Cisco IOS XE의 패킷 캡처에서 누락된 패킷 문제 해결

목차

소개

이 문서에서는 EPC(Embedded Packet Capture)에서 누락된 패킷을 트러블슈팅하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco IOS® XE의 Embedded Packet Capture에 대해 숙지하십시오. 이 내용은 Configure [and Capture Embedded Packet on Software](#)에서 [설명합니다.](#)

사용되는 구성 요소

이 문서의 예는 Cisco IOS XE 라우터를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

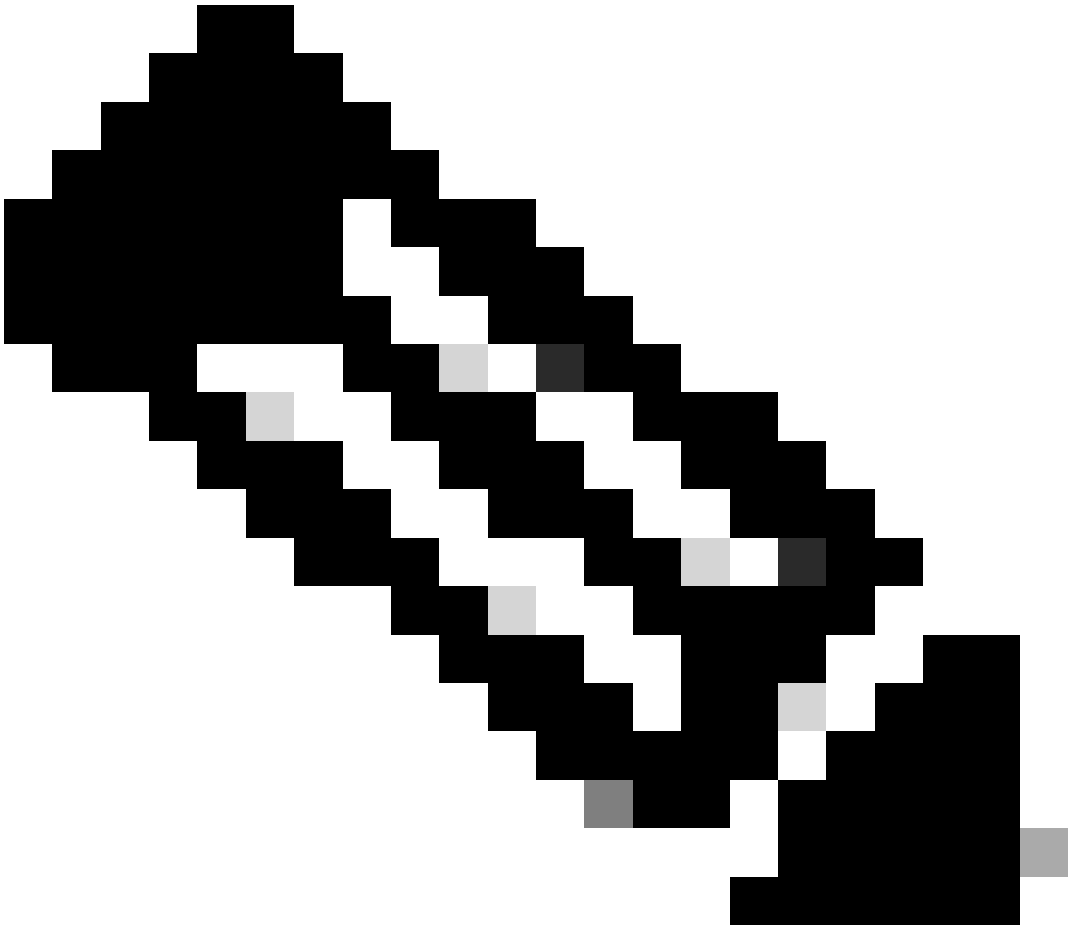
배경 정보

라우터를 통과하는 모든 패킷을 캡처하는 것이 중요한 시나리오도 있지만, Cisco IOS XE 시스템에는 컨트롤 플레인을 보호하는 기본 punt policer 메커니즘이 있습니다.

이 메커니즘은 정책 제한에 도달하면 캡처된 패킷 중 일부를 삭제할 수 있습니다.

또한 캡처할 pps(packets per second) 수를 늘리도록 구성할 수 있는 옵션도 있습니다.

이 두 요소는 성공적으로 캡처된 패킷의 양에 중요한 역할을 합니다.



> 참고: 이러한 매개변수의 기본값은 플랫폼 및 버전에 따라 다를 수 있습니다. 플랫폼 및 버전 관련 메모를 확인하고 필요한 경우 Cisco TAC에 추가 지원을 문의하십시오.

