Erfassung von Datenverkehr zwischen den USA mit dem Router der Serie 8000

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie der Datenverkehr für externe Benutzer auf dem Cisco Router der Serie 8000 erfasst wird.

Voraussetzungen

Anforderungen

Vertrautheit mit Cisco Routern der Serie 8000 und der Cisco IOS® XR-Software

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Routern der Serie 8000 und sind nicht auf bestimmte Software- und Hardwareversionen 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 kennen.

Hintergrundinformationen

Bei der Fehlerbehebung müssen Sie in bestimmten Fällen den Datenverkehr überprüfen, der zur weiteren Verarbeitung oder Verarbeitung an die CPU weitergeleitet wird.

Dieser Artikel erläutert, wie dieser Datenverkehr auf dem Cisco Router der Serie 8000 erfasst werden kann.

Vorgehensweise

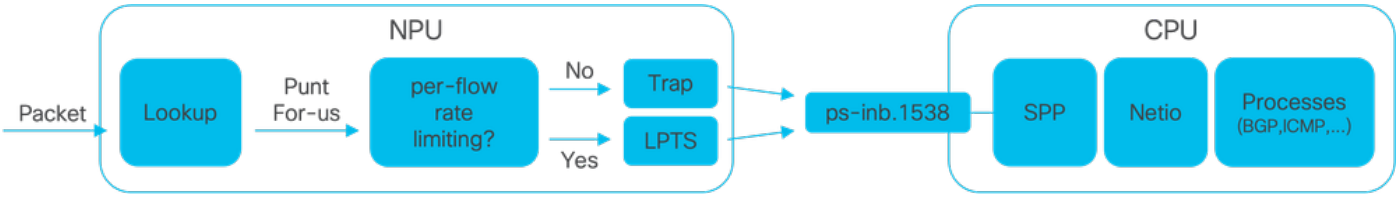

Bild 1: Vereinfachtes Diagramm für NPU und CPU beim Cisco Router der Serie 8000.

Beim Empfang eines Pakets Auf dem Cisco 8000-Router wird eine Suche von der Network Processing Unit (NPU) durchgeführt, die zu einer Weiterleitungsentscheidung führt.

Es kann einen Fall geben, in dem entschieden wird, das Paket zu testen, d. h. das Paket zur weiteren Verarbeitung oder Verarbeitung an die CPU zu übertragen.

Die NPU-Suche ermittelt außerdem, ob beim Switching des Pakets zur CPU die Datenflussrate begrenzt werden muss.

- Ist eine Durchsatzratenbegrenzung erforderlich, so wird das Paket über den Local Packet Transport Service (LPTS), beispielsweise ein Routing-Protokollpaket, an die CPU weitergeleitet.
- Ist keine Beschränkung auf Durchsatzraten erforderlich, wird ein Trap generiert und das Paket an die CPU weitergeleitet, z. B. ein Paket mit Time-to-Live (TTL) abgelaufen.

Die Pakete werden, sofern nicht ratenbegrenzt, über ein dediziertes internes VLAN mit der ID 1538 an die CPU weitergeleitet.

Sie können sowohl die Einträge in der LPTS-Tabelle als auch in der Traps-Tabelle überprüfen, indem Sie den Befehl show lpts pifib hardware entry brief und den Befehl show controllers npu stats traps-all verwenden.

Der Befehl show lpts pifib hardware entry brief zeigt die Einträge der LPTS-Tabelle an.

Hier ist die Ausgabe auf Einträge beschränkt, die mit dem Border Gateway Protocol (BGP) verknüpft sind.

```
RP/0/RP0/CPU0:8202#show lpts pifib hardware entry brief location 0/rp0/cpu0 | include "Type|BGP"

Type DestIP              SrcIP              Interface          vrf   L4   LPort/Type   RPort  npu  F
IPv4 10.4.11.2           10.4.11.3          any                0     6    Port:20656   179    0    B
IPv4 10.4.11.2           10.4.11.3          any                0     6    Port:179     0      0    B
IPv4 any                 any                any                0     6    Port:any     179    0    B
IPv4 any                 any                any                0     6    Port:179     0      0    B
IPv6 any                 any                any                0     6    Port:any     179    0    B
IPv6 any                 any                any                0     6    Port:179     0      0    B
RP/0/RP0/CPU0:8202#
```

Der Befehl show controllers npu stats traps-all listet alle Trap-Einträge und die zugehörigen Zähler auf.

