Cisco IOS XE에서 Punt Keepalive 실패 트러블슈팅

목차

[소개](#)

[사전 요구 사항](#)

- [요구 사항](#)
- [사용되는 구성 요소](#)

[배경 정보](#)

[Punt 디버그 로그 파일](#)

[LSMPI(Linux Shared Memory Punt Interface)](#)

[더 푼트 폴리서](#)

[데이터 수집을 위한 EEM(Embedded Event Manager)](#)

[실제적인 예](#)

[개선 사항](#)

소개

이 문서에서는 punt keep alive 오류를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco IOS® XE의 기본 지식

사용되는 구성 요소

이 문서는 CSR8000v, ASR1000 및 ISR4000 Series와 같은 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

Cisco IOS XE 기반 시스템의 짧은 경로는 내부 데이터 경로입니다. 컨트롤 플레인과 데이터 플레인 간의 통신이 이루어지는 경로입니다.

이 내부 경로는 라우터 사용을 위해 제어 평면 패킷을 전송하는 데 사용됩니다.

이 경로가 실패하면 로그에서 이 유형의 오류를 볼 수 있습니다.

```
%IOSXE_INFRA-4-NO_PUNT_KEEPALIVE:  Keepalive not received for 60 seconds
```

keep alive 메시지는 QFP와 RP 간의 경로 상태를 모니터링하는 메시지입니다.

이 경로는 시스템이 작동하는 데 매우 중요합니다.

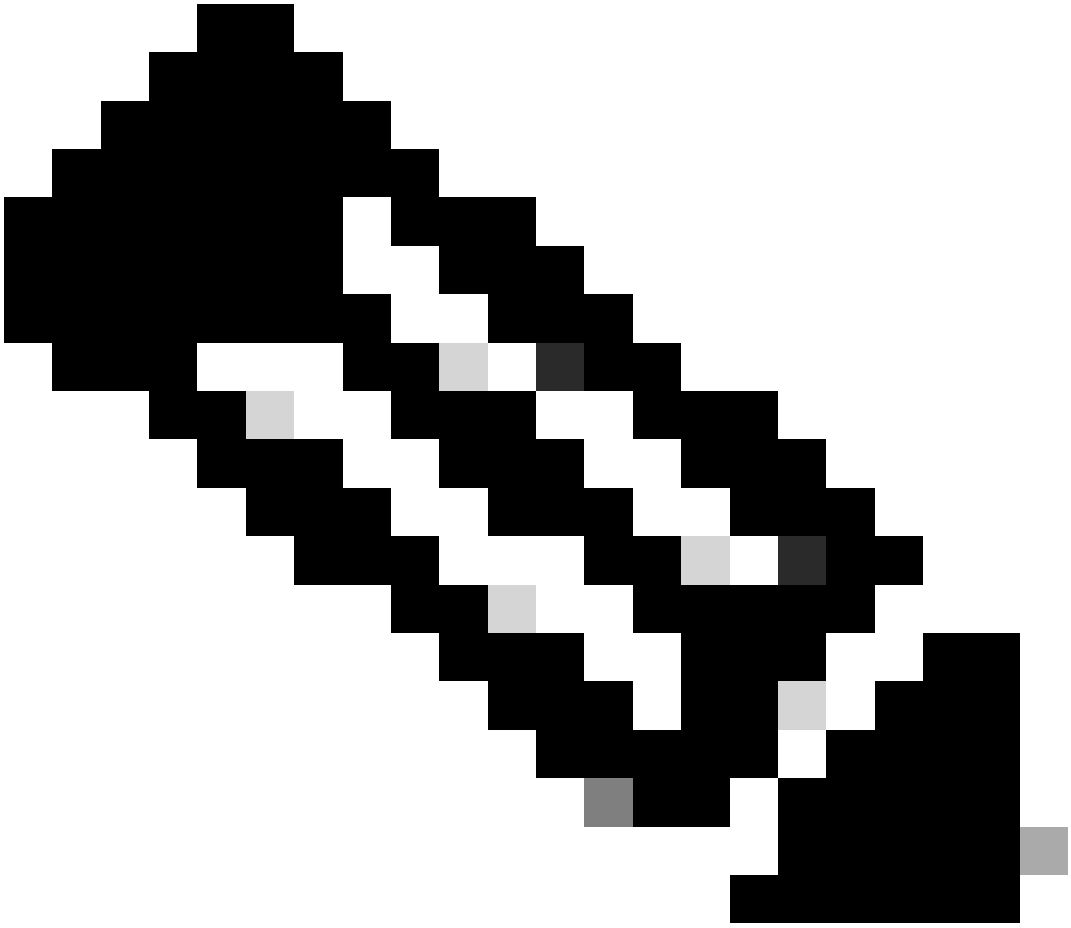
이러한 keep alives가 5분 내에 수신되지 않으면 다음과 같은 중요한 로그를 볼 수 있습니다.

```
%IOSXE_INFRA-2-FATAL_NO_PUNT_KEEPALIVE:  Keepalive not received for 300 seconds resetting
```

