8000 Series 라우터로 미국 내 트래픽 캡처

목차

소개

이 문서에서는 Cisco 8000 Series 라우터에서 us용 트래픽을 캡처하는 방법을 설명합니다.

사전 요구 사항

요구 사항

Cisco 8000 Series 라우터 및 Cisco IOS® XR 소프트웨어에 익숙합니다.

사용되는 구성 요소

이 문서의 정보는 Cisco 8000 Series 라우터를 기반으로 하며 특정 소프트웨어 및 하드웨어 버전으로 제한되지 않습니다.

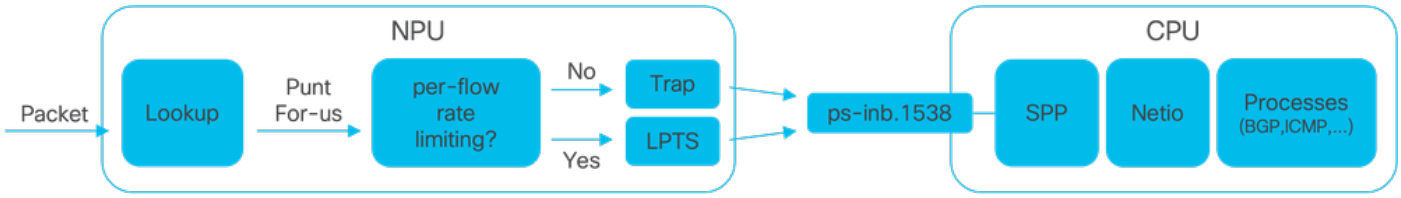
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

트러블슈팅 활동 중에 추가 처리 또는 처리를 위해 CPU(Central Processing Unit)로 전환되는 트래픽을 확인해야 하는 경우가 있습니다.

이 문서는 Cisco 8000 Series 라우터에서 이러한 트래픽을 캡처하는 방법을 설명하기 위한 것입니다.

절차



이미지1 - Cisco 8000 Series 라우터가 NPU 및 CPU 다이어그램을 간소화했습니다.

Cisco 8000 라우터에서 패킷을 수신하면 NPU(Network Processing Unit)에서 조회를 수행하여 포워딩 결정을 내립니다.

추가 처리 또는 처리를 위해 패킷을 CPU로 전환한다는 의미에서 패킷을 펀트하기로 결정한 경우가 있을 수 있습니다.

NPU 조회는 패킷을 CPU로 스위칭하는 동안 per-flow-rate-limiting이 필요한지 여부도 결정합니다.

- Per-flow-rate-limiting이 필요한 경우, 패킷은 LPTS(Local Packet Transport Service)를 통해 CPU로 스위칭됩니다(예: 라우팅 프로토콜 패킷).
- Per-flow-rate-limiting이 필요하지 않은 경우 트랩이 생성되고 패킷이 CPU로 전환됩니다(예: TTL(Time-to-Live)이 만료된 패킷).

속도 제한이 없는 경우 패킷은 ID가 1538인 전용 내부 VLAN을 통해 CPU로 스위칭됩니다.

show lpts pifib hardware entry brief 및 show controller npu stats traps-all 명령을 사용하여 LPTS 테이블과 Traps 테이블 항목을 모두 확인할 수 있습니다.

show lpts pifib hardware entry brief 명령은 LPTS 테이블 엔트리를 표시합니다.

여기서 출력은 BGP(Border Gateway Protocol)와 연결된 항목으로 제한됩니다.

```
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#
```

show controllers npu stats traps-all 명령은 모든 트랩 엔트리 및 관련 카운터를 나열합니다.

여기서 출력은 Packets Accepted 및 Packets Dropped 열에서 0을 표시하는 모든 항목을 제외하고 패킷 일치가 있는 항목으로 제한됩니다.

모든 트랩은 속도가 제한됩니다.

```
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#
```

셸 유틸리티 spp_platform_pcap를 사용하여 NPU와 CPU 간에 이 전용 내부 VLAN을 통과하는 패킷을 캡처할 수 있습니다. 이 유틸리티를 사용하면 라우터 관리 인터페이스를 통해 보내거나 받은 트래픽도 캡처할 수 있습니다.

spp_platform_pcap 셸 유틸리티는 셸 내에서 실행되며 여러 사용 옵션을 제공합니다. 셸에 액세스하거나 로그인하려면 run 명령을 실행합니다. 셸에서 로그아웃하려면 exit를 입력합니다.

```
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:~]$
```

capture direction 옵션 -Q에 유의하십시오. 여기서 IN 값은 펀트된 패킷(CPU에서 수신한 패킷)을 캡처함을 의미합니다. OUT 값은 삽입된 패킷(CPU에서 전송한 패킷)을 캡처함을 의미합니다. 옵션 -p를 사용하면 pcap 파일의 패킷을 캡처할 수 있습니다.

기본적으로 spp_platform_pcap 캡처는 다음과 같습니다.

- 60초 동안 실행됩니다.
- 최대 100개의 패킷을 캡처합니다.
- 캡처된 모든 패킷을 214바이트로 자릅니다.

예를 들어 CPU에서 수신한 모든 트래픽의 필터링되지 않은 캡처를 시작하려면 spp_platform_pcap -Q IN -p 명령을 입력합니다.

```
[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:~]$
```

캡처가 끝나면 로컬 디스크에서 결과 파일을 사용할 수 있습니다.

라우터에서 로컬 컴퓨터로 파일을 복사하고 기본 패킷 디코더 응용 프로그램을 사용하여 내용을 확인합니다.

```
[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#
```

캡처 의도와 관련하여 좀 더 구체화할 수 있습니다. 예를 들어, 특정 라우터 인터페이스, IP 주소 또는 특정 프로토콜과 관련된 사용 중 트래픽을 캡처하기 위해 유틸리티 필터 기능을 활용할 수 있습니다.

예를 들어 이 명령을 사용하면 특정 인터페이스의 특정 피어에서 BGP 트래픽을 캡처할 수 있습니다.

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

또한 spp_platform_pcap를 사용하여 라우터 관리 인터페이스를 통해 보내거나 받은 트래픽을 캡처할 수 있습니다.

예를 들어, 이 명령을 사용하면 관리 인터페이스에서 수신된 트래픽을 캡처할 수 있습니다.

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

이전의 모든 예는 독립형 Cisco 8000 Series 라우터에서 실행되었습니다. 분산형 Cisco 8000 Series 라우터로 작업하는 경우 어떤 노드, Route Processor 또는 라인 카드를 캡처할 것인지 고려하십시오.

관심이 있는 특정 트래픽이 특정 라인 카드 CPU에 의해 처리되는 경우일 수 있습니다. show controllers npu stats traps-all과 show lpts pifib 하드웨어 엔트리 브리프는 모두 punt 대상을 식별하는 데 도움이 됩니다.

<#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     0
IPv6 any                  any                  any                  0      89    any          0      1     0
IPv6 any                  any                  any                  0      89    any          0      2     0
RP/0/RP0/CPU0:8808#
```

식별되면 특정 라인 카드에 연결하고 앞에서 설명한 대로 spp_platform_pcap 유틸리티를 실행합니다.

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

관련 정보

Cisco TAC(Technical Assistance Center) 비디오

Cisco 8000 Series - Capture for-us 트래픽, 비디오

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.