Guía de SPAN de ACI

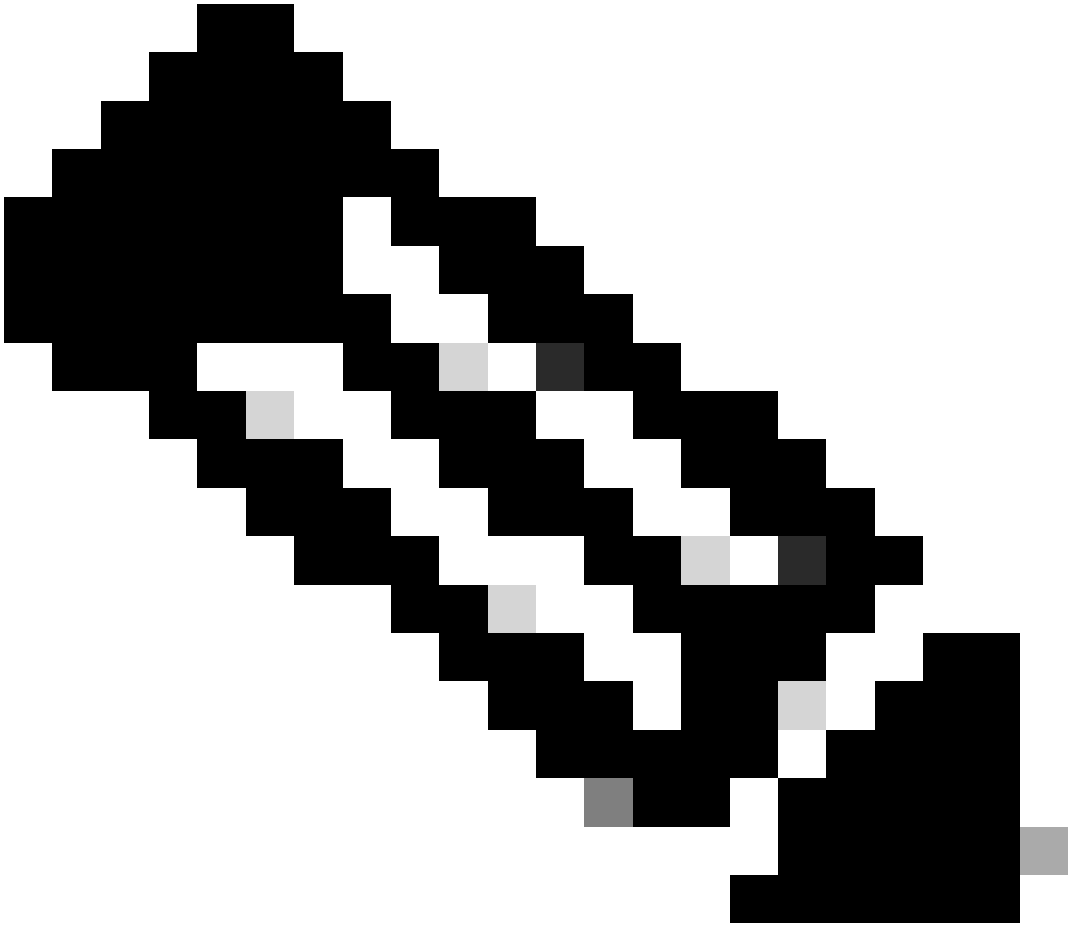
Contenido

Introducción

Este documento describe cómo configurar el Analizador de puerto conmutado (SPAN) en Cisco Application Centric Infrastructure (ACI).