이 상태에서 복구하기 위해 시스템이 재설정됩니다.

Punt 디버그 로그 파일

punt keep alive 실패가 발생하고 이로 인해 재설정되면 시스템은 punt_debug.log라는 파일을 생성하며, 이 파일은 문제 시 동작을 파악하기 위해 관련 데이터를 수집합니다.



참고: punt_debug.log 파일을 생성하기 위해 최신 Cisco IOS XE 소프트웨어 릴리스로 시스템을 최신 상태로 유지해야 합니다.

이 파일에는 여러 카운터를 이해하기 위해 여러 번 실행되는 이러한 명령이 포함되어 있습니다.

show platform software infra punt-keepalive

show platform software infra lsmpi

show platform software infrastructure lsmpi driver

show platform software infra lsmpi bufusage

show platform software punt-policer

show platform software status control-processor 개요

show process cpu platform sorted

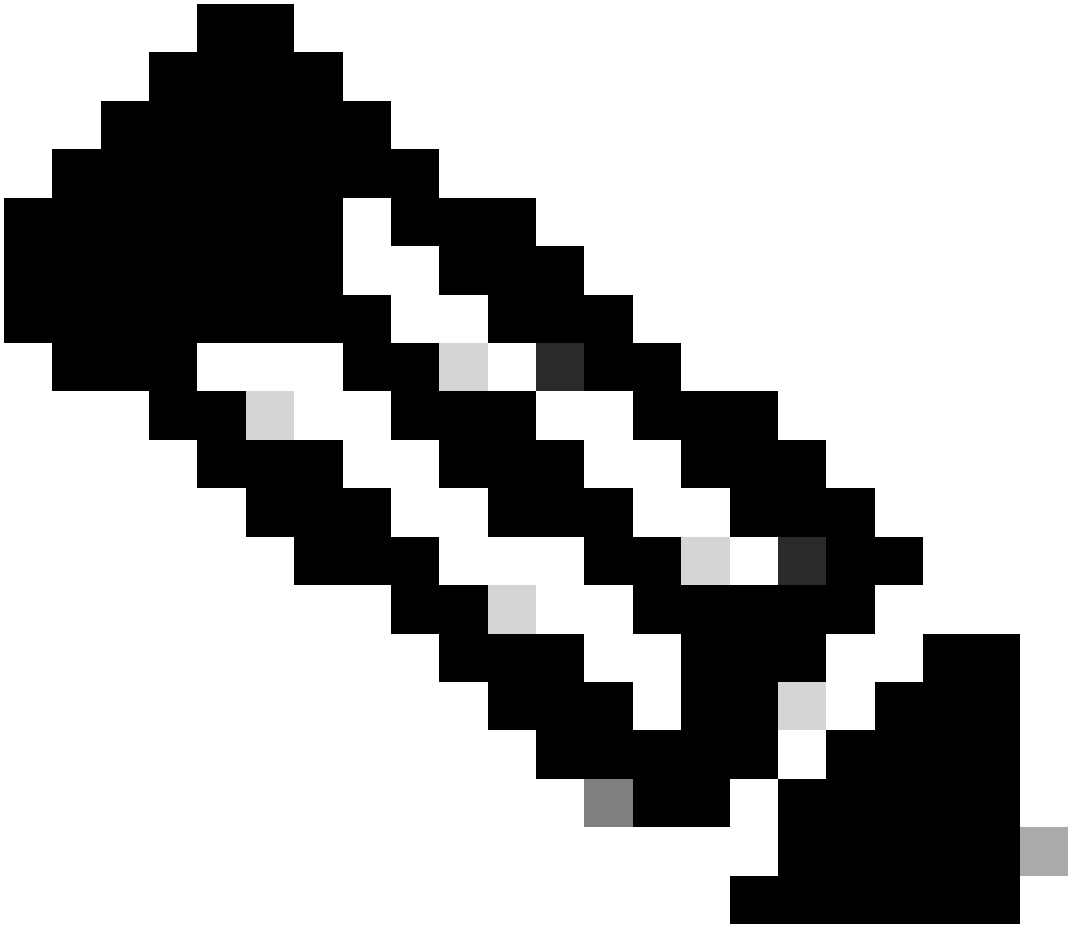
플랫폼 소프트웨어 인프라 펀트 표시

show platform hardware qfp active statistics drop(플랫폼 하드웨어 qfp 활성 통계 표시)

