Captura de tráfico para Estados Unidos con el router serie 8000

Contenido

Introducción

Este documento describe cómo capturar el tráfico para uso en el Cisco 8000 Series Router.

Prerequisites

Requirements

Familiaridad con los routers Cisco serie 8000 y el software Cisco IOS® XR.

Componentes Utilizados

La información de este documento se basa en los routers Cisco serie 8000 y no está restringida a una versión específica de software y hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Durante las actividades de solución de problemas, hay casos en los que es necesario verificar el tráfico que se está conmutando a la Unidad central de procesamiento (CPU) para su posterior procesamiento o gestión.

En este artículo se explica cómo se puede capturar este tráfico en el router de la serie Cisco 8000.

Procedimiento

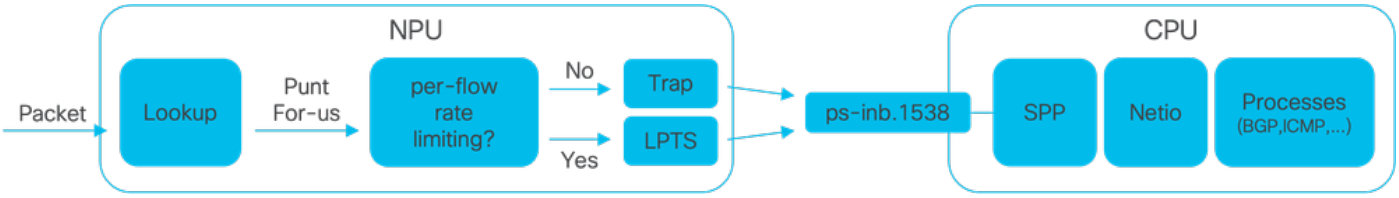

Imagen 1: diagrama simplificado de CPU y NPU de Cisco 8000 Series Router.

Cuando se recibe un paquete En el router Cisco 8000, la Unidad de procesamiento de red (NPU) realiza una búsqueda, lo que da como resultado una decisión de reenvío.

Puede haber un caso en el que la decisión sea perforar el paquete, lo que significa conmutar el paquete a la CPU para un procesamiento o manejo posterior.

La búsqueda de NPU también determina si se requiere limitación de velocidad de flujo al conmutar el paquete a la CPU.

- Si se requiere la limitación de velocidad por flujo, el paquete se conmuta a la CPU a través del Servicio de transporte de paquetes locales (LPTS), por ejemplo, un paquete de protocolo de ruteo.
- Si no se requiere la limitación de velocidad de flujo, se genera una trampa y el paquete se conmuta a la CPU; por ejemplo, un paquete con Tiempo de vida (TTL) caducado.

Los paquetes, si no están limitados por velocidad, se conmutan a la CPU a través de una VLAN interna dedicada con id 1538.

Puede verificar tanto la tabla LPTS como las entradas de la tabla Traps utilizando los comandos show lpts pifib hardware entry brief y show controllers npu stats traps-all.

El comando show lpts pifib hardware entry brief muestra las entradas de la tabla LPTS.

Aquí, la salida se limita a las entradas asociadas con el protocolo de gateway fronterizo (BGP).

```
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#
```

El comando show controllers npu stats traps-all enumera todas las entradas de trampas y los contadores asociados.

Aquí, la salida se limita a las entradas con coincidencias de paquetes excluyendo todas las entradas que muestran cero en las columnas Paquetes aceptados y Paquetes descartados.

Tenga en cuenta que todas las trampas están limitadas por velocidad.

```
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#
```

La utilidad shell spp_platform_pcap se puede utilizar para capturar paquetes que atraviesan esta VLAN interna dedicada entre la NPU y la CPU. Esta misma utilidad también permite capturar el tráfico enviado o recibido a través de la interfaz de administración del router.

La utilidad del shell spp_platform_pcap se ejecuta desde el shell y proporciona varias opciones de uso. Para acceder o iniciar sesión en el shell, ejecute el comando run. Para cerrar sesión desde el shell, escriba 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 la opción de dirección de captura, -Q, donde el valor IN significa que captura los paquetes punteados (los paquetes recibidos por la CPU). El valor OUT significa que captura los paquetes inyectados (los paquetes enviados por la CPU). La opción -p permite capturar paquetes en un archivo pcap.

Tenga en cuenta que, de forma predeterminada, la captura spp_platform_pcap:

- Se ejecuta durante 60 segundos.

- Captura un máximo de 100 paquetes.
- Trunca todos los paquetes capturados a 214 bytes.

Por ejemplo, para iniciar una captura sin filtrar de todo el tráfico recibido por la CPU, escriba el 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:~]$
```

Cuando finaliza la captura, el archivo resultante está disponible en el disco local.

Copie el archivo desde el router al equipo local y verifique su contenido mediante la aplicación de decodificación de paquetes que prefiera.

```
[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 posible ser más específico con respecto a la intención de su captura. Por ejemplo, puede aprovechar las capacidades de filtro de utilidad para capturar el tráfico de uso relacionado con una interfaz de router específica, o una dirección IP, o un protocolo determinado.

Como ejemplo, usando este comando, puede capturar el tráfico BGP desde un peer específico en una interfaz específica:

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

También puede utilizar spp_platform_pcap para capturar el tráfico enviado o recibido a través de la interfaz de administración del router.

Por ejemplo, mediante este comando, puede capturar el tráfico recibido desde la interfaz de administración.

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

Todos los ejemplos anteriores se ejecutaron en un router independiente Cisco serie 8000. Si trabaja con un Cisco 8000 Series Router distribuido, considere en qué nodo, procesador de ruta o tarjeta de línea, desea que se ejecute la captura.

Puede darse el caso de que el tráfico en particular que le interesa sea manejado por una CPU de tarjeta de línea determinada. Tanto el show controllers npu stats traps-all como el show lpts pifib hardware entry brief pueden ayudar a identificar el destino de 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#
```

Una vez identificado, adjunte a la tarjeta de línea específica y, desde allí, ejecute la utilidad spp_platform_pcap como se muestra anteriormente.

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

Información Relacionada

Vídeo del centro de asistencia técnica Cisco Technical Assistance Center (TAC)

[Cisco serie 8000 - Captura de tráfico para uso personal, vídeo]

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).