In diesem Fall ist die Ausgabe auf Einträge mit übereinstimmenden Paketen beschränkt. Ausgenommen sind alle Einträge, die in den Spalten "Akzeptierte Pakete" und "Paketverlust" 0 anzeigen.

Beachten Sie, dass alle Traps auf den Tarif beschränkt sind.

```
show controllers npu stats traps-all instance 0 location 0/rp0/cpu0 | exclude "0 0"

RP/0/RP0/CPU0:8202#show controllers npu stats traps-all instance 0 location 0/rp0/cpu0 | exclude "0

Traps marked (D*) are punted (post policing) to the local CPU internal VLAN 1586 for debugging
They can be read using "show captured packets traps" CLI
Traps marked (D) are dropped in the NPU
Traps punted to internal VLAN 1538 are processed by the process "spp" on the "Punt Dest" CPU
They can also be read using "show captured packets traps" CLI
"Configured Rate" is the rate configured by user (or default setting) in pps at the LC level
"Hardware Rate" is the actual rate in effect after hardware adjustments
Policer Level:
        NPU: Trap meter is setup per NPU in packets per second
        IFG: Trap meter is setup at every IFG in bits per second
        The per IFG meter is converted from the user configured/default rate (pps)
        based on the "Avg-Pkt Size" into bps.
        Due to hardware adjustments, the "Configured Rate" and
        "Hardware Rate" differ in values.


NOTE:The displayed stats are NOT real-time and are updated every 30 SECONDS from the hardware.

Trap Type                                       NPU  Trap  Punt       Punt  Punt  Punt Configured Hardwar
                                                ID   ID    Dest       VoQ   VLAN  TC   Rate(pps)  Rate(pp
================================================================================================================
ARP                                             0    3     RPLC_CPU   271   1538  7    542        533
NOT_MY_MAC(D*)                                  0    4     RPLC_CPU   264   1586  0    67         150
DHCPV4_SERVER                                   0    8     RPLC_CPU   265   1538  1    542        523
LLDP                                            0    26    RPLC_CPU   270   1538  6    4000       3862
ONLINE_DIAG                                     0    31    RPLC_CPU   271   1538  7    4000       3922
V4_MCAST_DISABLED(D*)                           0    69    RPLC_CPU   269   1586  5    67         150
V6_MCAST_DISABLED(D*)                           0    80    RPLC_CPU   264   1586  0    67         150
L3_IP_MULTICAST_NOT_FOUND(D*)                   0    125   RPLC_CPU   264   1586  0    67         150
RP/0/RP0/CPU0:8202#
```

Das Shell-Dienstprogramm spp_platform_pcap kann zum Erfassen von Paketen verwendet werden, die dieses dedizierte interne VLAN zwischen der NPU und der CPU durchlaufen. Mit diesem Dienstprogramm kann auch der Datenverkehr erfasst werden, der über die Verwaltungsschnittstelle des Routers gesendet oder empfangen wird.

Das Shell-Dienstprogramm spp_platform_pcap wird innerhalb der Shell ausgeführt und bietet mehrere Verwendungsoptionen. Um auf die Shell zuzugreifen oder sich bei ihr anzumelden, führen Sie den Befehl run aus. Um sich von der Shell abzumelden, geben Sie exit ein.

```
RP/0/RP0/CPU0:8202#run
[node0_RP0_CPU0:~]$spp_platform_pcap -h
Usage: spp_platform_pcap options
Use Ctrl-C to stop anytime
  -h  --help            Display this usage information.
  -D  --Drop            capture Drops in SPP.
  -i  --interface       Interface-name
                        Available from the output of
                        "show ipv4 interface brief"
  -Q  --direction       direction of the packet
                        Options: IN | OUT |
                        Mandatory option
                        (when not using the -d option)
  -s  --source          Originator of the packet.
                        Options: ANY | CPU | NPU | NSR | MGMT | PTP | LC_PKTIO | LC_REDIR
  -d  --destination     destination of the packet
                        Options: ANY | CPU | NPU | MGMT | PTP | LC_PKTIO | LC_REDIR |
  -l  --l4protocol      IANA-L4-protocol-number
                         (use with Address family (-a)
                        Interface (-i) and direction (-Q)
                        Options: min:0 Max:255
  -a  --addressFamily   address Family used with l4protocol (-l)
                        Interface (-i) and direction (-Q)
                        Options: ipv4 | ipv6 |
  -x  --srcIp           Src-IP (v4 or v6)
                        Used with -a, -i and -Q only
  -X  --dstIp           Dst-IP (v4 or v6)
                        Used with -a, -i and -Q only
  -y  --srcPort         Src-Port
                        Used with -a, -l, -i and -Q only
                        Options: min:0 Max:65535
  -Y  --dstPort         Dst-Port
                        Used with -a, -l, -i and -Q only
                        Options: min:0 Max:65535
  -P  --l2Packet        Based on L2 packet name/etype
                        Interface (-i) and direction (-Q) needed
                        Use for non-L3 packets
                        Options:ether-type (in hex format)
                        ARP | ISIS | LACP | SYNCE | PTP | LLDP | CDP |
  -w  --wait            Wait time(in seconds)
                        Use Ctrl-C to abort
  -c  --count           Count of packets to collect
                        min:1; Max:1024
  -t  --trapNameOrId    Trap-name(in quotes) or number(in decimal)
                        (direction "in" is a MUST).
                        Refer to "show controllers npu stats traps-all instance all location <LC|RP>
                        Note: Trap names with (D*) in the display are not punted to SPP.
                        They are punted to ps-inb.1586
  -S  --puntSource      Punt-sources
                        Options: LPTS_FORWARDING | INGRESS_TRAP | EGRESS_TRAP | INBOUND_MIRROR |
                        NPUH |
  -p  --pcap            capture packets in pcap file.
  -v  --verbose         Print the filter offsets.
[node0_RP0_CPU0:~]$
```