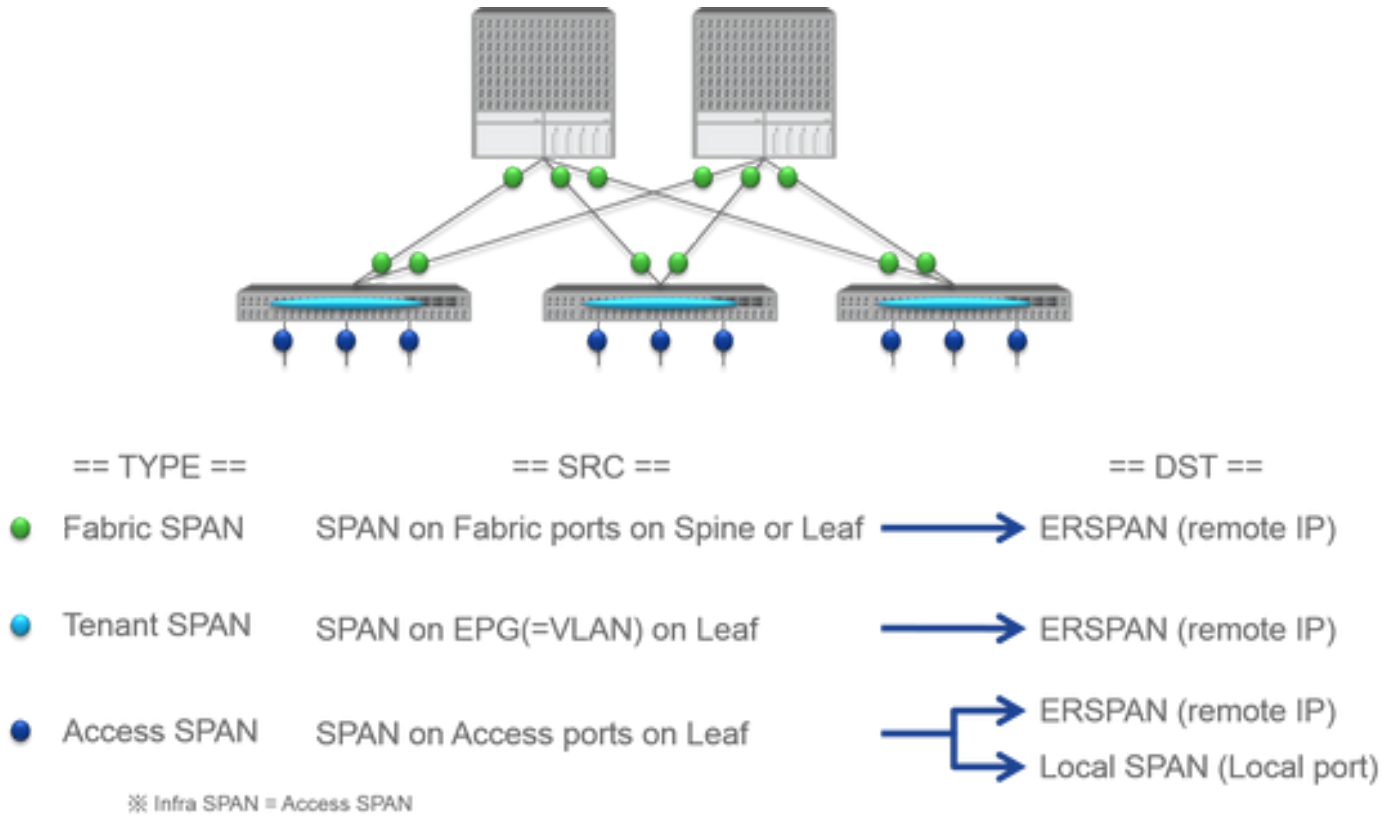
Antecedentes

En general, hay tres tipos de SPAN. SPAN local, SPAN remoto (RSPAN) y SPAN remoto encapsulado (ERSPAN). Las diferencias entre estos SPAN son principalmente el destino de los paquetes de copia. Cisco ACI admite SPAN local y ERSPAN.



Nota: Este documento asume que los lectores ya están familiarizados con SPAN en general, como las diferencias de SPAN local y ERSPAN.

Tipo de SPAN en Cisco ACI



Cisco ACI dispone de tres tipos de SPAN: Fabric SPAN, Tenant SPAN y Access SPAN. La diferencia entre cada SPAN es el origen de los paquetes de copia.

Como se mencionó anteriormente,

- **Fabric SPAN** es capturar los paquetes que entran y salen de **interfaces between Leaf and Spine switches**.
    - Access SPAN es capturar los paquetes que entran y salen de interfaces between Leaf switches and external devices.
    - Tenant SPAN es capturar los paquetes que entran y salen de EndPoint Group (EPG) on ACI Leaf switches.

Este nombre de SPAN corresponde a la ubicación que se debe configurar en la GUI de Cisco ACI.

- El SPAN de fabric se configura en Fabric > Fabric Policies
    - El SPAN de acceso se configura en Fabric > Access Policies

- El SPAN del arrendatario se configura en Tenants > {each tenant}

En cuanto al destino de cada SPAN, solo Access SPAN es capaz de ambos Local SPAN y ERSPAN. Los otros dos SPAN (Fabric y Tenant) sólo son capaces de ERSPAN.

