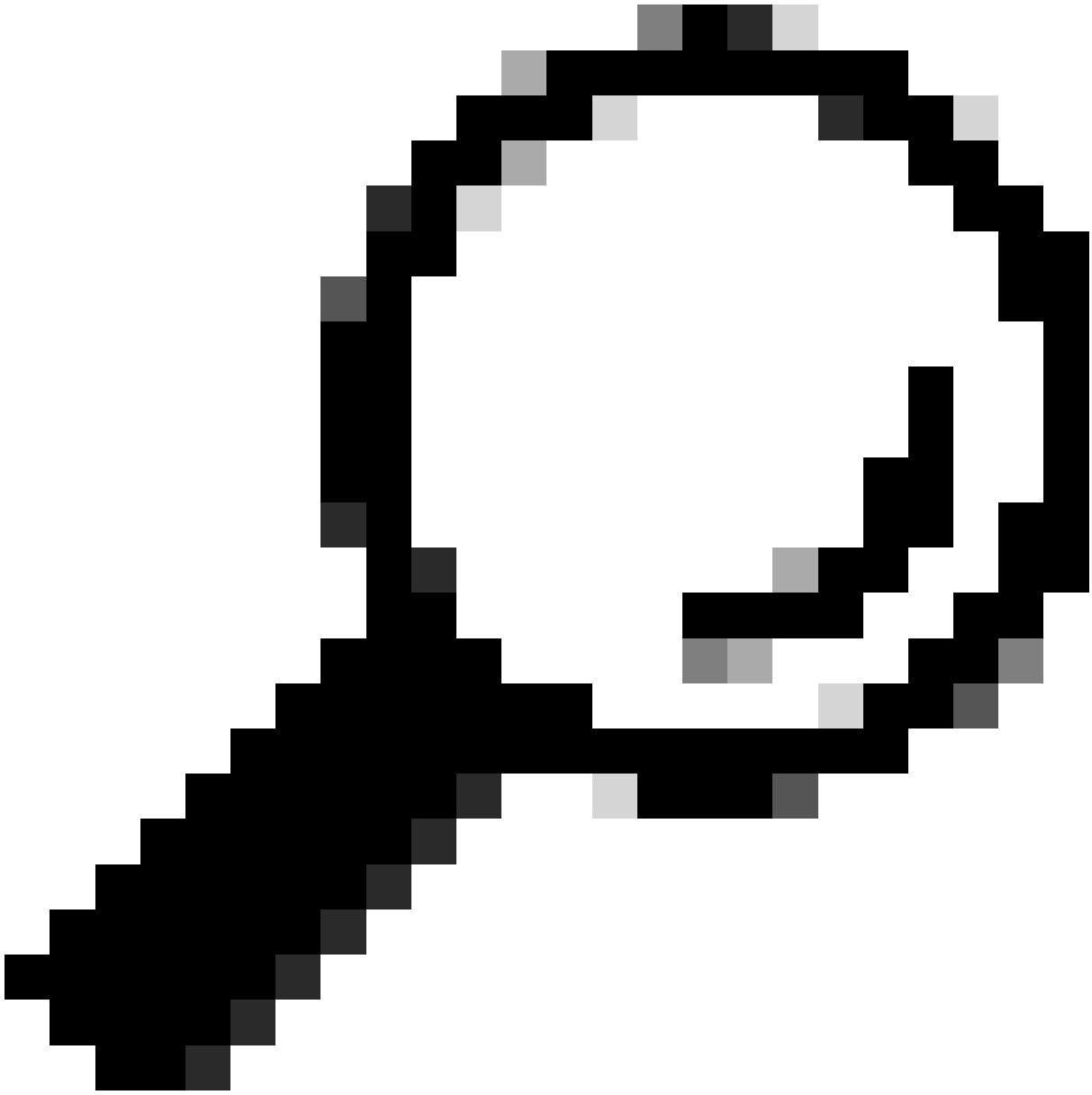
- show controller fabric fia stats location <>（コントローラのファブリックfia統計情報の場所を表示する）
- show controllers fabric fia drops ingress location <>（コントローラのファブリックfiaドロップ入力ロケーション）
- show controllers fabric fia drops出力ロケーション<>
- show controller fabric fia status location <>（コントローラのファブリックfiaステータスの場所を表示する）
- show controller pm vqi location <LC>（使用可能な場合）
- show controllers fabric vqi assignment location <>（コントローラのファブリックvqi割り当ての場所を表示）
- show tech fabric（登録ユーザ専用）
- show_sm15_ltrace -s 2 fab_xbar | grep "sm15_pcie_read_fpoe"

