Configurazione dell'acquisizione di pacchetti CPU FED sugli switch Catalyst 9000

Sommario

Introduzione

In questo documento viene descritto come utilizzare lo strumento di acquisizione CPU FED (Forwarding Engine Driver).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento è limitato alle piattaforme di switching Catalyst con Cisco IOS versione 16.X e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Lo strumento di acquisizione pacchetti CPU FED consente di identificare i dati che attraversano il control plane e fornisce informazioni sul traffico puntato (pacchetti da ASIC a CPU) o iniettato (pacchetti da CPU ad ASIC).

- Ad esempio, questo strumento è utile per identificare il traffico che ha attivato il CoPP (Control-Plane Policer) per l'accesso, causando l'eliminazione del traffico valido nel tentativo di proteggere la CPU.

Terminologia

- Driver motore di inoltro (FED): è responsabile dell'esecuzione dei comandi da Cisco IOS-XE e della programmazione degli ASIC hardware. Funge da ponte tra i componenti software e hardware di uno switch Catalyst.
- Control Plane (CP): raccolta di funzioni e traffico che coinvolgono la CPU dello switch Catalyst. ad esempio, il traffico STP (Spanning Tree Protocol), HSRP (Hot Standby Router Protocol) e i protocolli di routing destinati allo switch o inviati dallo switch.
- Data Plane (DP): comprende gli ASIC e il traffico non commutato a livello di software, ma inoltrato dall'hardware.
- Punt: azione di un pacchetto inviato alla CPU dal piano dati.
- Inserisci:azione di un pacchetto inviato dalla CPU verso la CPU.

Configura acquisizione pacchetti CPU FED

Utilizzare questa tabella per le opzioni di configurazione

Definizione	Configurazione
Impostazione predefinita dell'acquisizione pacchetti per punt o inject	debug platform software fed switch attivo <punt | inject> packet-capture <inizio | stop>
Visualizza i pacchetti acquisiti	show platform software fed switch attivo <punt | inject> packet-capture <breve | dettaglio>
Definire le dimensioni del buffer e il tipo di acquisizione	debug platform software fed switch attivo <punt | inject> packet-capture buffer [circolare] limite <#packets>
Definire il filtro di acquisizione per i pacchetti visualizzati	show platform software fed switch attivo <punt | inject> packet-capture display-filter <filtro> • I filtri possono essere combinati con l'operatore logico &&, || e parentesi. Ad esempio: "cdp || (ipv.src== 10.1.1.11 && tcp.port == 179) || stp" • Oltre ai filtri basati su intestazione di rete standard, sono stati aggiunti alcuni filtri specifici della piattaforma. Possono anche essere miscelati con quelli standard. Ad

	esempio, i pacchetti ARP ricevuti dall'ID interfaccia fisica 0x44. • Questo non è Wireshark, quindi non supporta tutti i filtri Wireshark. È disponibile un comando display-filter-help per verificare i filtri supportati.
Visualizza stato acquisizione	show platform software fed switch attivo <punt | inject> stato acquisizione pacchetti

Esempio di configurazione di base

Questo strumento crea un buffer per l'acquisizione di un massimo di 4096 (impostazione predefinita) pacchetti perforati o iniettati da quando è stato abilitato.

<#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], 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)
```

<#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], 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
```

Per convalidare lo stato corrente dell'acquisizione, è possibile utilizzare il comando successivo.

<#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
```

Modificare l'acquisizione del pacchetto

Lo strumento di acquisizione dei pacchetti FED punt/inject è stato migliorato per consentire la regolazione della configurazione del tipo e delle dimensioni del buffer dei pacchetti per creare acquisizioni lineari o circolari.

<#root>

```
Cat9k#
```

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

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

Acquisizione lineare dei pacchetti

La prima opzione di configurazione del buffer consiste nel limitare il numero di pacchetti (la dimensione predefinita è 4096 pacchetti) che vengono inviati al buffer. Una volta raggiunto il limite delle dimensioni del buffer, non vengono raccolti altri pacchetti (nessun wrapping del buffer).

<#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
```

Acquisizione circolare dei pacchetti

La seconda opzione di configurazione del buffer consiste nell'impostare un buffer circolare per i pacchetti (la dimensione predefinita del buffer è 4096 pacchetti). Una volta raggiunto il limite circolare delle dimensioni del buffer, i vecchi dati vengono sostituiti dai nuovi dati nel buffer (wrapping del buffer).

```
<#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
```

L'acquisizione del pacchetto può quindi essere eseguita di nuovo con gli stessi parametri.

```
<#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--
```

Filtro di visualizzazione e acquisizione

Lo strumento di acquisizione dei pacchetti FED Punt/Inject è stato migliorato per consentire la visualizzazione dei pacchetti e le opzioni di filtro.

Filtro visualizzazione

Una volta completata l'acquisizione senza filtro, è possibile esaminarla per visualizzare solo le informazioni a cui si è interessati.

<#root>

```
Cat9k#

show platform software fed switch active punt packet-capture display-filter "ip.src== 10.11.0.0/24" brie

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
```

Poiché questo non è Wireshark, non tutti i filtri Wireshark sono supportati. Utilizzare il comando display-filter-help per visualizzare le diverse opzioni disponibili per il filtraggio.

<#root>

```
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
```

Acquisisci filtro

Prima di avviare l'acquisizione del pacchetto, è possibile definire un filtro che aiuti a catturare solo il traffico specifico.

```
<#root>

C9300#

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

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
```

Ordina per Top Talker (17.6.X)

A partire dalla versione 17.6.1, è possibile ordinare i pacchetti acquisiti dai relatori più esperti in base a un campo specificato.

```
<#root>
```

```
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
```

Informazioni correlate

Per ulteriori informazioni sulla risoluzione dei problemi relativi alla CPU nelle piattaforme Cat9K:

[Risoluzione dei problemi di utilizzo elevato della CPU nelle piattaforme degli switch Catalyst con Cisco IOS-XE 16.x]

Lettura aggiuntiva

- Cisco IOS-XE 16 - In breve
- Risoluzione dei problemi di utilizzo intenso della CPU degli switch Catalyst serie 3850
- Esempio di acquisizione integrata dei pacchetti per Cisco IOS e Cisco IOS-XE
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).