Limitaciones y directrices

Revise las limitaciones y directrices de la guía de resolución de problemas de Cisco APIC. Se menciona en Troubleshooting Tools and Methodology > Using SPAN.

Configuración

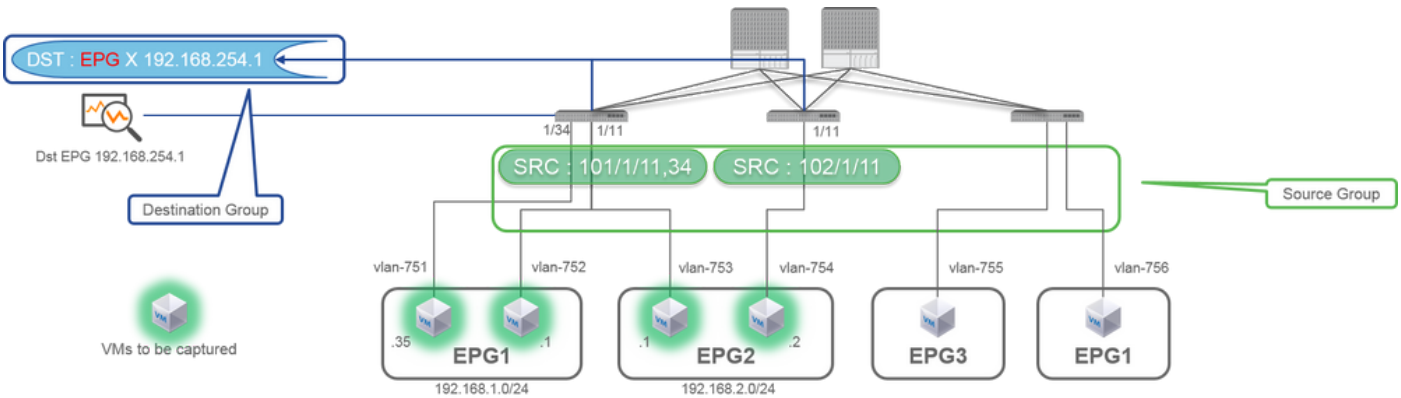
Esta sección presenta breves ejemplos relacionados con la configuración para cada tipo de SPAN. Hay casos de ejemplo específicos sobre cómo seleccionar el tipo de tramo en la sección posterior.

La configuración de SPAN también se describe en la Guía de solución de problemas de Cisco APIC: Herramientas y metodología de solución de problemas > Uso de SPAN.

