

Solucionar problemas de pacotes ausentes em uma captura de pacote no Cisco IOS XE

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Troubleshooting](#)

[O Vigilante de Punt](#)

[O Parâmetro de Captura de Pacotes Incorporados por Segundo \(pps\)](#)

[Utilização de QFP](#)

[Melhores práticas](#)

Introdução

Este documento descreve como solucionar problemas de pacotes ausentes em um EPC (Embedded Packet Capture).

Pré-requisitos

Requisitos

Familiarize-se com a Captura de Pacotes Incorporada no Cisco IOS® XE. Isso é descrito em [Configurar e Capturar Pacote Incorporado no Software](#).

Componentes Utilizados

Os exemplos deste artigo são baseados nos roteadores Cisco IOS XE.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

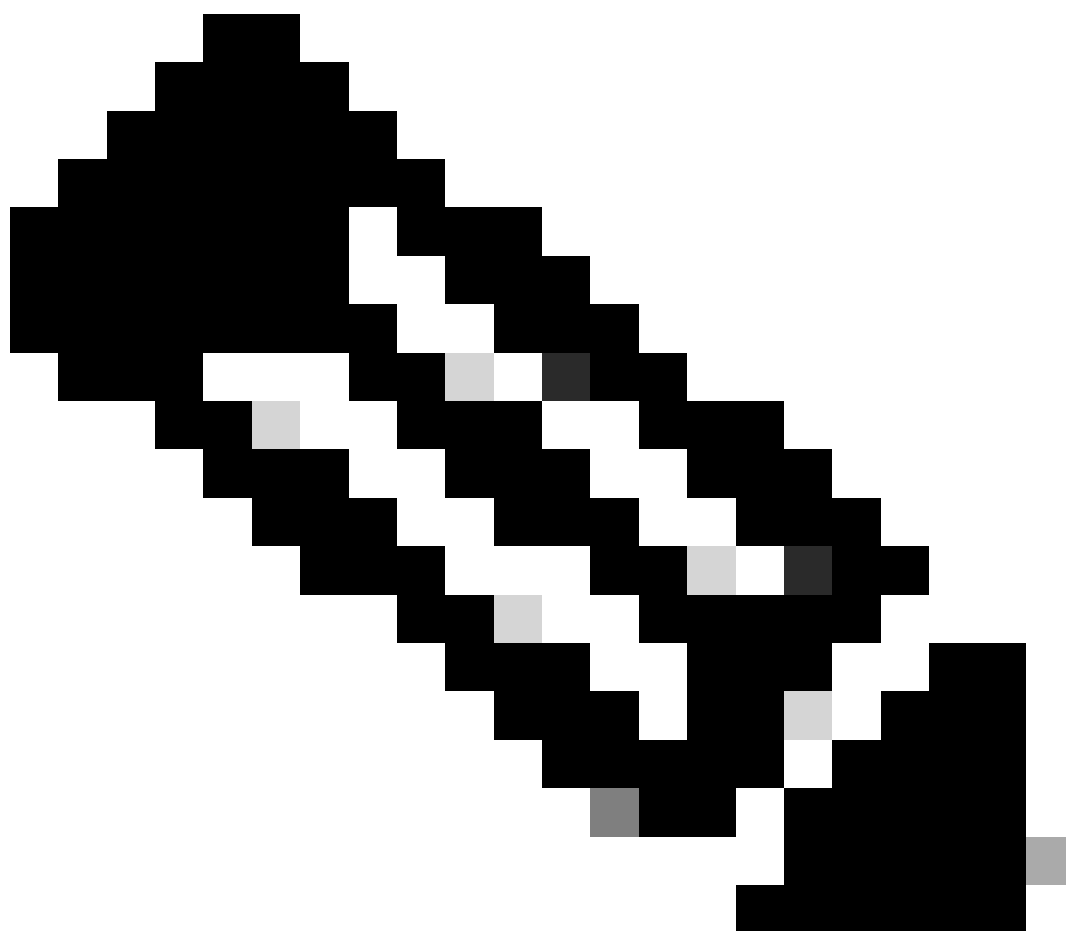
Informações de Apoio

Há cenários em que é vital capturar todos os pacotes que passam por um roteador, no entanto, o sistema Cisco IOS XE tem um mecanismo de política de punt padrão para proteger o plano de controle.

Esse mecanismo pode descartar alguns dos pacotes capturados se a limitação de política for atingida.

Além disso, há uma opção que você pode configurar para aumentar o número de pacotes por segundo (pps) a serem capturados.

Esses dois elementos desempenham um papel crucial na quantidade de pacotes capturados com êxito.



