# Capturer le trafic pour les États-Unis avec le routeur de la gamme 8000

## Table des matières


[Introduction](#)

[Conditions préalables](#)

- [Exigences](#)
- [Composants utilisés](#)

[Informations générales](#)

[Procédure](#)

[Informations connexes](#)


## Introduction

Ce document décrit comment capturer le trafic pour utilisation dans le routeur de la gamme Cisco 8000.

## Conditions préalables

### Exigences

Connaissance des routeurs de la gamme Cisco 8000 et du logiciel Cisco IOS® XR.

### Composants utilisés

Les informations contenues dans ce document sont basées sur les routeurs de la gamme Cisco 8000 et ne sont pas limitées à des versions logicielles et matérielles spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

## Informations générales

Au cours des activités de dépannage, il peut arriver que vous deviez vérifier le trafic qui est commuté vers l'unité centrale (UC) pour un traitement ou un traitement ultérieur.

Cet article explique comment ce trafic peut être capturé dans les routeurs de la gamme Cisco 8000.

## Procédure

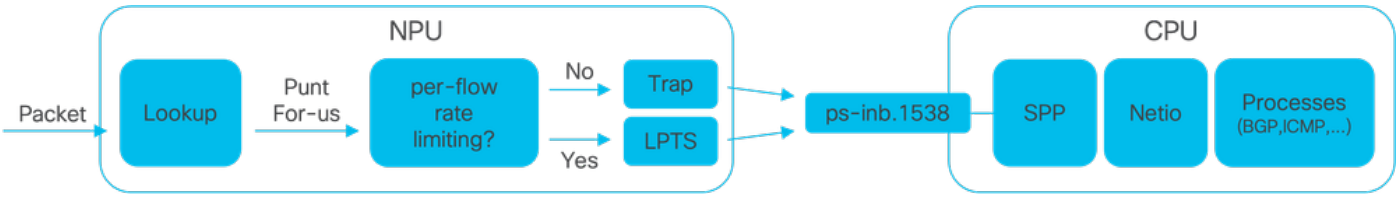


Image1 - Schéma simplifié du processeur et du processeur des routeurs de la gamme Cisco 8000.

Lorsqu'un paquet est reçu sur le routeur Cisco 8000, une recherche est effectuée par l'unité de traitement réseau (NPU), ce qui entraîne une décision de transmission.

Il peut arriver que la décision consiste à envoyer le paquet, c'est-à-dire à le transférer vers le processeur pour traitement ou traitement ultérieur.

La recherche NPU détermine également si une limitation du débit par flux est requise lors de la commutation du paquet vers le processeur.

- Si la limitation du débit par flux est requise, le paquet est commuté vers le processeur via le service LPTS (Local Packet Transport Service), par exemple un paquet de protocole de routage.
- Si la limitation du débit par flux n'est pas requise, un déroutement est généré et le paquet est commuté vers le processeur, par exemple, un paquet dont la durée de vie (TTL) a expiré.

Les paquets, s'ils ne sont pas limités en débit, sont commutés vers le CPU via un VLAN interne dédié avec l'ID 1538.

Vous pouvez vérifier à la fois les entrées de la table LPTS et de la table Traps en utilisant les commandes show lpts pifib hardware entry brief et show controllers npu stats traps-all.

La commande show lpts pifib hardware entry brief affiche les entrées de la table LPTS.

Ici, le résultat est limité aux entrées associées au protocole 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#
```

La commande show controllers npu stats traps-all répertorie toutes les entrées de traps et les compteurs associés.

Ici, le résultat est limité aux entrées avec des correspondances de paquets, à l'exclusion de toutes les entrées affichant zéro dans les colonnes Packets Accepted et Packets Dropped.

Notez que tous les déroutements sont à débit limité.

```
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#
```

L'utilitaire d'interpréteur de commandes spp_platform_pcap peut être utilisé pour capturer des paquets qui traversent ce VLAN interne dédié entre le NPU et le CPU. Ce même utilitaire permet également de capturer le trafic envoyé ou reçu via l'interface de gestion du routeur.

L'utilitaire shell spp_platform_pcap est exécuté à partir du shell et fournit plusieurs options d'utilisation. Pour accéder au shell ou s'y connecter, exécutez la commande run. Pour vous déconnecter de l'interpréteur de commandes, tapez 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:~]$
```

Notez l'option de direction de capture, -Q, où la valeur IN signifie qu'elle capture les paquets pointés (les paquets reçus par le CPU). La valeur OUT signifie qu'elle capture les paquets injectés (les paquets envoyés par le CPU). L'option -p permet de capturer des paquets dans un fichier pcap.

Veuillez considérer que, par défaut, la capture spp_platform_pcap :

- Fonctionne pendant 60 secondes.
- Capture un maximum de 100 paquets.
- Tronque tous les paquets capturés à 214 octets.

Par exemple, pour lancer une capture non filtrée de tout le trafic reçu par le processeur, tapez la commande 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:~]$
```

À la fin de la capture, le fichier obtenu est mis à disposition sur le disque local.

Copiez le fichier du routeur vers votre ordinateur local et vérifiez son contenu à l'aide de l'application de décodage de paquets de votre choix.

```
[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#
```

Il est possible d'être plus précis en ce qui concerne l'intention de votre capture. Par exemple, vous pouvez tirer parti des fonctionnalités de filtre d'utilitaire pour capturer le trafic à usage spécifique associé à une interface de routeur, une adresse IP ou un protocole spécifique.

Par exemple, en utilisant cette commande, vous pouvez capturer le trafic BGP d'un homologue spécifique sur une interface spécifique :

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

Vous pouvez également utiliser spp_platform_pcap pour capturer le trafic envoyé ou reçu via l'interface de gestion du routeur.

Par exemple, à l'aide de cette commande, vous pouvez capturer le trafic reçu de l'interface de gestion.

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

Tous les exemples précédents ont été exécutés sur un routeur Cisco 8000 autonome. Si vous travaillez avec un routeur Cisco 8000 distribué, déterminez dans quel noeud, processeur de routage ou carte de ligne vous souhaitez exécuter la capture.

Il peut arriver que le trafic particulier qui vous intéresse soit géré par un certain CPU de carte de ligne. Les deux instructions show controllers npu stats traps-all et show lpts pifib hardware entry brief peuvent aider à identifier la destination 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#
```

Une fois identifié, joignez-le à la carte de ligne spécifique, puis exécutez l'utilitaire spp_platform_pcap comme indiqué précédemment.

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

## Informations connexes

Vidéo du centre d'assistance technique Cisco (TAC)

[Gamme Cisco 8000 - Capture de trafic utilisateur, vidéo]

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.