Procedimiento de SPAN a CPU Nexus 9000 Cloud Scale ASIC NX-OS

Contenido

Introducción
Antecedentes
Hardware aplicable
Prerequisites
Requirements
Componentes Utilizados
Advertencias y limitaciones
Limitador de velocidad de hardware predeterminado de 50 kbps
No se Soportó el Contador Permitido de Límite de Velocidad de Hardware de SPAN a CPU
Los paquetes generados por el plano de control no aparecen en las sesiones del monitor TX SPAN a CPU
Procedimiento de ampliación de la nube de Cisco Nexus 9000 SPAN a CPU
Paso 1. Confirmar recursos suficientes para la nueva sesión SPAN
Paso 2. Configuración de la Sesión de Monitor SPAN a CPU
Paso 3. Verifique que la Sesión de Monitor SPAN a CPU esté Activa
Paso 4. Ver paquetes replicados en el plano de control
Paso 5. Apagar administrativamente la sesión de supervisión de SPAN a CPU
Paso 6. Eliminación de la configuración de sesión de SPAN a CPU Monitor (opcional)
Analizar los resultados de una captura de paquetes SPAN a CPU
Información Relacionada

Introducción

Este documento describe los pasos utilizados para realizar una captura de paquetes de analizador de puerto conmutado (SPAN) a CPU en una serie de módulos ASIC Cisco Nexus 9000 Cloud Scale. Este documento también describe las advertencias comunes encontradas al utilizar una captura de paquetes SPAN a CPU para resolver problemas de flujo de paquetes a través de un switch de la serie Cisco Nexus 9000 Cloud Scale.

Antecedentes

Una captura de paquetes de SPAN a CPU permite a los administradores de red validar rápida y fácilmente si paquetes específicos entran y salen de un switch Cisco Nexus serie 9000 Cloud Scale. De forma similar a una sesión normal de SPAN o SPAN remoto encapsulado (ERSPAN), una sesión de supervisión de SPAN a CPU implica la definición de una o más interfaces de origen y direcciones de tráfico. Cualquier tráfico que coincida con la dirección (TX, RX o ambos) definida en una interfaz de origen se replica en el plano de control del dispositivo Cisco Nexus 9000. Este tráfico replicado se puede filtrar y analizar con el uso de la utilidad de captura de paquetes del plano de control Ethanalyzer o guardarlo en un dispositivo de almacenamiento local para su posterior revisión.

Esta función está diseñada para uso temporal mientras se resuelve el flujo de paquetes a través de los switches Nexus de Cisco serie 9000. Cisco recomienda encarecidamente que las sesiones de supervisión de SPAN a CPU se cierren o eliminen administrativamente cuando no se utilizan activamente para solucionar un problema de flujo de paquetes. De lo contrario, el rendimiento del tráfico replicado en la red se vería afectado y se aumentaría la utilización de la CPU del switch Nexus de Cisco serie 9000.

Hardware aplicable

El procedimiento descrito en este documento sólo se aplica a este hardware:

- **Switches fijos Nexus 9200/9300** N9K-C92160YC-XN9K-C92300YCN9K-C92304QCN9K-C92348GC-XN9K-C9236CN9K-C9272QN9K-C9332CN9K-C9364CN9K-C93108TC-EXN9K-C93108TC-EX-24N9K-C93180LC-EXN9K-C93180YC-EXN9K-C93180YC-EX-24N9K-C93108TC-FXN9K-C93108TC-FX-24N9K-C93180YC-FXN9K-C93180YC-FX-24N9K-C9348GC-FXPN9K-C93240YC-FX2N9K-C93216TC-FX2N9K-C9336C-FX2N9K-C9336C-FX2-EN9K-C93360YC-FX2N9K-C93180YC-FX3N9K-C93108TC-FX3PN9K-C93180YC-FX3SN9K-C9316D-GXN9K-C93600CD-GXN9K-C9364C-GXN9K-C9364D-GX2AN9K-C9332D-GX2B
- **Tarjetas de línea del switch modular Nexus 9500** N9K-X97160YC-EXN9K-X9732C-EXN9K-X9736C-EXN9K-X97284YC-FXN9K-X9732C-FXN9K-X9788TC-FXN9K-X9716D-GX