문제 해결

더 푼트 폴리서

이 폴리서는 컨트롤 플레인으로 전달되는 패킷을 제어합니다.

이 punt 제어 메커니즘으로 인해 삭제되는 패킷의 자세한 통계를 보려면 show platform hardware qfp active infrastructure punt statistics type punt-drop 명령을 사용합니다.

이 명령은 여러 카테고리로 표시됩니다. 중점적으로 살펴보아야 할 범주는

PUNT_PER_CAUSE_POLICER입니다.

이 범주는 임베디드 패킷 캡처 기능을 참조하는 EPC 원인을 포함합니다.

```
---- 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
```

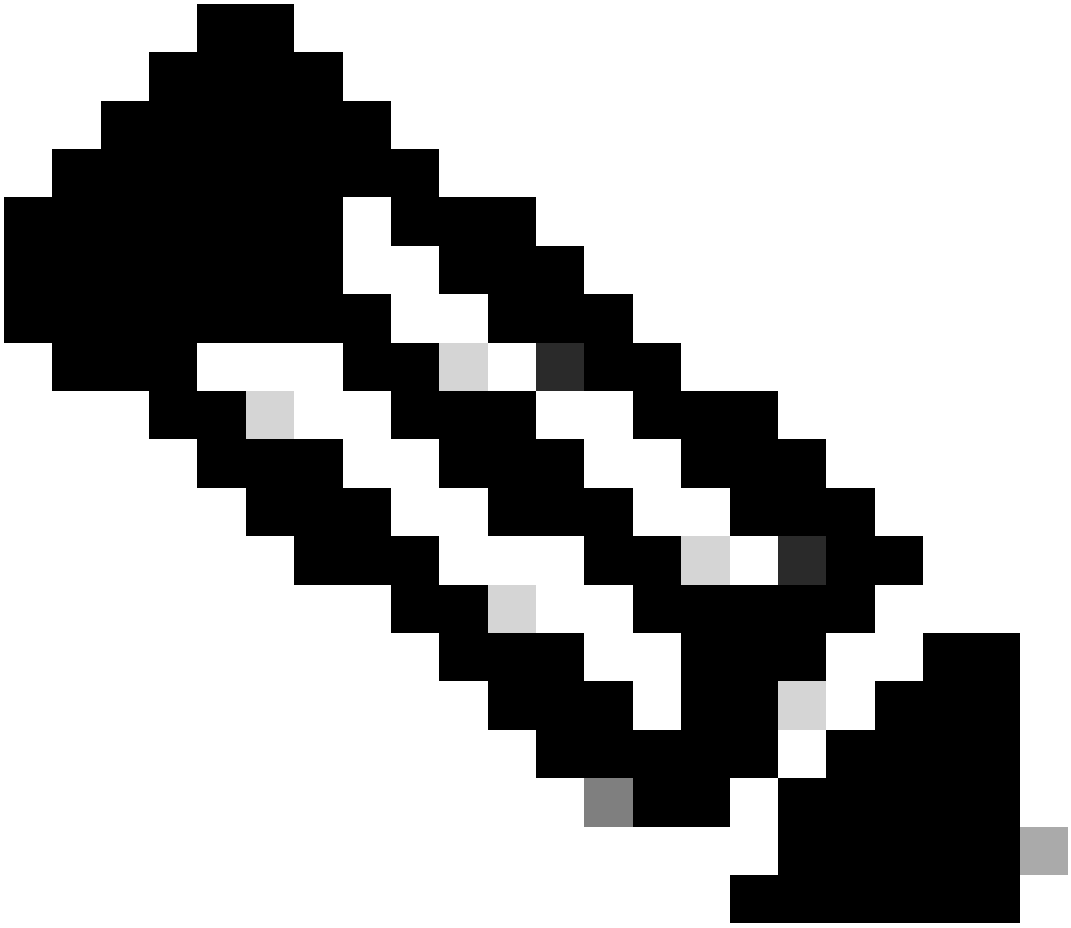
전반적으로 통계는 punt 원인 중에서 수신 및 전송된 punt 패킷의 수를 show platform hardware qfp active infrastructure punt statistics type per-cause 명령으로 확인할 수 있습니다.

