Troubleshooting Drops en NCS 5500

Comunidad de Cisco

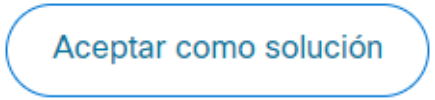
Adán de la Luz Márquez – Escalation Engineer (TAC)
Eduardo Ramírez – Technical Leader (TAC)
Héctor Carranza – Technical Leader (TAC)

Jueves 29 de febrero de 2024

Conecte, Interactúe, ¡Colabore!

Soluciones

Ayuda a otros usuarios a encontrar las respuestas correctas en el motor de búsqueda de la comunidad indicando que la duda fue resuelta al activar la opción “Aceptar como solución” u otórgales un voto de utilidad.



Votos de utilidad

¡Resalta el esfuerzo de otros miembros!

Los votos útiles motivan a otros miembros que colaboran en la comunidad, a seguir ayudándonos a contestar las preguntas abiertas, y ofreciéndoles la oportunidad de ganar premios. ¡Reconoce su esfuerzo!

Premios Spotlight Awards

¡Destaca por tu esfuerzo y compromiso para mejorar la comunidad y ayudar a otros miembros!

Los Premios Spotlight se otorgan trimestralmente para reconocer a los miembros más destacados.

Conoce a los ganadores de Noviembre-Enero 2024

¡Ahora también puedes nominar a un candidato! Haga clic aquí

Nuestros expertos

Adán De la Luz Márquez

Escalation Engineer SP XR

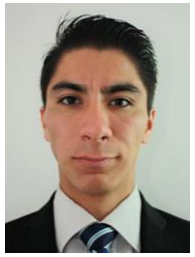
Es actualmente Ingeniero de Escalación para el equipo de Service Provider XR. Lleva cinco años trabajando en Cisco y es egresado de la Universidad Nacional Autónoma de México (UNAM).

Desde hace diez años ha trabajado en diferentes roles de telecomunicaciones y dentro de Cisco ha participado en distintas áreas. Adán está certificado en CCIE R&S #64201, Devnet y CCNP Service Provider

Descarga la presentación https://bit.ly/CL5doc-feb24

Nuestros expertos

Eduardo Ramírez



Technical Leader SP Access

Es Líder Técnico de Service Provider Access. Egresado del Instituto Politécnico Nacional (IPN) de México.

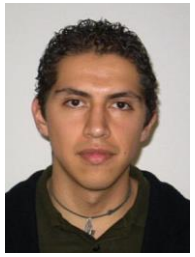
Lleva ocho años trabajando en Cisco dentro de diferentes áreas como Servicios Profesionales y TAC para proveedores de servicio de todo el mundo.

Eduardo también tiene diez años de experiencia laboral y está certificado CCIE de Service Provider, CCNP Enterprise y DevNet.

Descarga la presentación https://bit.ly/CL5doc-feb24

Nuestros expertos

Héctor Carranza



Technical Leader SP XR

Es Líder Ténico de Service Provider XR. Egresado del Instituto Tecnológico de Estudios Superiores de Monterrey, Campus Edo. de México (ITESM CEM) de la carrera de Ingeniería en Sistemas Computacionales.

Lleva 12 años trabajando en Cisco en el área de Soporte Técnico a proveedores de Servicio de Internet y Telefonía Celular de todo el mundo, con experiencia en tecnologías de Ruteo, Switching y conocimiento de plataformas como CRS, ASR9000, NCS5500 y Cisco 8000.

Además, Héctor tiene más de quince años de experiencia laboral y cuenta con certificación CCIE Enterprise R&S #42717, Devnet y CCNP Service Provider.

Descarga la presentación https://bit.ly/CL5doc-feb24

slido

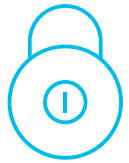
Join at

slido.com

#6878 562

Passcode: **wcdw71**

Agenda



1. ¿Qué es un drop?
2. Arquitectura
3. Vida del paquete
4. Herramientas para troubleshooting
5. Troubleshooting de paquetes dropeados
6. Laboratorio

Active poll

0

Join at

slido.com

#6878 562

Passcode:

wcdw71

¿Cuáles son los problemas operacionales más comunes que enfrenta en su red?

a) Pérdida de paquetes

0%

b) Inestabilidad en enlaces

0%

c) Gestión de sistema operativo

0%

d) Problemas de hardware

0%

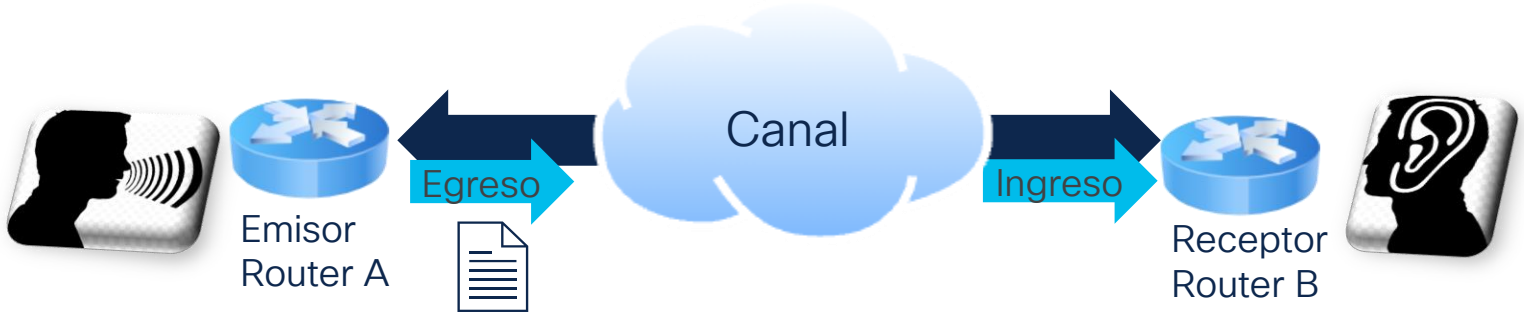
e) Licenciamiento

0%

¿Qué es un drop?

Elementos de comunicación

Tiempo 1



Unidireccional

Tiempo 2

Bidireccional

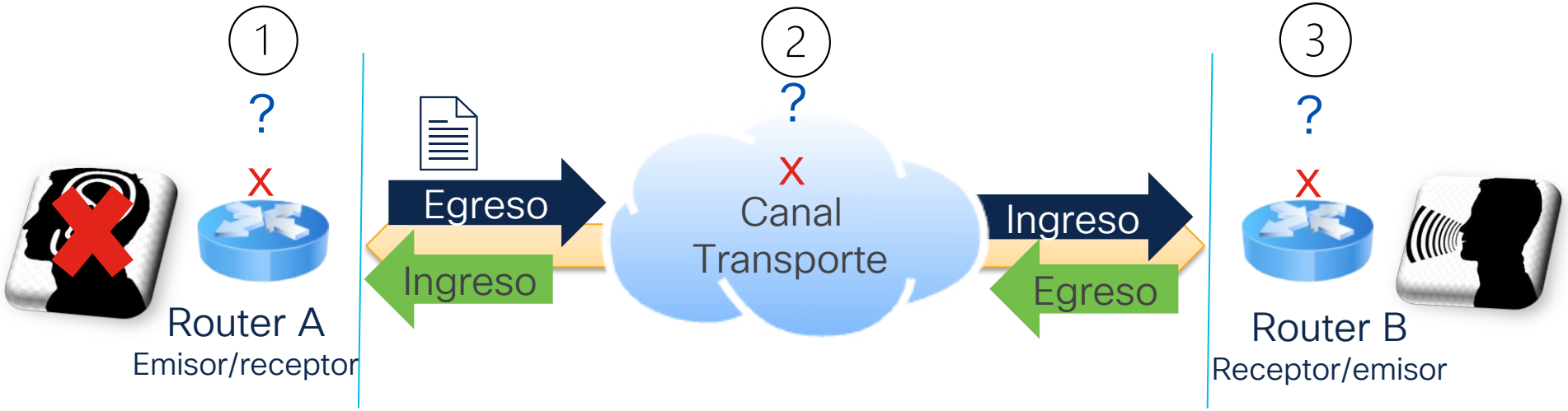
¿Qué es un drop?

La pérdida de paquetes se produce cuando al menos uno de los paquetes de datos que viajan por la red no alcanza su destino.

```
RP/0/RP0/CPU0:RouterA#ping 10.1.2.1 repeat 10

Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 10.1.2.1 timeout is 2 seconds:
..........
Success rate is 0 percent (0/10)
RP/0/RP0/CPU0:RouterA#
```

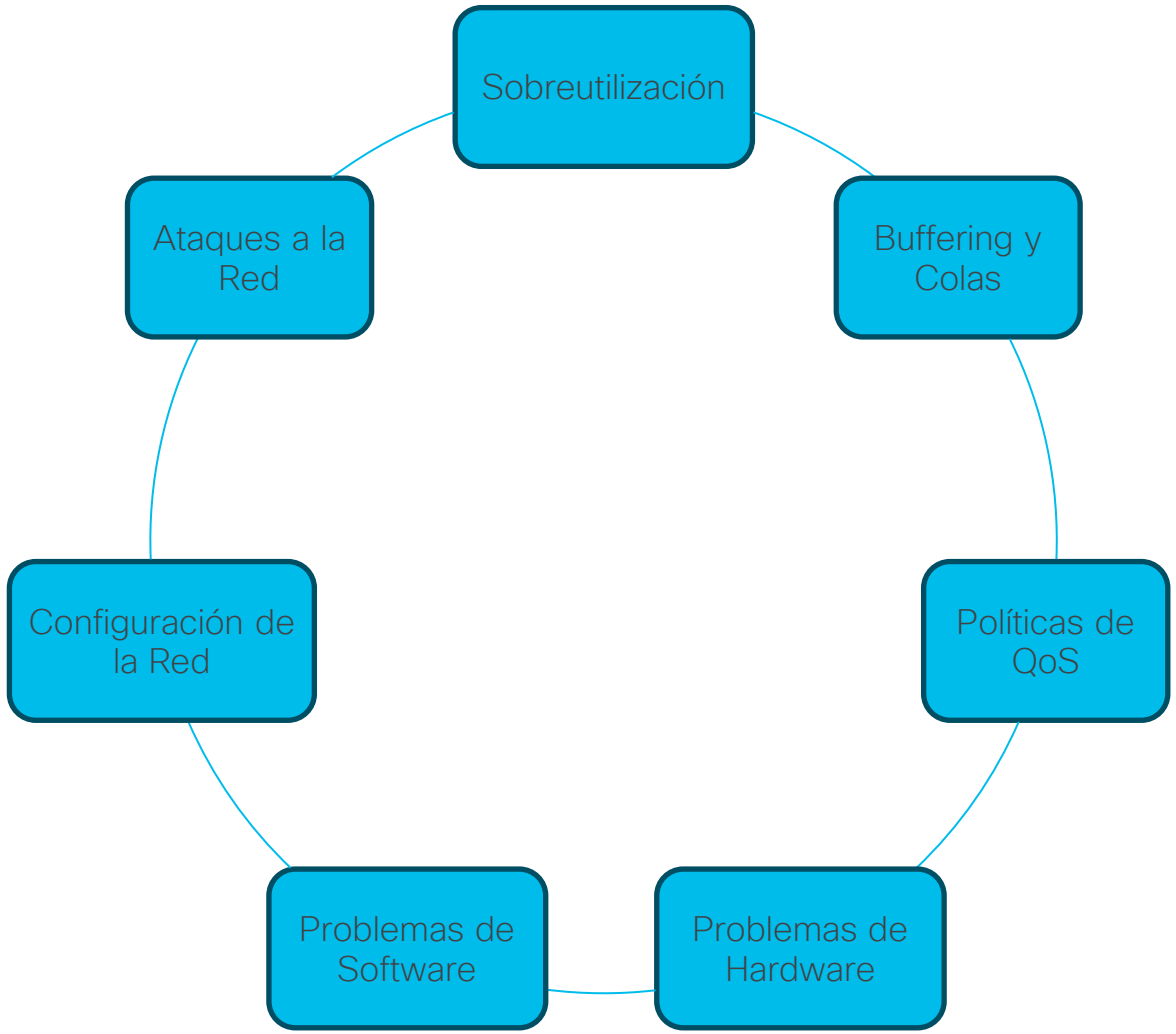
Se mide en porcentaje de paquetes perdidos por enviados.