Prerequisites

Requirements

Cisco recomienda que comprenda los aspectos básicos de la función Analizador de puertos conmutados Ethernet (SPAN) en los switches Nexus de Cisco serie 9000. Para obtener información sobre esta función, consulte los siguientes documentos:

- Guía de Configuración de Administración del Sistema Cisco Nexus serie 9000 NX-OS, Versión 9.3(x)
- Guía de Configuración de Administración del Sistema Cisco Nexus serie 9000 NX-OS, Versión 9.2(x)
- Guía de Configuración de Administración del Sistema Cisco Nexus serie 9000 NX-OS, Versión 7.0(3)I7(x)

Componentes Utilizados

La información de este documento se basa en los switches Nexus de Cisco serie 9000 con el ASIC Cloud Scale que ejecuta la versión 9.3(3) del software NX-OS.

La información de este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Advertencias y limitaciones

Las sesiones de supervisión de SPAN a CPU tienen algunas advertencias y limitaciones que deben tenerse en cuenta al resolver problemas de flujos de paquetes. Este documento cubrirá algunas advertencias que se han encontrado frecuentemente. Para obtener una lista completa de directrices y limitaciones, consulte los siguientes documentos:

- Guía de Configuración de Administración del Sistema Cisco Nexus serie 9000 NX-OS, Versión 9.3(x)
- Guía de Configuración de Administración del Sistema Cisco Nexus serie 9000 NX-OS, Versión 9.2(x)
- Guía de Configuración de Administración del Sistema Cisco Nexus serie 9000 NX-OS, Versión 7.0(3)I7(x)

Limitador de velocidad de hardware predeterminado de 50 kbps

De forma predeterminada, los switches Nexus de Cisco serie 9000 limitan la velocidad del tráfico replicado en el plano de control a través de una sesión de supervisión de SPAN a CPU a 50 kbps. Esta limitación de velocidad se realiza en el motor de reenvío/ASIC de escala de nube y es un mecanismo de autoprotección para garantizar que el plano de control del dispositivo no se vea saturado con tráfico replicado.

El comando **show hardware rate-limiter span** se puede utilizar para ver la configuración actual del limitador de velocidad de sesión de monitor de SPAN a CPU.

```
N9K# show hardware rate-limiter span Units for Config: kilo bits per second Allowed, Dropped &
Total: aggregated bytes since last clear counters Module: 1 R-L Class Config Allowed Dropped
Total +----------------+----------+--------------------+--------------------+--------------------
-+  span 50  0 0 0
```

Si el limitador de velocidad de hardware descarta el tráfico replicado, la columna Descartado será un valor distinto de cero, como se muestra en el siguiente resultado:

```
N9K# show hardware rate-limiter span Units for Config: kilo bits per second Allowed, Dropped &
Total: aggregated bytes since last clear counters Module: 1 R-L Class Config Allowed Dropped
Total +----------------+----------+--------------------+--------------------+--------------------
-+  span 50 0 499136  499136
```

El limitador de velocidad de hardware de sesión de monitor de SPAN a CPU se puede cambiar con el comando de configuración global **hardware rate-limiter span {kbps}**, como se muestra en el siguiente resultado.

```
N9K# configure terminal Enter configuration commands, one per line. End with CNTL/Z. N9K-
1(config)# hardware rate-limiter span 250 N9K-1(config)# end N9K# show running-config | inc
rate-limiter hardware rate-limiter span 250 N9K# show hardware rate-limiter span Units for
Config: kilo bits per second Allowed, Dropped & Total: aggregated bytes since last clear
counters Module: 1 R-L Class Config Allowed Dropped Total +----------------+----------+---------
----------+--------------------+--------------------+  span 250  0 0 0
```

> **Precaución:** Cisco no recomienda modificar el limitador de velocidad de hardware de sesión de supervisión SPAN a CPU lejos de su valor predeterminado de 50 kbps a menos que Cisco TAC se lo indique explícitamente. El aumento de este limitador de velocidad a un valor elevado puede provocar un aumento de la utilización de la CPU y una mayor inestabilidad del plano de control en el switch Nexus de Cisco serie 9000, lo que podría tener un impacto significativo en el tráfico de producción.