Note: Os valores padrão desses parâmetros podem depender da plataforma e da versão. Verifique as notas relevantes sobre a versão e a plataforma e, se necessário, entre em contato com o TAC da Cisco para obter assistência adicional.

Troubleshooting

O Vigilante de Punt

Esse vigilante controla os pacotes que são apontados para o plano de controle.

Use o comando `show platform hardware qfp active infrastructure punt statistics type punt-drop` para ver estatísticas detalhadas de pacotes sendo descartados devido a esse mecanismo de controle de punt.

O comando será exibido em categorias diferentes. A categoria na qual você precisa se concentrar é `PUNT_PER_CAUSE_POLICER`.

Esta é a categoria que inclui a causa EPC que se refere ao recurso Captura de pacotes incorporada.

```
---- 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
```

Em geral, as estatísticas mostram o número de pacotes punt recebidos e transmitidos entre as causas punt podem ser vistas com o comando `show platform hardware qfp active infrastructure punt statistics type per-cause`.

```
---- 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

Isso dá uma ideia de que tipo de causa de punt está consumindo principalmente o caminho de punt.

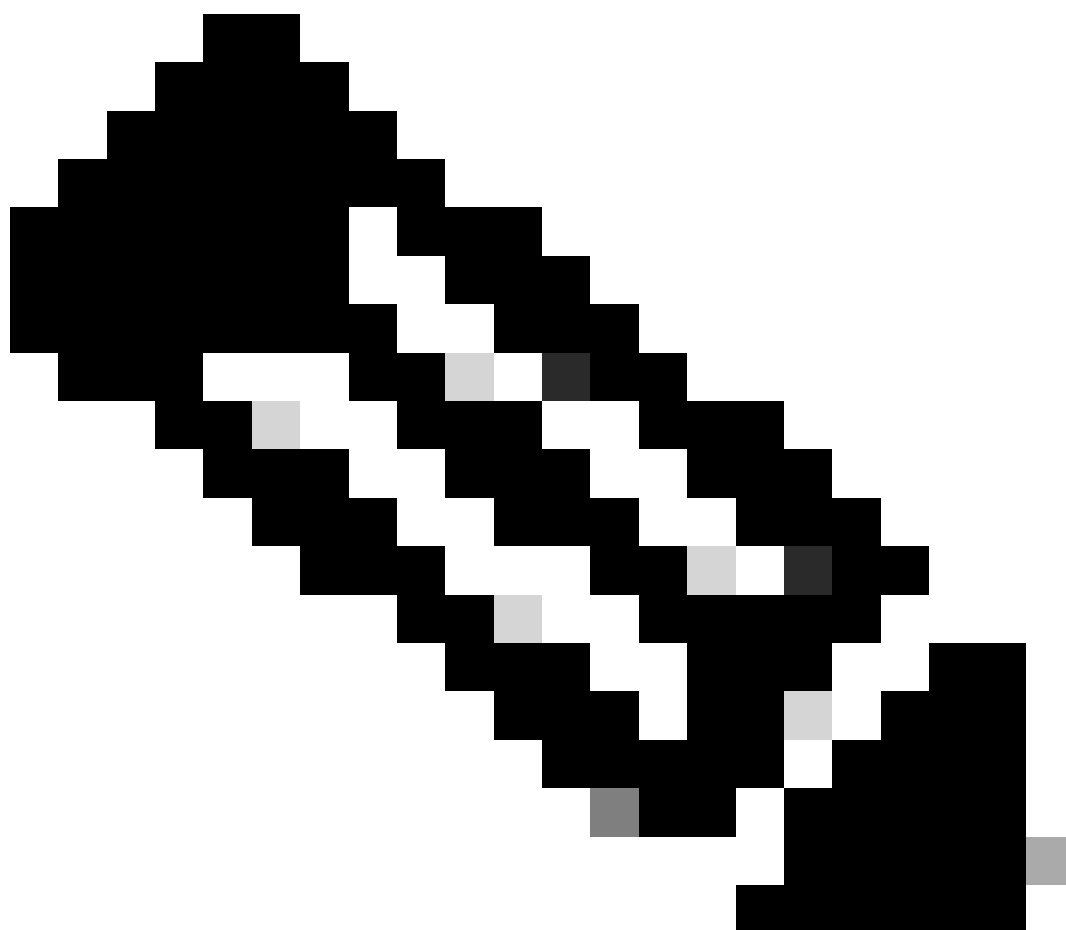
