8000シリーズルータでのUSトラフィックのキャプチャ

内容

はじめに

このドキュメントでは、Cisco 8000シリーズルータでfor-usトラフィックをキャプチャする方法について説明します。

前提条件

要件

Cisco 8000シリーズルータおよびCisco IOS® XRソフトウェアに関する知識。

使用するコンポーネント

このドキュメントの情報は、Cisco 8000シリーズルータに基づくものであり、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

トラブルシューティングの作業中に、処理や処理を進めるために中央処理装置(CPU)にスイッチングされているトラフィックを確認する必要がある場合があります。

この記事では、このトラフィックをCisco 8000シリーズルータでキャプチャする方法について説明します。

手順

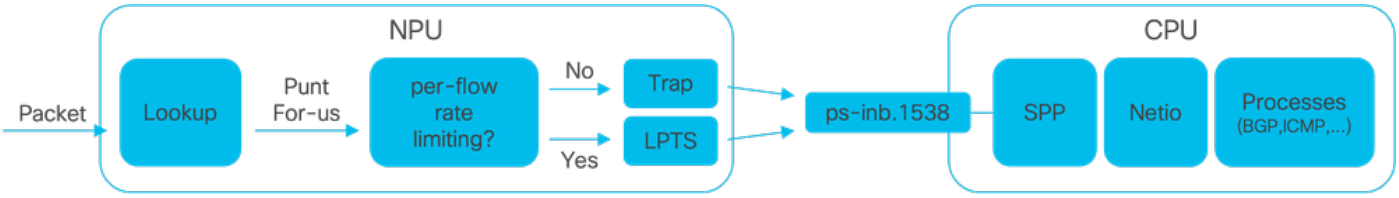

図1:Cisco 8000シリーズルータの簡単なNPUとCPUの図

Cisco 8000ルータでパケットが受信されると、ネットワーク処理ユニット(NPU)によってルックアップが実行され、転送の決定が行われます。

パケットをパントする、つまり、処理または処理のためにパケットをCPUに切り替えることを決定する場合があります。

NPUルックアップは、パケットをCPUにスイッチングする際にフローごとのレート制限が必要かどうかも判断します。

- フローごとのレート制限が必要な場合、パケットはLocal Packet Transport Service(LPTS)経由でCPUにスイッチングされます（ルーティングプロトコルパケットなど）。
- フローごとのレート制限が不要な場合は、トラップが生成され、パケットはCPUにスイッチングされます。たとえば、存続可能時間(TTL)が切れたパケットがこれに該当します。

レート制限されていないパケットは、ID 1538の専用の内部VLAN経由でCPUにスイッチングされます。

show lpts pifib hardware entry briefコマンドとshow controllers npu stats traps-allコマンドを使用すると、LPTSテーブルとTrapsテーブルの両方のエントリを確認できます。

show lpts pifib hardware entry briefコマンドは、LPTSテーブルエントリを表示します。

ここでは、出力はボーダーゲートウェイプロトコル(BGP)に関連付けられたエントリに限定されています。

```
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コマンドは、すべてのトラップエントリと関連カウンタをリストします。

ここでは、出力は、パケット一致があるエントリに限定され、Packets AcceptedカラムとPackets Droppedカラムの値が0であるすべてのエントリが除外されます。

すべてのトラップはレート制限されています。

```
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#
```

シェルユーティリティspp_platform_pcapを使用して、NPUとCPU間の専用の内部VLANを通過するパケットをキャプチャできます。この同じユーティリティを使用して、ルータ管理インターフェイスを介して送受信されるトラフィックをキャプチャすることもできます。

spp_platform_pcapシェルユーティリティはシェル内から実行され、複数の使用法オプションを提供します。シェルにアクセスまたはログインするには、runコマンドを実行します。シェルからログアウトするには、exitと入力します。

```
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:~]$
```

キャプチャ方向オプション-Qに注意してください。ここで、値INはパントされたパケット（CPUで受信されたパケット）をキャプチャすることを意味します。値OUTは、注入されたパケット（CPUによって送信されたパケット）をキャプチャすることを意味します。オプション-pを使用すると、pcapファイルでパケットをキャプチャできます。

デフォルトでは、spp_platform_pcapキャプチャは次の点に注意してください。

- 60秒間実行します。

- 最大100パケットをキャプチャします。
- キャプチャされたすべてのパケットを214バイトに切り捨てます。

たとえば、CPUが受信するすべてのトラフィックのフィルタリングされていないキャプチャを開始するには、コマンドspp_platform_pcap -Q IN -pを入力します。

```
[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:~]$
```

キャプチャが終了すると、結果のファイルがローカルディスクで使用できるようになります。

このファイルをルータからローカルコンピュータにコピーし、必要なパケットデコーダアプリケーションを使用してその内容を確認します。

```
[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#
```

キャプチャの目的に関して、より具体的になる場合があります。たとえば、ユーティリティフィルタ機能を利用して、特定のルータインターフェイス、IPアドレス、または特定のプロトコルに関連するFor-Usトラフィックをキャプチャできます。

たとえば、次のコマンドを使用して、特定のインターフェイスの特定のピアからのBGPトラフィックをキャプチャできます。

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

spp_platform_pcapを使用して、ルータ管理インターフェイスで送受信されるトラフィックをキャプチャすることもできます。

例として、このコマンドを使用して、管理インターフェイスから受信したトラフィックをキャプチャできます。

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

これまでの例はすべて、スタンドアロンのCisco 8000シリーズルータで実行しました。分散型のCisco 8000シリーズルータを使用する場合は、どのノード、ルートプロセッサ、またはラインカードでキャプチャを実行するかを検討します。

対象とする特定のトラフィックが特定のラインカードのCPUで処理されている場合があります。show controllers npu stats traps-allとshow lpts pifib hardware entry briefはどちらも、パントの宛先の識別に役立ちます。

<#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#
```

識別されたら、特定のラインカードに接続し、そこから前述のようにspp_platform_pcapユーティリティを実行します。

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

関連情報

Cisco Technical Assistance Center(TAC)ビデオ

[Cisco 8000シリーズ：米国のトラフィックのキャプチャ、ビデオ]

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。