

Cisco IOS XEのパケットキャプチャで見つからないパケットのトラブルシューティング

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[トラブルシューティング](#)

[パントポリサー](#)

[パケット/秒\(pps\)組み込みパケットキャプチャパラメータ](#)

[QFPの使用](#)

[ベストプラクティス](#)

はじめに

このドキュメントでは、Embedded Packet Capture(EPC)で欠落したパケットをトラブルシューティングする方法について説明します。

前提条件

要件

Cisco IOS® XEの組み込みパケットキャプチャに精通していること。これについては、「[ソフトウェアでの組み込みパケットの設定とキャプチャ](#)」で説明しています。

使用するコンポーネント

この記事の例は、Cisco IOS XEルータに基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

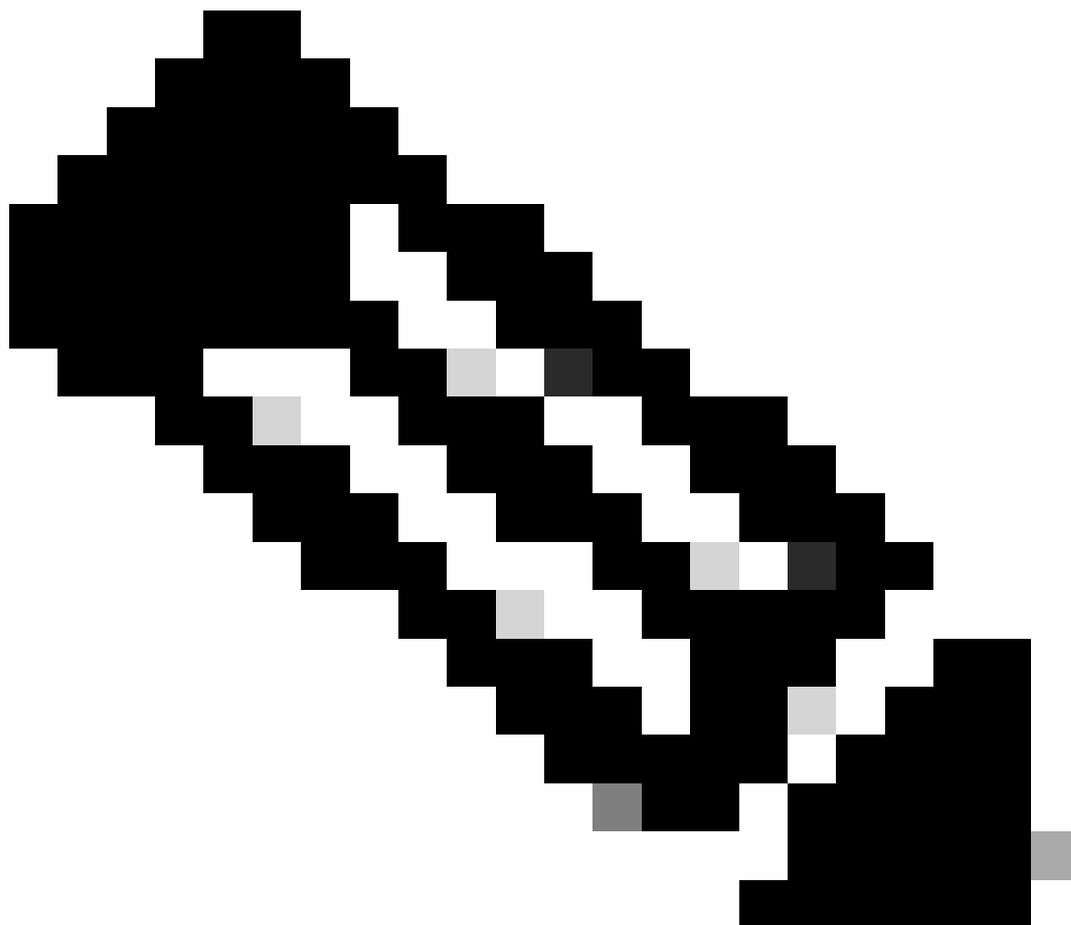
背景説明

ルータを通過するすべてのパケットをキャプチャすることが重要であるシナリオもありますが、Cisco IOS XEシステムには、コントロールプレーンを保護するためのデフォルトのパントポリサーメカニズムがあります。

