Herramientas de Solución de Problemas de NX-OS (Troubleshooting)

Comunidad de Cisco

Jorge García – Escalation Engineer DCRS TAC
Emmanuel Fierro– Captain Leader DCRS TAC

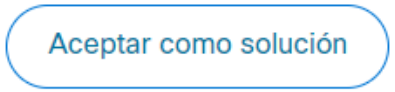
Jueves 26 de octubre de 2023

Conecte, Interactúe, ¡Colabore!

Soluciones

¡Acepte las soluciones correctas y felicite a quienes le ayudaron! Los foros de discusión tienen muchas entradas, de las cuales no todas cuentan con una respuesta correcta o válida.

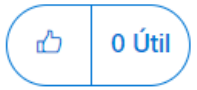
Ayude a otros usuarios a encontrar las respuestas correctas en el motor de búsqueda de la comunidad indicando que la duda fue resuelta al activar la opción “Aceptar como solución”.

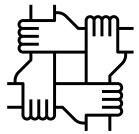


Agradecimientos

¡Resalte 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 además de ser una muestra valiosa de ¡nuestro reconocimiento!





Spotlight Awards

¡Nuevos ganadores en español!

Destaca por tu esfuerzo y compromiso para mejorar la comunidad y ayudar a otros miembros. Los Premios Spotlight se otorgan trimestralmente para destacar a los miembros más destacados.

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

Community Spotlight awards

Jorge García

Escalation Engineer

Ingeniero de Escalamiento en el equipo de Data Center Routing and Switching (DCRS) en el Centro de asistencia técnica global (TAC) de Cisco y brinda soporte a clientes de HTTS. Jorge es Ingeniero en Computación con cinco años de experiencia en enrutamiento y conmutación.

Emmanuel Fierro

Captain Leader

Capitán del equipo DCRS en el Cisco Global TAC. Emmanuel es Ingeniero de Telecomunicaciones, participando activamente en el desarrollo técnico y operativo del equipo de la Costa Oeste del DCRS.

Descargue la presentación

https://bit.ly/CL5doc-oct23

slido

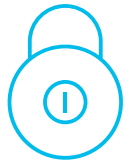
Join at

slido.com

#1977 283

Passcode: **23dgke**

Agenda



1. Nexus 9000: Plano de Datos y Plano de Control
2. Kit de herramientas y capturas de paquetes para solucionar problemas:
    a. Ethanalyzer
    b. PACL y RACL
    c. DMIRROR
    d. Packet Tracer
    e. SPAN y SPAN un CPU
    f. ELAM
3. Casos de uso más frecuentes (Laboratorio)

Objetivos de la sesión

1. Comprender que tráfico de red llega a Plano de Control o a Plano de Datos.
2. Identificar en qué nivel (Plano de control o Plano de Datos) trabajan las capturas
3. Aprender los diferentes tipos de capturas disponibles en los modelos de Nexus con NXOS.

Nexus 9000:

Plano de Datos y Plano de Control

- Nexus 9000: Plano de Datos y Plano de Control
- Kit de herramientas y capturas de pantalla para solucionar problemas
- Casos de uso más frecuentes (Laboratorio)

Active poll

0

Join at

slido.com

#1977 283

Passcode:

23dgke

¿Conoces la diferencia entre Control Plane y Data Plane?

a) Sí, Control Plane es el tráfico que fluye hacia ó desde un dispositivo, mientras que Data Plane es el tráfico que fluye a través de un dispositivo.

0%

b) Sí, Data Plane es el tráfico que fluye hacia ó desde un dispositivo, mientras que Control Plane es el tráfico que fluye a través de un dispositivo.

0%

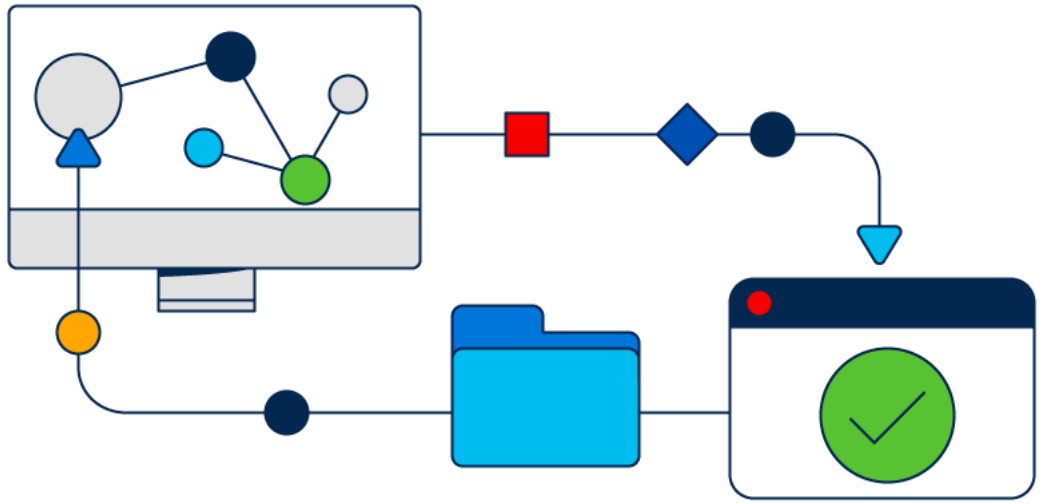
c) No hay diferencia en los Nexus 9k.

0%

Nexus 9000: Plano de Datos y Plano de Control

Control Plane (Plano de Control):

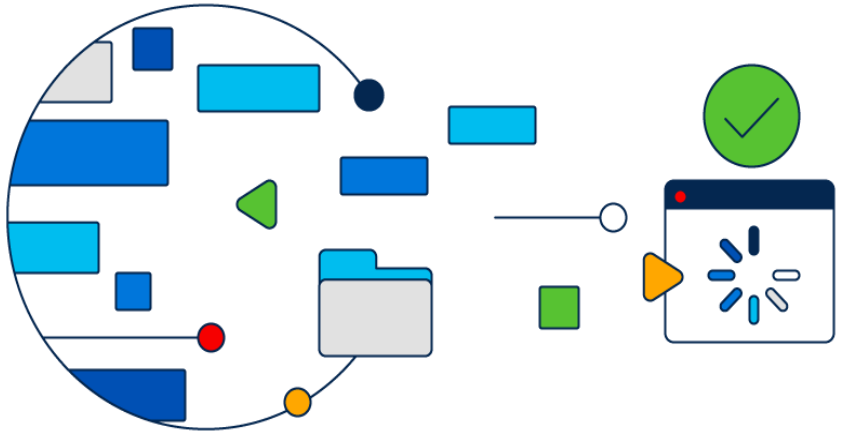
- ✓ Gestión y el control de las operaciones.
- ✓ Tareas de configuración, enrutamiento, establecimiento de políticas de seguridad, monitoreo, etc.
- ✓ Procesamiento de paquetes que van hacia el Nexus o que son generados por él mismo
- ✓ Algunos protocolos como OSPF, BGP, EIGRP, STP, LACP, CDP, Netflow, PTP, NTP, etc.