Causas comunes de drops

Pueden ocurrir debido a múltiples razones.

Comprender las causas puede ayudar a solucionar problemas en la red de una manera efectiva.



¿Cómo aislar los drops?

Para poder encontrar el elemento que está tirando paquetes en la red, debemos comprender, al menos los siguientes puntos:

Independiente de la plataforma

- Escenario, topología.
- Identificar fuente, destino, transporte.
- Herramientas para troubleshooting de drops, ACL, SPAN, comandos, ping, traceroute, etc.

Dependiente de la Plataforma

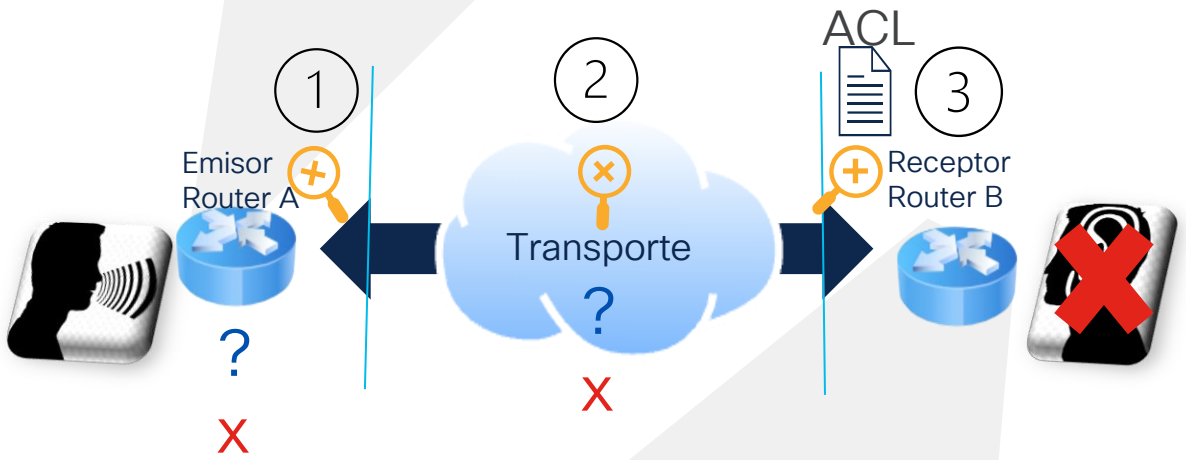
- Arquitectura de la plataforma (NCS5500).
- Ciclo de vida del paquete dentro de la plataforma (NCS5500).
- Tipos de tráfico internos en la plataforma: local, tránsito.
- Comandos

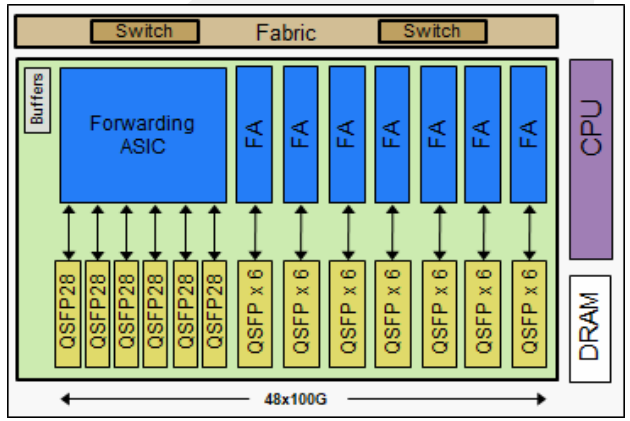
Se recomienda ir de lo general a lo particular.

¿Dónde está la falla?

RP (Route Processor)

LC (Line Card)





Active poll

0

Join at

slido.com

#6878 562

Passcode:

wcdw71

¿Cómo aislaría un problema de pérdida de paquetes en su red?

a) Con ping

0%

b) Traceroute

0%

c) Capturas

0%

d) Comandos

0%

e) Llamando a TAC

0%

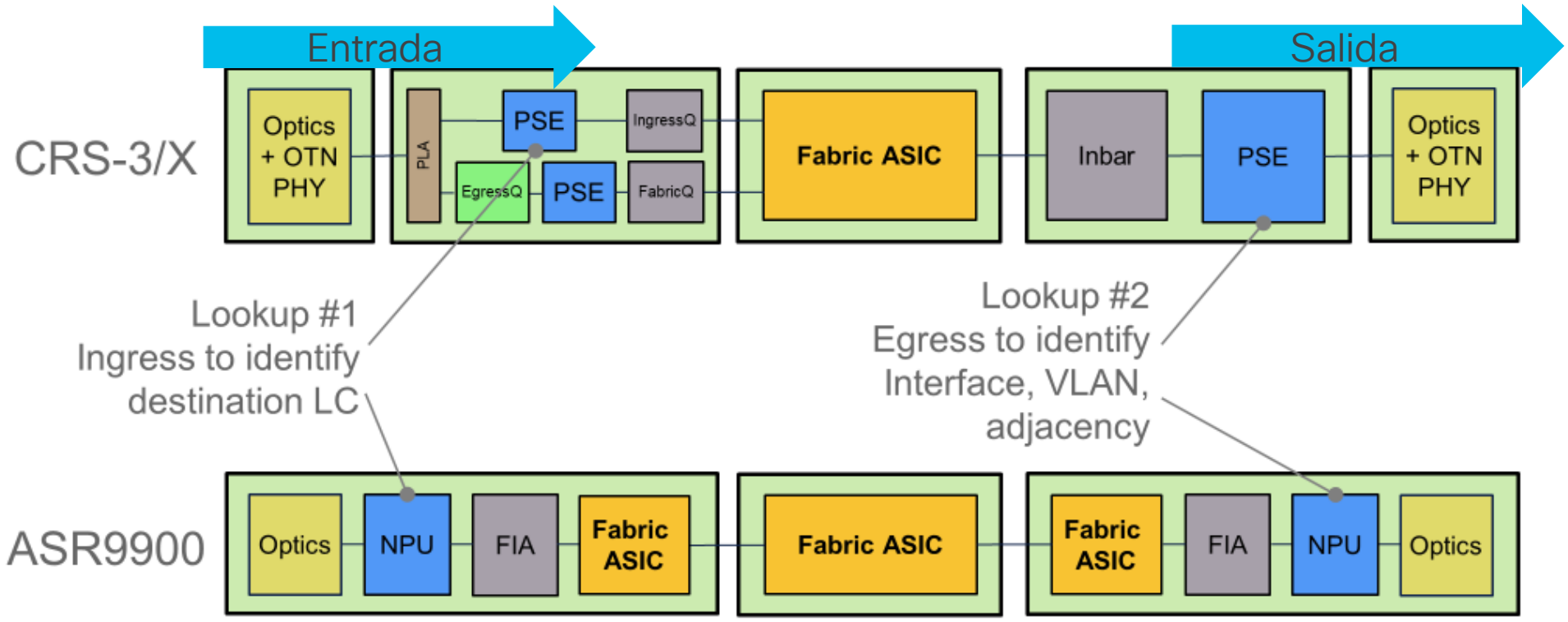
f) Lista de acceso

0%

Arquitectura

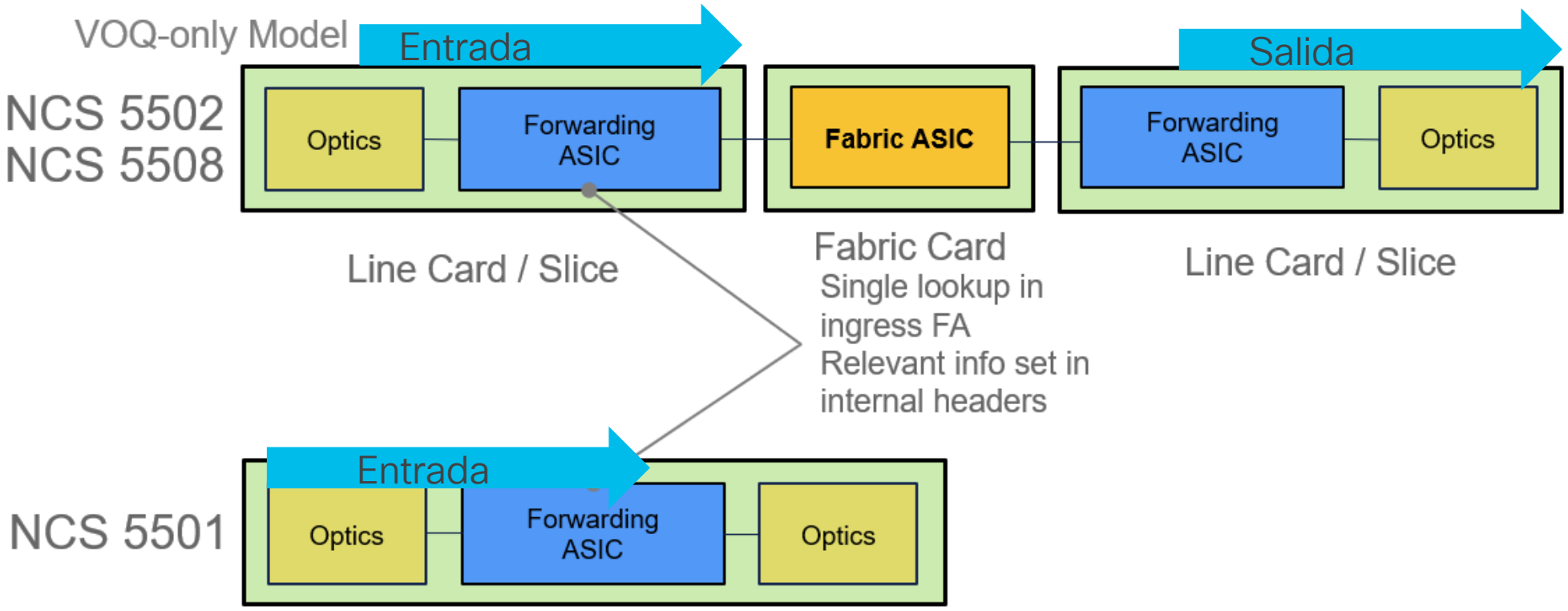
Comparación con arquitecturas tradicionales de XR

Dos búsquedas para el envío de tráfico.
En la tarjeta de entrada y en la tarjeta de salida.