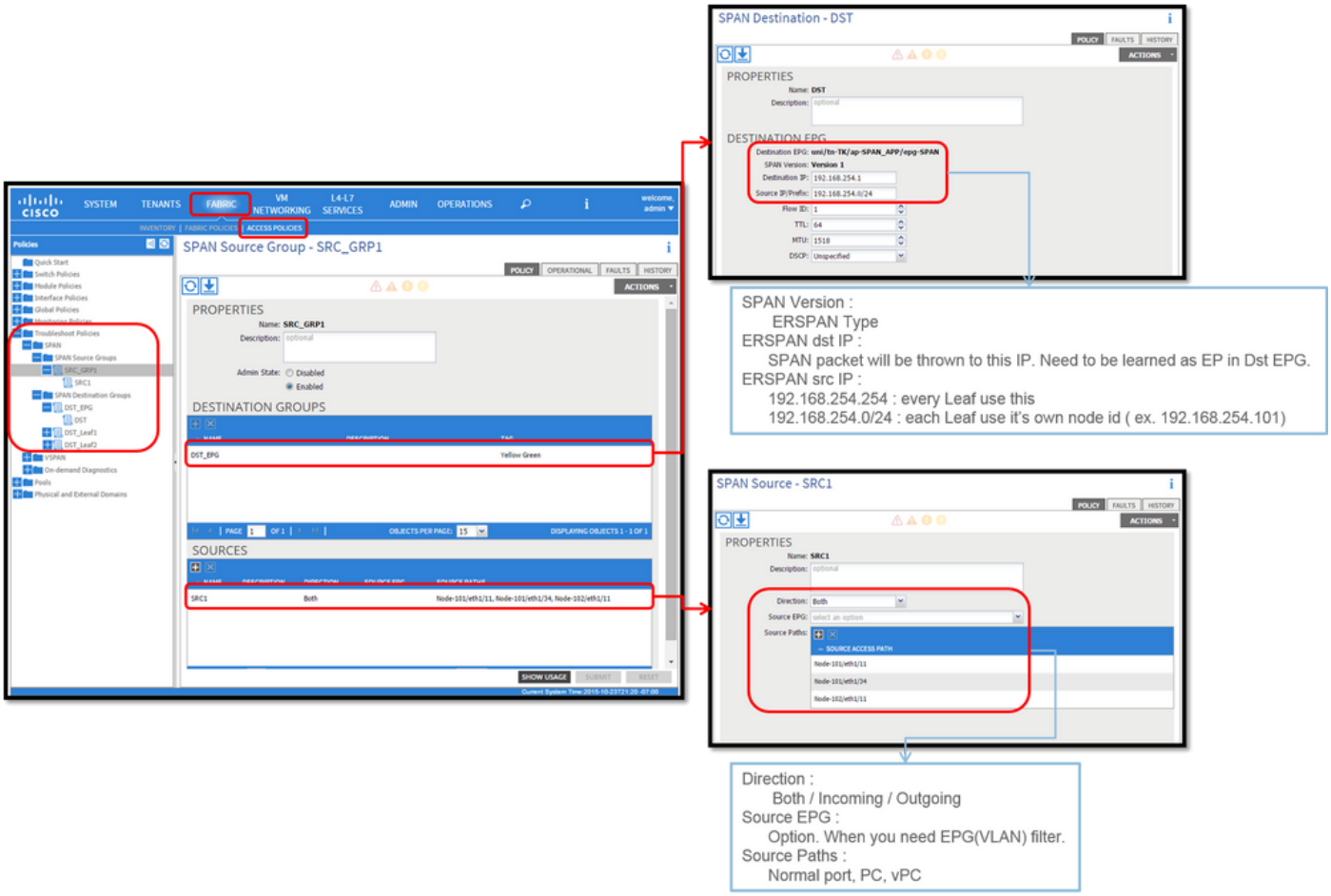
La interfaz de usuario puede tener un aspecto diferente al de las versiones actuales, pero el enfoque de configuración es el mismo.

SPAN de acceso (ERSPAN)

Topología de ejemplo



Ejemplo de configuración



Where:

Desplácese hasta FABRIC > ACCESS POLICIES > Troubleshoot Policies > SPAN.

- SPAN Source Groups
    - SPAN Destination Groups

SPAN Source Group lazos Destination y Sources.

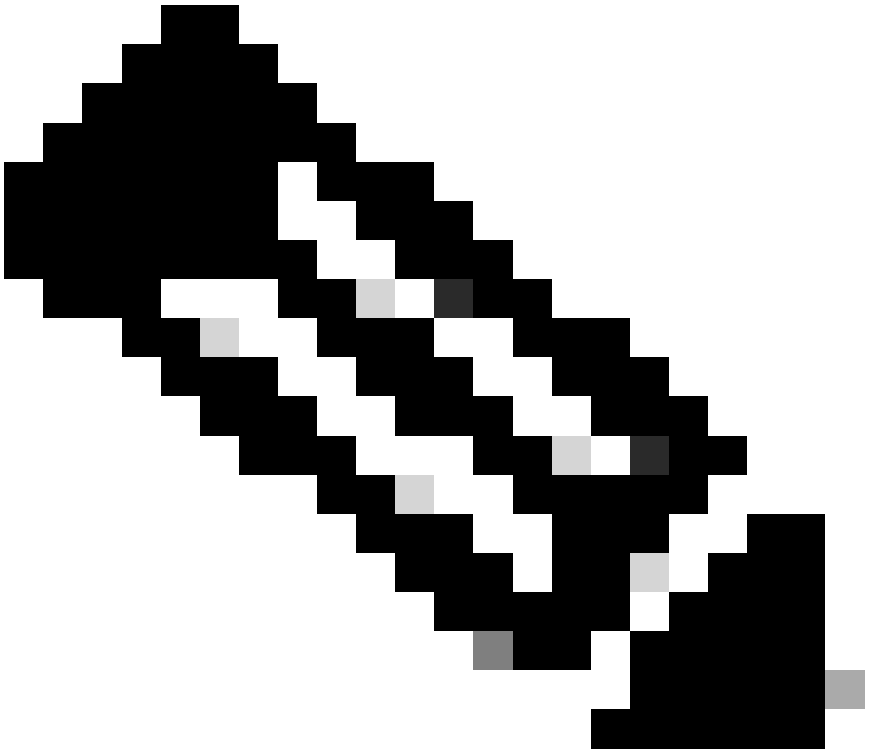
Cómo:

1. Crear SPAN Source Group (SRC_GRP1).

- Cree SPAN Source (SRC1) en SPAN Source Group (SRC_GRP1).

