

Configuration de la capture de paquets CPU FED sur les commutateurs Catalyst 9000

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configuration de la capture de paquets UC FED](#)

[Exemple de configuration de base](#)

[Modifier la capture de paquets](#)

[Capture linéaire de paquets](#)

[Capture Circulaire De Paquets](#)

[Filtrage d'affichage et de capture](#)

[Filtrage D'Affichage](#)

[Filtrage par capture](#)

[Trier par locuteur principal \(17.6.X\)](#)

[Informations connexes](#)

Introduction

Ce document décrit comment utiliser l'outil de capture du processeur FED (Forwarding Engine Driver).

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Ce document est limité aux plates-formes de commutation Catalyst qui exécutent Cisco IOS 16.X et versions ultérieures.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

L'outil de capture de paquets du processeur FED permet d'identifier les données qui traversent le plan de contrôle et fournit des informations sur le trafic ponté (paquets de l'ASIC au CPU) ou injecté (paquets du CPU à l'ASIC).

- Par exemple, cet outil est utile pour identifier le trafic qui a déclenché l'activation de CoPP (Control-Plane Policer), provoquant l'abandon du trafic valide dans un effort de protection du CPU.

Terminologie

- FED (Forwarding Engine Driver) : responsable de l'exécution des commandes à partir de Cisco IOS-XE et de la programmation des circuits ASIC matériels. Sert de pont entre les composants logiciels et matériels d'un commutateur Catalyst.
- Control Plane (CP) : ensemble de fonctions et de trafic impliquant le processeur du commutateur Catalyst. Cela peut inclure le trafic comme le protocole Spanning Tree (STP), le protocole HSRP (Hot Standby Router Protocol) et les protocoles de routage qui sont destinés au commutateur ou envoyés à partir du commutateur.
- Plan de données (DP) : englobe le ou les ASIC et le trafic qui n'est pas commuté par logiciel, mais transféré par matériel.
- Punt : action d'un paquet envoyé au processeur à partir du plan de données.
- Injection : action d'un paquet envoyé du processeur vers le processeur.

Configuration de la capture de paquets UC FED

Utilisez ce tableau pour les options de configuration

Définition	Configuration
Paramètre par défaut de la capture de paquets pour l'injection	<code>debug platform software fed switch active <punt inject> packet-capture <start stop></code>
Afficher les paquets capturés	<code>show platform software fed switch active <punt inject> packet-capture <brief détail></code>
Définissez la taille et le type de la mémoire tampon	<code>debug platform software fed switch active <punt inject> packet-capture buffer [circulaire] limit <#packets></code>
Définir le filtrage de capture pour les paquets affichés	<code>show platform software fed switch active <punt inject> packet-capture display-filter <filter></code> <ul style="list-style-type: none">• Les filtres peuvent être combinés avec le && logique et les crochets. Par exemple : « <code>cdp (ipv.src== 10.1.1.11 && tcp.port == 179) étape</code> »• Outre le filtrage basé sur l'en-tête réseau standard, certains filtres spécifiques à la plate-forme ont été ajoutés.

	<p>Ils peuvent également être mélangés avec des standards. Par exemple, les paquets ARP reçus de l'interface physique id 0x44.</p> <ul style="list-style-type: none"> • Il ne s'agit pas de Wireshark et ne prend donc pas en charge tous les filtres Wireshark. Une commande display-filter-help est disponible pour vérifier les filtres pris en charge.
Afficher l'état de capture	show platform software fed switch active <punt inject> packet-capture status

Exemple de configuration de base

Cet outil crée une mémoire tampon pour la capture de 4 096 (paramètre par défaut) paquets injectés ou injectés depuis qu'il a été activé.

<#root>

Cat9k#

```
debug platform software fed switch active punt packet-capture start
```

Punt packet capturing started.