Comparación con arquitecturas tradicionales de XR

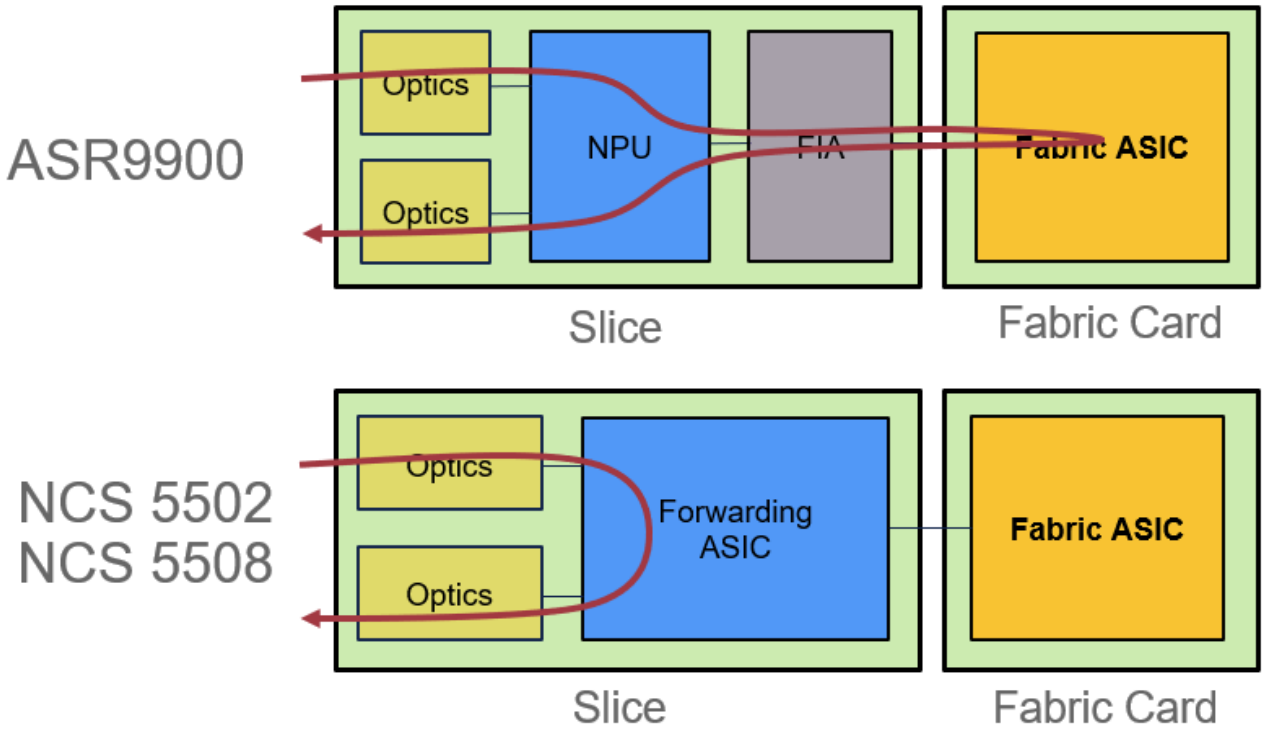
Se simplifica el proceso.
Solo una búsqueda en la tarjeta de entrada.



Envío de tráfico en la misma Line Card

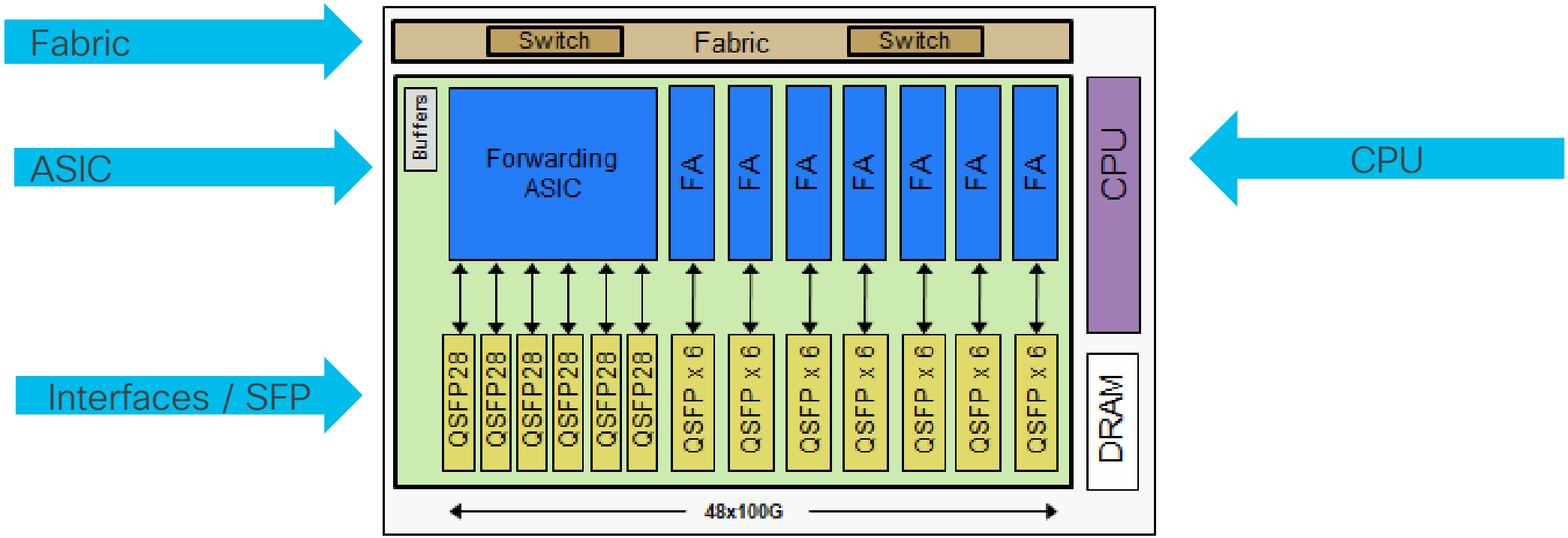
El envío de tráfico dentro de la misma tarjeta se maneja de manera local.

Disminuye la latencia de los paquetes.



NCS 5502 Base / Scale

TAC Tip

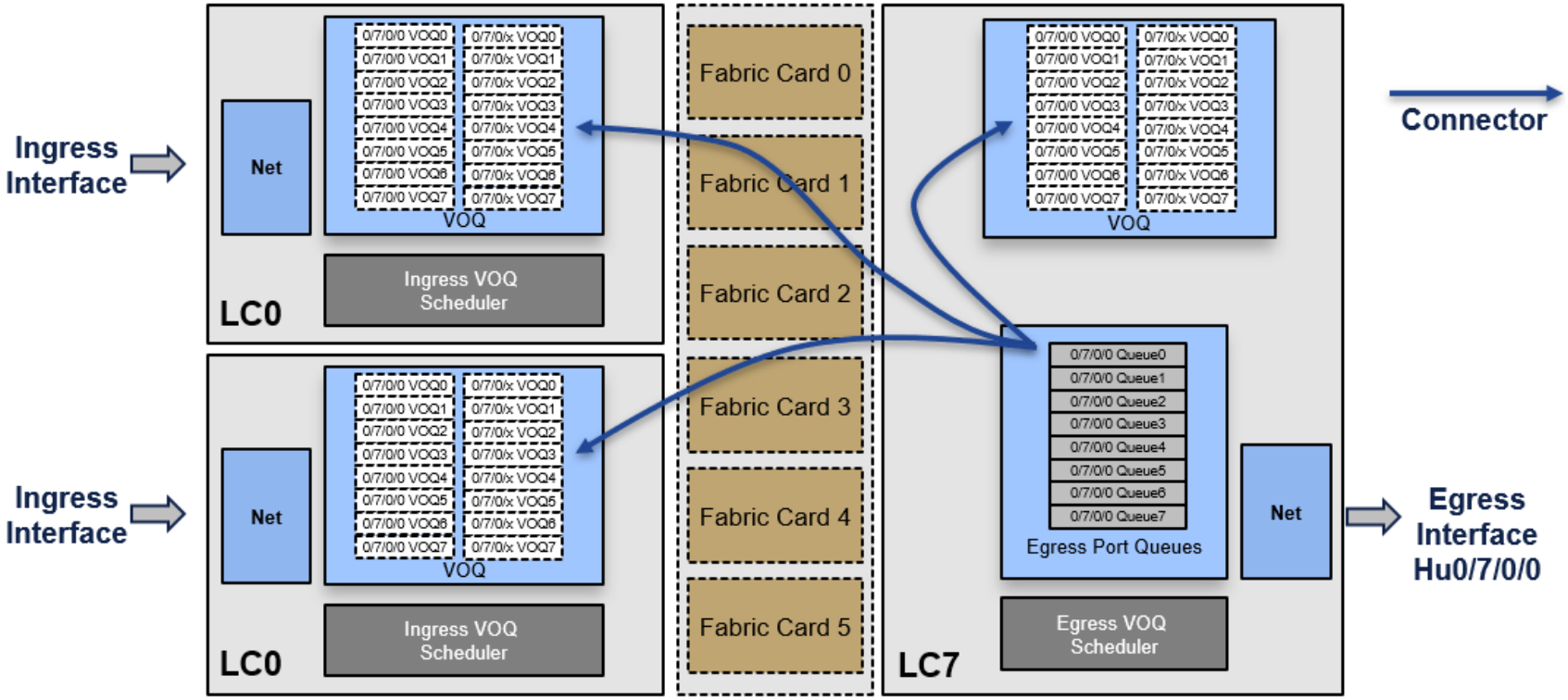


4.8 Tbps line-rate 100G < 2000W (SR optics)
48x 100G QSFP28 (or QSFP+)
8x 600 Gbps Forwarding ASICs
720 Mpps per FA

Virtual Output Queue (VOQ)

Representa las colas de espera o "buffers" de todas las interfaces de salida.

Son replicadas a todas las tarjetas o dispositivos de entrada, así todas las tarjetas tienen un mapeo de los buffers de las demás tarjetas.