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

Global Per Cause Statistics

  Number of punt causes =   165

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




      075 EPC 1527458 532817
```

이는 주로 펀트 경로를 소비하는 펀트 원인의 유형에 대한 아이디어를 제공한다.

show platform software punt-policer 명령은 구성된 pps, 컨피그레이션 패킷, 폴리서에 의해 삭제된 패킷, 다양한 punt 원인에 대한 구성된 버스트 in 패킷의 스냅샷을 제공합니다. 이 경우 EPC punt cause에 중점을 둡니다.

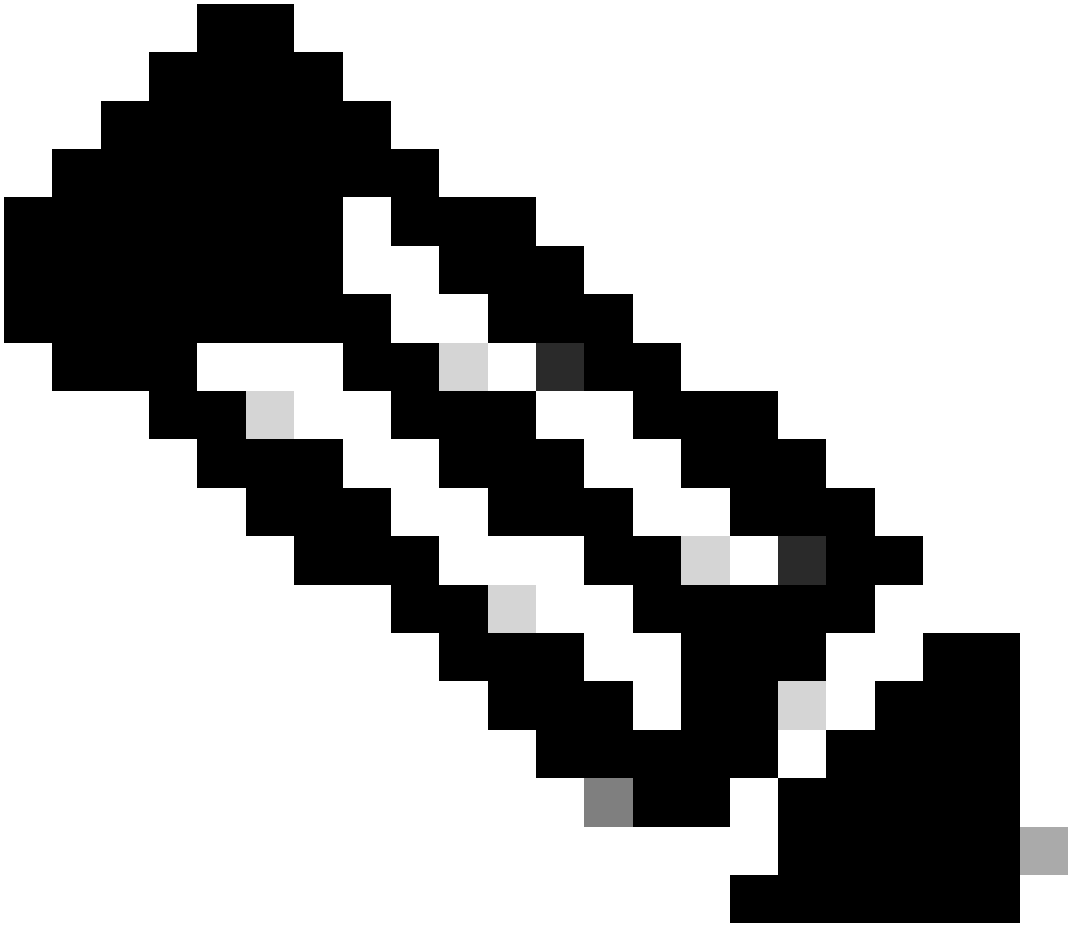
```
Router#show platform software punt-policer

Per Punt-Cause Policer Configuration and Packet Counters

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




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



참고: 구성된 속도 및 구성된 버스트 패킷의 기본값은 플랫폼 및 버전에 따라 다를 수 있습니다.

---

punt cause 카테고리에 대한 punt 폴리서 패킷 및 버스트 패킷 수는 명령 플랫폼 punt-policer epc <10-32000> [<1-100000000>]를 사용하여 수정할 수 있습니다.