アプリケーション

- show ipv4 traffic brief location <>（ipv4トラフィックの簡単な場所を表示）

サイレントドロップ

アカウンティングなしではパケットは廃棄されませんが、実稼働環境のセットアップでは複数のカウンタが増分され、カウンタ名が直接ドロップを指していない場合があります。着信パケットがドロップされたのか、転送されたのかを判断するのが難しい場合があります。パケットトレースを使用して、セットアップ上のパケットフローを監視し、パケットが送信されているかどうかを検証できます。パケットトレースの出力例を次に示します。



ヒント:Embedded packet tracer、詳細情報@ PRM Embedded Packet Trace。
(https://xrdocs.io/asr9k//tutorials/xr-embedded-packet-tracer/)

CLIコマンドの概要

コマンド構文	説明
clear packet-trace conditions all（すべてのパケットトレース条件をクリア）	バッファされているすべてのパケットトレース条件をクリアします。コマンドは、パケットトレースが非アクティブな間だけ使用できます。
clear packet-trace counters all（すべてのパケットトレースカウンタをクリア）	すべてのパケットトレースカウンタを0にリセットします。
パケットトレース条件インターフェイス	ルータをトレースするパケットを受信すると予想されるインターフェイスを指定します。

コマンド構文	説明
パケットトレース conditionnoffsetoffsetvaluemaskmask	対象のフローを定義するオフセット/値/マスクのセットを指定します。
パケットトレーススタート	パケットトレースを開始します。
パケットトレースの停止	パケットトレースを停止します。
show packet-traceの説明	Packet Tracerフレームワークに登録されているすべてのカウンタとその説明を参照してください。
show packet-trace status[detail]	アクティブRPで実行されているpkt_trace_masterプロセスによってバッファされた条件と、パケットトレーサのステータス（アクティブ/非アクティブ）を参照してください。 コマンドのdetailedオプションは、ルータ内のすべてのカードでPacket Tracerフレームワークに登録されているプロセスを示します。Packet Tracerのステータスが Activeの場合、出力にはデータパスで正常にプログラムされた条件も表示されます。
show packet-traceの結果	ゼロ以外のパケットトレーサのカウンタを参照してください。
show packet-trace result countername[sourcesource] [locationlocation]	特定のパケットトレースカウンタの最新の1023単位の増分を参照してください。

RP/0/RSP1/CPU0:ios#sh packet-trace results Jan 24 19:28:56.151 UTC T: D – ドロップカウンタ； p – パスカウンタの場所|送信元|カウンタ| T |最終属性|カウント---------- ---------- ---------- - ---------- ---------- 0/0/CPU0 NP1 PACKET_MARKED P FortyGigE0_0_1_0 1522128420 0/0/CPU0 NP1 PACKET_ING_DROP D 2000908208 0/0/CPU0 NP1 PACKET_TO_FABRIC P 1522238547 0/0/CPU0 NP1 PACKET_TO_PUNT P0/0 296246 /CPU0 NP1 PACKET_INGR_TOP_LOOPBACK P 1000371630 0/0/CPU0 NP1 PACKET_INGR_TM_LOOPBACK P 1000375084 0/0/CPU0 spp-LIB ENTRY_COUNT P SPP PD Punt: stage1 299311 0/0/CPU0 NP1 PACKET_FROM_FABRIC P 1522238531 0/0/CPU0 NP1 PACKET_EGR_TOP_LOOPBACK p 1000371546 0/0/CPU0 NP1 PACKET_EGR_TM_LOOPBACK P 1000375020 0/0/CPU0 NP1 PACKET_TO_INTERFACE P FortyGigE0_0_1_0 1522241940