Beachten Sie die Option für die Erfassungsrichtung, -Q, wobei der Wert IN bedeutet, dass die gesendeten Pakete (die von der CPU empfangenen Pakete) erfasst werden. Der Wert OUT bedeutet, dass die eingekoppelten Pakete (die von der CPU gesendeten Pakete) erfasst werden.

Mit der Option -p können Pakete in einer pcap-Datei erfasst werden.

Bitte beachten Sie, dass die spp_platform_pcap-Erfassung standardmäßig Folgendes umfasst:

- Läuft 60 Sekunden lang.
- Erfasst maximal 100 Pakete.
- Alle erfassten Pakete werden auf 214 Byte gekürzt.

Um beispielsweise eine ungefilterte Erfassung des gesamten von der CPU empfangenen Datenverkehrs zu starten, geben Sie den Befehl spp_platform_pcap -Q IN -p ein:

```
[node0_RP0_CPU0:~]$spp_platform_pcap -Q IN -p
All trace-enabled SPP nodes will be traced.
Node "socket/rx" set for trace filtering. Index: 1
Wait time is 60 seconds. Use Ctrl-C to stop
Collecting upto 100 packets (within 60 seconds)
^CSignal handling initiated <<<<<<<< Here: 'Ctrl-C' was used to stop the capture.
Tracing stopped with 10 outstanding...
Wrote 90 traces to /tmp/spp_bin_pcap
All trace-enabled SPP nodes will be traced.
pcap: Captured pcap file for packets saved at "/tmp/spp_pcap_capture_0_RP0_CPU0.pcap"

[node0_RP0_CPU0:~]$
```

Nach Beendigung der Erfassung wird die resultierende Datei auf dem lokalen Datenträger verfügbar gemacht.

Kopieren Sie die Datei vom Router auf Ihren lokalen Computer, und überprüfen Sie ihren Inhalt mithilfe der von Ihnen bevorzugten Paketdecoder-Anwendung.

```
[node0_RP0_CPU0:~]$ls -la /tmp
total 44
<snip>
-rw-r--r--.  1 root  root  8516 Aug  7 06:58 spp_pcap_capture_0_RP0_CPU0.pcap
<snip>
[node0_RP0_CPU0:~]$
[node0_RP0_CPU0:~]$cp /tmp/spp_pcap_capture_0_RP0_CPU0.pcap /harddisk:/
[node0_RP0_CPU0:~]$exit
logout

RP/0/RP0/CPU0:8202#dir harddisk: | include spp_pcap

16 -rw-r--r--. 1 8516 Aug 8 07:01 spp_pcap_capture_0_RP0_CPU0.pcap
RP/0/RP0/CPU0:8202#
```

Es ist möglich, im Hinblick auf die Absicht Ihrer Erfassung genauer zu sein. Sie können beispielsweise die Funktionen des Dienstprogramms Filter nutzen, um den für den Benutzer bestimmten Datenverkehr zu erfassen, der sich auf eine bestimmte Router-Schnittstelle, eine IP-

Adresse oder ein bestimmtes Protokoll bezieht.