show platform hardware qfp active infra punt statistics type per-cause

show platform hardware qfp active infrastructure bqs queue output default all

---



참고: punt_debug.log 내에서 오류 표시기와 문제를 일으킬 수 있는 많은 양의 패킷에 초점을 맞춥니다.

LSMPI(Linux Shared Memory Punt Interface)

이 구성 요소는 포워딩 프로세서에서 라우팅 프로세서로 패킷 및 메시지를 전송하는 데 사용됩니다.

더 푼트 폴리서

punt 폴리서는 시스템이 컨트롤 플레인 패킷을 보호하고 폴리싱할 수 있도록 하는 컨트롤 플레인 보호 메커니즘입니다.

show platform software punt-policer 명령을 사용하면 conform 패킷과 이 폴리서로 인해 삭제된 를 확인할 수 있습니다.

```
 ----------------- show platform software punt-policer -----------------


Per Punt-Cause Policer Configuration and Packet Counters


Punt                                Config Rate(pps)     Conform Packets                  Dropped Packe
Cause  Description                   Normal   High     Normal           High             Normal
-------------------------------------------------------------------------------------------------------
  2    IPv4 Options                   874      655      0                0                0
  3    Layer2 control and legacy      8738     2185     0                0                0
  4    PPP Control                    437      1000     0                0                0
  -- snip : output omitted for brevity  --
```

명령 show platform software infrastructure punt는 punt 원인에 대한 카운터 데이터를 표시합니다.

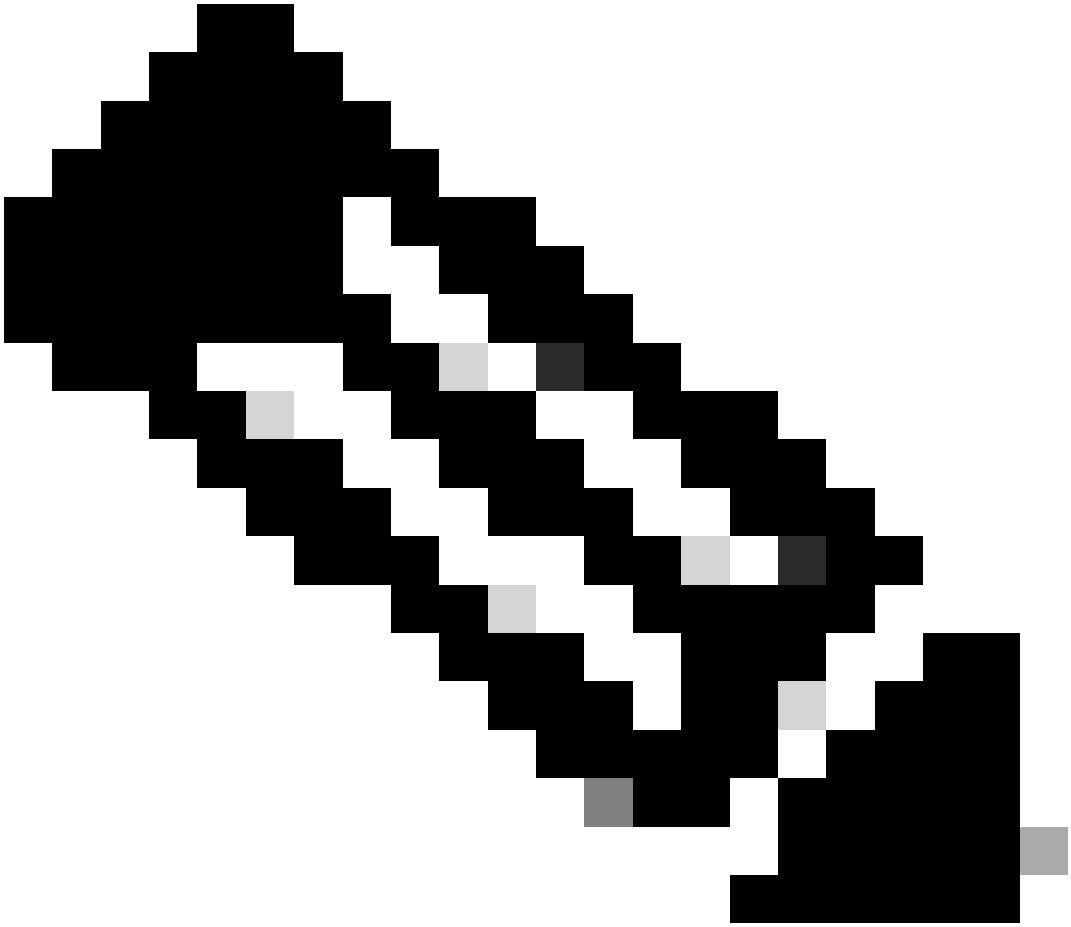
```
------------------ show platform software infrastructure punt ------------------


LSMPI interface internal stats:
enabled=0, disabled=0, throttled=0, unthrottled=0, state is ready
Input Buffers = 51181083
Output Buffers = 51150283
-- snip : output omitted for brevity  --
EPC CP RX Pkt cleansed 0
Punt cause out of range 0
IOSXE-RP Punt packet causes:
     3504959 ARP request or response packets
          27 Incomplete adjacency packets
-- snip : output omitted for brevity  --

   FOR_US Control IPv4 protcol stats:
        2369262 TCP packets

   FOR_US Control IPv6 protcol stats:
           6057 ICMPV6 packets
Packet histogram(500 bytes/bin), avg size in 119, out 95:
 Pak-Size      In-Count        Out-Count
      0+:      51108211         51144723
    500+:         22069             2632
   1000+:          2172                0
   1500+:          3170                0
```