<#root>

Cat9k#

```
debug platform software fed switch active punt packet-capture stop
```

Punt packet capturing stopped. Captured 263 packet(s)

<#root>

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], pa1: 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], pa1: 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)
```

<#root>

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], pa1: 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
0000000000000030 00200000000000B00 380000532F000100 0000002F00000000
```

Pour valider l'état actuel de la capture, vous pouvez utiliser la commande suivante.

```
<#root>
```

```
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
```

Modifier la capture de paquets

L'outil de capture de paquets à injection/injection FED est amélioré pour permettre l'ajustement de la taille et du type de la mémoire tampon de paquets afin de créer des captures de paquets linéaires ou circulaires.

```
<#root>
```

```
Cat9k#
```

```
debug platform software fed switch active punt packet-capture buffer ?
```

```
  circular  Circular capture
  limit     Number of packets to capture
```

Capture linéaire de paquets

La première option de configuration du tampon consiste à limiter le nombre de paquets (la taille par défaut est de 4 096 paquets) envoyés au tampon. Une fois la taille limite de la mémoire tampon atteinte, aucun paquet supplémentaire n'est collecté (pas d'encapsulation de la mémoire tampon).

```
<#root>
```

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
```

Capture Circulaire De Paquets

La deuxième option de configuration de tampon consiste à définir un tampon circulaire pour les paquets (la taille de tampon par défaut est de 4 096 paquets). Une fois la limite de taille de tampon circulaire atteinte, les anciennes données sont remplacées par de nouvelles données dans le tampon (encapsulation du tampon).

<#root>

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
```

La capture de paquets peut alors être exécutée à nouveau avec les mêmes paramètres.

<#root>

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--

Filtrage d'affichage et de capture

L'outil Punt/Inject FED de capture de paquets a été amélioré pour permettre l'affichage des paquets et les options de filtrage.

Filtrage D'Affichage

Une fois qu'une capture sans filtre est terminée, elle peut être révisée pour afficher uniquement les informations qui vous intéressent.

<#root>

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
```

Comme il ne s'agit pas de Wireshark, tous les filtres Wireshark ne sont pas pris en charge. Utilisez la commande `display-filter-help` pour afficher les différentes options de filtrage disponibles.

<#root>

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 IPv6 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

Filtrage par capture

Avant le début de la capture des paquets, vous pouvez définir un filtre pour capturer uniquement le trafic spécifique.

```
<#root>
```

```
C9300#
```

```
debug platform software fed switch active punt packet-capture set-filter "ip.src== 10.1.1.0/24 && tcp.p
```

```
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
```

Trier par locuteur principal (17.6.X)

À partir de la version 17.6.1, vous pouvez trier les paquets capturés par les principaux correspondants en fonction d'un champ spécifié.

```
<#root>
```

Switch#

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

```
cause-code      occurrences of cause-code
dst_ipv4        occurrences on dst_ipv4
dst_ipv6        occurrences on dst_ipv4
dst_l4          occurrences of L4 destination
dst_mac         Occurrences of dst_mac
eth_type        Occurrences of eth_type
incoming-interface occurrences of incoming-interface
ipv6_hop1t     occurrences of hop1t
protocol        occurrences of layer4 protocol
src_dst_port    occurrences of layer4 src_dst_port
src_ipv4        occurrences on src_ipv4
src_ipv6        occurrences on src_ipv6
src_l4          occurrences of L4 source
src_mac         Occurrences of src_mac
summary        occurrences 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
```

Informations connexes

Pour plus d'informations sur le dépannage de CPU dans les plates-formes Cat9K :

[Dépannage de l'utilisation CPU élevée dans les plates-formes de commutation Catalyst exécutant Cisco IOS-XE 16.x](#)

Lectures supplémentaires

- [Cisco IOS-XE 16 - En quelques mots](#)
- [Dépannage lors de l'utilisation élevée du processeur des commutateurs de la gamme Catalyst 3850](#)
- [Exemple de configuration de capture de paquets intégrée pour Cisco IOS et Cisco IOS-XE](#)
- [Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.