O comando `show platform software punt-policer` fornece um instantâneo de pps configurados, pacotes em conformidade, pacotes descartados por vigilante e intermitência configurada em pacotes para várias causas de punt. Neste caso, o enfoque é a causa principal do EPC.

Router#show platform software punt-policer

Per Punt-Cause Policer Configuration and Packet Counters

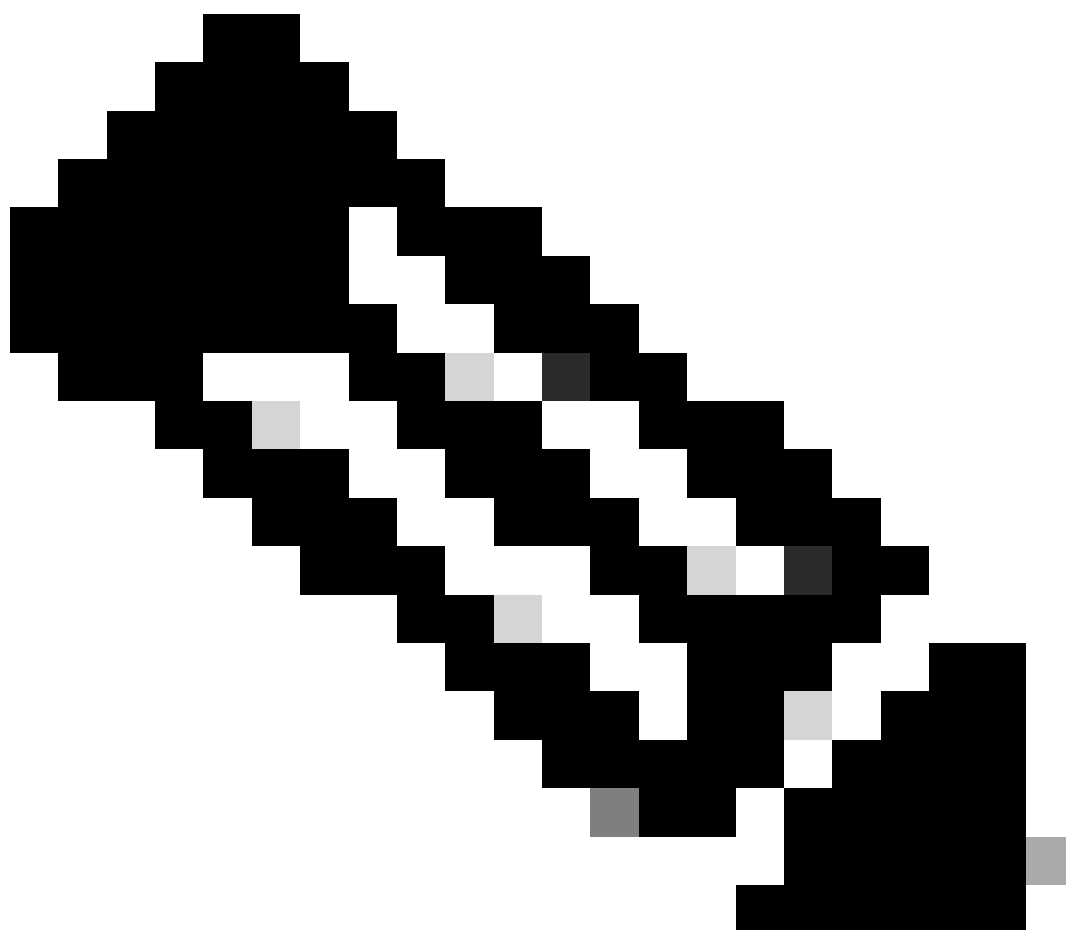
Punt Cause	Description	Config Rate(pps)		Conform Packets		Dropped Pack
		Normal	High	Normal	High	Normal

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



Note: Lembre-se de que os valores padrão para pacotes de taxa configurada e intermitência configurada podem variar entre plataformas e versões.

Os pacotes punt policer por segundo e o número de pacotes burst para uma categoria de causa punt podem ser modificados usando o comando `platform punt-policer epc <10-32000> [<1-100000000>]`.



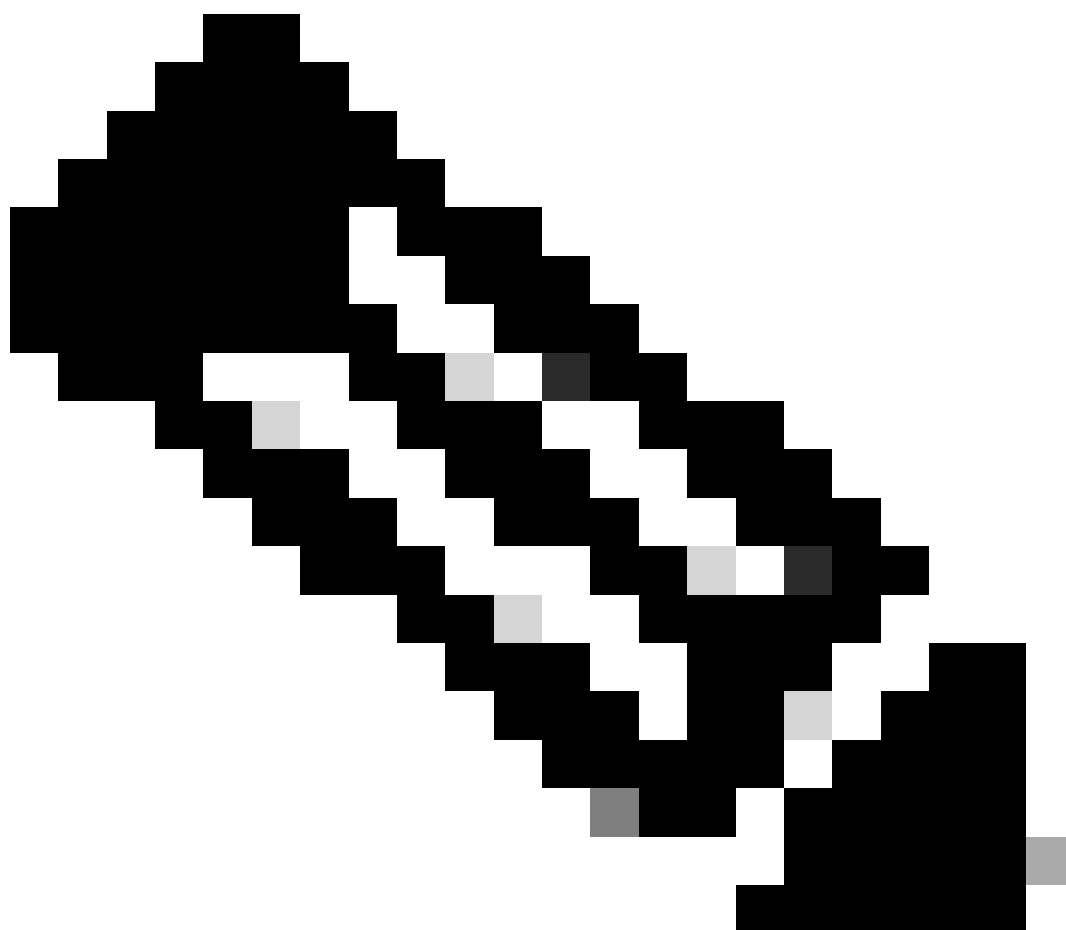
Note: Tome cuidado ao alterar os valores de punt configurados padrão, já que o vigilante de punt é um mecanismo de proteção do plano de controle.

O Parâmetro de Captura de Pacotes Incorporados por Segundo (pps)

O parâmetro pacotes por segundo limita o número de pacotes por segundo a serem capturados.

O parâmetro packets per second (pacotes por segundo) dentro da configuração de captura de pacotes incorporada pode ser indicado com o comando