Nexus 9000: Plano de Datos y Plano de Control

Data Plane (Plano de Datos):

- ✓ Procesa los paquetes que entran y salen de la red de acuerdo con las decisiones tomadas en el *“Plano de control”*.
- ✓ Transferencia de datos a través del dispositivo de red, los datos viajan a través del Nexus, pero no están destinados a quedarse en él.
- ✓ ASICs (Application-Specific Integrated Circuits), hardware especializado que se utiliza para garantizar un procesamiento rápido y eficiente de paquetes.

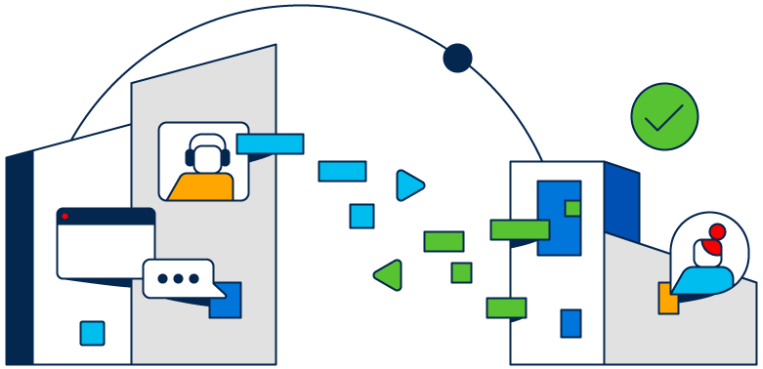


Kit de herramientas y capturas de paquetes para solucionar problemas

- Nexus 9000: Plano de Datos y Plano de Control
- Kit de herramientas y capturas de pantalla para solucionar problemas
- Casos de uso más frecuentes (Laboratorio)

Kit de herramientas y capturas de pantalla para solucionar problemas

- ✓ En la resolución de problemas diarios en redes, es necesario rastrear paquetes para entender el camino que recorren, donde entran, donde salen o dónde se pierden.
- ✓ NX-OS nos brinda varias herramientas, dependiendo de la plataforma y la versión, para realizar capturas de paquetes que nos permiten aislar diversos problemas.
- ✓ Cada herramienta será útil según el escenario.



HERRAMIENTAS
ACL (PACL & RACL)
DMIRROR
ELAM
ETHANALYZER
INTERFACE COUNTERS
PACKET TRACER
SPAN & SPAN A CPU

Active poll

0

Join at

slido.com

#1977 283

Passcode:

23dgke

¿Estás familiarizando con las herramientas de troubleshooting disponibles en los Nexus 93180?

a) Sí, conozco algunas

0%

b) No conozco las herramientas disponibles

0%

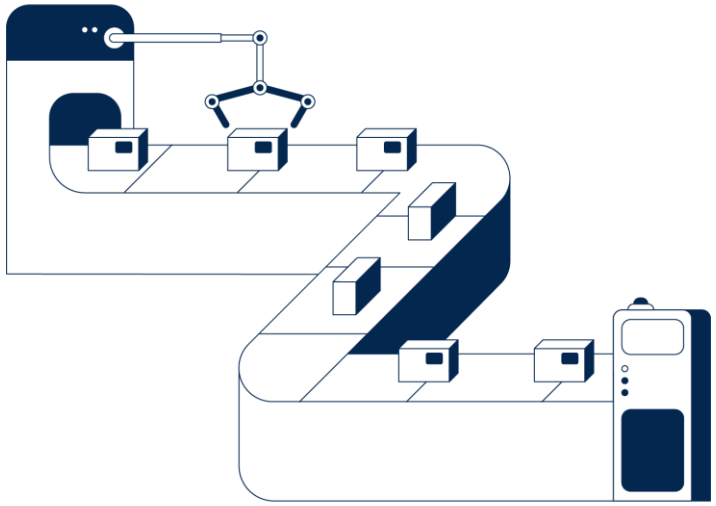
c) Conozco algunas pero no las he utilizado

0%

Kit de herramientas y capturas de pantalla para solucionar problemas

ACL

- ✓ Una ACL (Lista de Control de Acceso) es un conjunto ordenado de reglas que puedes utilizar para filtrar el tráfico.
  - La primera regla que coincide determina si se permite o se deniega el paquete.
- ✓ Según el lugar donde se aplique el ACL, se le asignará un nombre:
  - *VACL (VLAN ACL)*
    Lista de acceso aplicada en una VLAN.
  - *RACL (Routed ACL)*
    Lista de acceso aplicada en una interfaz de capa 3.
  - *PACL (Port ACL)*
    Lista de acceso aplicada en una interfaz de capa 2.



Active poll

0

Join at

slido.com

#1977 283

Passcode:

23dgke

¿Puedo hacer PACL a la entrada y a la salida?