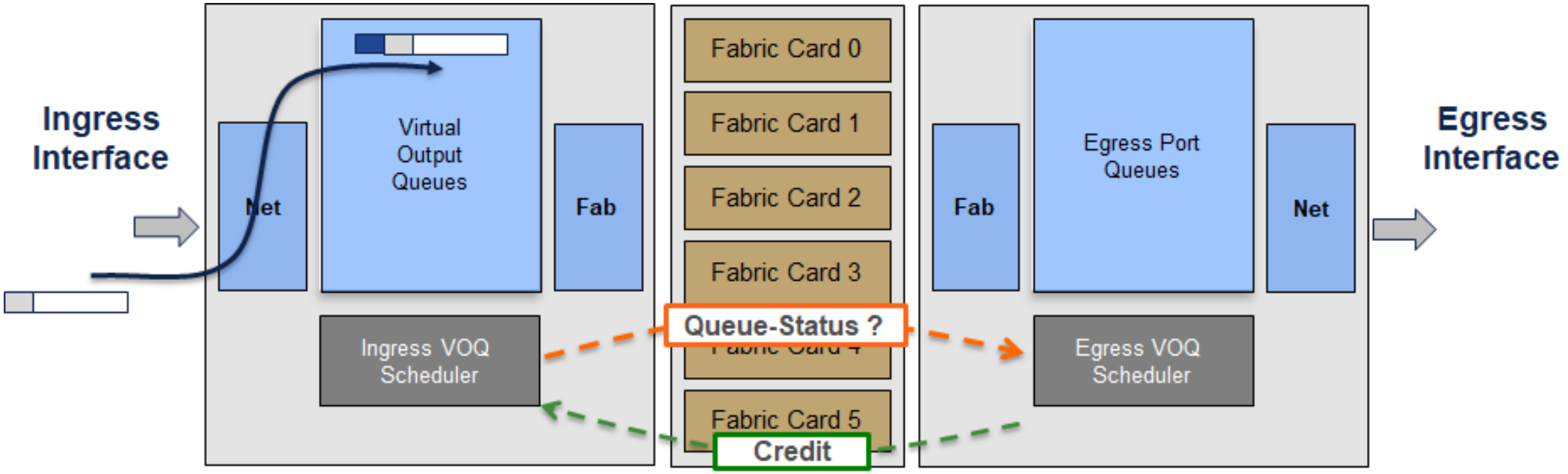


VOQ Architecture

Al recibirse el paquete se clasifica y almacena en pequeños buffers.

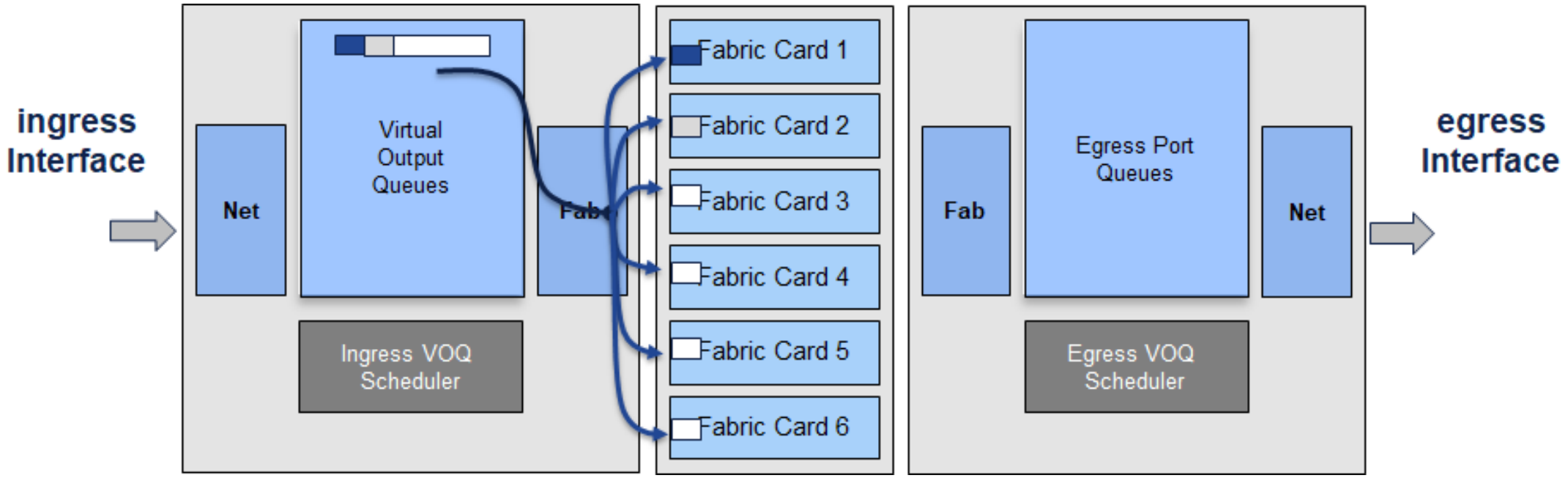
Se realiza una única búsqueda para determinar LC y puerto de salida.

Ingress-VOQ scheduler solicita por créditos para mandar el tráfico al Egress-VOQ scheduler.



VOQ Architecture

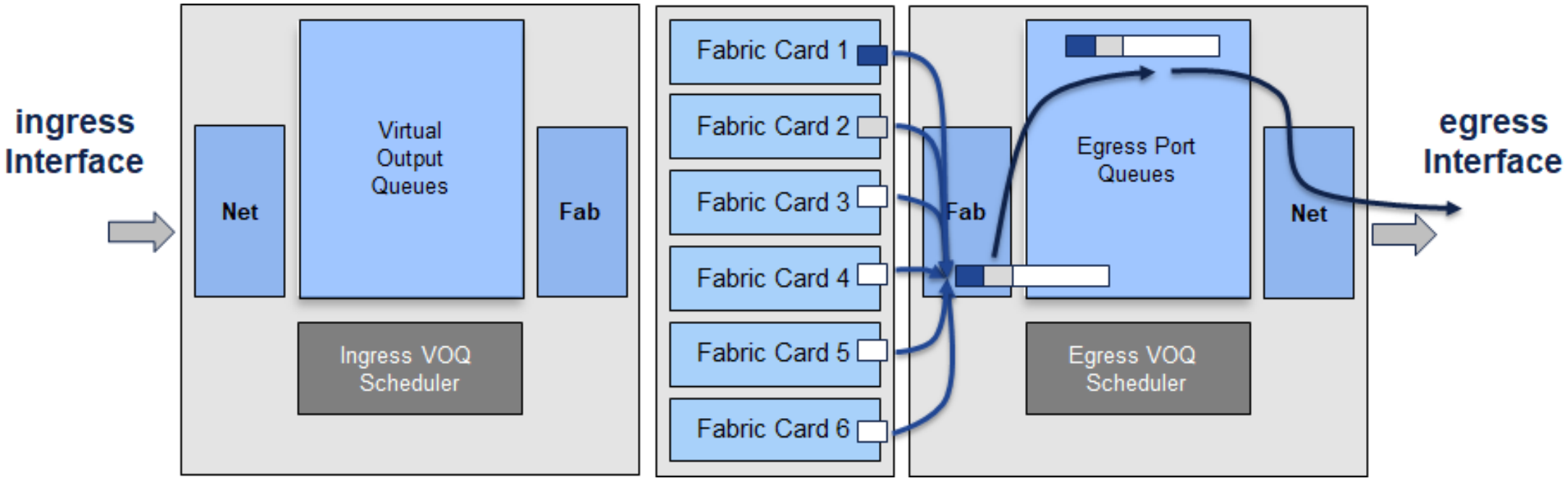
El paquete se divide en células y es repartido entre las diferentes Fabric Cards para su envío y transporte a la tarjeta de salida.



VOQ Architecture

Finalmente las células se reciben en la tarjeta de salida.

El paquete es reensamblado y almacenado en el buffer de salida de la interfaz, listo para ser enviado.



Active poll

0

Join at

slido.com

#6878 562

Passcode:

wcdw71

¿En el día a día con cuáles plataformas IOS-XR, IOS-XE interactúa?

a) ASR 900

0%

b) ASR 9000

0%

c) Cisco 8000

0%

d) NCS 500

0%

e) NCS 5500 y/o NCS 5000

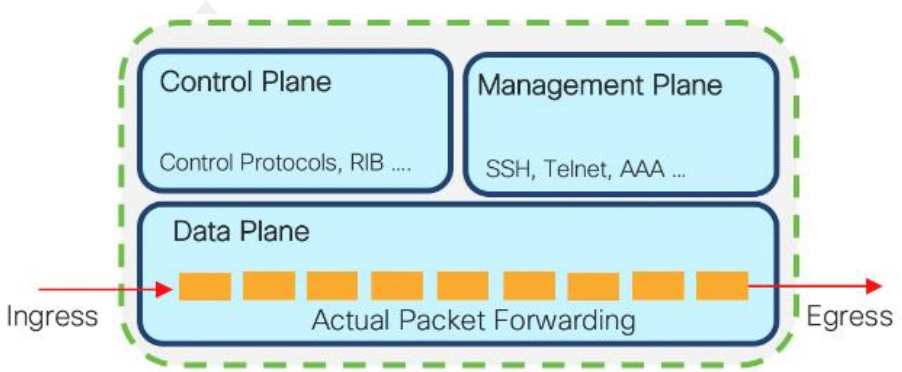
0%

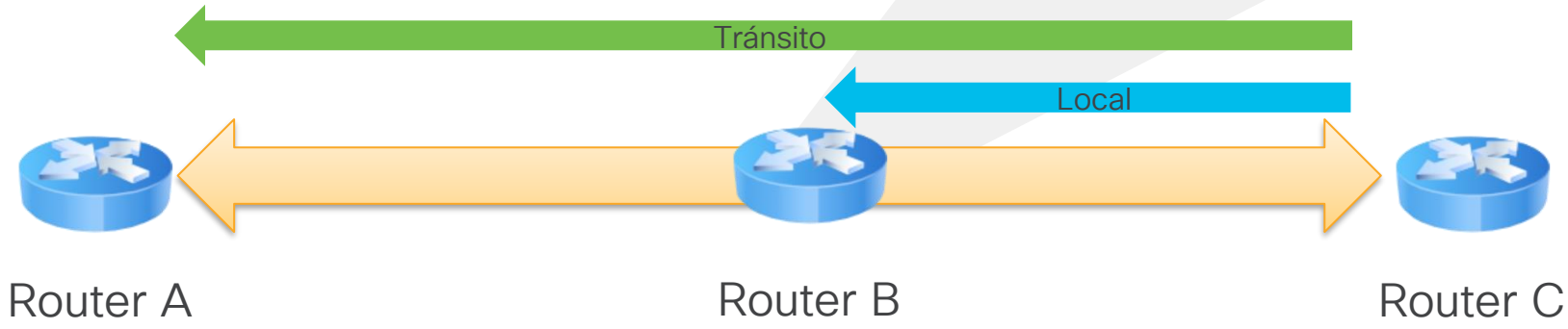
Vida del Paquete

Tipos de Tráfico

Dentro de la vida del paquete tenemos dos tipos de tráfico:

- Tránsito – El paquete cruza el equipo.
- Local – El paquete se origina o termina en el equipo

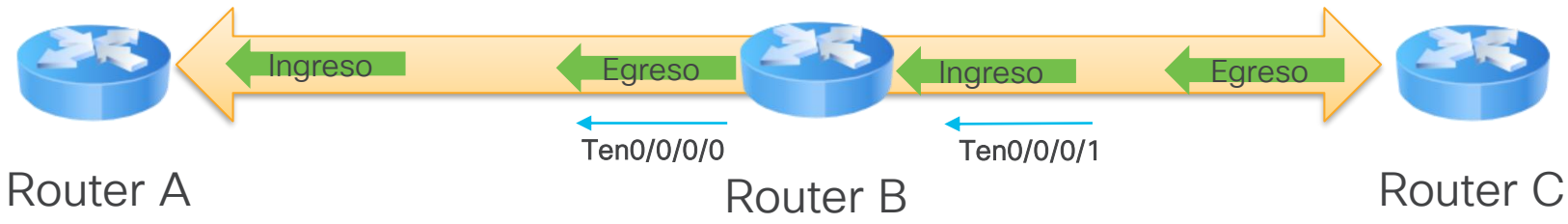




Tráfico de tránsito

Son los paquetes que no están destinados al router, por lo tanto, sus características son:

- Interface de entrada.
- Procesamiento en el router.
- Interface de salida.



