Catalyst 9000 스위치에서 FED CPU 패킷 캡처 구성

목차

소개

이 문서에서는 FED(Forwarding Engine Driver) CPU 캡처 툴을 사용하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 Cisco IOS 16.X 이상을 실행하는 Catalyst 스위칭 플랫폼으로 제한됩니다.

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

FED CPU 패킷 캡처 툴은 컨트롤 플레인을 통과하는 데이터를 식별하고 **퓬트**(ASIC에서 CPU로 패킷) 또는 **주입(CPU에서 ASIC로 패킷)** 트래픽에 대한 정보를 제공합니다.

- 예를 들어, 이 도구는 CoPP(컨트롤 플레인 폴리서)가 시작하도록 트리거한 트래픽을 식별하여 CPU를 보호하기 위해 유효한 트래픽이 삭제되도록 하는 데 유용합니다.

용어

- **FED(Forwarding Engine Driver)**: Cisco IOS-XE에서 명령을 받고 하드웨어 ASIC를 프로그래밍합니다. Catalyst 스위치의 소프트웨어 및 하드웨어 구성 요소 간의 브리지 역할을 합니다.
- **CP(Control Plane):** Catalyst 스위치의 CPU와 관련된 기능 및 트래픽 수집. 여기에는 STP(Spanning Tree Protocol), HSRP(Hot Standby Router Protocol), 스위치를 대상으로 하거나 스위치에서 전송되는 라우팅 프로토콜과 같은 트래픽이 포함될 수 있습니다.
- **DP(Data Plane):** 소프트웨어 스위칭이 아니라 하드웨어가 포워딩되는 ASIC 및 트래픽을 포함합니다.
- **Punt:** 데이터 플레인에서 CPU로 전송된 패킷의 작업입니다.
- **Inject:**CPU에서 CPU로 하향 전송된 패킷의 작업

FED CPU 패킷 캡처 구성

구성 옵션에 이 표를 사용합니다.

정의	설정
punt 또는 inject에 대한 패킷 캡처의 기본 설정	디버그 플랫폼 소프트웨어 fed 스위치 active <punt | inject> packet-capture <start | 중지>
캡처된 패킷 표시	show platform software fed switch active <punt | inject> 패킷 캡처 <| 세부 정보>
버퍼 크기 및 캡처 유형 정의	디버그 플랫폼 소프트웨어 fed 스위치 active <punt | inject> packet-capture buffer [circular] limit <#packets>
표시된 패킷에 대한 캡처 필터링 정의	show platform software fed switch active <punt | inject> packet-cap display-filter <filter> • 논리적 && , || 및 대괄호 예: "cdp || (ipv.src== 10.1.1.11 && tcp == 179) || stp" • 표준 네트워크 헤더 기반 필터링 외에 일부 플랫폼별 필터가 추 었습니다. 또한 표준 제품과 함께 혼합될 수도 있습니다. 예를 들 물리적 인터페이스 ID 0x44에서 수신된 ARP 패킷입니다. • 이는 Wireshark가 아니므로 모든 Wireshark 필터를 지원하지 않 다. display-filter-help 명령을 사용하여 지원되는 필터를 확인할 습니다.
캡처 상태 표시	show platform software fed switch active <punt | inject> packet-cap 상태