a) Sólo de entrada

0%

b) Sólo de Salida

0%

c) Ambas son posibles

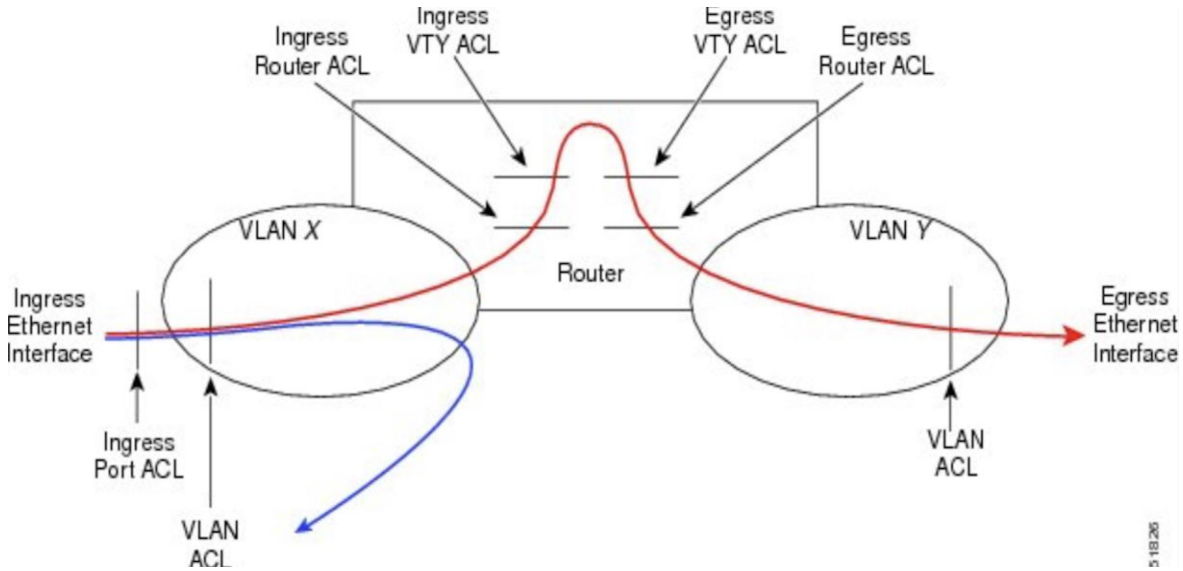
0%

Kit de herramientas y capturas de pantalla para solucionar problemas

```
ip access-list test
1 permit tcp X.X.X.X/32 Y.Y.Y.Y/32 eq 443
permit ip X.X.X.X/32 Y.Y.Y.Y/32
2 permit ip any top
3 statistics per-entry

int po 20.   <<< L2 Interfaces
4 ip port access-group test in

int eth1/1  <<< L3 Interfaces
ip access-group test in
```




```
#show ip access-list test
        statistics per-entry
        10 permit ip 10.133.128.0/20 10.133.129.11/32 [match=0]
        15 permit ip 10.133.130.43/32 10.133.128.0/20 [match=103]
        16 permit ip 10.133.128.192/27 10.133.130.43/32 [match=0]
        20 permit ip 10.133.130.43/32 10.133.0.0/16 [match=0]
        30 permit ip 10.133.129.161/27 10.133.129.203/32 [match=382]
```

Active poll

0

Join at

slido.com

#1977 283

Passcode:

23dgke

¿Se necesita hacer TCAM carving para configurar PACL en Nexus9000?

a) Sí

0%

b) No

0%

c) ACL no existe en Nexus 9k

0%

d) No sé

0%

Kit de herramientas y capturas de pantalla para solucionar problemas

- ✓ En los Nexus 9000 PACL y VACL no se pueden aplicar por default, ya que debido a la arquitectura se tiene que asignar memoria en la TCAM para que las access-list funcionen.

```
Ejemplo de TCAM carving

Nexus9300(config)# hardware access-list tcam region ing-racl 768
Warning: Please save config and reload the system for the configuration to take effect

Nexus9300(config)# hardware access-list tcam region vacl 512
Warning: Please save config and reload the system for the configuration to take effect

Nexus9300(config)# hardware access-list tcam region ing-ifacl 1024
Warning: Please save config and reload the system for the configuration to take effect
```

```
NEXUS-1# sh hardware access-list tcam region
                NAT ACL[nat] size =    0
          Ingress PACL [ing-ifacl] size =    0          <<<<<<<<<<
               VACL [vacl] size =    0                 <<<<<<<<<<
          Ingress RACL [ing-racl] size = 2304
         Ingress RBACL [ing-rbacl] size =    0
       Ingress L2 QOS [ing-l2-qos] size =  256
  Ingress L3/VLAN QOS [ing-l3-vlan-qos] size =  512
          Ingress SUP [ing-sup] size =  512
Ingress L2 SPAN filter [ing-l2-span-filter] size =  256
Ingress L3 SPAN filter [ing-l3-span-filter] size =  256
         Ingress FSTAT [ing-fstat] size =    0
               span [span] size =  512
         Egress RACL [egr-racl] size = 1792
          Egress SUP [egr-sup] size =  256
     Ingress Redirect [ing-redirect] size =    0
       Egress L2 QOS [egr-l2-qos] size =    0
  Egress L3/VLAN QOS [egr-l3-vlan-qos] size =    0
Ingress Netflow/Analytics [ing-netflow] size =  512
          Ingress NBM [ing-nbm] size =    0
        TCP NAT ACL[tcp-nat] size =    0
  Egress sup control plane[egr-copp] size =    0
Ingress Flow Redirect [ing-flow-redirect] size =    0
       Ingress CNTACL [ing-cntacl] size =    0
       Egress CNTACL [egr-cntacl] size =    0
     MCAST NAT ACL[mcast-nat] size =    0
          Ingress DACL [ing-dacl] size =    0
```

Kit de herramientas y capturas de pantalla para solucionar problemas

Ethanalyzer

- ✓ Para analizar el tráfico enviado y recibido por el CPU (Supervisora), se utiliza el código de Wireshark (software de código abierto)
- ✓ Esto es útil para la resolución de problemas relacionados con la alta utilización de la CPU, así como para abordar problemas en el *"Plano de Control"* por ejemplo, relacionados con protocolos como OSPF, PIM y eventos como la fluctuación de STP.

```
N9k1# ethanalyzer local interface inband display-filter stp limit-captured-frames 0
Capturing on 'ps-inb'
1     1 2023-10-19 16:19:38.350392224 00:26:f0:64:00:00 ,Üí 01:80:c2:00:00:00 STP 60 RST. Root = 0/215/00:23:04:ee:be:01  Cost = 0  Port = 0x9063
1     6 2023-10-19 16:19:39.425257438 00:26:f0:64:00:00 ,Üí 01:80:c2:00:00:00 STP 60 RST. Root = 0/215/00:23:04:ee:be:01  Cost = 0  Port = 0x9063
2    15 2023-10-19 16:19:40.350636620 00:26:f0:64:00:00 ,Üí 01:80:c2:00:00:00 STP 60 RST. Root = 0/215/00:23:04:ee:be:01  Cost = 0  Port = 0x9063

N9k1# ethanalyzer local interface inband display-filter "icmp" limit-captured-frames 0
Capturing on 'ps-inb'
 1320 2023-10-23 19:26:41.478748035    10.2.0.47 -> 10.2.0.34    ICMP 98 Echo (ping) request  id=0x622b, seq=0/0, ttl=255
 1321 2023-10-23 19:26:41.479096164    10.2.0.34 -> 10.2.0.47    ICMP 98 Echo (ping) reply    id=0x622b, seq=0/0, ttl=255 (request in 1320)
 1322 2023-10-23 19:26:41.479684809    10.2.0.47 -> 10.2.0.34    ICMP 98 Echo (ping) request  id=0x622b, seq=256/1, ttl=255
 1323 2023-10-23 19:26:41.479919190    10.2.0.34 -> 10.2.0.47    ICMP 98 Echo (ping) reply    id=0x622b, seq=256/1, ttl=255 (request in 1322)
```

Kit de herramientas y capturas de pantalla para solucionar problemas

Packet Tracer

- ✓ Herramienta basada en *SPAN* (Switched Port Analyzer), *ACL* (Control de Acceso de Lista) y *TCAM* (Tabla de Control de Acceso a la Tarjeta) para contabilizar el número de coincidencias de *ACL* para un flujo para rastrear el paquete a través del sistema.