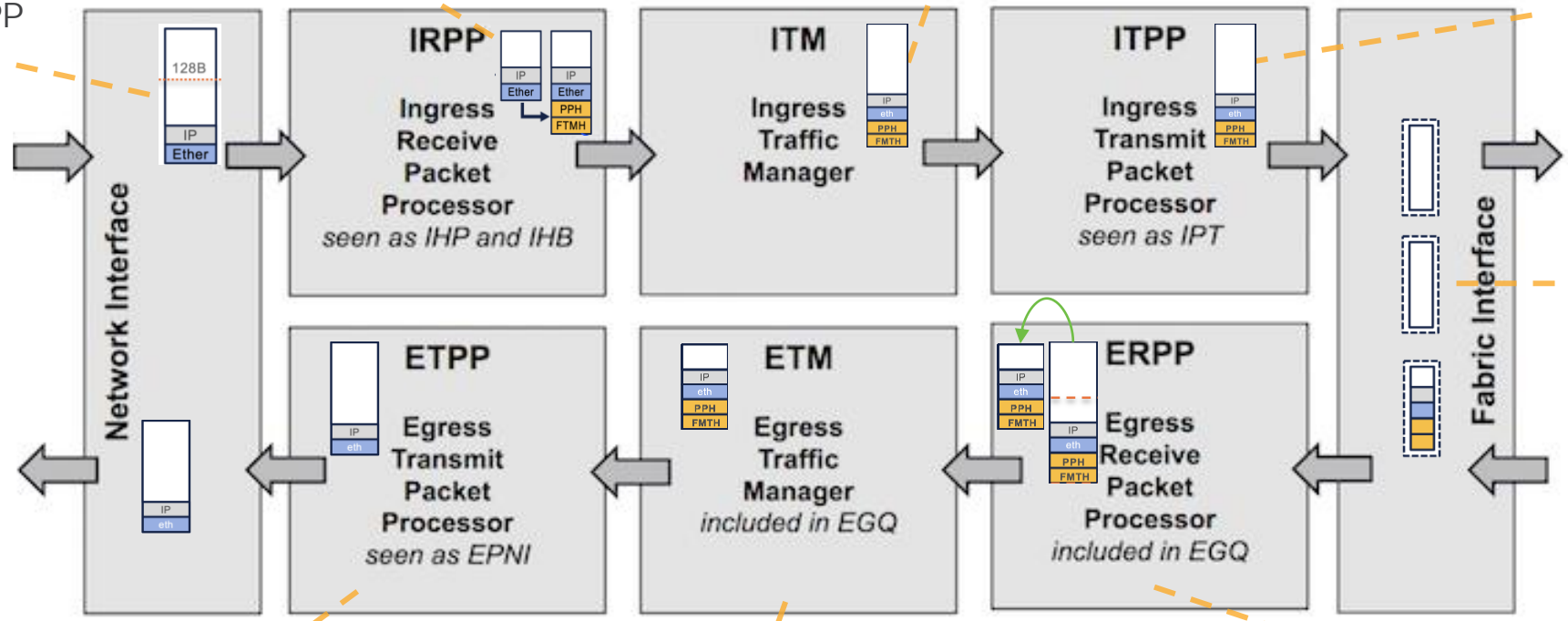
Tráfico de tránsito – Procesamiento en el router

Los primeros 128 bytes son removidos y procesados. Como resultado un encabezado interno es agregado y se elige la VOQ.

El paquete es guardado en memoria DRAM, las políticas de QoS son aplicadas y se solicitan créditos.

Los paquetes son divididos en células y se envían al Fabric. Se edita el encabezado interno si hay necesidad (SPAN, Replicación de multicast, etc.)

Se recibe un paquete en la interface de entrada/CPU/recirculación, se envía al IRPP



Las células se propagan por el/los fabric card(s)

Se remueven los encabezados del sistema y el paquete se envía a la interface de salida

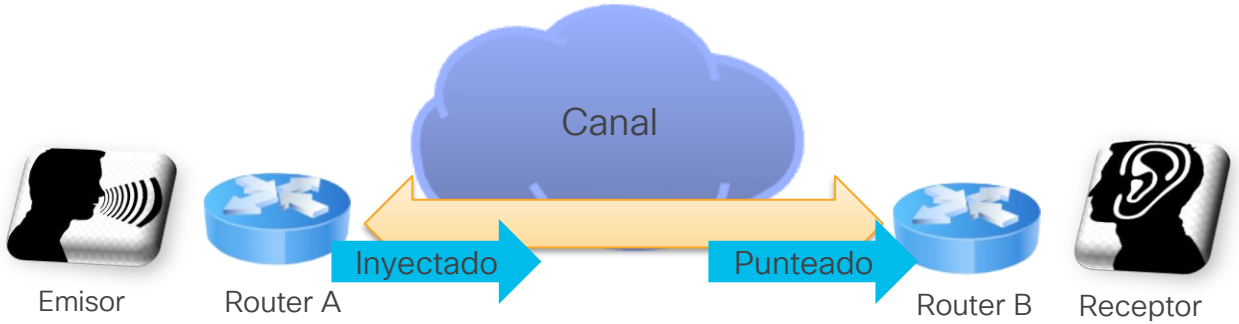
El paquete entero es guardado en buffer hasta que es despachado para la transmisión

Las células son recibidas y los paquetes son reensamblados. Se extraen los primeros 128 bytes, se elige el puerto de salida (replicación de multicast) y se aplican los filtros de capa 2, ACL de salida.

Tráfico Local

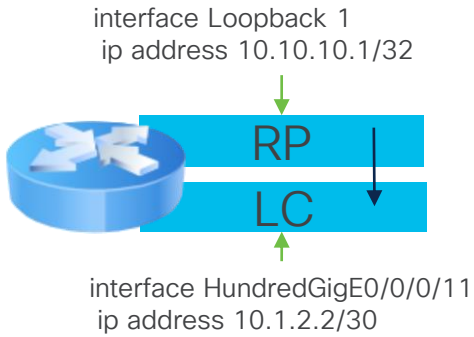
Son paquetes que se originan o terminan en el router. La dirección del paquete es tratada con relación al equipo.

- Si el paquete es recibido y destinado al router, se denomina *tráfico punteado*.
- Si el paquete es generado por el router, se denomina *tráfico inyectado.*



Ejemplo con ping de tráfico local

Inyectado desde RP hacia la LC




```
ping 10.1.2.2 source 10.10.10.1
```

Punteado e Inyectado

(ARP Resuelto y Ping de Router A al Router B)


```
ping 10.1.2.1 source 10.1.2.2
```

- Echo Request enviado desde Router A (Se inyecta)
- Echo Request recibido por Router B (Se puntea)
- Echo Reply enviado de Router B (Se inyecta)
- Echo Reply recibido por Router A (Se puntea)

RP: Route Processor
LC: Line Card

Manejo especial de paquetes

Tráfico punteado al CPU

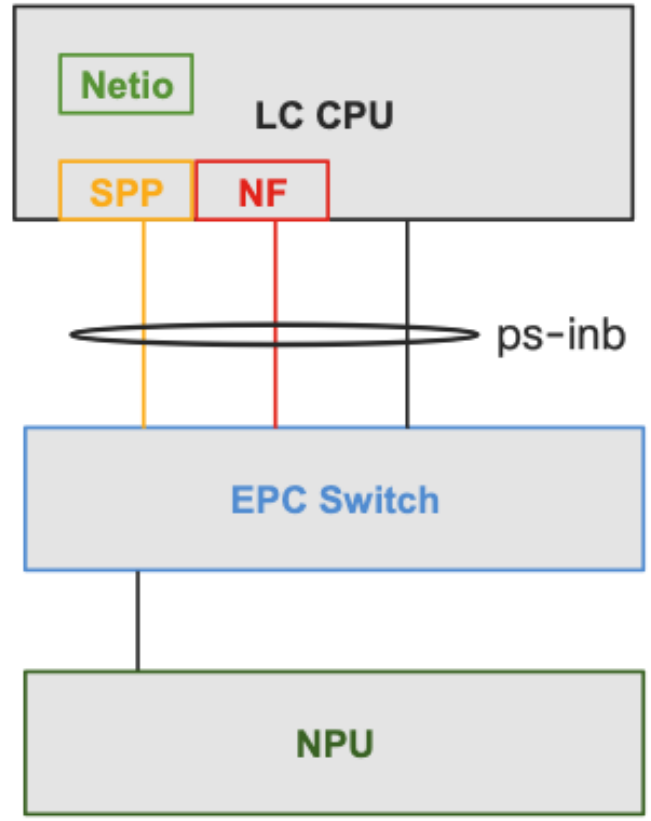
- Protocolos de ruteo, SSH, SNMP, etc. (Route Processor **CPU**)
- E-OAM, BFD, ICMP y Netflow, etc. (Line Card **CPU**)

Paquetes punteados son manejados por el componente LPTS en dos maneras:

- Por tipo de flujo
- Por Trap

Fragmentación

- Paquetes IPv4 que requieren fragmentación son punteados al CPU de la LC a través del componente SPP.
- Paquetes MPLS que requieren fragmentación son dropeados
- IPv6 no soporta fragmentación (por estándar)



Active poll

0

Join at

slido.com

#6878 562

Passcode:

wcdw71

¿Qué herramientas para troubleshooting conoce?

a) SPAN

0%

b) ACL

0%

c) PING

0%

d) Netflow

0%

e) Packet tracer

0%

Herramientas para troubleshooting

Herramientas para troubleshooting

Ping	Útil para realizar pruebas de conectividad entre dos routers o dentro del mismo.
ACL	Ayuda a identificar tipos de paquetes que llegan al equipo.
SPAN	Duplica el tráfico de una interface con fines de capturar los paquetes en un período.
Netflow	Ayuda a identificar las tendencias de tráfico de tránsito y sus características mediante un muestreo.
Comandos	Útiles para extraer información de cada módulo interno del router.

