使用8000系列路由器捕获for-US流量

目录

简介

本文档介绍如何在Cisco 8000系列路由器中捕获for-us流量。

先决条件

要求

熟悉Cisco 8000系列路由器和Cisco IOS® XR软件。

使用的组件

本文档中的信息基于Cisco 8000系列路由器，并不限于特定的软件和硬件版本。

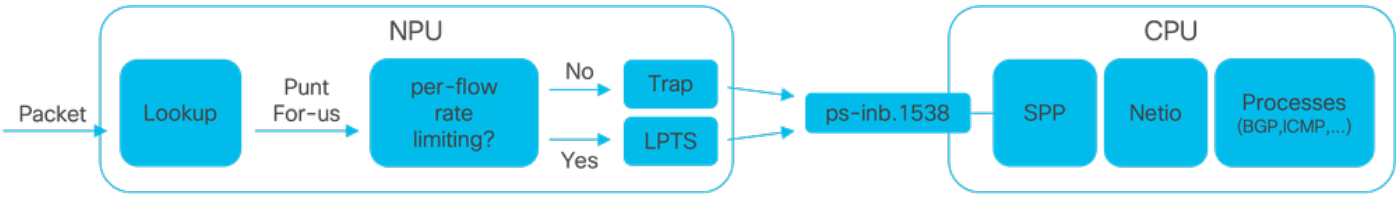
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

在故障排除活动期间，有些情况下需要验证正在切换到中央处理器(CPU)以便进一步处理或处理的流量。

本文旨在说明如何在Cisco 8000系列路由器中捕获此流量。

步骤



映像1 - Cisco 8000系列路由器简化了NPU和CPU图。

当思科8000路由器收到数据包时，网络处理单元(NPU)会执行查找，从而做出转发决策。

有时可能决定传送数据包，即将数据包切换到CPU进行进一步处理或处理。

NPU查找还确定在将数据包交换到CPU时是否需要每流速率限制。

- 如果需要每流量速率限制，则数据包通过本地数据包传输服务(LPTS)（例如路由协议数据包）交换到CPU。
- 如果不需要按流速率限制，则会生成陷阱并将数据包交换到CPU，例如，生存时间(TTL)已过期的数据包。

如果没有速率限制，数据包将通过id为1538的专用内部VLAN交换到CPU。

可以使用show lpts pifib hardware entry brief和show controllers npu stats traps-all命令验证LPTS表和陷阱表条目。

show lpts pifib hardware entry brief命令显示LPTS表条目。

此处，输出仅限于与边界网关协议(BGP)关联的条目。

```
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条目和相关计数器。

此处，输出仅限于数据包匹配项条目，不包括在Packets Accepted和Packets Dropped列中显示为零的所有条目。

请注意，所有陷阱均受速率限制。

```
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#
```

外壳实用程序spp_platform_pcap可用于捕获通过NPU和CPU之间的此专用内部VLAN的数据包。此实用程序还可用于捕获通过路由器管理接口发送或接收的流量。

spp_platform_pcap shell实用程序从shell内部执行，并提供多个使用选项。要访问或登录Shell，请执行run命令。要从shell注销，请键入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:~]$
```

请注意capture direction选项-Q，其中值IN表示捕获传送的数据包（CPU接收的数据包）。值OUT意味着捕获注入的数据包（CPU发送的数据包）。选项-p允许在pcap文件中捕获数据包。

请考虑以下情况：默认情况下，spp_platform_pcap捕获：

- 运行60秒。
- 最多可捕获100个数据包。
- 将所有捕获的数据包中继为214字节。

例如，要开始对CPU接收的所有数据流进行未过滤的捕获，请键入命令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:~]$
```

捕获结束时，本地磁盘上会提供生成的文件。

将文件从路由器复制到本地计算机，然后使用首选数据包解码器应用验证其内容。

```
[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#
```

对于捕获的意图，可以更加具体。例如，您可以利用实用程序过滤器功能捕获与特定路由器接口、IP地址或特定协议相关的for-us流量。

例如，使用此命令，您可以捕获来自特定接口上特定对等体的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
```

您还可以使用spp_platform_pcap 捕获通过路由器管理接口发送或接收的流量。

例如，使用此命令可以捕获从管理接口接收的流量。

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

前面的所有示例都是在独立的Cisco 8000系列路由器上执行的。如果使用分布式Cisco 8000系列路由器，请考虑在哪个节点、路由处理器或线路卡中执行捕获。

您感兴趣的特定流量可能由特定的线卡CPU处理。show controllers npu stats traps-all和show lpts pifib hardware entry brief都有助于识别传送目标。

<#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#
```

识别后，连接到特定板卡，然后从该板卡执行spp_platform_pcap实用程序（如前所示）。

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

相关信息

思科技术支持中心(TAC)视频

思科8000系列-捕获for-us流量、视频

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。