이 데이터는 punt keep alive 경로에 영향을 줄 수 있는 요소를 파악하는 데 적합합니다.

데이터 수집을 위한 EEM(Embedded Event Manager)

punt_debug.log가 문제를 진단하기에 충분한 데이터를 제공하지 않는 경우 EEM 스크립팅을 사용하여 문제 발생 시 더 많은 데이터 포인트를 얻을 수 있습니다.

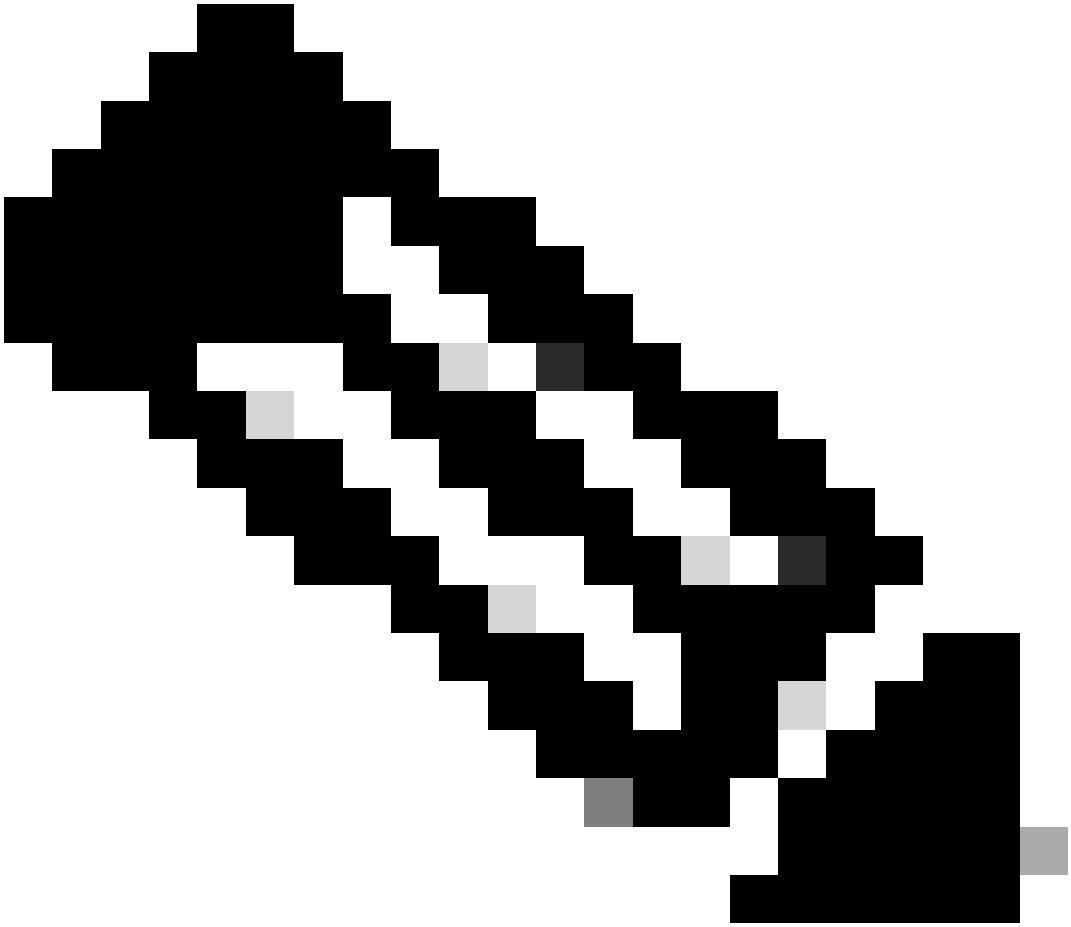
```
event manager applet punt_script authorization bypass
event syslog pattern "IOSXE_INFRA-4-NO_PUNT_KEEPALIVE" maxrun 1000
action 0.0 cli command "enable"
action 0.1 set i "0"
action 0.2 cli command "test platform software punt-keepalive ignore-fault"
action 0.3 while $i lt 10
action 0.4 syslog msg "iteration $i"
action 0.9 cli command "show clock | append bootflash:qfp_lsmpi.txt"
action 1.0 cli command "show platform software infrastructure lsmpi | append bootflash:qfp_lsmpi.txt"
action 1.1 cli command "show platform software infrastructure lsmpi driver | append bootflash:qfp_lsmpi
action 1.2 cli command "show platform software infrastructure lsmpi driver 0 | append bootflash:qfp_lsm
action 1.3 cli command "show platform software infrastructure lsmpi bufusage | append bootflash:qfp_lsm
action 1.4 cli command "show platform software infrastructure lsmpi bufusage 0 | append bootflash:qfp_l
action 1.5 cli command "show platform software infrastructure punt-keepalive | append bootflash:qfp_lsm
action 1.6 cli command "show platform software infrastructure punt | append bootflash:qfp_lsmpi.txt"
action 1.7 cli command "show platform software punt-policer | append bootflash:qfp_lsmpi.txt"