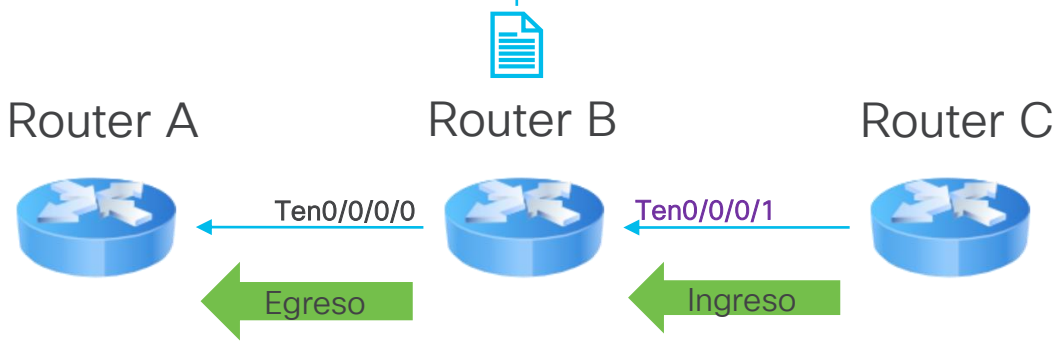
Troubleshooting de paquetes dropeados

Listas de acceso – ACL

TAC Tip

Listas de acceso son muy útiles al momento de analizar un flujo que tenga drops.

Por defecto, sólo los "deny" generan que los contadores incrementen.
Para habilitar los “permit”, se necesita habilitar el perfil hw-module profile stats acl-permit



Paso 1. Configurar ACL

```
ipv4 access-list TAC
 permit icmp any host 10.1.2.1
 permit icmp 10.1.2.1 any host
 permit ipv4 any any
```

Paso 2 – Aplicar lista de acceso en la interface de entrada

```
interface TenGig 0/0/0/1
 ipv4 access-group TAC ingress
```

Paso 3 – Verificar las ocurrencias de la ACL

```
show access-list TAC hardware ingress location 0/0/CPU0
```

*En NCS 5500, cuando es configurado el perfil hw-module profile stats acl-permit, se necesita reiniciar el router o line card (modular) para que tome efecto el perfil.

Identificación de traps

TAC Tip

Se define un conjunto de traps que agrupan los tipos paquetes más comunes en una red.

```
RP/0/RP0/CPU0:RouterB#show drops all ongoing location 0/0/CPU0

====================================
Checking for ongoing drops on 0/0/CPU0
====================================

show controllers npu stats counters-all instance all location:
[np:FIA Statistics Rack: 0, Slot: 0, Asic instance: 0] ENQ_DISCARDED_PACKET_COUNTER   : +12
[np:FIA Statistics Rack: 0, Slot: 0, Asic instance: 0] PQP_DSCRD_UC_PKT_CNT          : +21
[np:FIA Statistics Rack: 0, Slot: 0, Asic instance: 0] PQP_DSCRD_MC_PKT_CNT          : +95

show controllers npu stats counters-all detail instance all location:
[np:FIA Statistics Rack: 0, Slot: 0, Asic instance: 0] EGQ0 EhpDscrdPktCnt                 : +102
[np:FIA Statistics Rack: 0, Slot: 0, Asic instance: 0] IQM1 QueueEnqDscrdPktCnt            : +125
[np:FIA Statistics Rack: 0, Slot: 0, Asic instance: 0] IQM1 TotDscrdByteCnt                : +1813

show controllers npu stats traps-all instance all location:
[np:] RxTrapAuthSaPortFail (L3 wrong MAC)          : +1235
[np:] RxTrapFailover1Plus1Fail                     : +31
```

```
RP/0/RP0/CPU0:RouterB#show controllers npu stats traps-all instance all loc 0/0/CPU0

Trap Type                                    NPU  Trap TrapStats   Policer Packet              Packet

                                             ID    ID      ID              Accepted            Dropped
=============================================================================================================
RxTrapMimDiscardMacsaDrop (IRB)              0    1    0x1         32045   0                   0
RxTrapMimDiscardMacsaTrap
(ERP_BDL)           0    2    0x2         32041   0                   0
RxTrapAuthSaLookupFail (IPMC default)        0    8    0x8         32035   0                   0
RxTrapAuthSaPortFail (L3 wrong MAC)          0    9    0x9         32020   1235                0
RxTrapAuthSaVlanFail (L3 unknown-MC/BC)      0    10   0xa         32020   3                   0
RxTrapSaMulticast                            0    11   0xb         32020   0                   0
RxTrapArpMyIp (Unknown VLAN)                 0    14   0xe         32020   0                   0
<snip>
```

Mapeo de Puertos

Todos los puertos físicos tienen las siguientes características:

- NPU: Muestra el NPU que sirve a la interface.
- NPU Core: Identifica el núcleo que se encarga de procesar el tráfico dentro del NPU.
- PP Port: Identificador de terminación del puerto.
- System Port ID: Identificador de entrada (usado para salida).
- VOQ Base: Identificador local del VOQ.
- Flow Base: Identificador del conector de la VOQ a los elementos de planificación de salida.

```
RP/0/RP0/CPU0:RouterB#show controllers npu voq-usage interface all instance 0 location 0/0/CPU0

--------------------------------------------------------------------
Node ID: 0/0/CPU0
Intf         Intf      NPU NPU  PP    Sys   VOQ   Flow   VOQ     Port
name         handle     #  core Port  Port  base  base   port    speed
             (hex)                                 type
--------------------------------------------------------------------
Hu0/0/1/5    8          0   1     1     1   1416   6152 local   100G
Hu0/0/1/4    28         0   1     5     5   1424   6160 local   100G
Hu0/0/1/3    48         0   1     9     9   1432   6168 local   100G
Hu0/0/1/0    68         0   1    13    13   1408   6144 local   100G
Hu0/0/1/2    88         0   1    17    17   1440   6176 local   100G
Hu0/0/1/1    a8         0   1    21    21   1448   6184 local   100G
Te0/0/0/20   c8         0   0    25    25   1232   6360 local    10G
Te0/0/0/3    d0         0   0    26    26   1096   6224 local    10G
Te0/0/0/5    d8         0   0    27    27   1112   6240 local    10G
Te0/0/0/21   e0         0   0    28    28   1240   6368 local    10G
Te0/0/0/4    e8         0   0    29    29   1104   6232 local    10G
<snip>
```

Validación de VOQ

Se puede obtener la cantidad de paquetes de tránsito dropeados en función de la clase de tráfico (marcado en calidad de servicio).

```
RP/0/RP0/CPU0:RouterB#show controllers npu stats voq ingress interface hundredGigE 0/0/1/1 instance all location 0/0/CPU0

Interface Name    =    Hu0/0/1/1
Interface Handle  =          a8
Location          =     0/0/CPU0
Asic Instance     =           0
VOQ Base          =        1448
Port Speed(kbps)  =   100000000
Local Port        =       local
       ReceivedPkts    ReceivedBytes   DroppedPkts     DroppedBytes
-----------------------------------------------------------------
Core-0:
TC_0 = 0               0               0               0
TC_1 = 0               0               0               0
TC_2 = 0               0               0               0
TC_3 = 0               0               0               0
TC_4 = 0               0               0               0
TC_5 = 0               0               0               0
TC_6 = 0               0               0               0
TC_7 = 184             34069           0               0
Core-1:
TC_0 = 0               0               0               0
TC_1 = 0               0               0               0
TC_2 = 0               0               0               0
TC_3 = 0               0               0               0
TC_4 = 0               0               0               0
TC_5 = 0               0               0               0
TC_6 = 0               0               0               0
TC_7 = 0               0               0               0
```

Comandos para troubleshooting - Tráfico de tránsito

TAC Tip

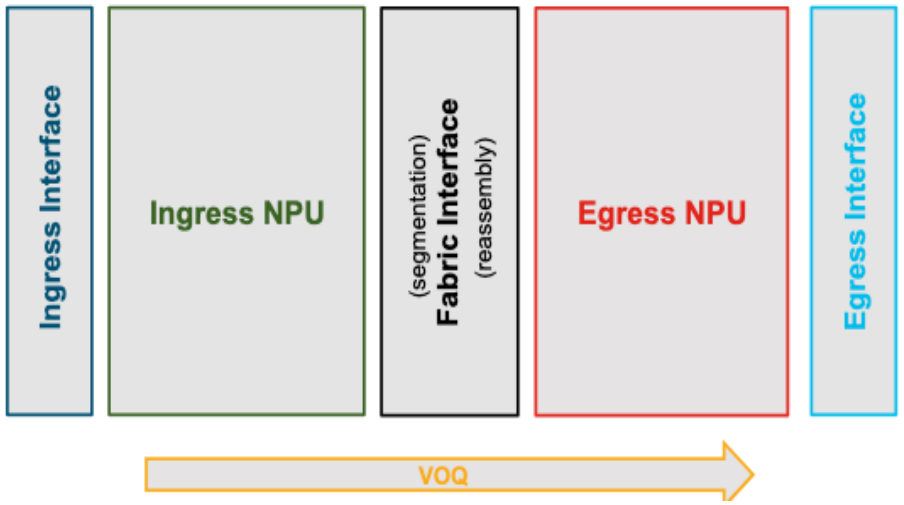
```
show controllers npu stats counters-all instace <> loc <>
show controllers np diag counters graphical cdsp instace < loc <>
show controllers npu stats traps-all instance <> loc <>
show interfaces <> accounting

show captured packets ingress loc <>
show access-lists <> hardware ingress interface <> loc <>
show flow-monitor <> cache match <> loc <>
show controllers npu diag last interface <> loc <>
show controllers npu diag pp ParsingInfo instance <> loc <>
```

```
show controllers npu stats counters-all instace <> loc <>
show controllers np diag counters graphical cdsp instace < loc <>

show controllers npu stats traps-all instance <> loc <>
show interfaces <> accounting
show captured packets egress loc <>
show controllers npu diag  pp EncapsulationInfo instance <> loc <>
```

```
show interfaces <interface>
show controllers <interface> stats
show controllers <interface> phy
```




```
show interfaces <interface>
show controllers <interface> stats
show controllers <interface> phy
```

```
show controllers npu voq-usage interface <egress-int> instance all loc <>
show controllers npu stats voq ingress <egress-int> instance all loc <>
show controllers npu stats voq base <voq-base> instance <> loc <>
```

LPTS (Local Packet Transport Services)

LPTS nos muestra los flujos más comunes direccionados al router, así como la cantidad de ancho de banda permitido en cada flujo.

```
RP/0/RP0/CPU0:RouterB#show lpts pifib hardware police location 0/0/CPU0
--------------------------------------------------------------
                Node 0/0/CPU0:
--------------------------------------------------------------
FlowType                Policer Type    Cur. Rate Burst     npu       Domain
----------------------- ------- ------- --------- --------- --------- ---------
Fragment                32102   Static  1000      98        0         0-default
OSPF-mc-known           32103   Static  2000      2000      0         0-default
OSPF-mc-default         32104   Static  100       8         0         0-default
OSPF-uc-known           32105   Static  2000      2000      0         0-default
OSPF-uc-default         32106   Static  100       8         0         0-default
```

```
RP/0/RP0/CPU0:RouterB#show lpts pifib hardware entry brief location 0/0/CPU0
--------------------------------------------------------------
            Node: 0/0/CPU0

Type DestIP           SrcIP           Interface       vrf   L4    LPort/Type    RPort  npu  Flowtype          DestNode   PuntPrio Accept Drop   Domain
---- ---------------- --------------- --------------- ----- ----- ------------- ------ ---- ----------------- ---------- -------- ------ ------ ----------
IPV4 any              any             any             0     0     any           0      0    Fragment          Local LC   LOW      0      0      0-default
IPV4 224.0.0.5        any             BE12            0     89    any           0      0    OSPF-mc-known     Dlvr RP0   HIGH     61902  0      0-default
IPV4 224.0.0.5        any             BE151           0     89    any           0      0    OSPF-mc-known     Dlvr RP0   HIGH     61902  0      0-default
IPV4 224.0.0.6        any             BE12            0     89    any           0      0    OSPF-mc-known     Dlvr RP0   HIGH     0      0      0-default
IPV4 224.0.0.6        any             BE151           0     89    any           0      0    OSPF-mc-known     Dlvr RP0   HIGH     0      0      0-default
IPV4 224.0.0.5        any             any             0     89    any           0      0    OSPF-mc-default   Dlvr RP0   LOW      1      0      0-default
IPV4 224.0.0.6        any             any             0     89    any           0      0    OSPF-mc-default   Dlvr RP0   LOW      0      0      0-default
IPV4 any              any             BE12            0     89    any           0      0    OSPF-uc-known     Dlvr RP0   HIGH     4      0      0-default
```