No se Soportó el Contador Permitido de Límite de Velocidad de Hardware de SPAN a CPU

La salida del comando **show hardware rate-limiter span** contiene un contador permitido. En otros limitadores de velocidad de hardware, este contador indica cuántos bytes pasan correctamente a través del limitador de velocidad de hardware. Sin embargo, el contador permitido para el limitador de velocidad de hardware de SPAN a CPU no aumenta debido a una limitación de software. Un ejemplo de esto se muestra en el siguiente resultado:

```
N9K# show hardware rate-limiter span

Units for Config: kilo bits per second
Allowed, Dropped & Total: aggregated bytes since last clear counters


Module: 1
R-L Class Config Allowed              Dropped                Total
+---------------+----------+-------------------+--------------------+--------------------+
span 50 0               499136               499136
```

Esta limitación del software afecta a todas las versiones del software NX-OS y se documenta a través de CSCva37512.

Para determinar cuánta cantidad de tráfico se ha replicado en el plano de control de un dispositivo Nexus 9000 configurado con una sesión de monitor SPAN a CPU activa, utilice el comando **show system internal access-list tcam ingress region span**. A continuación se muestra un ejemplo del resultado filtrado del comando mencionado que muestra los contadores de paquetes y bytes relevantes.

```
N9K# show system internal access-list tcam ingress region span | include pkts:
<snip>
pkts: 56582127, bytes: 4119668263
```

Los paquetes generados por el plano de control no aparecen en las sesiones del monitor TX SPAN a CPU

Los paquetes creados por el plano de control y transmitidos desde una interfaz de origen para una sesión de monitor de SPAN a CPU no serán capturados por la sesión de monitor de SPAN a CPU. Estos paquetes saldrán de la interfaz correctamente, pero no pueden capturarse a través de una sesión de monitor de SPAN a CPU en el mismo dispositivo donde se genera el paquete.

Por ejemplo, considere un dispositivo Cisco Nexus serie 9000 donde Ethernet1/1 es una interfaz L3/enrutada conectada a otro router. El proceso OSPF 1 se activa en Ethernet1/1, que es la única interfaz activada por OSPF en el dispositivo Cisco Nexus 9000.

```
N9K# show running-config ospf  !Command: show running-config ospf !Running configuration last done at: Wed Feb 26 16:16:30 2020 !Time: Wed Feb 26 16:16:37 2020 version 9.3(3) Bios:version 05.39 feature ospf router ospf 1 interface Ethernet1/1 ip router ospf 1 area 0.0.0.0 N9K# show ip ospf interface brief  OSPF Process ID 1 VRF default Total number of interface: 1 Interface ID Area Cost State Neighbors Status Eth1/1 1 0.0.0.0 4 DR 0 up
```

La utilidad de captura de paquetes del plano de control Ethanalyer muestra que los mensajes Hello OSPF son generados por el plano de control del dispositivo una vez cada 10 segundos.

```
N9K# ethanalyzer local interface inband display-filter ospf limit-captured-frames 0 Capturing on
inband 2020-02-26 16:19:13.041255 192.168.1.1 -> 224.0.0.5 OSPF Hello Packet  2020-02-26
16:19:22.334692 192.168.1.1 -> 224.0.0.5 OSPF Hello Packet  2020-02-26 16:19:31.568034
192.168.1.1 -> 224.0.0.5 OSPF Hello Packet  ^C 3 packets captured
```