"Solo se pueden rastrear los paquetes en la dirección de ingreso de un flujo."

```
N9K-9508# test packet-tracer src-ip 10.1.1.1 dst-ip 10.2.2.1 protocol 1 <<< Filtro para matchear el
tráfico ICMP.
Protocol 1 to match icmp traffic

N9K-9508# test packet-tracer src-ip 10.2.2.1 dst-ip 10.1.1.1 protocol 1 <<< <<< Filtro para
matchear el tráfico ICMP REPLY.

N9K-9508# test packet-tracer start <<< Iniciar packet tracer
```

```
N9K-9508# test packet-tracer show non-zero <<< Desplegar estadisticas de los paquetes.
Packet-tracer stats
Packet-tracer stats
---------------------

Module 1:
Filter 1 installed: src-ip 10.1.1.1 dst-ip 10.2.2.1 protocol 1
ASIC instance 0:
Entry 0: id = 7425, count = 5, active, fp, <<< 5 Paquetes ECHO ingresando en el Modulo 1
Filter 2 installed: src-ip 10.2.2.1 dst-ip 10.1.1.1 protocol 1
Filter 3 uninstalled:
Filter 4 uninstalled:
Filter 5 uninstalled:

Module 2:
Filter 1 installed: src-ip 10.1.1.1 dst-ip 10.2.2.1 protocol 1
Filter 2 installed: src-ip 10.2.2.1 dst-ip 10.1.1.1 protocol 1
ASIC instance 0:
Entry 0: id = 7457, count = 5, active, fp, <<< 5 Paquetes ECHO REPLY ingresando en el Modulo 2
Filter 3 uninstalled:
Filter 4 uninstalled:

Filter 5 uninstalled:
r
```

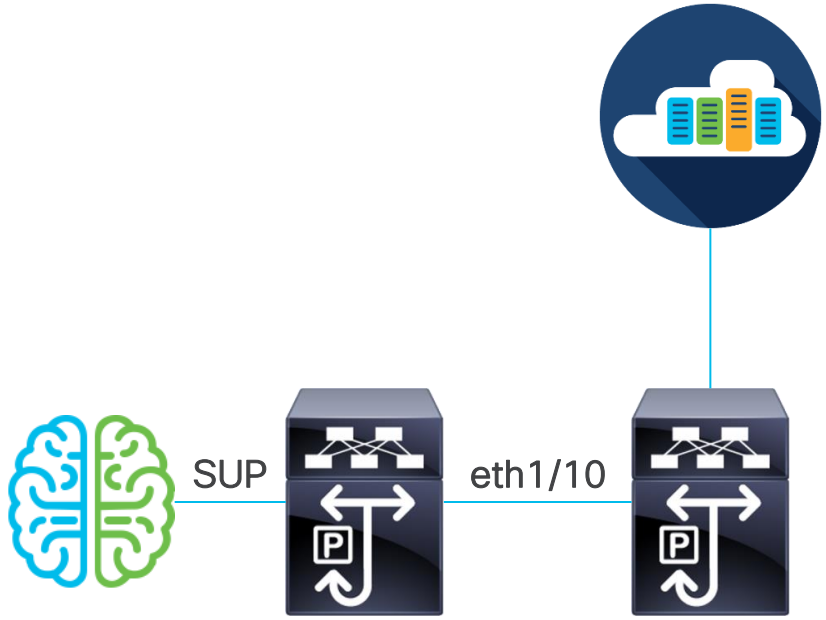
Kit de herramientas y capturas de pantalla para solucionar problemas

Dmirror

- ✓ Esta característica se implementó únicamente para la ruta interna de datos utilizando la interfaz de línea de comandos de bcm-shell. Debido a estas limitaciones, no existe una CLI de NX-OS que permita a los usuarios configurar sesiones SPAN en el Supervisor (Sup).

```
9396-B# show system internal ethpm info interface ethernet 1/10 | i dpid
  IF_STATIC_INFO:
port_name=Ethernet1/10,if_index:0x1a001200,ltl=6135,slot=0,nxos_port=9,dmod=1,dpid=22,unit=0,queue=240,xbar_unitbmp=0x1
,ns_pid=255
Configuration:
--------------
9396-B# pktmgr internal span-drop enable
9396-B# bcm-shell module 1
bcm-shell.0> dmirror xe9 DestPort=cpu0 Mode=All
Verify:
--------------
bcm-shell.0> dmirror show
 xe9: Mirror all to module 7, port 134219776

ethanalyzer local interface inband mirror display-filter 'icmp' limit-captured-frames 0
Capturing on inband
2016-06-29 20:53:53.708776  192.168.1.1 -> 192.168.1.2  ICMP Echo (ping) request
2016-06-29 20:53:53.709238  192.168.1.2 -> 192.168.1.1  ICMP Echo (ping) reply
```



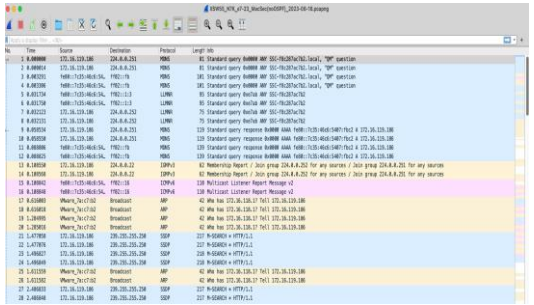
Kit de herramientas y capturas de pantalla para solucionar problemas