기본 컨피그레이션 예

이 도구는 활성화된 이후 최대 4096개(기본 설정)의 펀트되거나 삽입된 패킷을 캡처하기 위한 버퍼를 생성합니다.

```
Cat9k#debug platform software fed switch active punt packet-capture start
Punt packet capturing started.
```

```
Cat9k#debug platform software fed switch active punt packet-capture stop
Punt packet capturing stopped. Captured 263 packet(s)

Cat9k#show platform software fed switch active punt packet-capture brief
Punt packet capturing: disabled. Buffer wrapping: disabled
Total captured so far: 263 packets. Capture capacity : 4096 packets

------ Punt Packet Number: 1, Timestamp: 2020/04/10 18:15:53.499 ------
 interface : physical: GigabitEthernet1/0/1[if-id: 0x00000008], pal: Vlan20 [if-id: 0x00000076]
 metadata  : cause: 29 [RP handled ICMP], sub-cause: 0, q-no: 6, linktype: MCP_LINK_TYPE_IP [1]
 ether hdr : dest mac: 084f.a940.fa56, src mac: 380e.4d77.4f66
 ether hdr : vlan: 20, ethertype: 0x8100
 ipv4  hdr : dest ip: 10.11.0.3, src ip: 10.11.0.3
 ipv4  hdr : packet len: 40, ttl: 255, protocol: 17 (UDP)
 udp   hdr : dest port: 3785, src port: 49152

------ Punt Packet Number: 2, Timestamp: 2020/04/10 18:15:53.574 ------
 interface : physical: GigabitEthernet1/0/1[if-id: 0x00000008], pal: Vlan20 [if-id: 0x00000076]
 metadata  : cause: 45 [BFD control], sub-cause: 0, q-no: 27, linktype: MCP_LINK_TYPE_IP [1]
 ether hdr : dest mac: 084f.a940.fa56, src mac: 380e.4d77.4f66
 ether hdr : vlan: 20, ethertype: 0x8100
 ipv4  hdr : dest ip: 10.11.0.1, src ip: 10.11.0.1
 ipv4  hdr : packet len: 40, ttl: 254, protocol: 17 (UDP)

Cat9k#show platform software fed switch active punt packet-capture detailed
F340.04.11-9300-1#$e fed switch active punt packet-capture detailed
Punt packet capturing: disabled. Buffer wrapping: disabled
Total captured so far: 263 packets. Capture capacity : 4096 packets

------ Punt Packet Number: 1, Timestamp: 2020/04/10 18:15:53.499 ------
 interface : physical: GigabitEthernet1/0/1[if-id: 0x00000008], pal: Vlan20 [if-id: 0x00000076]
 metadata  : cause: 29 [RP handled ICMP], sub-cause: 0, q-no: 6, linktype: MCP_LINK_TYPE_IP [1]
 ether hdr : dest mac: 084f.a940.fa56, src mac: 380e.4d77.4f66
 ether hdr : vlan: 20, ethertype: 0x8100
 ipv4  hdr : dest ip: 10.11.0.3, src ip: 10.11.0.3
 ipv4  hdr : packet len: 40, ttl: 255, protocol: 17 (UDP)
 udp   hdr : dest port: 3785, src port: 49152

 Packet Data Hex-Dump (length: 68 bytes) :
   084FA940FA56380E  4D774F668100C014  080045C00028CC8E  0000FF11DA5A0A0B
   00030A0B0003C000  0EC90014B6BE0000  0000000000010009  6618000000000000
   D54ADEEB

 Doppler Frame Descriptor :
   fdFormat                 = 0x4           systemTtl                = 0xc
   loadBalHash1             = 0x10          loadBalHash2             = 0x2
   spanSessionMap           = 0             forwardingMode           = 0
   destModIndex             = 0x1           skipIdIndex              = 0x38
   srcGpn                   = 0x1           qosLabel                 = 0
   srcCos                   = 0x4           ingressTranslatedVlan    = 0x5
   bpdu                     = 0             spanHistory              = 0
   sgt                      = 0             fpeFirstHeaderType       = 0
   srcVlan                  = 0x14          rcpServiceId             = 0x3
   wccpSkip                 = 0             srcPortLeIndex           = 0
   cryptoProtocol           = 0             debugTagId               = 0
   vrfId                    = 0             saIndex                  = 0
   pendingAfdLabel          = 0             destClient               = 0xb
   appId                    = 0             finalStationIndex        = 0
   decryptSuccess           = 0             encryptSuccess           = 0
   rcpMiscResults           = 0             stackedFdPresent         = 0
   spanDirection            = 0             egressRedirect           = 0x1
   redirectIndex            = 0             exceptionLabel           = 0x20
   destGpn                  = 0x1           inlineFd                 = 0x1
```

```
   suppressRefPtrUpdate      = 0             suppressRewriteSideEfects = 0
   cmi2                      = 0x320         currentRi                 = 0x1
   currentDi                 = 0             dropIpUnreachable         = 0
   srcZoneId                 = 0             srcAsicId                 = 0
   originalDi                = 0x5338        originalRi                = 0
   srcL3IfIndex              = 0x2f          dstL3IfIndex              = 0x2f
   dstVlan                   = 0             frameLength               = 0x44
   fdCrc                     = 0x4c          tunnelSpokeId             = 0
   isPtp                     = 0             ieee1588TimeStampValid    = 0
   ieee1588TimeStamp55_48    = 0             lvxSourceRlocIpAddress    = 0
   sgtCachingNeeded          = 0

 Doppler Frame Descriptor Hex-Dump :
   0000010044004C02  8004424C00000100  0000000040000100  0000230514000000
   0000000000000030  0020000000000B00  380000532F000100  0000002F00000000
```