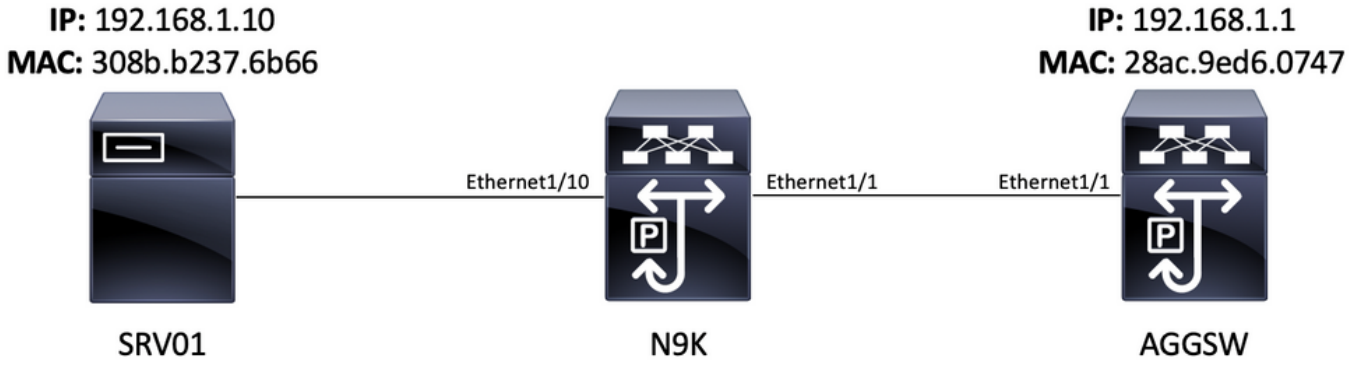
Sin embargo, un SPAN-to-CPU de salida/TX en la interfaz Ethernet1/1 no muestra estos paquetes Hello de Open Shortest Path First (OSPF) transmitidos en esta interfaz después de 60 segundos de tiempo.

```
N9K# show running-config monitor  !Command: show running-configmonitor !Running configuration
last done at: Wed Feb 26 16:20:48 2020 !Time: Wed Feb 26 16:20:51 2020 version 9.3(3)
Bios:version 05.39 monitor session 1 source interface Ethernet1/1 tx destination interface sup-
eth0 no shut N9K# show monitor  Session State Reason Description ------- ----------- -----------
----------- ------------------------------- 1 up The session is up N9K# ethanalyzer local
interface inband mirror display-filter ospf autostop duration 60 Capturing on inband 0 packets
captured
```

Para verificar si los paquetes generados por el plano de control de un dispositivo Cisco Nexus 9000 se transmiten desde una interfaz específica, Cisco recomienda utilizar una utilidad de captura de paquetes en el dispositivo remoto conectado a la interfaz.

Procedimiento de ampliación de la nube de Cisco Nexus 9000 SPAN a CPU

Tenga en cuenta la siguiente topología:



Un paquete de protocolo de mensajes de control de Internet (ICMP) originado en el servidor SRV01 en la VLAN 10 (192.168.10.10) está destinado al gateway 10 de VLAN 192.168.10.1. Se utilizará una sesión de supervisión de SPAN a CPU para confirmar que este paquete ICMP atraviesa el dispositivo N9K (un Cisco Nexus 93180YC-EX que ejecuta la versión 9.3(3) del software NX-OS), que actúa como switch de Capa 2 que conecta el SRV01 con AGGSW en la VLAN 10.

Paso 1. Confirmar recursos suficientes para la nueva sesión SPAN

Los switches Nexus de Cisco serie 9000 con el ASIC Cloud Scale que ejecutan el software NX-OS admiten un máximo de cuatro sesiones SPAN o ERSPAN activas por ASIC/motor de reenvío. Además, si las primeras tres sesiones SPAN o ERSPAN se configuran con interfaces de origen bidireccionales (TX y RX), la interfaz de origen de la cuarta sesión SPAN o ERSPAN debe ser un origen RX/de ingreso.

Antes de configurar una sesión de monitor SPAN a CPU, verifique la cantidad de otras sesiones SPAN o ERSPAN configuradas actualmente en el dispositivo. Esto se puede hacer con los comandos **show running-config monitor** y **show monitor**. El siguiente ejemplo muestra el resultado de ambos comandos cuando no se configuran otras sesiones SPAN o ERSPAN en el dispositivo.

```
N9K# show running-config monitor  !Command: show running-configmonitor !Running configuration
last done at: Tue Feb 25 20:34:04 2020 !Time: Tue Feb 25 20:34:06 2020 version 9.3(3)
Bios:version 07.66 N9K# show monitor  Note: No sessions configured
```

> **Nota:** Puede encontrar información adicional sobre el número máximo de sesiones SPAN/ERSPAN y otras limitaciones en la Guía de Escalabilidad Verificada de Cisco Nexus serie 9000 NX-OS para la versión 9.3(3) del software NX-OS.