このメカニズムでは、ポリシーの制限に達すると、キャプチャされたパケットの一部が廃棄される可能性があります。

また、キャプチャされる1秒あたりのパケット数(pps)を増やすように設定できるオプションもあります。

これらの2つの要素は、正常にキャプチャされたパケットの量において重要な役割を果たします。



注：これらのパラメータのデフォルト値は、プラットフォームおよびバージョンに依存する場合があります。プラットフォームとバージョンに関する注意事項を確認し、必要に応じてCisco TACに連絡して、サポートを依頼してください。

トラブルシューティング

パントポリサー

このポリサーは、コントロールプレーンにパントされるパケットを制御します。

show platform hardware qfp active infrastructure punt statistics type punt-dropコマンドを使用し、このパント制御メカニズムによってドロップされるパケットの詳細な統計情報を表示します。

コマンドはさまざまなカテゴリで表示されます。注目する必要があるカテゴリはPUNT_PER_CAUSE_POLICERです。

これは、Embedded Packet Capture(EPC)機能を参照するEPC causeを含むカテゴリです。

```
---- show platform hardware qfp active infrastructure punt statistics type punt-drop ----
```

Punt Drop Statistics

Number of punt causes = 165

```
Drop Counter ID 11 Drop Counter Name PUNT_PER_CAUSE_POLICER Counter ID Punt Cause Name Packets --
```

```
075 EPC 994641
```

全体的には、統計情報はパント原因で送受信されたパントパケットの数を示し、show platform hardware qfp active infrastructure punt statistics type per-causeコマンドで参照できます。

```
---- show platform hardware qfp active infrastructure punt statistics type per-cause ----
```

Global Per Cause Statistics

Number of punt causes = 165

Per Punt Cause Statistics

Counter ID	Punt Cause Name	Packets Received	Packets Transmitted
------------	-----------------	------------------	---------------------