action 1.8 cli command "show platform hardware qfp active infrastructure punt stat type per-cause | app
action 1.9 cli command "show platform hardware qfp active infrastructure punt statistics type punt-drop
action 1.a cli command "show platform hardware qfp active infrastructure punt statistics type inject-dr
action 1.b cli command "show platform hardware qfp active infrastructure bqs queue output default inter
action 1.c cli command "show platform hardware qfp active statistics drop | append bootflash:qfp_lsmpi.
action 1.d cli command "show platform hardware qfp active datapath utilization | append bootflash:qfp_l
action 1.e cli command "show platform hardware qfp active datapath infrastructure sw-hqf | append bootf
action 1.f cli command "show platform hardware qfp active datapath infrastructure sw-distrib | append b
action 1.g cli command "show platform hardware qfp active datapath infrastructure sw-pktmem | append bo
action 1.h cli command "show platform software status control-processor brief | append bootflash:qfp_ls
action 2.0 increment i
action 2.1 wait 3
action 2.4 end
action 3.0 syslog msg "End of data collection. Please transfer the file at bootflash:qfp_lsmpi.txt"
action 5.0 cli command "debug platform hardware qfp active datapath crashdump"
```



참고: 스크립트에 포함된 명령은 구성된 플랫폼에 따라 달라집니다.

이 스크립트를 사용하면 문제 발생 시간 동안 lsmpi, 리소스 및 펀트 상태를 이해할 수 있습니다.

EEM 스크립트에는 개발자 팀 및 TAC에 필요한 qfp 코어 덤프를 생성하는 명령 디버그 플랫폼 하드웨어 qfp 활성 데이터 경로 크래시 덤프가 포함되어 있습니다.