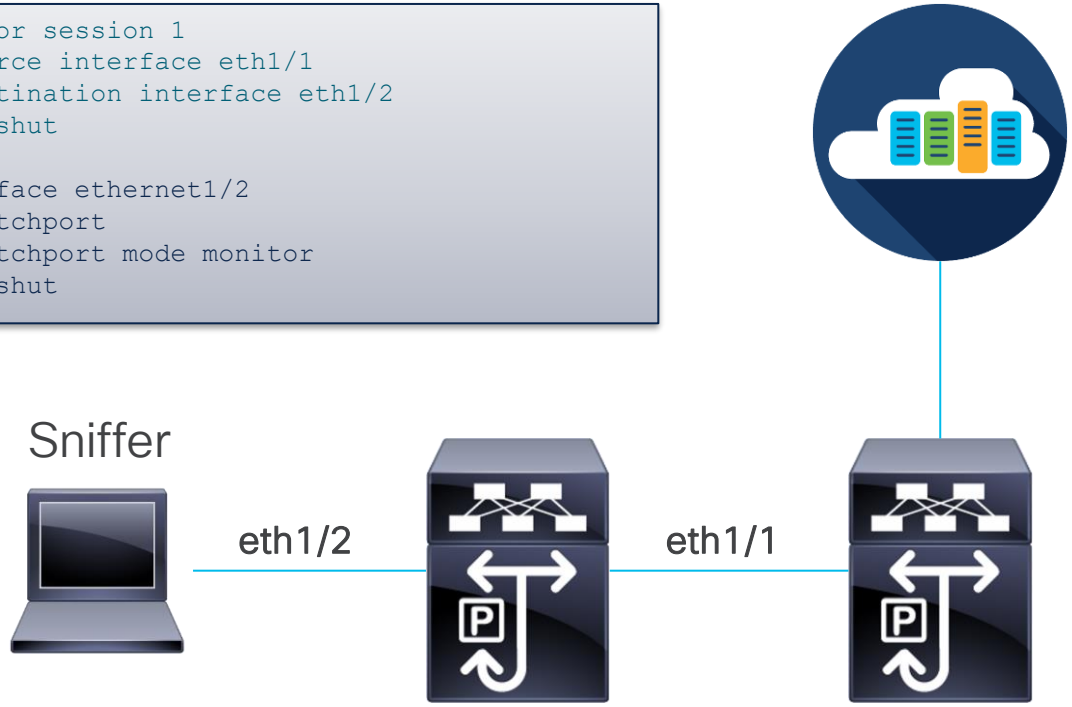
SPAN

- ✓ SPAN (Switched Port Analyzer) analiza todo el tráfico entre los puertos de origen al dirigir el tráfico de la sesión SPAN hacia un puerto de destino al que se ha conectado un analizador externo.

```
monitor session 1
  source interface eth1/1
  destination interface eth1/2
  no shut

interface ethernet1/2
  switchport
  switchport mode monitor
  no shut
```





Active poll

0

Join at

slido.com

#1977 283

Passcode:

23dgke

¿SPAN a CPU causa alguna afectación?

a) Sí, afecta el Control Plane

0%

b) No, es seguro utilizar este feature

0%

c) No existe este feature en Nexus 9k

0%

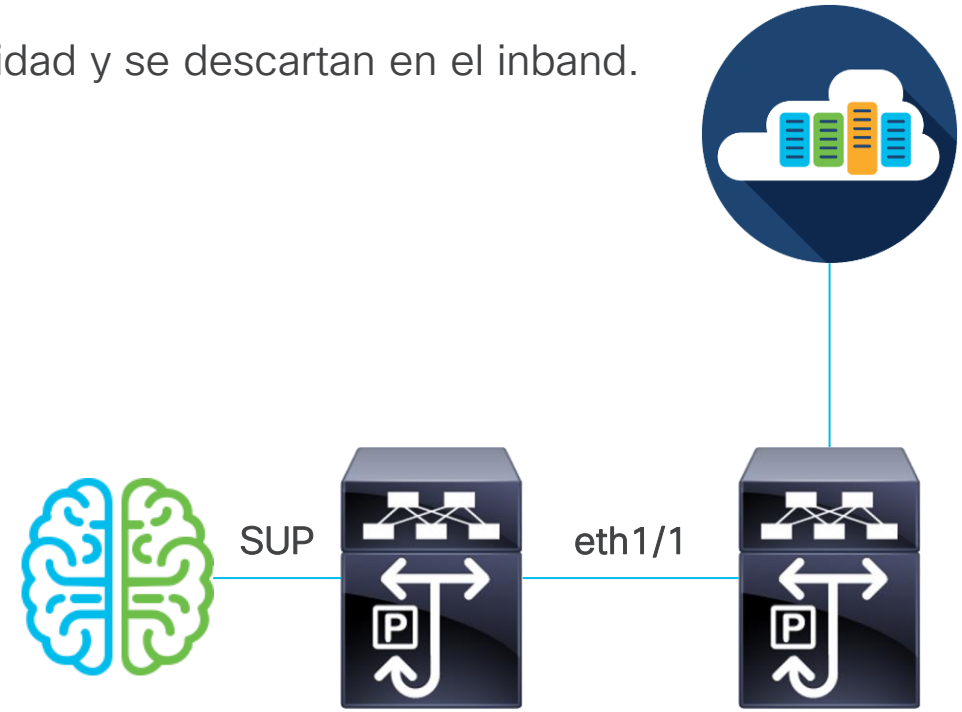
Kit de herramientas y capturas de pantalla para solucionar problemas

SPAN A CPU

- CPU o la Supervisora es el destino del SPAN.
- Los paquetes se pueden analizar utilizando Ethanalyzer en la Supervisora.
- Los paquetes SPAN enviados al CPU tienen limitación de velocidad y se descartan en el inband.

```
monitor session 1
  source interface eth1/1
  destination interface sup-eth 0
  no shut

ethanalyzer local interface inband mirror display-filter 'ospf' limit-
captured-frames 0
```



TIP

Span a CPU no causa ningún problema de performance o high CPU ya que contamos con CoPP y políticas para filtrar el tráfico que llega a CPU

Active poll

0

Join at

slido.com

#1977 283

Passcode:

23dgke

¿Para qué sirve la herramienta ethanalyzer?

a) Sirve para hacer capturas en CPU del tráfico que pasa a través del switch

0%

b) Sirve para capturar tráfico en CPU destinado al Nexus

0%

c) Sirve para capturar tráfico que pasa por el Nexus y que es destinado hacia el Nexus

0%

d) Nunca había escuchando esa herramienta

0%

Kit de herramientas y capturas de pantalla para solucionar problemas

ELAM

- ✓ ELAM es una herramienta que se utiliza para capturar un solo paquete para su inspección. Solo se puede capturar un paquete a la vez. Antes de que ELAM pueda capturar un paquete, es necesario definir un filtro. Este filtro estará compuesto por campos específicos en el paquete que se utilizarán para determinar si el paquete debe ser capturado.