075 EPC 1527458 532817

これにより、どのタイプのパント原因がパントパスを最も消費しているかがわかります。

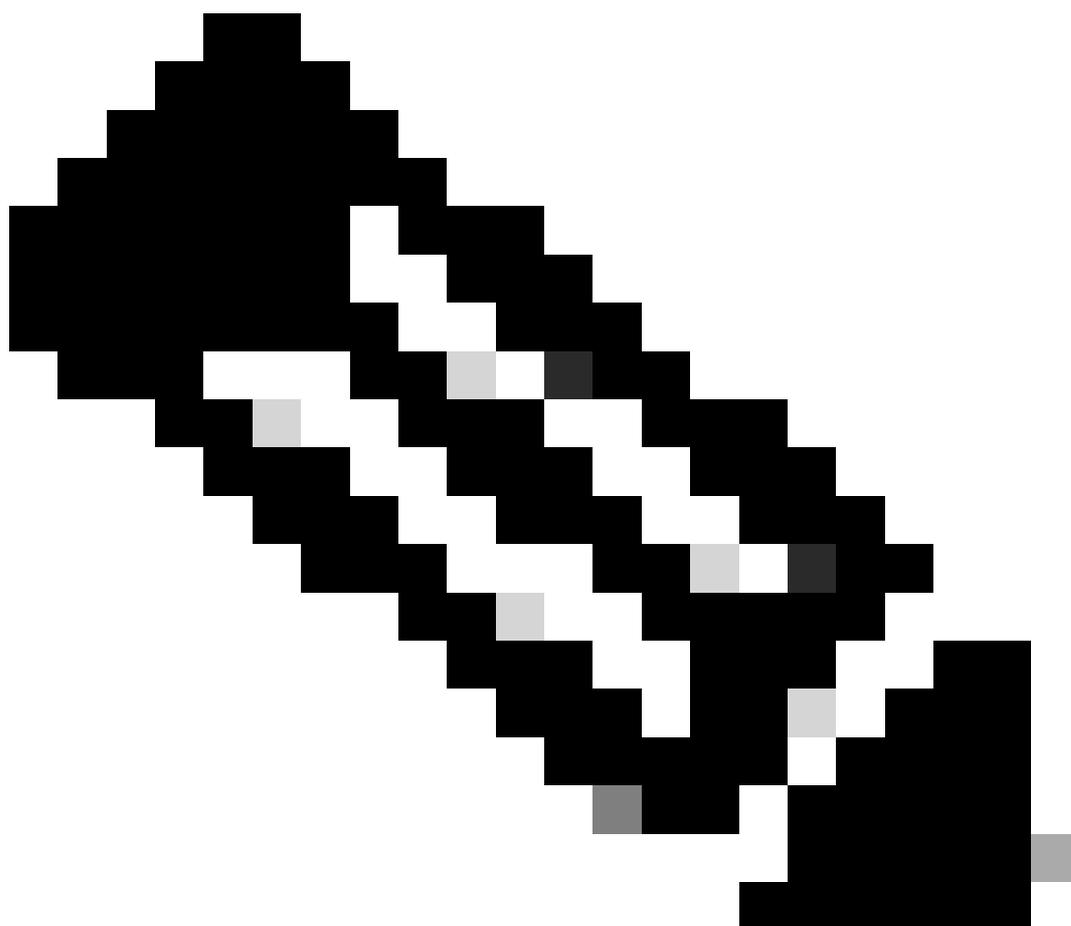
コマンドshow platform software punt-policerは、さまざまなパントの原因について、設定されたpps、適合パケット、ポリサーによって廃棄されたパケット、およびパケットに設定されたバーストのスナップショットを示します。この場合、焦点はEPCパントの原因です。

```
Router#show platform software punt-policer
```

```
Per Punt-Cause Policer Configuration and Packet Counters
```