Decodificación de los últimos paquetes procesados

TAC Tip

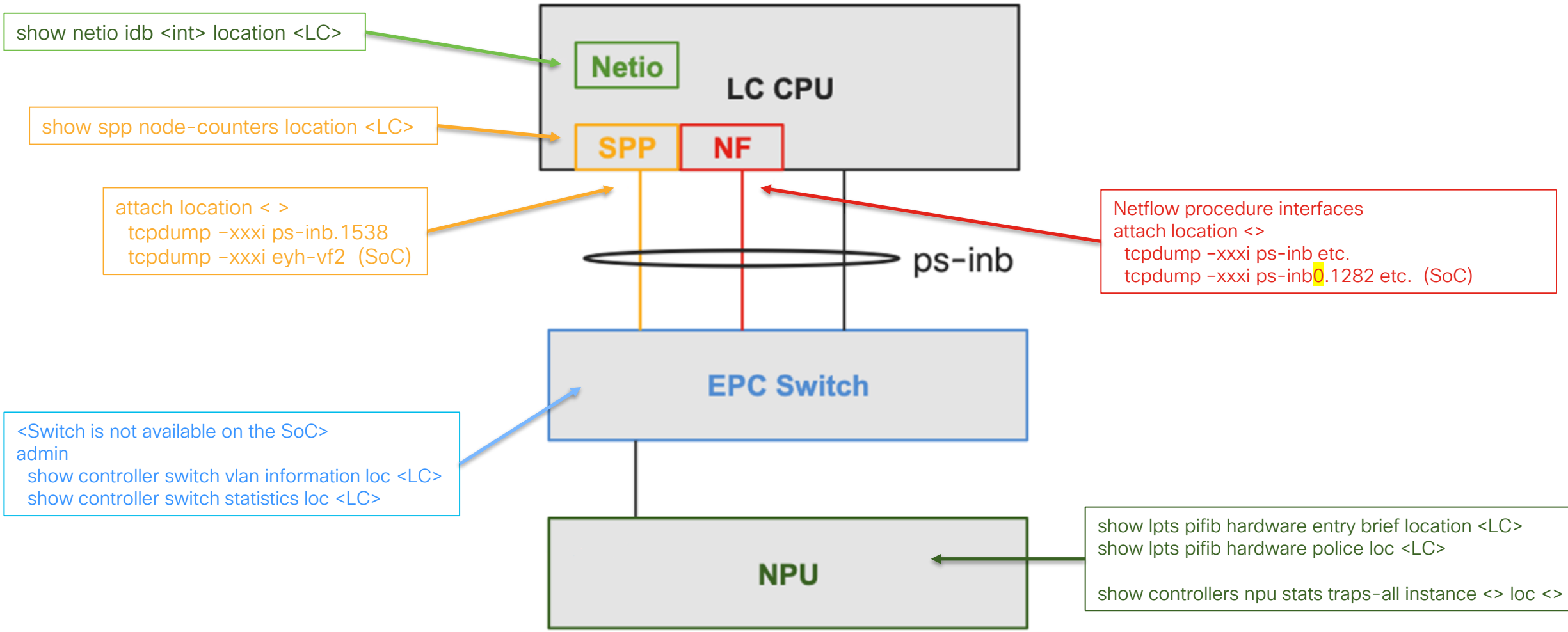
Se puede obtener la decodificación en hexadecimal del último paquete punteado en cada core del NPU.

```
RP/0/RP0/CPU0:RouterB#show controllers npu diag last instance 0 location 0/0/CPU0
----------------------------------
 Node ID: 0/0/CPU0
----------------------------------

Core 0:
Last packet information: is_valid=1  tm_port=232
pp_port=240  src_syst_port=295  port_header_type=tm packet_size=73
Packet start, offset in bytes:
00: 70e84109 6e0f011a 07010a00 00000000 00000000 0045c000 34000000 00ff1186
20: c5000000 00010133 33c0010e c8002000 0020c803 18000000 04000000 08000186
40: a0000186 a0000000 00000000 00000000 00000000 00000000 00000000 00000000
60: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
Core 1:
Last packet information: is_valid=1  tm_port=13
pp_port=13  src_syst_port=32772  port_header_type=eth packet_size=66
Packet start, offset in bytes:
00: c08b2a43 2ce0e85c 0a1cd8e2 080045c0 00340000 0000ff11 52c30101 33330101
20: 3301c001 0ec80020 000020c8 03180000 00080000 00040001 86a00001 86a00000
40: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
60: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
```

Comandos para troubleshooting - Tráfico Local

TAC Tip



Laboratorio

Objetivos

- Ir de lo general a lo particular, aislando elemento de falla con lista de acceso en el destino del paquete.
- Capturar paquete tirado vía comando.
- Decodificar paquete para encontrar información de la fuente y el destino.

Topología

Descripción del problema:

- Ping de "Router A" a "Router B" no funciona.

Pasos de troubleshooting:

En ambos routers:

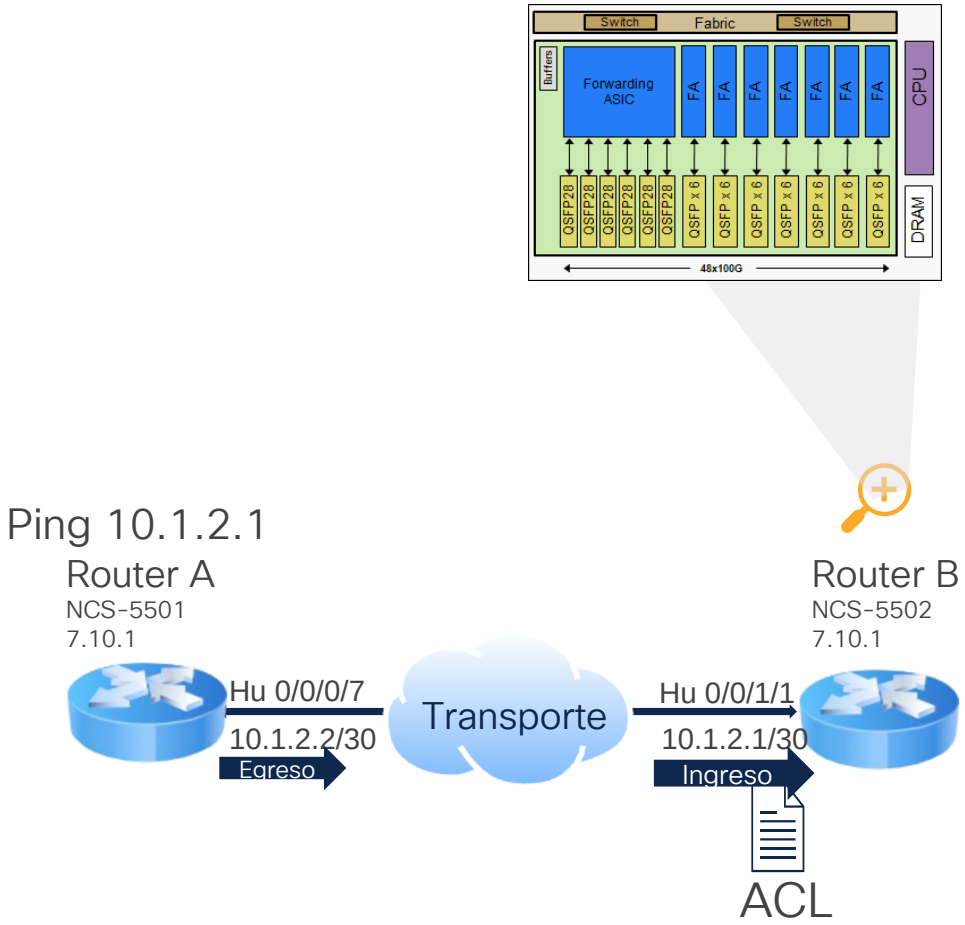
- Verificar ruta al destino
- Checar interfaz de salida up/up
- Checar tabla ARP

En Router A:

- Ping extendido

En Router B:

- Mapeo de interfaz
- ACL
- Checar drops
- Captura de paquete vía cli



Ping perdidos

Ping

```
RP/0/RP0/CPU0:RouterA#ping 10.1.2.1 repeat 10

Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 10.1.2.1 timeout is 2 seconds:
..........
Success rate is 0 percent (0/10)
```

Ruta aprendida

```
RP/0/RP0/CPU0:RouterA#show route 10.1.2.1


Routing entry for 10.1.2.0/30
  Known via "connected", distance 0, metric 0 (connected)
  Installed Feb 22 15:12:29.376 for 3d23h
  Routing Descriptor Blocks
    directly connected, via HundredGigE0/0/0/7
      Route metric is 0
  No advertising protos.
RP/0/RP0/CPU0:RouterA#
```

Mapeo de Puerto

TAC Tip

```
RP/0/RP0/CPU0:RouterB#show route 10.1.2.1


Routing entry for 10.1.2.1/32
  Known via "local", distance 0, metric 0 (connected)
  Installed Feb 22 15:12:29.380 for 3d23h
  Routing Descriptor Blocks
    directly connected, via HundredGigE0/0/1/1
      Route metric is 0
  No advertising protos.
RP/0/RP0/CPU0:RouterB#
```

- NPU: 0
- NPU Core: 1
- PP Port: 21
- VOQ Port: 1448

Mapeo

```
RP/0/RP0/CPU0:RouterB#show controllers npu voq-usage interface hundredGigE 0/0/1/1 instance 0 location 0/0/CPU0


--------------------------------------------------------------------
Node ID: 0/0/CPU0
Intf         Intf      NPU NPU  PP   Sys   VOQ   Flow   VOQ     Port
name         handle     #  core Port Port  base  base   port    speed
             (hex)                                   type
--------------------------------------------------------------------
Hu0/0/1/1    a8         0   1    21    21   1448   6184 local   100G
RP/0/RP0/CPU0:RouterB#
```

Identificación de "Trap"

```
RP/0/RP0/CPU0:RouterB#show drops all ongoing location all


====================================
Checking for ongoing drops on 0/RP0/CPU0
====================================



====================================
Checking for ongoing drops on 0/0/CPU0
====================================

show controllers npu stats traps-all instance all location:
[np:] RxTrapAuthSaPortFail (L3 wrong MAC)          : +287

RP/0/RP0/CPU0:RouterB#
```