- Configure estos parámetros para SPAN Source (SRC1).

- Dirección - Origen EPG (opción)
- Rutas de origen (pueden ser interfaces múltiples)



Nota: Consulte la imagen para obtener detalles de cada parámetro.

- Crear SPAN Destination Group (DST_EPG).

- Crear SPAN Destination (DST).

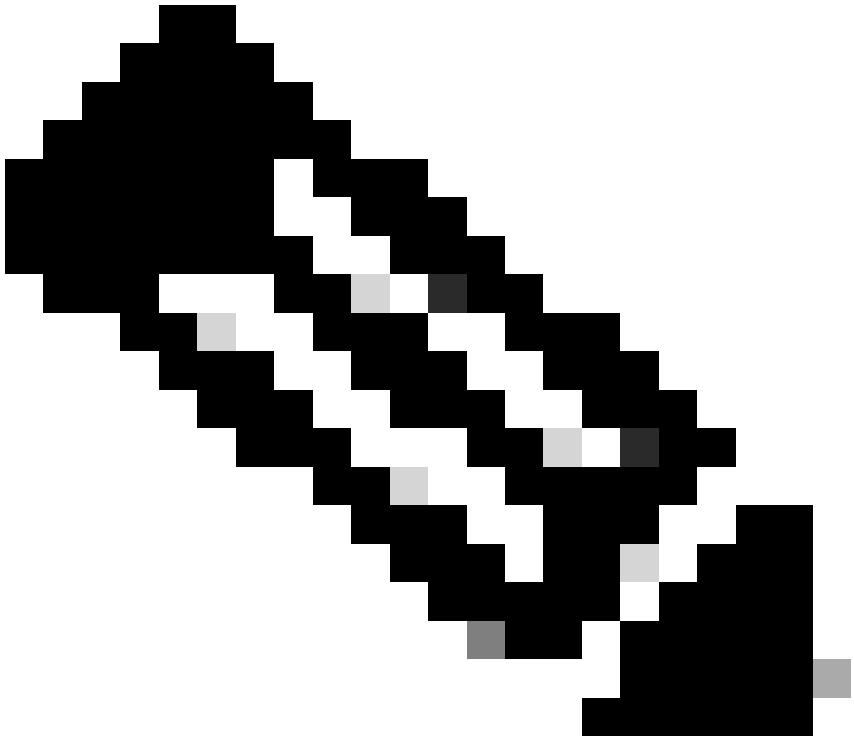
- Configure estos parámetros para SPAN Destination (DST)

- EPG de destino

-IP de destino

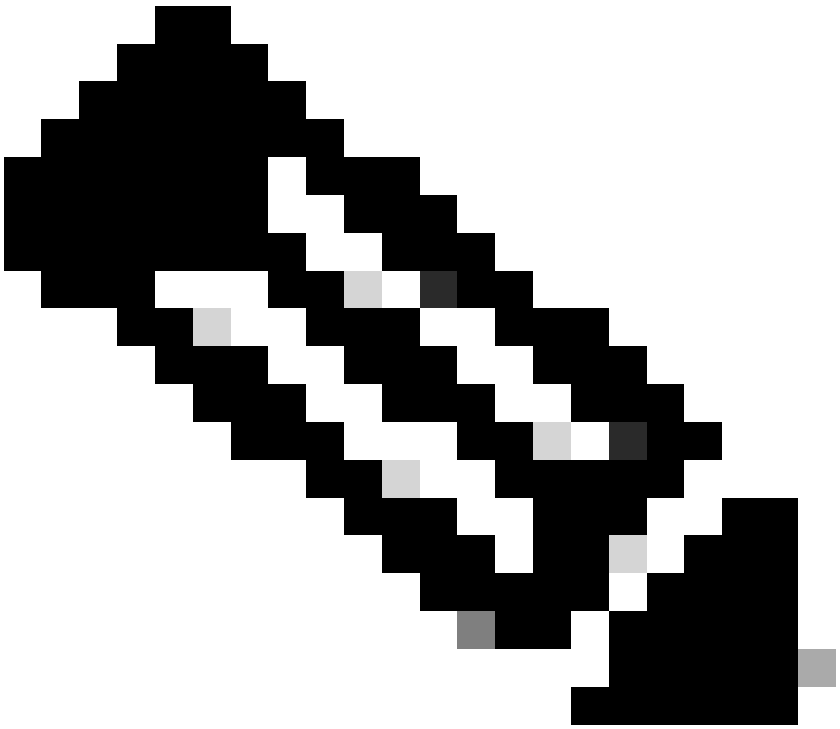
- IP/prefijo de origen (puede ser cualquier IP. Si se utiliza el prefijo, se utiliza node-id del nodo de origen para los bits no definidos. Por ejemplo, prefix: 1.0.0.0/8 on node-101 => src IP 1.0.0.101)