Paso 2. Configuración de la Sesión de Monitor SPAN a CPU

El elemento de configuración clave que define una sesión de monitor de SPAN a CPU es una interfaz de destino de "sup-eth0", que es la interfaz dentro de banda del supervisor. El siguiente ejemplo muestra la configuración de una sesión de monitor de SPAN a CPU donde los paquetes de ingreso/RX de Ethernet1/10 se replican al supervisor del switch Nexus de Cisco serie 9000.

```
N9K# configure terminal Enter configuration commands, one per line. End with CNTL/Z. N9K-
1(config)# monitor session 1 N9K-1(config-monitor)# source interface Ethernet1/10 rx N9K-
1(config-monitor)# destination interface sup-eth0 N9K-1(config-monitor)# no shut N9K-1(config-
monitor)# end N9K#
```

Paso 3. Verifique que la Sesión de Monitor SPAN a CPU esté Activa

Utilice los comandos **show running-config monitor** y **show monitor** para verificar que la sesión del monitor de SPAN a CPU esté configurada y en funcionamiento. La configuración de la sesión del monitor de SPAN a CPU se puede verificar a través del resultado del comando **show running-config monitor**, como se muestra en el siguiente ejemplo.

```
N9K# show running-config monitor  !Command: show running-configmonitor !Running configuration
last done at: Tue Feb 25 20:47:50 2020 !Time: Tue Feb 25 20:49:35 2020 version 9.3(3)
Bios:version 07.66 monitor session 1 source interface Ethernet1/10 rx destination interface sup-
eth0 no shut
```

El estado operativo de la sesión de monitor de SPAN a CPU se puede verificar a través del resultado del comando **show monitor**. El resultado debe informar que el estado de la sesión de supervisión de SPAN a CPU está "activo" con una razón de "La sesión está activa", como se muestra en el ejemplo siguiente.

```
N9K# show monitor  Session State Reason Description - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - 1 up The session is up
```

Paso 4. Ver paquetes replicados en el plano de control

La utilidad de captura de paquetes del plano de control Ethanalyer se puede utilizar para ver el tráfico replicado en el plano de control del dispositivo Cisco Nexus 9000. La palabra clave **Mirror** del comando Ethanalyzer filtra el tráfico de modo que sólo se muestra el tráfico replicado por una sesión de monitor de SPAN a CPU. Los filtros de captura y visualización de Ethanalyzer se

pueden utilizar para limitar aún más el tráfico mostrado. Puede encontrar información adicional sobre filtros útiles de captura y visualización de Ethanalyzer en la Guía de Troubleshooting de Nexus 7000. Tenga en cuenta que, aunque este documento se ha escrito para la plataforma Cisco Nexus 7000, también se aplica principalmente a la plataforma Cisco Nexus 9000.

A continuación se muestra un ejemplo del uso de la utilidad de captura de paquetes del plano de control Ethanalyzer para filtrar el tráfico replicado por una sesión de monitor de SPAN a CPU. Tenga en cuenta que se utiliza la palabra clave **reflejada**, así como un filtro de visualización que define los paquetes ICMP originados o destinados a 192.168.10.10 (la dirección IP de SRV01 en la topología mencionada).

```
N9K# ethanalyzer local interface inband mirror display-filter "icmp && ip.addr==192.168.10.10"
limit-captured-frames 0
Capturing on inband
2020-02-25 21:01:07.592838 192.168.10.10 -> 192.168.10.1 ICMP Echo (ping) request 2020-02-25
21:01:08.046682 192.168.10.10 -> 192.168.10.1 ICMP Echo (ping) request 2020-02-25
21:01:08.047720 192.168.10.10 -> 192.168.10.1 ICMP Echo (ping) request 2020-02-25
21:01:08.527646 192.168.10.10 -> 192.168.10.1 ICMP Echo (ping) request 2020-02-25
21:01:08.528659 192.168.10.10 -> 192.168.10.1 ICMP Echo (ping) request 2020-02-25
21:01:08.529500 192.168.10.10 -> 192.168.10.1 ICMP Echo (ping) request 2020-02-25
21:01:08.530082 192.168.10.10 -> 192.168.10.1 ICMP Echo (ping) request 2020-02-25
21:01:08.530659 192.168.10.10 -> 192.168.10.1 ICMP Echo (ping) request 2020-02-25
21:01:08.531244 192.168.10.10 -> 192.168.10.1 ICMP Echo (ping) request ^C 9 packets captured
```

> **Nota:** Utilice la combinación de teclas Control-C para salir de la utilidad de captura de paquetes del plano de control Ethanalyzer.

