Konfigurieren der FED-CPU-Paketerfassung auf Catalyst 9000-Switches

Inhalt

Einleitung

In diesem Dokument wird die Verwendung des FED-Tools (Forwarding Engine Driver) zur CPU-Erfassung beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist auf Catalyst Switching-Plattformen mit Cisco IOS 16.X und höher beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Das FED-Tool zur CPU-Paketerfassung hilft bei der Identifizierung von Daten, die die Kontrollebene passieren, und liefert Informationen über **unterbrochenen** Datenverkehr (Pakete von ASIC zu CPU) oder **injizierten** (Pakete von CPU zu ASIC).

- Dieses Tool ist beispielsweise hilfreich, um Datenverkehr zu identifizieren, der die Aktivierung von CoPP (Control-Plane Policer) ausgelöst hat, sodass gültiger Datenverkehr verworfen wird, um die CPU zu schützen.

Terminologie

- **Forwarding Engine Driver (FED)**: Verantwortlich für die Übernahme von Befehlen aus Cisco IOS-XE und die Programmierung von Hardware-ASICs. Dient als Brücke zwischen Software- und Hardwarekomponenten eines Catalyst Switches.
- **Kontrollebene (CP):**Sammlung von Funktionen und Datenverkehr, die die CPU des Catalyst Switches betreffen. Dies kann Datenverkehr wie Spanning Tree Protocol (STP), Hot Standby Router Protocol (HSRP) und Routing-Protokolle einschließen, die für den Switch bestimmt sind oder vom Switch gesendet werden.
- **Datenebene (DP):** Umfasst die ASICs und den Datenverkehr, der nicht über Software, sondern über Hardware weitergeleitet wird.
- **Punt:** Aktion eines Pakets, das von der Datenebene an die CPU gesendet wird.
- **Inject (Einschleusen**): Aktion eines Pakets, das von der CPU nach unten an die CPU gesendet wird

FED-CPU-Paketerfassung konfigurieren

Diese Tabelle für Konfigurationsoptionen verwenden

Definition	Konfiguration
Standardeinstellung der Paketerfassung für Punt oder Inject	debug plattform software fed switch active | inject> Paketerfassung <start | Stopp>
Erfasste Pakete anzeigen	show platform software fed switch active | inject> Paketerfassung <Kurzbeschreibung | Detail>
Definition der Puffergröße und des Erfassungstyps	debug plattform software fed switch active | inject> Paketerfassungspuffer [Zirkular] Grenze <#packets>
Erfassungsfilterung für angezeigte Pakete definieren	show platform software fed switch active | inject> Packet-Capture Display-Filter <filter> • Filter können mit logischen && kombiniert werden. || und Klam Beispiel: "cdp || (ipv.src== 10.1.1.11 && tcp.port == 179) | | stp • Zusätzlich zur standardmäßigen, auf Netzwerk-Headern basierenden Filterung wurden einige plattformspezifische Filte hinzugefügt. Sie können auch mit Standardmischungen gemis werden. Beispiel: ARP-Pakete, die von der physischen Schnitt mit der ID 0x44 empfangen wurden. • Dies ist nicht Wireshark, daher werden nicht alle Wireshark-Fil unterstützt. Es steht ein Befehl display-filter-help zur Verfügun unterstützte Filter zu überprüfen.
Erfassungsstatus anzeigen	show platform software fed switch active | inject> Status der Paketerfassung

Einfaches Konfigurationsbeispiel

Dieses Tool erstellt einen Puffer für die Erfassung von bis zu 4096 (Standardeinstellung) gelochten oder injizierten Paketen, da es aktiviert wurde.

```
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
```

Um den aktuellen Status für die Erfassung zu validieren, können Sie den nächsten Befehl verwenden.

```
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
```

Ändern der Paketerfassung

Das Punt/Inject FED-Paketerfassungstool wurde verbessert, um eine Anpassung der Paketpuffergröße und des Pakettyps zu ermöglichen und lineare oder zirkuläre Paketerfassungen zu erstellen.

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

Lineare Paketerfassung

Die erste Option für die Pufferkonfiguration besteht darin, die Anzahl der Pakete zu begrenzen (die Standardgröße beträgt 4096 Pakete), die an den Puffer gesendet werden. Sobald die Puffergrößenbeschränkung erreicht ist, werden keine weiteren Pakete gesammelt (kein Buffer-Wrapping).

```
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
```

Zirkuläre Paketerfassung

Die zweite Pufferkonfigurationsoption dient zum Festlegen eines zirkulären Puffers für Pakete (die Standardpuffergröße beträgt 4096 Pakete). Sobald die Grenze der zirkulären Puffergröße erreicht ist, werden alte Daten durch neue Daten im Puffer ersetzt (Buffer-Wrapping).

```
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
```

Die Paketerfassung kann dann mit den gleichen Parametern erneut ausgeführt werden.

```
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--
```

Anzeige- und Erfassungsfilterung

Das Punt/Inject FED-Paketerfassungstool wurde erweitert, um Paketanzeige- und Filteroptionen zu ermöglichen.

Anzeigefilterung

Sobald eine Erfassung ohne Filter abgeschlossen wurde, kann sie überprüft werden, um nur die Informationen anzuzeigen, an denen Sie interessiert sind.

```
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
```

Da es sich nicht um Wireshark handelt, werden nicht alle Wireshark-Filter unterstützt. Verwenden Sie den Befehl display-filter-help, um die verschiedenen verfügbaren Filteroptionen anzuzeigen.

```
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
```

Erfassungsfilterung

Vor Beginn der Paketerfassung können Sie einen Filter definieren, der nur bestimmten Datenverkehr erfasst.

```
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
```

Sortieren nach Top Talker (17.6.X)

Ab Version 17.6.1 können Sie die von Top Talkers erfassten Pakete anhand eines festgelegten Felds sortieren.

```
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
```

Zugehörige Informationen

Weitere Informationen zur CPU-Fehlerbehebung in Cat9K-Plattformen finden Sie unter:

Fehlerbehebung bei hoher CPU-Auslastung auf Catalyst Switch-Plattformen mit Cisco IOS-XE 16.x

Zusätzliche Lektüre

- Cisco IOS-XE 16 - Informationen auf einen Blick
- Catalyst Switches der 3850-Serie – Fehlerbehebung bei hoher CPU-Auslastung
- Integrierte Paketerfassung für Cisco IOS und Cisco IOS-XE - Konfigurationsbeispiel
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.