Mit diesem Befehl können Sie z. B. den BGP-Datenverkehr eines bestimmten Peers an einer bestimmten Schnittstelle erfassen:

```
spp_platform_pcap -Q IN -a ipv4 -l 6 -i HundredGigE0/0/0/1 -x 10.100.0.1 -Y 179 -p
```

Sie können auch spp_platform_pcap verwenden, um den über die Router-Management-Schnittstelle gesendeten oder empfangenen Datenverkehr zu erfassen.

Mit diesem Befehl können Sie z. B. den von der Verwaltungsschnittstelle empfangenen Datenverkehr erfassen.

```
spp_platform_pcap -Q IN -p -i MgmtEth0/RP0/CPU0/0
```

Alle vorherigen Beispiele wurden auf einem Standalone-Router der Cisco Serie 8000 ausgeführt. Wenn Sie mit einem verteilten Router der Cisco Serie 8000 arbeiten, überlegen Sie, in welchem Knoten, Routingprozessor oder Linecard die Erfassung ausgeführt werden soll.

Es kann der Fall sein, dass der jeweilige Datenverkehr, den Sie interessieren, von einer bestimmten Linecard-CPU verarbeitet wird. Sowohl die show controller npu stats traps-all als auch die show lpts pifib hardware entry brief können helfen, das Ziel des Punt zu identifizieren.

<#root>

```
RP/0/RP0/CPU0:8808#show controllers npu stats traps-all instance 0 location 0/0/cpu0 | include "Type|Ac

Trap Type                                       NPU  Trap

Punt

       Punt  Punt  Punt Configured Hardware   Policer Avg-Pkt Packets              Packets
                                               ID   ID

Dest

       VoQ   VLAN  TC   Rate(pps)  Rate(pps)  Level   Size    Accepted             Dropped
=============================================================================================================
ARP                                            0    10   LC_CPU      239   1538  7    542         531
ISIS/L3                                        0    129  BOTH_RP-CPU 239   1538  7    10000       9812
RP/0/RP0/CPU0:8808#

RP/0/RP0/CPU0:8808#show lpts pifib hardware entry brief location 0/0/cpu0 | include "Type|--|Fragment|O

-------------------------------------------------------------------------
Type DestIP              SrcIP               Interface          vrf   L4   LPort/Type   RPort  npu  F

DestNode
```

```
     PuntPrio       Accept Drop
---- ------------------- ------------------- -------------     ----- ---  ------------ ------ ---- -
IPv4 any                 any                 any               0     0    any          0      0    F
IPv4 any                 any                 any               0     0    any          0      0    F
IPv4 any                 any                 any               0     0    any          0      1    F
IPv4 any                 any                 any               0     0    any          0      1    F
IPv4 any                 any                 any               0     0    any          0      2    F
IPv4 any                 any                 any               0     0    any          0      2    F
IPv4 any                 any                 any               0     89   any          0      0    O
IPv4 any                 any                 any               0     89   any          0      0    O
IPv4 any                 any                 any               0     89   any          0      1    O
IPv4 any                 any                 any               0     89   any          0      2    O
IPv4 any                 any                 any               0     89   any          0      0    O
IPv4 any                 any                 any               0     89   any          0      0    O
IPv4 any                 any                 any               0     89   any          0      1    O
IPv4 any                 any                 any               0     89   any          0      2    O
IPv6 any                 any                 any               0     0    any          0      0    F
IPv6 any                 any                 any               0     0    any          0      1    F
IPv6 any                 any                 any               0     0    any          0      2    F
IPv6 any                 any                 any               0     89   any          0      0    O
IPv6 any                 any                 any               0     89   any          0      1    O
IPv6 any                 any                 any               0     89   any          0      2    O
IPv6 any                 any                 any               0     89   any          0      0    O
IPv6 any                 any                 any               0     89   any          0      1    O
IPv6 any                 any                 any               0     89   any          0      2    O
RP/0/RP0/CPU0:8808#
```

Schließen Sie das Dokument an die entsprechende Linecard an, und führen Sie von dort das Dienstprogramm spp_platform_pcap aus, wie zuvor gezeigt.

```
attach location 0/0/cpu0
spp_platform_pcap -Q IN -p
! --- execute 'Ctrl-C' to stop the capture
```

Zugehörige Informationen

Video zum Cisco Technical Assistance Center (TAC)

[Cisco Serie 8000 - Erfassung von E-Mail-Verkehr, Video]

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.