Se puede ver información detallada sobre este tráfico incluyendo la palabra clave **detail** en el comando Ethanalyzer. A continuación se muestra un ejemplo de esto para un único paquete de Solicitud de eco ICMP.

```
N9K# ethanalyzer local interface inband mirror display-filter "icmp && ip.addr==192.168.10.10"
limit-captured-frames 0 detail
Capturing on inband Frame 2 (114 bytes on wire, 114 bytes captured) Arrival Time: Feb 25, 2020
21:56:40.497381000 [Time delta from previous captured frame: 1.874113000 seconds] [Time delta
from previous displayed frame: 1.874113000 seconds] [Time since reference or first frame:
1.874113000 seconds] Frame Number: 2 Frame Length: 114 bytes Capture Length: 114 bytes [Frame is
marked: False] [Protocols in frame: eth:ip:icmp:data] Ethernet II, Src: 30:8b:b2:37:6b:66
(30:8b:b2:37:6b:66), Dst: 28:ac:9e:d6:07:47 (28:ac:9e:d6:07:47) Destination: 28:ac:9e:d6:07:47
(28:ac:9e:d6:07:47) Address: 28:ac:9e:d6:07:47 (28:ac:9e:d6:07:47) .... ...0 .... .... .... ....
= IG bit: Individual address (unicast) .... ..0. .... .... .... .... = LG bit: Globally unique
address (factory default) Source: 30:8b:b2:37:6b:66 (30:8b:b2:37:6b:66) Address:
30:8b:b2:37:6b:66 (30:8b:b2:37:6b:66) .... ...0 .... .... .... .... = IG bit: Individual address
(unicast) .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default) Type
: IP (0x0800) Internet Protocol, Src: 192.168.10.10 (192.168.10.10), Dst: 192.168.10.1
(192.168.10.1) Version : 4 Header length: 20 bytes Differentiated Services Field: 0x00 (DSCP
0x00: Default; ECN: 0x00) 0000 00.. = Differentiated Services Codepoint: Default (0x00) ....
..0. = ECN-Capable Transport (ECT): 0 .... ...0 = ECN-CE: 0 Total Length: 100 Identification:
0x00e1 (225) Flags: 0x00 0.. = Reserved bit: Not Set .0. = Don't fragment: Not Set ..0 = More
fragments: Not Set Fragment offset: 0 Time to live: 254 Protocol: ICMP (0x01) Header checksum :
0x265c [correct] [Good: True] [Bad : False] Source: 192.168.10.10 (192.168.10.10) Destination:
192.168.10.1 (192.168.10.1) Internet Control Message Protocol Type : 8 (Echo (ping) request)
Code: 0 () Checksum : 0xf1ed [correct] Identifier: 0x0004 Sequence number: 0 (0x0000) Data (72
bytes) 0000 00 00 00 00 ed 9e 9e b9 ab cd ab cd ab cd ab cd ..............  0010 ab cd ab cd ab
cd ab cd ab cd ab cd ab cd ab cd ..............  0020 ab cd ab cd ab cd ab cd ab cd ab cd ab cd
ab cd ..............  0030 ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd ..............
0040 ab cd ab cd ab cd ab cd ........ Data: 00000000ED9E9EB9ABCDABCDABCDABCDABCDABCDABCD...
```

```
[Length: 72] ^C 1 packet captured
```

Paso 5. Apagar administrativamente la sesión de supervisión de SPAN a CPU

Utilice el comando de configuración **shut** en el contexto de la sesión de monitor SPAN a CPU para cerrar de forma correcta la sesión de supervisión SPAN a CPU y detener la replicación del tráfico en el plano de control del dispositivo Cisco Nexus 9000.

```
N9K# configure terminal Enter configuration commands, one per line. End with CNTL/Z. N9K-
1(config)# monitor session 1 N9K-1(config-monitor)# shut N9K-1(config-monitor)# end N9K#
```