トリアージフロー：

最初に、「show drops, show drops all ongoing location all」の出力を複数回確認し、ドロップが発生しているモジュール/コードコンポーネントを特定します。

特定されたコンポーネントやモジュール固有のコマンドを使用して、問題をさらに切り分けることができます。

show drops all ongoing location all→これはNP/FIA/LPTS/CEFのためのリアルタイムドロップ情報を示します

```
RP/0/RP1/CPU0:R1# show drops all location 0/7/CPU0
5月20日（金）09:31:34.585 UTC
====================================
0/7/CPU0でのドロップの確認
====================================
show arp trafficの出力は次のとおりです。
[arp:ARP] IPパケットドロップカウント、ノード0/7/CPU0:265
show cef drops:
[cef:0/7/CPU0] No route drops packets : 30536808
show spp node-counters:
[spp:pd_utility]オフロードのドロップ：インターフェイスの停止： 1
[spp:port3/classify]無効：logged n dropped:10
[spp:client/punt]クライアントクォータドロップ： 445639
show spp client detail:
[spp:ASR9K SPIOクライアントストリームID 50、JID 253(pid 7464)]現在： 0、制限
： 20000、使用可能： 0、エンキュー： 0、ドロップ： 445639
RP/0/RP1/CPU0:R1#
```

ドロップの表示

RP/0/RP1/CPU0:R1# show drops all location 0/7/CPU0 5月20日（金）09:31:34.585 UTC ==========
0/7/CPU0でのドロップのチェック ========== show arp traffic:[arp:ARP] IP Packet drop count for node 0/7/CPU0: 265 show cef drops:[cef:0/7/CPU0] No route drops : 30536808 show spp node-counters:[sppd_utility] Offload ：インターフェイス Down: 1 [spp:port3/classify]無効：logged n dropped: 10 [spp:client/punt]クライアントクォータdrop: 445639 show spp client detail: [spp:ASR9K SPIO client stream ID 50, JID 253 (pid 7464)]現在：0、制限：20000、使用可能：0、キューに入れられた状態：0、ドロップ：445639 RP/0/RP1/CPU0:R1#

show pfm location all:ASICエラ→、Punt_data_path_failed(PFM-all-failed)などのシステム関連アラームを提供します。