캡처의 현재 상태를 확인하려면 다음 명령을 사용할 수 있습니다.

```
Cat9k#show platform software fed switch active punt packet-capture status
Punt packet capturing: enabled. Buffer wrapping: enabled (wrapped 0 times)
Total captured so far: 110 packets. Capture capacity : 6000 packets
```

패킷 캡처 수정

punt/inject FED 패킷 캡처 툴이 향상되어 패킷 버퍼 크기 및 유형 컨피그레이션 조정으로 선형 또는 원형 패킷 캡처를 생성할 수 있습니다.

```
Cat9k#debug platform software fed switch active punt packet-capture buffer ?
  circular  Circular capture
  limit     Number of packets to capture
```

선형 패킷 캡처

첫 번째 버퍼 컨피그레이션 옵션은 버퍼로 전송되는 패킷 수(기본 크기는 4096개 패킷)를 제한하는 것입니다. 버퍼 크기 제한에 도달하면 더 이상 패킷이 수집되지 않습니다(버퍼 래핑 없음).

```
Cat9k#debug platform software fed switch active punt packet-capture buffer limit ?
  <256-16384>  Number of packets to capture
Cat9k#debug platform software fed switch active punt packet-capture buffer limit 5000
Punt PCAP buffer configure: one-time with buffer size 5000...done
```

순환 패킷 캡처

두 번째 버퍼 구성 옵션은 패킷에 대한 순환 버퍼를 설정하는 것입니다(기본 버퍼 크기는 4096개 패킷). 순환 버퍼 크기 제한에 도달하면 이전 데이터가 버퍼의 새 데이터로 교체됩니다(버퍼 래핑).

```
Cat9k#debug platform software fed switch active punt packet-capture buffer circular ?
  limit  Number of packets to capture

Cat9k#debug platform software fed switch active punt packet-capture buffer circular limit ?
  <256-16384>  Number of packets to capture
Cat9k#debug platform software fed switch active punt packet-capture buffer circular limit 6000
Punt PCAP buffer configure: circular with buffer size 6000...done
```

그런 다음 패킷 캡처를 동일한 매개변수로 다시 실행할 수 있습니다.

```
Cat9k#debug platform software fed switch active punt packet-capture start
Punt packet capturing started.

Cat9k#show platform software fed switch active punt packet-capture status
Punt packet capturing: enabled. Buffer wrapping: enabled (wrapped 0 times)
Total captured so far: 110 packets. Capture capacity : 6000 packets

Cat9k#debug platform software fed switch active punt packet-capture stop
Punt packet capturing stopped. Captured 426 packet(s)

Cat9k#show platform software fed switch active punt packet-capture brief
Punt packet capturing: disabled. Buffer wrapping: enabled (wrapped 0 times)
Total captured so far: 426 packets. Capture capacity : 6000 packets

------ Punt Packet Number: 1, Timestamp: 2020/04/10 23:37:14.884 ------
 interface : physical: GigabitEthernet1/0/1[if-id: 0x00000008], pal: Vlan20 [if-id: 0x00000076]
 metadata  : cause: 29 [RP handled ICMP], sub-cause: 0, q-no: 6, linktype: MCP_LINK_TYPE_IP [1]
 ether hdr : dest mac: 084f.a940.fa56, src mac: 380e.4d77.4f66
 ether hdr : vlan: 20, ethertype: 0x8100
 ipv4  hdr : dest ip: 10.11.0.3, src ip: 10.11.0.3
 ipv4  hdr : packet len: 40, ttl: 255, protocol: 17 (UDP)
 udp   hdr : dest port: 3785, src port: 49152

------ Punt Packet Number: 2, Timestamp: 2020/04/10 23:37:14.899 ------
 interface : physical: GigabitEthernet1/0/1[if-id: 0x00000008], pal: Vlan20 [if-id: 0x00000076]
 metadata  : cause: 45 [BFD control], sub-cause: 0, q-no: 27, linktype: MCP_LINK_TYPE_IP [1]
 ether hdr : dest mac: 084f.a940.fa56, src mac: 380e.4d77.4f66
 ether hdr : vlan: 20, ethertype: 0x8100
 ipv4  hdr : dest ip: 10.11.0.1, src ip: 10.11.0.1
 ipv4  hdr : packet len: 40, ttl: 254, protocol: 17 (UDP)
 udp   hdr : dest port: 3785, src port: 49152
--snip--
```

표시 및 캡처 필터링

패킷 표시 및 필터 옵션을 허용하도록 Punt/Inject FED 패킷 캡처 툴이 향상되었습니다.