Verifique el estado operativo de la sesión de monitor de SPAN a CPU con el comando **show monitor**. El estado operativo de la sesión de supervisión de SPAN a CPU debe mostrarse como "inactivo" con una razón de "cierre de administración de sesión", como se muestra en el ejemplo siguiente:

```
N9K# show monitor  Session State Reason Description - - - - - - - - - - - - - - - - - - - - - -
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- - 1 down Session admin shut
```

Paso 6. Eliminación de la configuración de sesión de SPAN a CPU Monitor (opcional)

Si lo desea, quite la configuración de la sesión SPAN-to-CPU monitor con el **comando de configuración no monitor session {id}**. Un ejemplo de esto se muestra en el siguiente resultado.

```
N9K# configure terminal Enter configuration commands, one per line . End with CNTL/Z. N9K-
1(config)# no monitor session 1 N9K-1(config)# end
```

Verifique que la configuración de la sesión del monitor de SPAN a CPU se haya eliminado correctamente con el comando **show running-config monitor**, como se muestra en el siguiente ejemplo.

```
N9K# show running-config monitor  !Command: show running-configmonitor !Running configuration
last done at: Tue Feb 25 21:46:25 2020 !Time: Tue Feb 25 21:46:29 2020 version 9.3(3)
Bios:version 07.66 N9K#
```

Analizar los resultados de una captura de paquetes SPAN a CPU

El ejemplo anterior de este procedimiento muestra que los paquetes de solicitud de eco ICMP originados en 192.168.10.10 (SRV01) destinados a 192.168.10.1 (AGGSW) ingresan a la interfaz Ethernet1/10 del dispositivo Cisco Nexus 9000 con un nombre de host N9K ... Esto prueba que el SRV01 envía este tráfico fuera de su tarjeta de interfaz de red. Esto también demuestra que el paquete de solicitud de eco ICMP avanza lo suficiente en la canalización de reenvío de ASIC de Cisco Cloud Scale para que se replique en el plano de control del dispositivo.

Sin embargo, esto no prueba que el dispositivo Cisco Nexus 9000 reenvíe el paquete de solicitud de eco ICMP de Ethernet1/1 a AGGSW. Es necesario realizar más troubleshooting para validar si el paquete se reenvía fuera de Ethernet1/1 hacia AGGSW. En orden de fiabilidad:

1. Si el dispositivo remoto de la interfaz de salida esperada (Ethernet1/1 de N9K en el ejemplo) es un dispositivo Cisco Nexus serie 9000 con un ASIC de escala de nube, puede realizar una sesión de monitor de SPAN a CPU de ingreso/RX en el dispositivo remoto (Eth1/1 de AGGSW en el

ejemplo anterior). Si el dispositivo remoto de la interfaz de salida esperada no es un dispositivo Cisco Nexus serie 9000 con un ASIC de escala de nube, entonces un SPAN, duplicación de puertos u otra captura de paquetes similar en el dispositivo remoto es equivalente.

2. Realice una ELAM de ingreso/RX en la interfaz de ingreso (Ethernet1/10 de N9K en el ejemplo anterior) del dispositivo Cisco Nexus 9000. Puede encontrar información adicional sobre este procedimiento en la nota técnica de solución de problemas de ELAM de Nexus 9000 Cloud Scale ASIC NX-OS.

3. Realice una SPAN de salida/TX a CPU en la interfaz de salida del dispositivo Cisco Nexus 9000 (Ethernet1/1 de N9K en el ejemplo anterior).

Información Relacionada

- Guía de solución de problemas de Cisco Nexus serie 9000 NX-OS, versión 9.3(x)
- Guía de solución de problemas de Cisco Nexus serie 9000 NX-OS, versión 9.2(x)
- Guía de solución de problemas de Cisco Nexus serie 9000 NX-OS, versión 7.0(3)I7(x)
- Guía de solución de problemas de Ethanalyzer en Nexus 7000
- Nexus 9000 Cloud Scale ASIC (Tahoe) NX-OS ELAM