使用8000系列路由器捕獲美國流量

目錄

簡介

本文檔介紹如何在Cisco 8000系列路由器中捕獲for-us流量。

必要條件

需求

熟悉Cisco 8000系列路由器和Cisco IOS® XR軟體。

採用元件

本文檔中的資訊基於Cisco 8000系列路由器，並不侷限於特定的軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

在故障排除活動期間，有時您需要驗證正在切換到中央處理器(CPU)以進行進一步處理或處理的流量。

本文旨在說明如何在Cisco 8000系列路由器中捕獲此流量。

程式

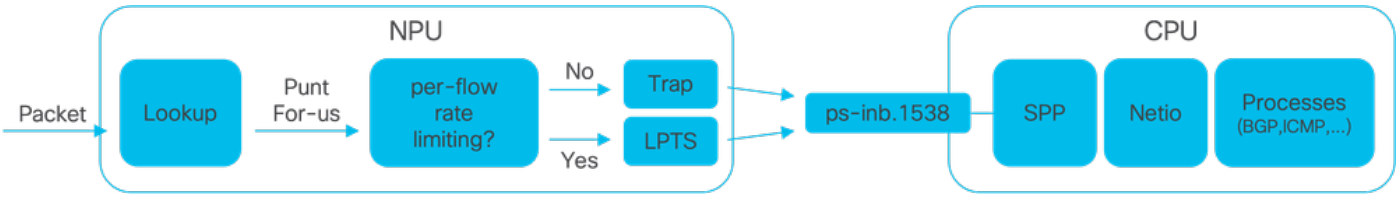

圖1 - Cisco 8000系列路由器簡化了NPU和CPU圖。

在Cisco 8000路由器收到資料包時，網路處理單元(NPU)會執行查詢，從而做出轉發決策。

在某些情況下，可能會決定傳送資料包，即將資料包切換到CPU進行進一步處理或處理。

NPU查詢還確定在將資料包交換到CPU時是否需要按流速率限制。

- 如果需要每流量速率限制，則封包會透過本機封包傳輸服務(LPTS)（例如路由通訊協定封包）交換到CPU。
- 如果不需要每流速率限制，則會產生陷阱並將封包切換到CPU，例如生存時間(TTL)過期的封包。

如果資料包不受速率限制，則透過ID為1538的專用內部VLAN交換到CPU。

可以使用show lpts pifib hardware entry brief和show controllers npu stats traps-all 命令驗證LPTS表和Traps表條目。

show lpts pifib hardware entry brief 命令顯示LPTS表條目。

此處，輸出僅限於與邊界網關協定(BGP)關聯的條目。

```
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 命令可列出所有陷阱條目和關聯的計數器。

此處，輸出僅限於「已接受的資料包」和「已丟棄的資料包」列中除所有顯示零的條目以外具有資料包匹配的條目。

請注意，所有陷阱都有速率限制。

```
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#
```

Shell實用程式spp_platform_pcap可用於捕獲NPU與CPU之間透過此專用內部VLAN的資料包。此公用程式也允許擷取透過路由器管理介面傳送或接收的流量。

spp_platform_pcap shell實用程式從shell中執行，並提供多個使用選項。要訪問或登入到shell，請執行run命令。要從shell註銷，請鍵入exit。

```
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:~]$
```

請注意捕獲方向選項-Q，其中值IN表示捕獲傳送的資料包（CPU接收的資料包）。值OUT表示捕獲注入的資料包（CPU傳送的資料包）。選項-p允許捕獲pcap檔案中的資料包。

請考慮以下情況：預設情況下，spp_platform_pcap捕獲：

- 運行60秒。
- 最多可捕獲100個資料包。
- 將所有捕獲的資料包中繼為214位元組。

例如，要開始對CPU接收的所有流量進行未過濾的捕獲，請鍵入命令spp_platform_pcap -Q IN -p：

```
[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:~]$
```

當捕獲結束時，生成的檔案在本地磁碟上可用。

將檔案從路由器複製到您的本機電腦，並使用您偏好的封包解碼器應用程式驗證其內容。

```
[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#
```

您可以針對您的擷取意圖進行更具體的說明。例如，您可以使用實用程式過濾功能來捕獲與特定路由器介面、IP地址或特定協定相關的for-us流量。

例如，使用此命令，您可以捕獲來自特定介面上特定對等體的BGP流量：

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

您還可以使用spp_platform_pcap捕獲透過路由器管理介面傳送或接收的流量。

例如，使用此命令，您可以捕獲從管理介面接收的流量。

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

之前的所有示例都是在獨立的Cisco 8000系列路由器上執行的。如果使用分散式Cisco 8000系列路由器，請考慮在哪個節點、路由處理器或板卡中執行捕獲。

您感興趣的特定流量可能是由特定線卡CPU處理。show controllers npu stats traps-all 和show lpts pifib hardware entry brief 都有助於確定傳送目標。

<#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#
```

辨識後，連線到特定板卡，然後從那裡執行spp_platform_pcap實用程式（如前所示）。

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

相關資訊

Cisco Technical Assistance Center (TAC)影片

思科8000系列-捕獲美國流量、影片

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。