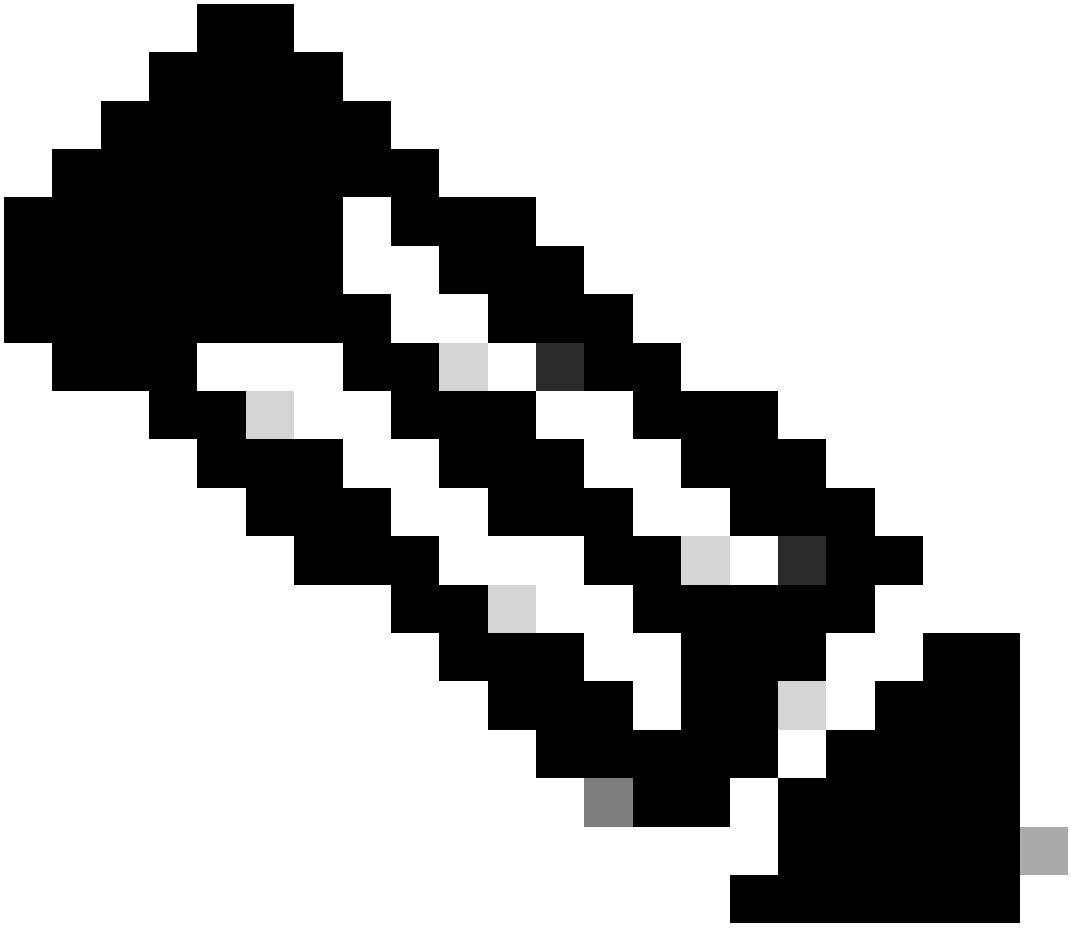
참고: punt 폴리서는 컨트롤 플레인 보호 메커니즘이므로 구성된 기본 punt 값을 변경하는 것에 주의하십시오.

Pps(Packets per Second) 포함 패킷 캡처 매개변수

packets per second 매개변수는 캡처할 초당 패킷 수를 제한합니다.

내장형 패킷 캡처 컨피그레이션 내의 초당 패킷 수를 명령으로 표시할 수 있습니다

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



참고: punt policer packet per second 컨피그레이션을 EPC의 pps 매개변수 컨피그레이션과 맞춰야 합니다. 기본값을 유지하는 것이 좋습니다.

임베디드 패킷 캡처의 사용 가능한 매개변수에 대한 자세한 내용은 Cisco IOS Embedded Packet Capture Command Reference에서 확인할 수 있습니다.

QFP 사용

punt policer show 명령을 사용하여 EPC 원인 카테고리가 삭제되었는지 확인합니다.

EPC 값이 증가하는 것을 볼 수 없는 경우, 다른 이유로 인해 인터페이스 혼잡, 플랫폼 제한 등과 같은 누락된 패킷이 발생할 수 있습니다.

캡처를 시작하기 전에 show platform hardware active qfp datapath utilization summary 명령을 사용하여 초당 패킷 수를 확인합니다. punt 폴리서 및 내장된 패킷 캡처 모두에서 초당 패킷 수 매개변수 값을 구성합니다.

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

Router#
```

모범 사례

더 나은 캡처 결과를 얻으려면 monitor capture capture -name access-list access-list-name 명령을 사용합니다. 이렇게 하면 캡처한 패킷 수를 늘려 관련 트래픽만 캡처할 수 있습니다.

대신 SPAN(Switched Port Analyzer) 기반 툴과 같은 대체 툴을 사용하여 캡처된 패킷 측면에서 더 우수한 캡처 결과를 얻을 수 있습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.