- Otros parámetros se pueden dejar como predeterminados



Nota: Consulte la imagen para obtener detalles de cada parámetro.

- Asegúrese de que SPAN Destination Group está vinculado a un SPAN Source Group adecuado.
- Asegúrese Admin Statede que está habilitado.

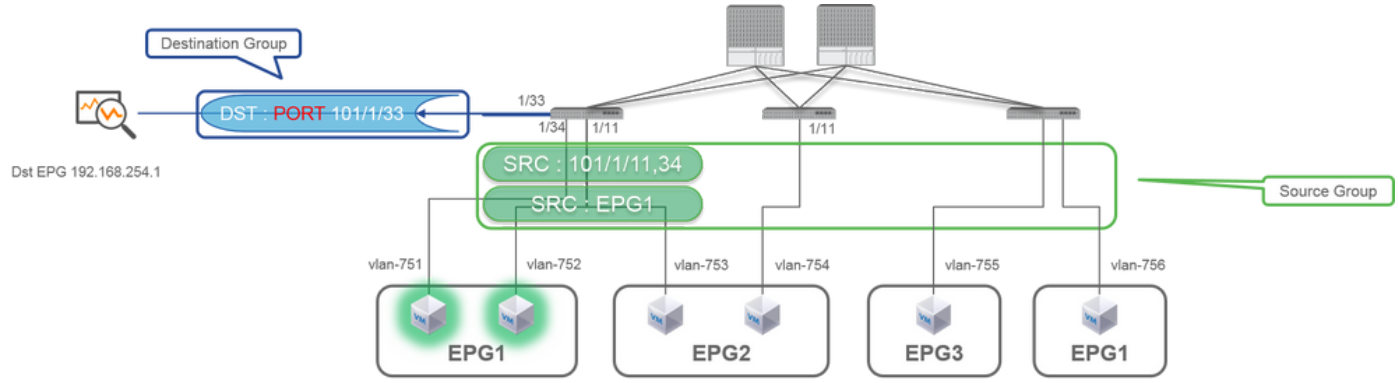


Nota: SPAN se detiene cuando se selecciona Disabled (Desactivado) en este estado de administración. No es necesario eliminar todas las directivas si las vuelve a utilizar más adelante.