참고: Cisco TAC에 케이스를 접수할 경우 스크립트로 생성한 코어 파일을 제공하십시오.

패킷 추적이 필요한 경우 이 수정 사항을 스크립트에 추가할 수 있습니다.

먼저 EEM 스크립트에서 수행할 수 있는 패킷 추적 컨피그레이션을 설정합니다.

debug platform packet-trace packet 8192 fia-trace circular
둘 다 플랫폼 상태 디버깅
debug platform packet-trace copy packet both L2

그런 다음 EEM 스크립트 내에서 다음 작업을 수행하여 시작 및 중지합니다.

action 6.2 cli 명령 "debug platform condition start"
작업 6.3 대기 8
action 6.4 cli 명령 "debug platform condition stop"

그런 다음 이러한 명령이 포함된 데이터를 별도의 파일에 덤프합니다.

action 6.5 cli 명령 "show platform packet-trace statistics | bootflash 추가:traceAll.txt"
action 6.6 cli 명령 "show platform packet-trace summary | bootflash 추가:traceAll.txt"
action 6.7 cli 명령 "show platform packet-trace packet all decode | bootflash 추가:traceAll.txt"

이 패킷 추적 작업 로직은 EEM 스크립트 내에서 while 주기의 end 문 바로 뒤에 추가됩니다.

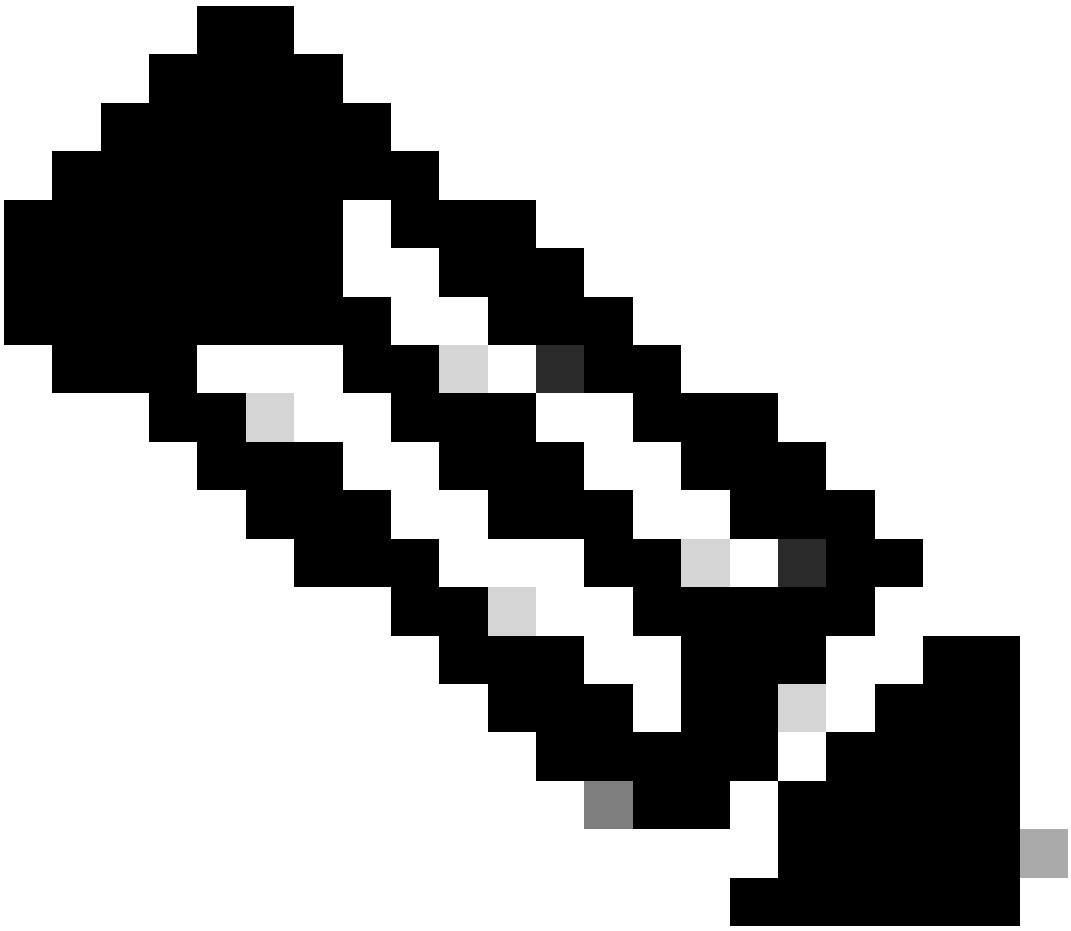
이 스크립트를 사용하면 문제를 일으킬 수 있는 패킷 유형을 파악할 수 있습니다.