El comando "Debug" es parte de la sintaxis, esto no significa que se esté corriendo un "Debug", no hay impacto operativo en correr este comando.

```
N9k(TAH-elam-insel6)# report.  <<< Reporte luego de detectar tráfico con las características del filtro aplicado.
HOMEWOOD ELAM REPORT SUMMARY
slot - 1, asic - 0, slice - 0
============================
Incoming Interface: sup-eth
Src Idx : 0x0, Src BD : 4146
Outgoing Interface Info: dmod 1, dpid 70
Dst Idx : 0xb9, Dst BD : 4146

Packet Type: IPv4

Dst MAC address: 44:B6:BE:11:17:67
Src MAC address: F8:A7:3A:4E:40:07

Dst IPv4 address: 10.10.10.1
Src IPv4 address: 10.10.10.2
[redacted], Don't Fragment = 0
Proto  =  1, TTL    =  255, More Fragments = 0
Hdr len = 20, Pkt len =  84, Checksum      = 0xb96a

L4 Protocol  : 1
ICMP type    : 0
ICMP code    : 0

Drop Info:
----------
LUA:
LUB:
LUC:
LUD:
Final Drops:
vntag:
vntag_valid   : 0
vntag_vir     : 0
vntag_svif    : 0
```

```
show system internal ethpm info global | i dpid=70
IF_STATIC_INFO: port_name=Ethernet1/47,if_index:0x1a005c00,ltl=5960,slot=0,
nxos_port=184,dmod=1,dpid=70,unit=0,queue=65535,xbar_unitbmp=0x0,ns_pid=255,slice_
num=0,port_on_slice=70,src_id=140
```

Active poll

Join at

slido.com

#1977 283

Passcode:

23dgke

¿Qué herramientas de troubleshooting has usado en plataformas que corren NX-OS?

a) Ethanalizer

0%

b) ELAM

0%

c) Ninguna

0%

d) Ambas

0%

Nexus 9000: Plano de Datos y Plano de Control

Contadores de la Interfaz

Como recurso adicional se pueden ocupar los contadores de la Interfaz tanto en RX como en TX. Estos contadores se toman directamente de hardware por lo que tienden a ser muy confiables al momento de saber si el tráfico está llegando o saliendo de la interfaz.

```
N9k1# show interface ethernet 1/1 counters detailed

Ethernet1/1
  Rx Packets:                          550911
  Rx Unicast Packets:                    3860
  Rx Multicast Packets:                547046
  Rx Broadcast Packets:                     5
  Rx Bytes:                         38901055
  Rx Packets from 0 to 64 bytes:         102483
  Rx Packets from 65 to 127 bytes:       431442
  Rx Packets from 128 to 255 bytes:      10192
  Rx Packets from 256 to 511 bytes:      6794
  Tx Packets:                          17174
  Tx Unicast Packets:                    6979
  Tx Multicast Packets:                10195
  Tx Bytes:                         2546340
  Tx Packets from 0 to 64 bytes:           789
  Tx Packets from 65 to 127 bytes:       6193
  Tx Packets from 128 to 255 bytes:      6795
  Tx Packets from 256 to 511 bytes:      3397
```

Kit de herramientas y capturas de pantalla para solucionar problemas

Tabla de compatibilidad:

HERRAMIENTAS	NEXUS 3000	NEXUS 3100/3200	NEXUS 3400	NEXUS 3500	NEXUS 3600-R /9500-R	NEXUS 50X0	NEXUS 56XX/600X	NEXUS 7000	NEXUS 9000 (NON-EX/FX/R)	NEXUS 9000 (EX/FX)
ELAM							✓	✓	✓	✓
ETHANALYZER	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
PACL/RACL	✓			✓	✓	✓	✓	✓	✓	✓
DMIRROR									✓	
PACKET TRACER		✓							✓	
SPAN	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SPAN TO CPU										✓

Nexus 9000: Plano de Datos y Plano de Control

¿Qué herramientas son mejores cuando hay 100% de perdida de paquetes?

HERRAMIENTAS
ELAM
PACL
RACL
Contadores de la Interfaz
Packet Tracer
DMIRROR
SPAN a CPU
SPAN

Nexus 9000: Plano de Datos y Plano de Control

¿Qué herramientas son mejores cuando hay intermitencia de perdida de paquetes?

HERRAMIENTAS
PACL
RACL
Contadores de la Interfaz
Packet Tracer
SPAN

Casos de uso más frecuentes (Laboratorio)

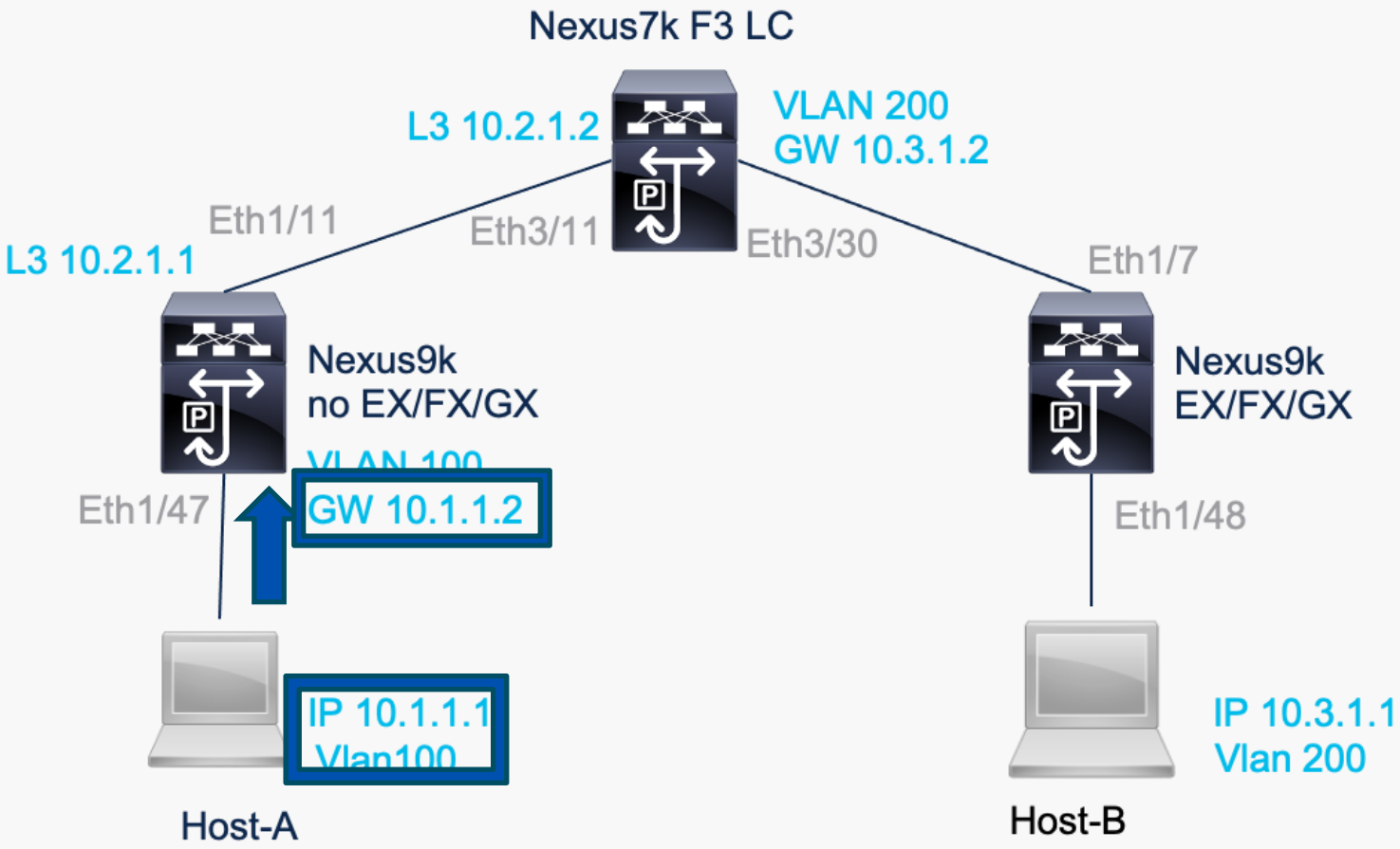
Nexus 9000: Plano de Datos y Plano de Control

