

在Catalyst 9000交換機上配置FED CPU資料包捕獲

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[配置FED CPU資料包捕獲](#)

[基本配置示例](#)

[修改資料包捕獲](#)

[線性資料包捕獲](#)

[循環資料包捕獲](#)

[顯示和擷取篩選](#)

[顯示篩選](#)

[擷取篩選](#)

[按最大通話者排序\(17.6.X\)](#)

[相關資訊](#)

簡介

本文檔介紹如何使用FED (轉發引擎驅動程式) CPU捕獲工具。

必要條件

需求

本文件沒有特定需求。

採用元件

本文只限於執行Cisco IOS 16.X及更高版本的Catalyst交換平台。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

FED CPU資料包捕獲工具幫助識別穿越控制平面的數據，並提供有關點 (從ASIC到CPU的包) 或點 (從CPU到ASIC的包) 的流量資訊。

- 例如，此工具有助於識別觸發CoPP (控制平面管制器) 啟動並導致有效流量被丟棄的流量，以

保護CPU。

技術

- **轉發引擎驅動程式(FED)**：負責從Cisco IOS-XE獲取命令並對硬體ASIC進行程式設計。充當Catalyst交換機軟體和硬體元件之間的橋樑。
- **控制平面(CP)**：涉及Catalyst交換器CPU的功能和流量的集合。這可能包括目的地為交換器或來自交換器的流量，例如跨距樹狀目錄通訊協定(STP)、熱待命路由器通訊協定(HSRP)和路由通訊協定。
- **資料平面(DP)**：包括ASIC以及並非軟體交換而是硬體轉送的流量。
- **轉發**：從資料平面傳送到CPU的資料包的操作。
- **注入**：從CPU向下傳送到CPU的資料包的操作。

配置FED CPU資料包捕獲

此表用於配置選項

定義

用於點進或插入的資料包捕獲的預設設定

顯示捕獲的資料包

定義緩衝區大小和捕獲型別

為顯示的資料包定義捕獲過濾

顯示捕獲狀態

組態

```
debug platform software fed switch active <punt | inject> packet-ca  
<start | 停止>
```

```
show platform software fed switch active <punt | inject> packet-cap  
<brief | 詳細資訊>
```

```
debug platform software fed switch active <punt | inject> packet-ca  
buffer [circular] limit <#packets>
```

```
show platform software fed switch active <punt | inject> packet-cap  
display-filter <filter>
```

- 過濾器可以與logical &&、||，和括弧。例如：「`cdp ||(ipv.src=10.1.1.11和& tcp.port == 179) || stp`」

- 除了基於標準網路報頭的過濾之外，還新增了一些特定於平台的過濾器。它們還可以與標準混合。例如，從物理介面id 0x44接收的ARP資料包。

- 這不是Wireshark，因此它不支援所有Wireshark過濾器。display-filter-help命令可用於檢查支援的過濾器。

```
show platform software fed switch active <punt | inject> packet-cap  
status
```

基本配置示例

此工具會建立一個緩衝區，用於捕獲自啟用以來最多4096 (預設設定) 的打孔或注入的資料包。

```
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	suppressRewriteSideEffects	= 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
00000000000000030 00200000000000B00 380000532F000100 0000002F00000000
```

要驗證捕獲的當前狀態，可以使用下一命令。

```
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
```

修改資料包捕獲

經增強的/注入FED分組捕獲工具允許分組緩衝器大小和類型配置調整以建立線性或循環分組捕獲。

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

線性資料包捕獲

第一個緩衝區配置選項是限制向緩衝區傳送的資料包數量（預設大小為4096個資料包）。一旦達到緩衝區大小限制，就不會收集更多資料包（無緩衝區包裝）。

```
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
```

循環資料包捕獲

第二個緩衝區配置選項是為資料包設定循環緩衝區（預設緩衝區大小為4096資料包）。一旦達到循環緩衝區大小限制，就會用緩衝區中的新資料（緩衝區包裝）替換舊資料。

```
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
```

然後，可使用相同的引數再次運行資料包捕獲。

```
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--

顯示和擷取篩選

Punt/Injected FED資料包捕獲工具已經得到增強，以允許資料包顯示和過濾選項。

顯示篩選

完成沒有過濾器的捕獲後，可以對其進行檢視，以便僅顯示您感興趣的資訊。

```
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
```

由於這不是Wireshark，因此並非所有Wireshark過濾器都受支援。使用display-filter-help命令檢視過濾的不同可用選項。

```
Cat9k#show platform software fed switch active punt packet-capture display-filter-help
```

```
FED Punct 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 hop 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 |

擷取篩選

在開始捕獲資料包之前，可以定義一個過濾器，以僅幫助捕獲特定流量。

```
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

按最大通話者排序(17.6.X)

從17.6.1版開始，您可以根據指定的欄位對最大流量生成者捕獲的資料包進行排序。

```
Switch#show platform software fed switch active punt packet-capture cpu-top-talker ?
```

cause-code	occurences of cause-code
dst_ipv4	occurences on dst_ipv4
dst_ipv6	occurences on dst_ipv6
dst_l4	occurences of L4 destination
dst_mac	Occurences of dst_mac
eth_type	Occurences 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	occurences on src_ipv4
src_ipv6	occurences on src_ipv6
src_l4	occurences of L4 source
src_mac	Occurences of src_mac
summary	occurences of all in summary
ttl	occurences on ttl
vlan	Occurences 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

相關資訊

有關Cat9K平台中CPU故障排除的詳細資訊：

[對執行Cisco IOS-XE 16.x的Catalyst交換器平台中的高CPU使用率進行故障排除](#)

附加閱讀

- [Cisco IOS-XE 16 — 概覽](#)
- [Catalyst 3850 系列交換器高 CPU 使用率疑難排解](#)
- [適用於Cisco IOS和Cisco IOS-XE的嵌入式封包擷取組態範例](#)
- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。