패킷 추적은 Troubleshoot with the IOS XE Datapath 패킷 추적 기능에 설명된 기능입니다

실제적인 예

CSR8000v가 계속 재부팅됩니다.

시스템 보고서를 추출한 후 크래시덤프를 관찰할 수 있으며, 스택 추적 내에서 punt keep alive 관련 기능을 나타내는 iosd 코어 파일을 관찰할 수 있습니다.



참고: 스택 추적 디코딩의 경우 TAC 지원이 필요합니다.

그러나 crashinfo 파일은 일반 텍스트이며 다음과 같은 증상을 볼 수 있습니다.

```
Jan 15 14:29:41.756 AWST: %IOSXE_INFRA-4-NO_PUNT_KEEPALIVE:  Keepalive not received for 160 seconds
Jan 15 14:30:01.761 AWST: %IOSXE_INFRA-4-NO_PUNT_KEEPALIVE:  Keepalive not received for 180 seconds
Jan 15 14:30:21.766 AWST: %IOSXE_INFRA-4-NO_PUNT_KEEPALIVE:  Keepalive not received for 200 seconds
Jan 15 14:30:41.776 AWST: %IOSXE_INFRA-4-NO_PUNT_KEEPALIVE:  Keepalive not received for 220 seconds
Jan 15 14:31:01.780 AWST: %IOSXE_INFRA-4-NO_PUNT_KEEPALIVE:  Keepalive not received for 240 seconds
Jan 15 14:31:41.789 AWST: %IOSXE_INFRA-4-NO_PUNT_KEEPALIVE:  Keepalive not received for 280 seconds
Jan 15 14:32:01.791 AWST: %IOSXE_INFRA-4-NO_PUNT_KEEPALIVE:  Keepalive not received for 300 seconds
Jan 15 14:32:01.791 AWST: %IOSXE_INFRA-2-FATAL_NO_PUNT_KEEPALIVE:  Keepalive not received for 300 secon

%Software-forced reload

Exception to IOS Thread:
Frame pointer 0x7F0AE0EE29A8, PC = 0x7F0B342C16D2

UNIX-EXT-SIGNAL: Aborted(6), Process = PuntInject Keepalive Process
-Traceback= 1#7b5996c3
```

영향을 받는 프로세스는 PuntInject Keepalive 프로세스입니다.

keepalive가 300초 임계값 마크에 도달하면 시스템에서 중단 신호를 트리거해야 합니다.

punt_debug.log는 show platform software infrastructure lsmpi driver:

```
Reason for TX drops (sticky):
    Bad packet len   : 0
    Bad buf len      : 0
    Bad ifindex      : 0
    No device        : 0
    No skbuff        : 0
    Device xmit fail : 82541   >>>>>>>>>>>>>>>>>>>> Tx failure
```

이는 일반적인 오류입니다.

이 카운터는 파일에서 가져온 여러 샘플 내에서 증가합니다.

리소스, punt data path 및 기타 인프라 관련 명령에 대한 추가 데이터를 얻기 위해 EEM 스크립트가 제공되었습니다.

lsmpi 트래픽 punt 카운터를 검사하면 EIGRP 컨트롤 플레인 패킷이 눈에 띄게 표시됩니다. 이는 us 패킷으로 식별된 패킷입니다.

```
17660574 For-us data packets
543616 RP<->QFP keepalive packets
1004 Glean adjacency packets
3260636 BFD control packets
122523839 For-us control packets<<<<
```

```
FOR_US Control IPv4 protcol stats:
153551 TCP packets
2663105 GRE packets
104394559 EIGRP packets<<<<
```

나중에 하이퍼바이저가 초과 서브스크립션되어 기본 컴퓨팅 리소스에 영향을 주는 것으로 나타났습니다.

CSR8000v는 다른 하이퍼바이저에 구축되었으며, 이는 문제를 완화하는 데 도움이 되었습니다.

개선 사항

Cisco 버그 ID CSCwf를 통해 Cisco IOS XE 17.15 버전부터 자동 qfp 코어 파일 생성이 향상되었습니다85505

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.