```
monitorcapturecapture-namelimit[durationseconds][algarismos][tamanho de pacote][númerodepacotes][número]
```



Note: Certifique-se de alinhar a configuração de pacote de vigilante de punt por segundo com a configuração do parâmetro pps do EPC. É recomendável manter os padrões.

Informações detalhadas sobre os parâmetros disponíveis para a captura de pacotes incorporada podem ser encontradas na [Referência de Comandos de Captura de Pacotes Incorporados do Cisco IOS](#).

Utilização de QFP

Use os comandos `punt policer show` para verificar se a categoria de causa EPC tem quedas.

Se você não vir o aumento do valor de EPC, então, um motivo diferente pode causar os pacotes perdidos, como congestionamento de interface, limitação de plataforma e assim por diante.

Use o comando `show platform hardware active qfp datapath usage summary` antes de iniciar a captura para ver o número de pacotes por segundo. Configure o valor do parâmetro de pacotes por segundo no vigilante de punt e na captura de pacote incorporada.

```
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#

Melhores práticas

Para obter melhores resultados de captura, use o comando `monitor capture capture-name access-list access-list-name`. Isso permite que você capture apenas o tráfego relevante, aumentando o número de pacotes capturados com êxito.

Alternativas como ferramentas baseadas no Switched Port Analyzer (SPAN) podem ser usadas para obter melhores resultados de captura em termos de pacotes capturados.

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.