디스플레이 필터링

필터 없는 캡처가 완료되면 관심 있는 정보만 표시하도록 검토할 수 있습니다.

```
Cat9k#show platform software fed switch active punt packet-capture display-filter "ip.src==
10.11.0.0/24" brief
Punt packet capturing: disabled. Buffer wrapping: enabled (wrapped 0 times)
Total captured so far: 426 packets. Capture capacity : 6000 packets

------ Punt Packet Number: 2, Timestamp: 2020/04/10 23:37:14.899 ------
 interface : physical: GigabitEthernet1/0/1[if-id: 0x00000008], pal: Vlan20 [if-id: 0x00000076]
 metadata  : cause: 45 [BFD control], sub-cause: 0, q-no: 27, linktype: MCP_LINK_TYPE_IP [1]
 ether hdr : dest mac: 084f.a940.fa56, src mac: 380e.4d77.4f66
 ether hdr : vlan: 20, ethertype: 0x8100
 ipv4  hdr : dest ip: 10.11.0.1, src ip: 10.11.0.1
 ipv4  hdr : packet len: 40, ttl: 254, protocol: 17 (UDP)
 udp   hdr : dest port: 3785, src port: 49152

------ Punt Packet Number: 4, Timestamp: 2020/04/10 23:37:15.023 ------
 interface : physical: GigabitEthernet1/0/1[if-id: 0x00000008], pal: Vlan20 [if-id: 0x00000076]
 metadata  : cause: 29 [RP handled ICMP], sub-cause: 0, q-no: 6, linktype: MCP_LINK_TYPE_IP [1]
 ether hdr : dest mac: 084f.a940.fa56, src mac: 380e.4d77.4f66
```

```
 ether hdr : vlan: 20, ethertype: 0x8100
 ipv4  hdr : dest ip: 10.11.0.3, src ip: 10.11.0.3
 ipv4  hdr : packet len: 40, ttl: 255, protocol: 17 (UDP)
 udp   hdr : dest port: 3785, src port: 49152
```

Wireshark가 아니므로 모든 Wireshark 필터가 지원되지 않습니다. display-filter-help 명령을 사용하여 필터링에 사용할 수 있는 여러 옵션을 확인할 수 있습니다.

```
Cat9k#show platform software fed switch active punt packet-capture display-filter-help
FED Punject specific filters :
   1. fed.cause              FED punt or inject cause
   2. fed.linktype           FED linktype
   3. fed.pal_if_id          FED platform interface ID
   4. fed.phy_if_id          FED physical interface ID
   5. fed.queue              FED Doppler hardware queue
   6. fed.subcause           FED punt or inject sub cause
Generic filters supported :
   7. arp                    Is this an ARP packet
   8. bootp                  DHCP packets [Macro]
   9. cdp                    Is this a CDP packet
  10. eth                    Does the packet have an Ethernet header
  11. eth.addr               Ethernet source or destination MAC address
  12. eth.dst                Ethernet destination MAC address
  13. eth.ig                 IG bit of ethernet destination address (broadcast/multicast)
  14. eth.src                Ethernet source MAC address
  15. eth.type               Ethernet type
  16. gre                    Is this a GRE packet
  17. icmp                   Is this a ICMP packet
  18. icmp.code              ICMP code
  19. icmp.type              ICMP type
  20. icmpv6                 Is this a ICMPv6 packet
  21. icmpv6.code            ICMPv6 code
  22. icmpv6.type            ICMPv6 type
  23. ip                     Does the packet have an IPv4 header
  24. ip.addr                IPv4 source or destination IP address
  25. ip.dst                 IPv4 destination IP address
  26. ip.flags.df            IPv4 dont fragment flag
  27. ip.flags.mf            IPv4 more fragments flag
  28. ip.frag_offset         IPv4 fragment offset
  29. ip.proto               Protocol used in datagram
  30. ip.src                 IPv4 source IP address
  31. ip.ttl                 IPv4 time to live
  32. ipv6                   Does the packet have an IPv4 header
  33. ipv6.addr              IPv6 source or destination IP address
  34. ipv6.dst               IPv6 destination IP address
  35. ipv6.hlim              IPv6 hot limit
  36. ipv6.nxt               IPv6 next header
  37. ipv6.plen              IPv6 payload length
  38. ipv6.src               IPv6 source IP address
  39. stp                    Is this a STP packet
  40. tcp                    Does the packet have a TCP header
  41. tcp.dstport            TCP destination port
  42. tcp.port               TCP source OR destination port
  43. tcp.srcport            TCP source port
  44. udp                    Does the packet have a UDP header
  45. udp.dstport            UDP destination port
  46. udp.port               UDP source OR destination port
  47. udp.srcport            UDP source port
  48. vlan.id                Vlan ID (dot1q or qinq only)
  49. vxlan                  Is this a VXLAN packet
```