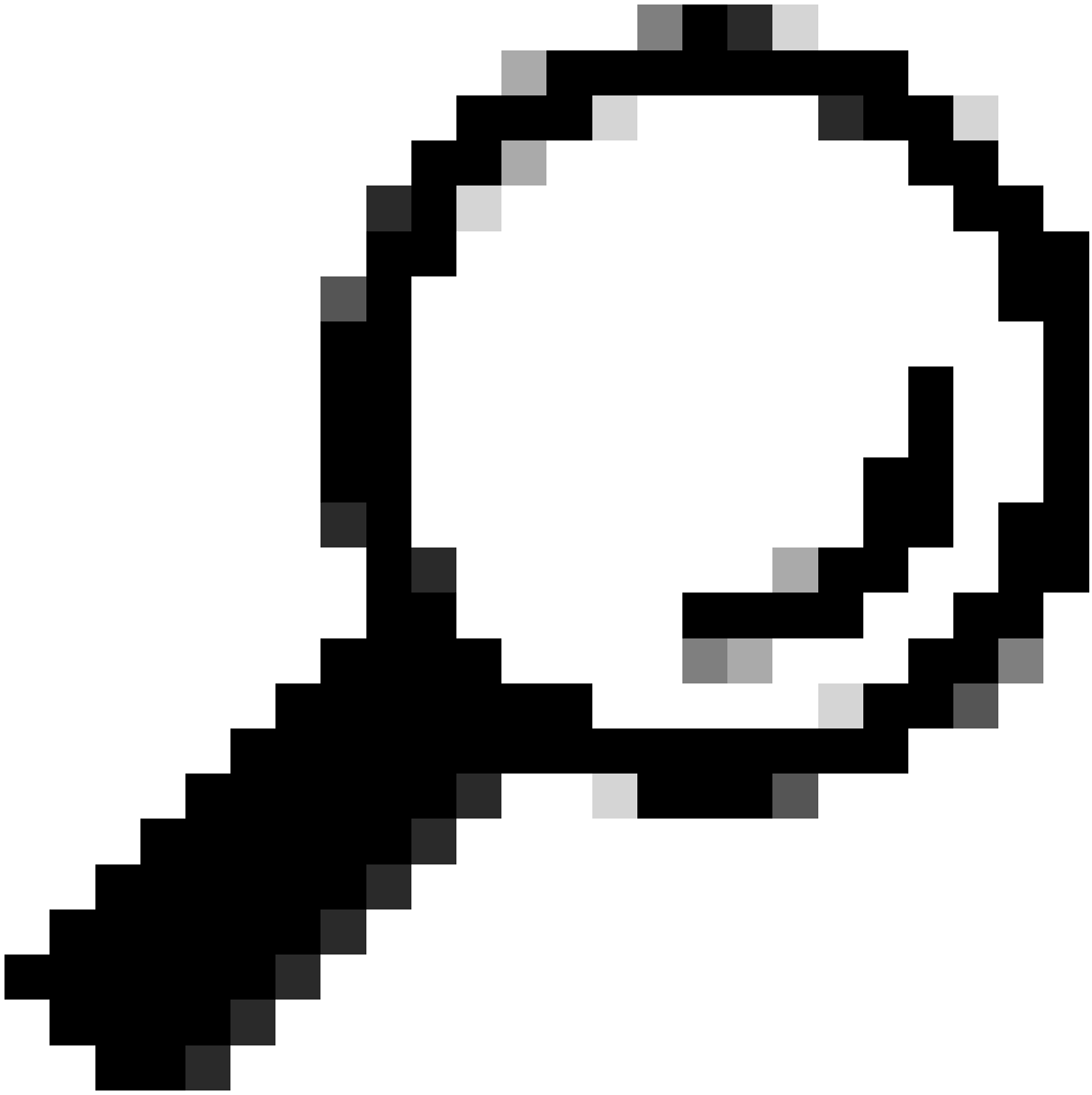
RP/0/RP0/CPU0:l51#show pfm location all Mon Apr 1 10:02:49.952 UTCノード： node0_0_CPU0 ----------現在の時刻：4月1日10:02:50 2024 PFM合計： 0緊急/アラート(E/A): 0重大(CR): 0エラー(ER): 0発生---------- ----------時間|S#|障害名前|Sev|Proc_ID|開発/パス名|Handle ----------+—+---------- ----------+—+-------+----------+---------- Mon Jan 01 00:00:000|—|NONE |NO |0000000|NONE |0x00000000 node: node0_RP0_CPU0 ---------- CURRENT TIME: Apr 10:02:50 2024 PFM TOTAL: 0 EMERGENCY/ALERT(E/A): 0(CRITICAL) CR): 0 ERROR(ER): 0 ---------- Raised Time |S#|Fault Name |Sev|Proc_ID|Dev/Path Name |Handle ----------+—+----------+—+-------+---------- ----+---------- Mon Jan 01 00:00:000|—|NONE |NO |0000000|NONE |0x00000000 RP/0/RP0/CPU0:l51#

「当社の」パケットドロップ

インターフェイス統計情報の確認

NPカウンタの確認

SPPカウンタの確認



ヒント:

アプリケーションレベルの統計情報の確認
debug punt-inject l3/l2-packets <protocol> location <>を有効にします。
netioカウンタの確認
SPPカウンタの確認
SRPMポートの統計情報の確認
NPカウンタの確認
インターフェイス統計情報の確認

その他の役立つリンク：

フィードバック

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。