- Contador: L3 wrong MAC
- Paquetes tirados: +287

Paquetes perdidos genéricos

Validando trap

```
RP/0/RP0/CPU0:RouterB#show controllers npu stats traps-all instance all location 0/0/CPU0 | ex "0                    0"


Trap Type                                NPU  Trap TrapStats   Policer Packet             Packet
                                         ID    ID      ID                Accepted         Dropped
=============================================================================================================
====
RxTrapAuthSaPortFail (L3 wrong MAC)      0    9    0x9         32020   96786              131597
RxTrapIgmpReportLeaveMsg (EGR-INLIF BUM DROP) 0   17   0x11        32043   0                  22
RxTrapFibDrop                            0    43   0x2b        32020   38                 115
RxTrapFailover1Plus1Fail                 0    56   0x38        32043   0                  3729
RxTrapTrillUnknownUc (flooding UC disable) 0  83   0x53        32044   41                 0
RxTrapReceive                            0    169  0xa9        32019   5418641            0
RxTrapUserDefine_RECEIVE_L2              0    179  0xb3        32019   185909             0
RP/0/RP0/CPU0:RouterB#
```

Decodificación del último paquete procesado

TAC Tip

Paquete capturado

```
RP/0/RP0/CPU0:RouterB#show controllers npu diag last instance 0 location 0/0/CPU0

----------------------------------
 Node ID: 0/0/CPU0
----------------------------------

Core 0:
Last packet information: is_valid=1  tm_port=232
pp_port=240  src_syst_port=295  port_header_type=tm packet_size=73
Packet start, offset in bytes:
00: 70e84109 6e0f011a 07010a00 00000000 00000000 0045c000 34000000 00ff1186
20: c5000000 00010133 33c0010e c8002000 0020c803 18000000 04000000 08000186
40: a0000186 a0000000 00000000 00000000 00000000 00000000 00000000 00000000
60: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
Core 1:
Last packet information: is_valid=1  tm_port=21
pp_port=21  src_syst_port=21  port_header_type=eth packet_size=114
Packet start, offset in bytes:
00: c08b2a43 2cc1e85c 0a1cd81c 08004500 006470ba 0000ff01 32da0a01 02020a01
20: 02010800 61a599cb 70bacafe cafecafe cafecafe cafecafe cafecafe cafecafe
40: cafecafe cafecafe cafecafe cafecafe cafecafe cafecafe cafecafe cafecafe
60: cafecafe cafecafe cafecafe cafecafe cafe0000 00000000 00000000 00000000
:
RP/0/RP0/CPU0:RouterB#
```

```
RP/0/RP0/CPU0:RouterB#show interfaces HundredGigE 0/0/1/1 | in Hardware

  Hardware is HundredGigE, address is c08b.2a43.2cc4 (bia c08b.2a43.2cc4)
RP/0/RP0/CPU0:RouterB#
```

Decodificación del último paquete procesado

```
00: c08b2a43 2cc1e85c 0a1cd81c 08004500 006471f4 0000ff01 31a00a01 02020a01
20: 02010800 606b99cb 71f4cafe cafecafe cafecafe cafecafe cafecafe cafecafe
40: cafecafe cafecafe cafecafe cafecafe cafecafe cafecafe cafecafe cafecafe
60: cafecafe cafecafe cafecafe cafecafe cafe0000 00000000 00000000 00000000
```

Remover primer columna

Decodificamos paquete hexadecimal que obtuvimos vía comando.

```
RP/0/RP0/CPU0:RouterB#show interfaces hundredGigE 0/0/1/1

  Hardware is HundredGigE, address is c08b.2a43.2cc4 (bia
RP/0/RP0/CPU0:RouterB#
```

MAC destino

10.1.2.2 → 10.1.2.1 ICMP Echo (ping) request

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
C0	8B	2A	43	2C	C1	E8	5C	0A	1C	D8	1C	08	00	45	00
00	64	71	F4	00	00	FF	01	31	A0	0A	01	02	02	0A	01
02	01	08	00	60	6B	99	CB	71	F4	CA	FE	CA	FE	CA	FE
CA	FE	CA	FE	CA	FE	CA	FE	CA	FE	CA	FE	CA	FE	CA	FE
CA	FE	CA	FE	CA	FE	CA	FE	CA	FE	CA	FE	CA	FE	CA	FE
CA	FE	CA	FE	CA	FE	CA	FE	CA	FE	CA	FE	CA	FE	CA	FE
CA	FE	CA	FE	CA	FE	CA	FE	CA	FE	CA	FE	CA	FE	CA	FE
CA	FE	00	00	00	00	00	00	00	00	00	00	00	00	00	00

3 protocols in packet:

Ethernet | IPv4 | ICMP

\+ | Width: 16 bytes | Export

- Frame 1: 128 bytes on wire (1024 bits)
- Ethernet II
  - Destination: Cisco_43:2c:c1 (c0:8b:2a:43:2c:c1)
  - Source: Cisco_1c:d8:1c (e8:5c:0a:1c:d8:1c)
  - Type: IPv4 (0x0800)
  - Trailer: 00000000000000000000
  - Frame check sequence: 0x00000000
  - FCS Status: Unverified
- Internet Protocol Version 4
- Internet Control Message Protocol

Apéndice

Apéndice

Término	Descripción
RP	Route procesor
LC	Line Card
LPTS	Local Packet Transport Service
Netio	Un proceso IOS-XR que realiza envío de paquetes en software, equivalente a “process switching”.
“For-us” packets	Paquetes de "Control/management plane" destinados a o para ser procesados por un nodo/elemento en IOS-XR.
SPP	Software Path Process. Este es un multiplexor/demultiplexor en LC/RP CPU
ACL	Access Control List
SPIO	Streamlined Packet IO es para procesar paquetes de control de capa 2.
NPU	Network Processor Unit
ASIC	Circuito integrado de aplicación específica.
SPAN	Switched Port Analyzer
QoS	Quality of Service

Enlaces

Ciclo de vida del paquete dentro de NCS55xx
https://www.cisco.com/c/en/us/support/docs/routers/network-convergence-system-5500-series/217276-ncs5500-life-of-a-packet-transit-punt.html

LPTS en NCS55xx
https://xrdocs.io/ncs5500/tutorials/introduction-to-ncs55xx-and-ncs5xx-lpts/

Perfiles en NCS55xx
https://xrdocs.io/ncs5500//tutorials/ncs5500-hw-module-profiles/

ACL en NCS55xx
https://xrdocs.io/ncs5500//tutorials/acl-ip-fragments-matching-ncs55xx-and-ncs5xx/

Q&A

Cisco Public

¿Aún tiene dudas?

Si hizo una pregunta en el panel de preguntas y respuestas o regresa a la comunidad en los días posteriores a nuestro webinar

¡Nuestros expertos aún pueden ayudarlo!

Participe en el foro Ask Me Anything (AMA) antes del viernes 8 de marzo de 2024

https://bit.ly/CL5ama-feb24

Haga valer su opinión

Responda a nuestra encuesta para...

- Sugerir nuevos temas
- Calificar a nuestros expertos y el contenido
- Enviar sus comentarios o sugerencias

¡Ayúdenos respondiendo a 5 preguntas de opción múltiple!

Al término de esta sesión, se abrirá una encuesta en su navegador.

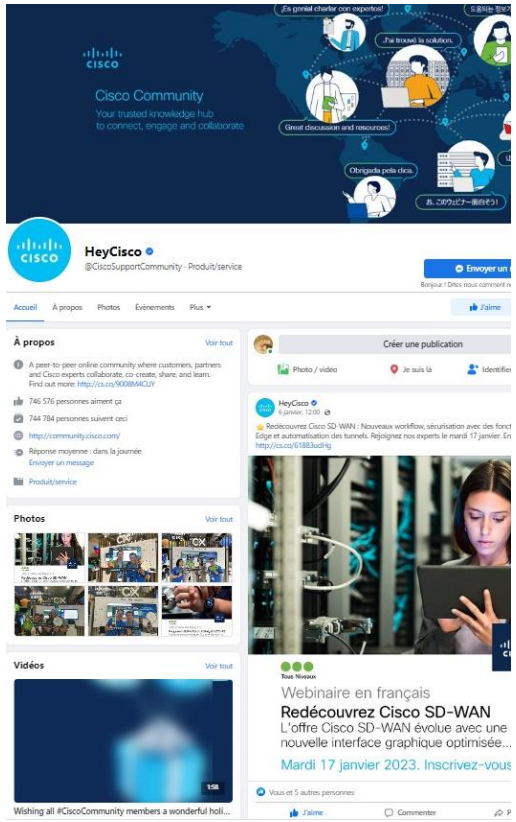
Nuestras Redes Sociales

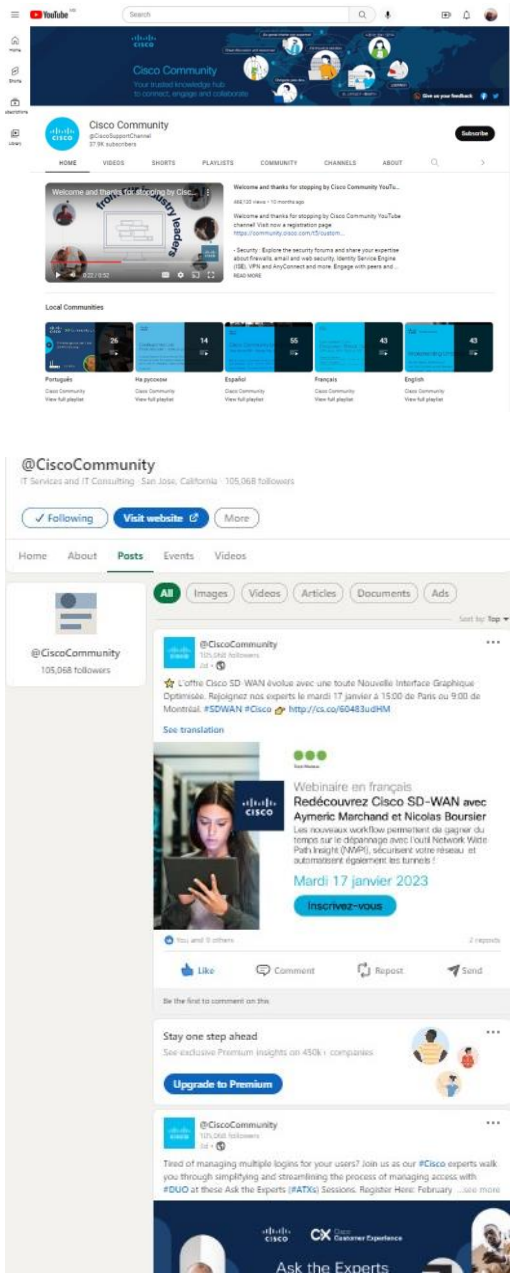
LinkedIn
[Cisco Community]

Twitter
[@CiscoCommunity]

YouTube
[CiscoCommunity]

Facebook
[CiscoCommunity]





The bridge to possible