캡처 필터링

패킷 캡처를 시작하기 전에 특정 트래픽만 캡처하도록 도와주는 필터를 정의할 수 있습니다.

```
C9300#debug platform software fed switch active punt packet-capture set-filter "ip.src==
10.1.1.0/24 && tcp.port == 179"
Filter setup successful. Captured packets will be cleared

C9300#show platform software fed switch active punt packet-capture status
Punt packet capturing: disabled. Buffer wrapping: enabled (wrapped 0 times)
Total captured so far: 0 packets. Capture capacity : 6000 packets
Capture filter : "ip.src== 10.1.1.0/24 && tcp.port == 179"

C9300#debug platform software fed switch active punt packet-capture clear-filter
Filter cleared. Captured packets will be cleared

C9300#show platform software fed switch active punt packet-capture status
Punt packet capturing: disabled. Buffer wrapping: enabled (wrapped 0 times)
Total captured so far: 0 packets. Capture capacity : 6000 packets
```

Top Talker(17.6.X)별 정렬

17.6.1 이후부터는 지정된 필드를 기준으로 상위 토커에서 캡처한 패킷을 정렬할 수 있습니다.

```
Switch#show platform software fed switch active punt packet-capture cpu-top-talker ?
  cause-code          occurences of cause-code
  dst_ipv4            occurrences on dst_ipv4
  dst_ipv6            occurrences on dst_ipv4
  dst_l4              occurences of L4 destination
  dst_mac             Occurrences of dst_mac
  eth_type            Occurrences of eth_type
  incoming-interface  occurences of incoming-interface
  ipv6_hoplt          occurences of hoplt
  protocol            occurences of layer4 protocol
  src_dst_port        occurences of layer4 src_dst_port
  src_ipv4            occurrences on src_ipv4
  src_ipv6            occurrences on src_ipv6
  src_l4              occurences of L4 source
  src_mac             Occurrences of src_mac
  summary             occurences of all in summary
  ttl                 occurrences on ttl
  vlan                Occurrences of vlan

Switch#show platform software fed switch active punt packet-capture cpu-top-talker dst_mac
Punt packet capturing: disabled. Buffer wrapping: disabled
Total captured so far: 224 packets. Capture capacity : 4096 packets
Sr.no.  Value/Key       Occurrence
1       01:80:c2:00:00:00       203
2       01:00:0c:cc:cc:cc       21

Switch#show platform software fed switch active punt packet-capture cpu-top-talker summary
Punt packet capturing: disabled. Buffer wrapping: disabled
Total captured so far: 224 packets. Capture capacity : 4096 packets

L2 Top Talkers:
224     Source mac      00:27:90:be:20:84
203     Dest mac        01:80:c2:00:00:00

L3 Top Talkers:

L4 Top Talkers:
```

```
Internal Top Talkers:
224     Interface       FortyGigabitEthernet2/1/2
224     CPU Queue       Layer2 control protocols
```

관련 정보

Cat9K 플랫폼의 CPU 트러블슈팅에 대한 자세한 내용은 다음을 참조하십시오.

Cisco IOS-XE 16.x를 실행하는 Catalyst 스위치 플랫폼의 높은 CPU 사용량 문제 해결

추가 읽기

- Cisco IOS-XE 16 - 요약
- Catalyst 3850 시리즈 스위치 높은 CPU 사용량 문제 해결
- Embedded Packet Capture for Cisco IOS and Cisco IOS-XE 컨피그레이션 예
- 기술 지원 및 문서 – Cisco Systems

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.