Capturar o tráfego para-US com o roteador 8000 Series

Contents

Introdução

Este documento descreve como capturar o tráfego for-us no roteador Cisco 8000 Series.

Pré-requisitos

Requisitos

Familiaridade com os roteadores Cisco 8000 Series e o software Cisco IOS® XR.

Componentes Utilizados

As informações neste documento são baseadas nos Cisco 8000 Series Routers e não estão restritas a versões específicas de software e hardware.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Durante as atividades de solução de problemas, há casos em que você precisa verificar o tráfego que está sendo comutado para a Unidade Central de Processamento (CPU) para processamento ou tratamento posterior.

O objetivo deste artigo é explicar como esse tráfego pode ser capturado no Cisco 8000 Series Router.

Procedimento

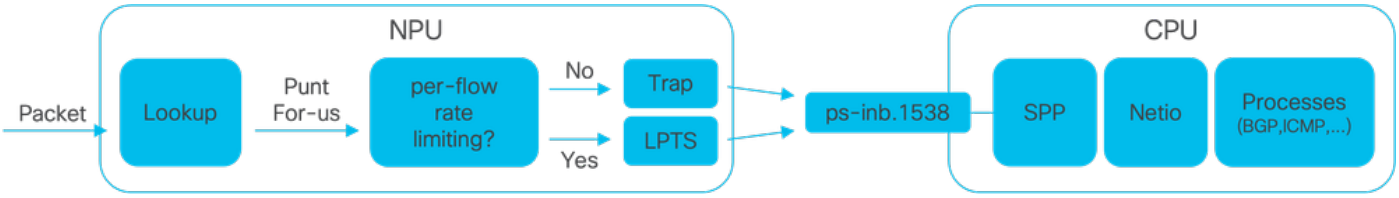

Imagem 1 - O roteador Cisco 8000 Series simplificou o diagrama de NPU e CPU.

Quando um pacote é recebido no roteador Cisco 8000, uma consulta é feita pela NPU (Network Processing Unit, Unidade de processamento de rede), o que resulta em uma decisão de encaminhamento.

Pode haver um caso em que a decisão é apontar o pacote, o que significa comutar o pacote para a CPU para processamento ou tratamento posterior.

A pesquisa de NPU também determina se o limite de taxa por fluxo é necessário durante a comutação do pacote para a CPU.

- Se a limitação de taxa por fluxo for necessária, o pacote será comutado para a CPU através do LPTS (Local Packet Transport Service), por exemplo, um pacote do protocolo de roteamento.
- Se o limite de taxa por fluxo não for necessário, uma interceptação (trapping) será gerada e o pacote será comutado para a CPU, por exemplo, um pacote com Time-to-Live (TTL) expirado.

Os pacotes, se não forem limitados por taxa, são comutados para a CPU através de uma VLAN interna dedicada com id 1538.

Você pode verificar a tabela LPTS e as entradas da tabela Traps usando os comandos show lpts pifib hardware entry brief e show controllers npu stats traps-all.

O comando show lpts pifib hardware entry brief exibe as entradas da tabela LPTS.

Aqui, a saída é limitada às entradas associadas ao BGP (Border Gateway Protocol).

```
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#
```

O comando show controllers npu stats traps-all lista todas as entradas de interceptações e os contadores associados.

Aqui, a saída é limitada a entradas com correspondências de pacotes, excluindo todas as entradas que mostram zero nas colunas Pacotes aceitos e Pacotes descartados.

Observe que todas as interceptações são limitadas por taxa.

```
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#
```

O utilitário shell spp_platform_pcap pode ser usado para capturar pacotes que cruzam essa VLAN interna dedicada entre a NPU e a CPU. Esse mesmo utilitário também permite capturar o tráfego enviado ou recebido através da interface de gerenciamento do roteador.

O utilitário de shell spp_platform_pcap é executado de dentro do shell e fornece várias opções de uso. Para acessar ou fazer login no shell, execute o comando run. Para fazer logout do shell, digite 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:~]$
```

Observe a opção de direção de captura, -Q, em que o valor IN significa que ele captura os pacotes pontuados (os pacotes recebidos pela CPU). O valor OUT significa que ele captura os pacotes injetados (os pacotes enviados pela CPU). A opção -p permite capturar pacotes em um arquivo pcap.

Considere que, por padrão, a captura spp_platform_pcap:

- É executado por 60 segundos.
- Captura um máximo de 100 pacotes.
- Trunca todos os pacotes capturados para 214 bytes.

Por exemplo, para iniciar uma captura não filtrada de todo o tráfego recebido pela CPU, digite o comando 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:~]$
```

Quando a captura termina, o arquivo resultante é disponibilizado no disco local.

Copie o arquivo do roteador para o computador local e verifique seu conteúdo usando seu aplicativo de decodificação de pacotes preferido.

```
[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#
```

É possível ser mais específico em relação à intenção de sua captura. Por exemplo, você pode aproveitar os recursos de filtro do utilitário para capturar o tráfego para uso relacionado a uma interface de roteador específica, a um endereço IP ou a um determinado protocolo.

Como exemplo, usando esse comando, você pode capturar o tráfego BGP de um peer específico em uma interface específica:

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

Você também pode usar spp_platform_pcap para capturar o tráfego enviado ou recebido através da interface de gerenciamento do roteador.

Como exemplo, usando esse comando, você pode capturar o tráfego recebido da interface de gerenciamento.

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

Todos os exemplos anteriores foram executados em um roteador Cisco 8000 Series autônomo. Se estiver trabalhando com um Cisco 8000 Series Router distribuído, considere em que nó, processador de rota ou placa de linha, você deseja que a captura seja executada.

Pode ser que o tráfego específico no qual você está interessado seja manipulado por uma determinada CPU de placa de linha. Os comandos show controllers npu stats traps-all e show lpts pifib hardware entry brief podem ajudar a identificar o destino do punt.

<#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#
```

Uma vez identificado, anexe à placa de linha específica e, a partir daí, execute o utilitário spp_platform_pcap como mostrado antes.

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

Informações Relacionadas

Vídeo do Cisco Technical Assistance Center (TAC)

[Cisco 8000 Series - Captura de tráfego para usuários, vídeo]

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.