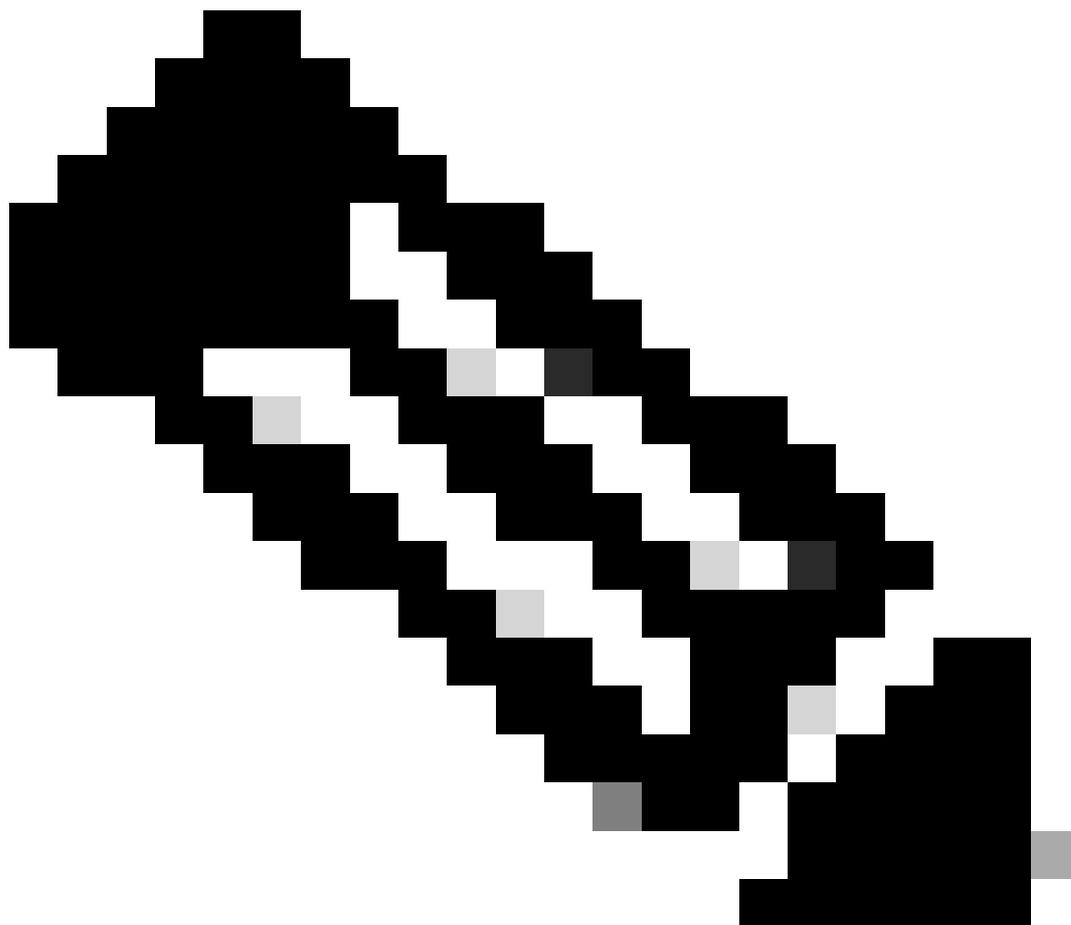
Punt Cause	Description	Config Rate(pps)		Conform Packets		Dropped Pack
		Normal	High	Normal	High	Normal

```
75 EPC 40000 1000 0 0 0 0 40000 1000 Off Off
```



注：設定レートおよび設定バーストパケットのデフォルト値は、プラットフォームおよびバージョンによって異なる可能性があることに注意してください。

パントポリサーの1秒あたりのパケット数およびパント原因カテゴリのバーストパケット数は、コマンド `platform punt-policer epc <10-32000> [<1-100000000>]` を使用して変更できます。