Kit de herramientas y capturas de pantalla para solucionar problemas

Casos de uso más frecuentes (Laboratorio)

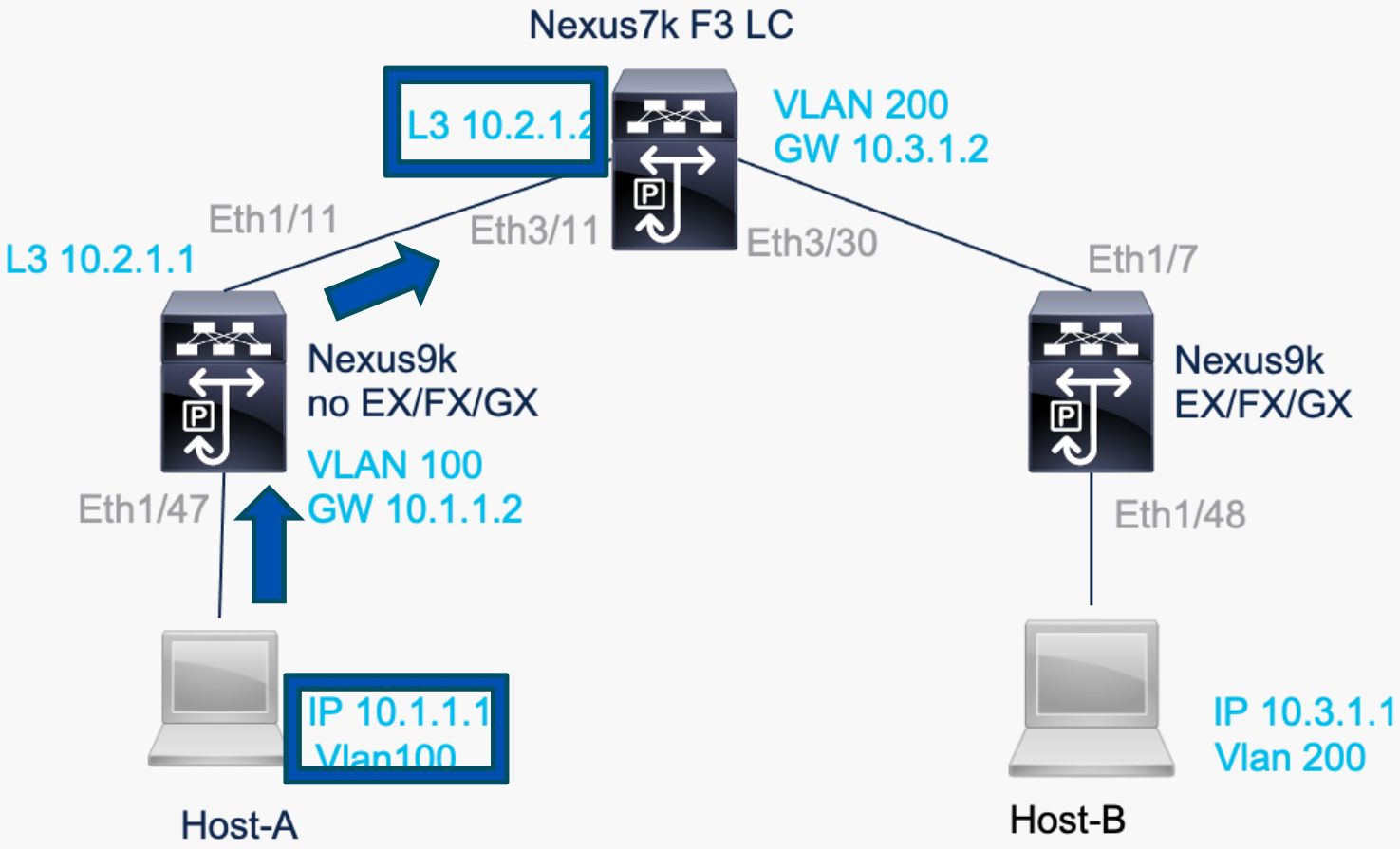
Casos de uso más frecuentes (Laboratorio)

Escenario 1:



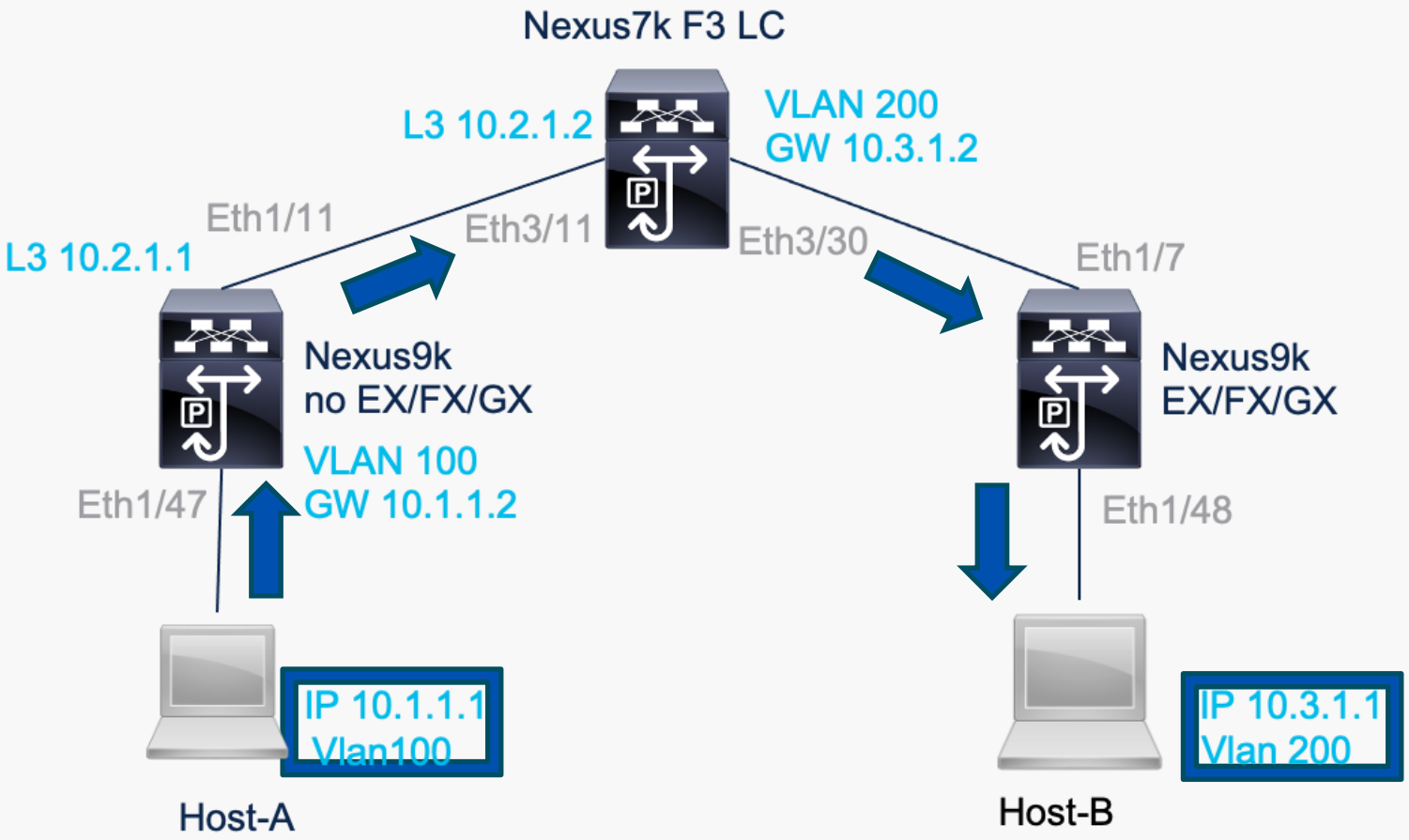
Casos de uso más frecuentes (Laboratorio)

Escenario 2:



Casos de uso más frecuentes (Laboratorio)

Escenario 3:



Preguntas y respuestas

¿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.

¡Nuestras expertas aún pueden ayudarlo!

Participe en el foro Ask Me Anything (AMA) antes del viernes 2 de noviembre de 2023

https://bit.ly/CL5ama-oct23

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

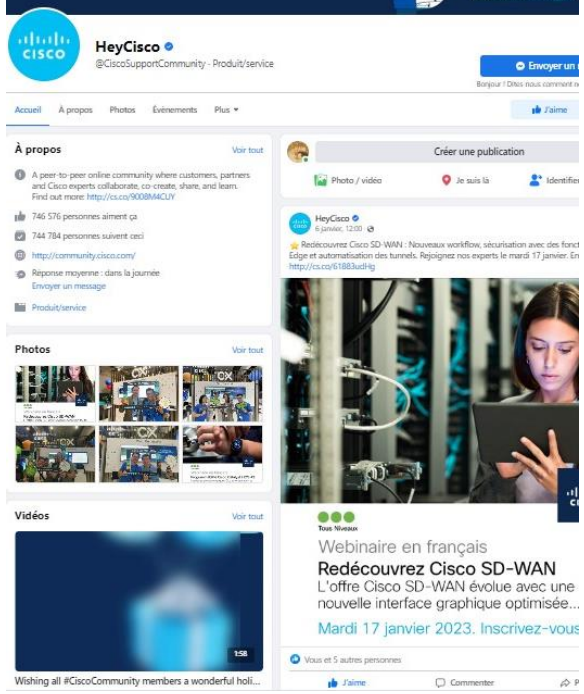
@CiscoCommunity

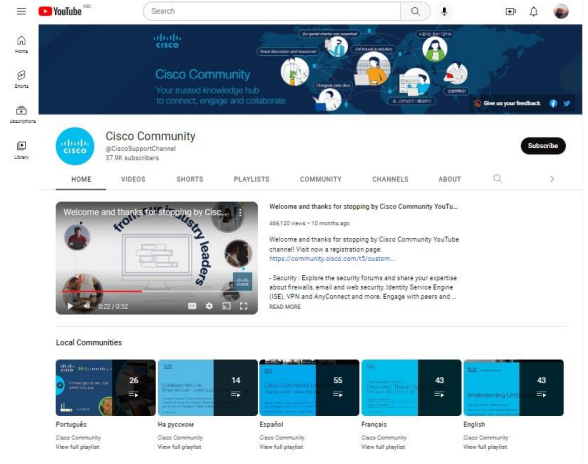
YouTube

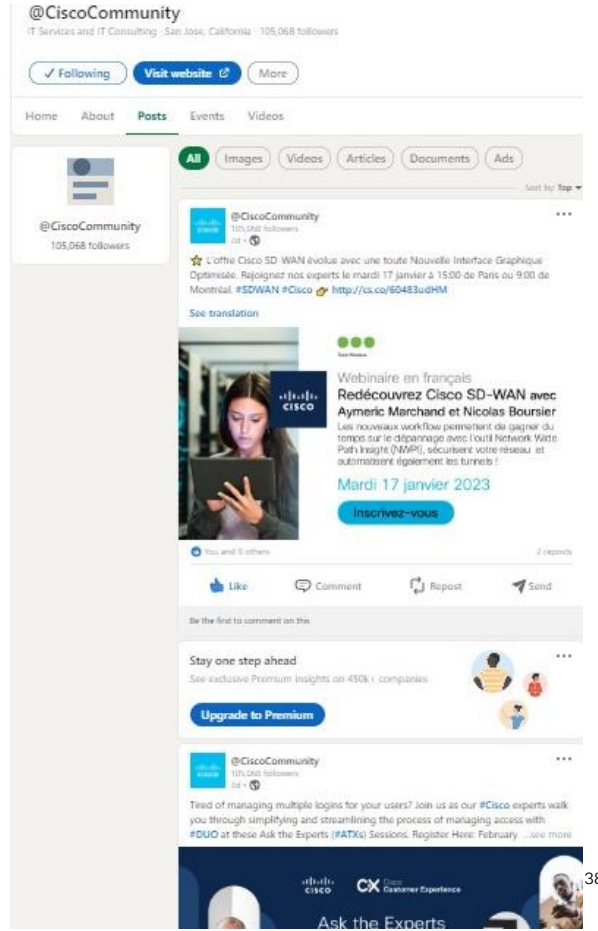
CiscoCommunity

Facebook

CiscoCommunity







The bridge to possible