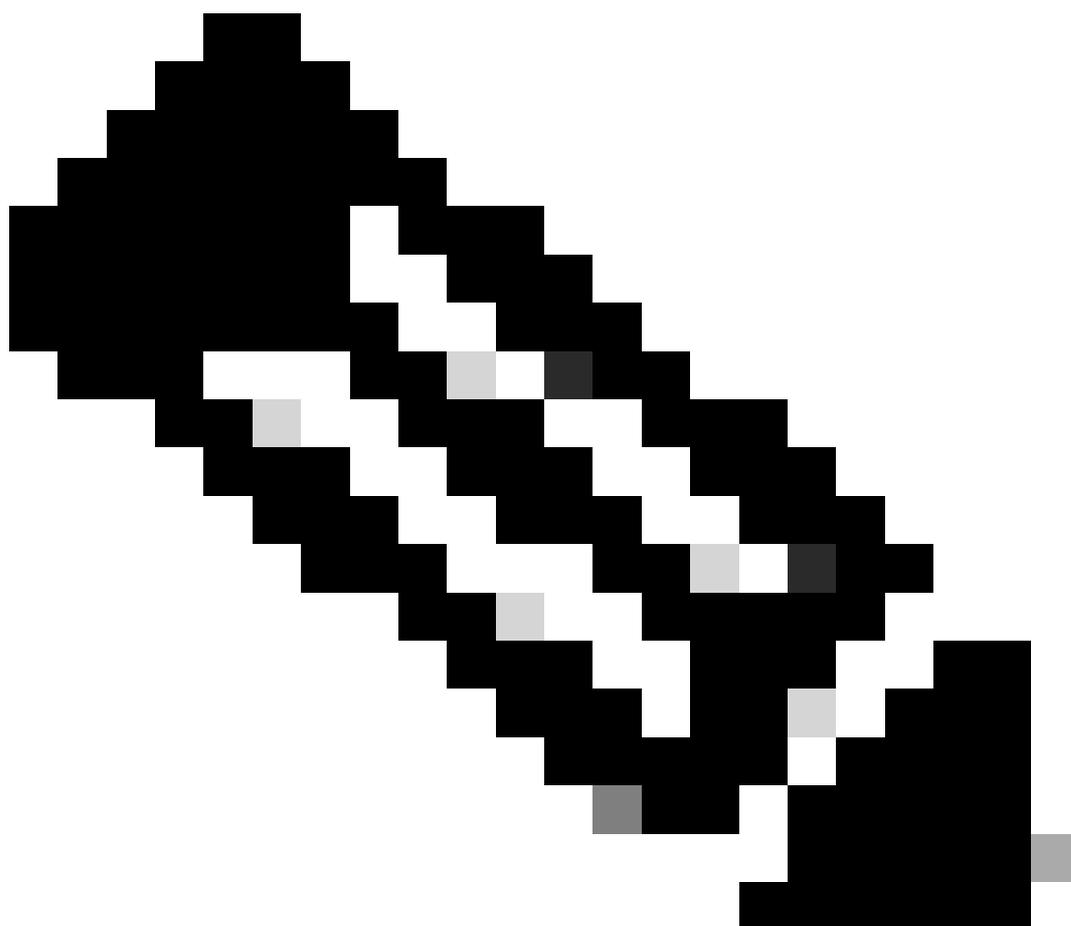
注：パントポリサーはコントロールプレーンの保護メカニズムであるため、デフォルトの設定済みパント値を変更する際には注意が必要です。

パケット/秒(pps)組み込みパケットキャプチャパラメータ

packets per secondパラメータは、キャプチャする1秒あたりのパケット数を制限します。

埋め込みパケットキャプチャ設定の1秒あたりのパケット数パラメータは、コマンドで指定できません

```
monitorcapturecapture-namelimit[durationseconds][everynumber][packet-lengthsize][packetsnumber][ppsnumber]
```



注：パントポリサーパケット/秒の設定は、必ずEPCのppsパラメータの設定に合わせてください。デフォルトを維持することをお勧めします。

組み込みパケットキャプチャで利用できるパラメータの詳細については、『[Cisco IOS Embedded Packet Capture Command Reference](#)』を参照してください。

QFPの使用

パントポリサーのshowコマンドを使用して、EPC原因カテゴリにドロップがあるかどうかを確認します。

EPC値の増加が見られない場合、インターフェイスの輻輳やプラットフォームの制限など、さまざまな理由でパケットが欠落する可能性があります。

キャプチャを開始する前に、`show platform hardware active qfp datapath utilization summary` コマンドを使用して、1秒あたりのパケット数を確認します。パントポリサーと組み込みパケットキャプチャの両方で、1秒あたりのパケット数のパラメータ値を設定します。

```
Router#show platform hardware qfp active datapath utilization summary
  CPP 0:
Input:   Total (pps)      5 secs      1 min      5 min      60 min
         (bps)           0           0           0           0
         Total (pps)      200         400        392        200
Output:  Total (pps)      2           1           1           0
         (bps)          15016      9136      9144      4080
Processing: Load (pct)    1           1           1           1
```

Router#

ベスト プラクティス

より適切なキャプチャ結果を得るには、コマンド `monitor capture capture-name access-list access-list-name` を使用します。これにより、キャプチャに成功したパケットの数を増やす、関連するトラフィックのみをキャプチャできます。

代わりに、スイッチドポートアナライザ(SPAN)ベースのツールなどの代替手段を使用して、キャプチャされたパケットに関してより適切なキャプチャ結果を得ることができます。

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。