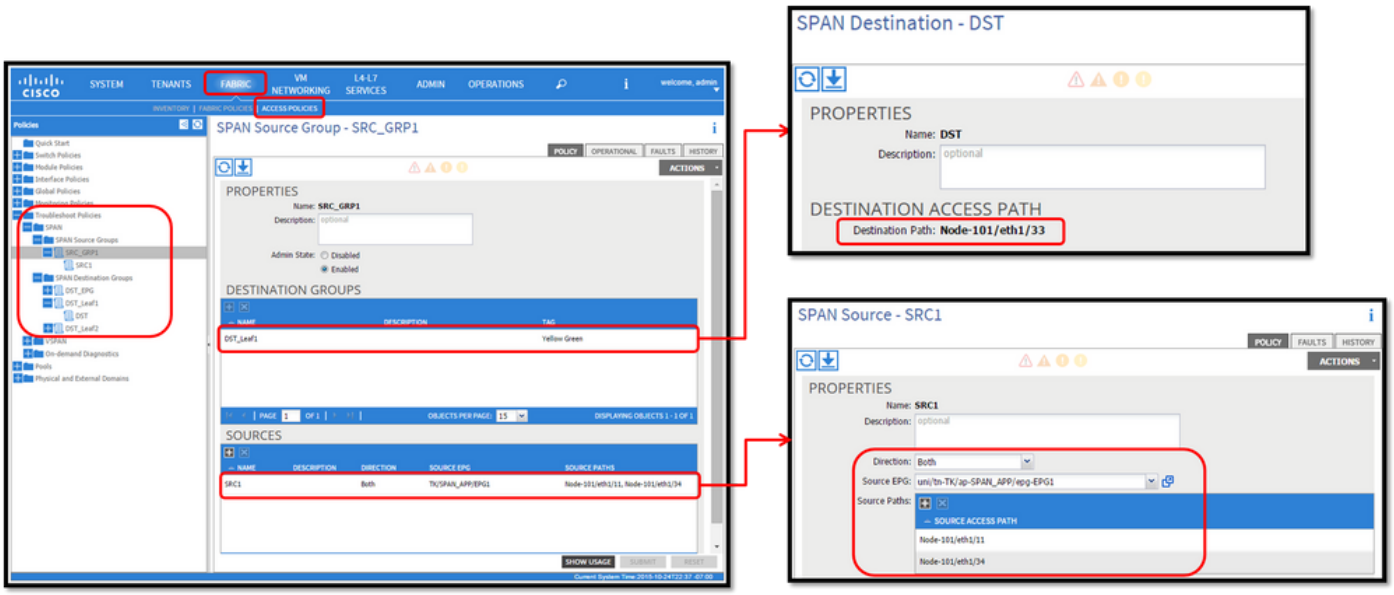
También asegúrese de que la IP de destino para ERSPAN se aprende como un punto final bajo el EPG de destino especificado. En el ejemplo mencionado anteriormente, 192.168.254.1 debe aprenderse en Tenant TK > Application profile SPAN_APP > EPG SPAN. O bien, la IP de destino se puede configurar como un punto final estático en este EPG si el dispositivo de destino es un host silencioso.

SPAN de acceso (local)

Topología de ejemplo



Ejemplo de configuración



- Where:

Fabric > ACCESS POLICIES > Troubleshoot Policies > SPAN

- SPAN Source Groups

- SPAN Destination Groups

SPAN Source Group lazos Destination y Sources.

- Cómo:

1. Crear SPAN Source Group (SRC_GRP1)

   - Crear SPAN Source(SRC1) en SPAN Source Group (SRC_GRP1)

   - Configure estos parámetros para SPAN Source (SRC1)
   -Dirección:
   - EPG de origen (opción)
   - Rutas de origen (pueden ser interfaces múltiples)
   ※ consulte la imagen para obtener detalles de cada parámetro.

   - Crear SPAN Destination Group(DST_Leaf1)

   - Crear SPAN Destination(DST)

   - Configure estos parámetros para SPAN Destination (DST)
   - Nodo e interfaz de destino.

   - Asegúrese de que SPAN Destination Group está vinculado a un SPAN Source Group adecuado.

   -

   Asegúrese Admin State de que está habilitado.
   ※ SPAN se detiene cuando selecciona Disabled (Desactivado) en este estado de administración. No es necesario eliminar todas las directivas si las vuelve a utilizar más adelante.

La interfaz de destino no requiere ninguna configuración por parte de los grupos de directivas de interfaz. Funciona cuando se conecta un cable a la interfaz en ACI Leaf.

Limitaciones:

- Para SPAN local, una interfaz de destino e interfaces de origen deben configurarse en la misma hoja.

- La interfaz de destino no requiere que esté en un EPG mientras esté ACTIVO.

- Cuando se especifica la interfaz de canal de puerto virtual (vPC) como puerto de origen, no se puede utilizar SPAN local
  Sin embargo, existe una solución alternativa. En una hoja de primera generación, un puerto físico individual que es miembro de vPC o PC se puede configurar como origen SPAN. Con este SPAN local se puede utilizar para el tráfico en los puertos vPC.
  Sin embargo, esta opción no está disponible en una hoja de segunda generación (CSCvc1053). En su lugar, se añadió soporte para SPAN en "VPC component PC" mediante CSCvc44643en 2.1(2e), 2.2(2e) y versiones posteriores. Con esto, cualquier hoja de generación puede configurar un canal de puerto, que es un miembro de vPC, como fuente SPAN. Esto permite que cualquier hoja de generación utilice SPAN local para el tráfico en los puertos vPC.

- La especificación de los puertos individuales de un canal de puerto en las hojas de segunda generación hace que solo un subconjunto de los paquetes se extienda (también debido a CSCvc1053).

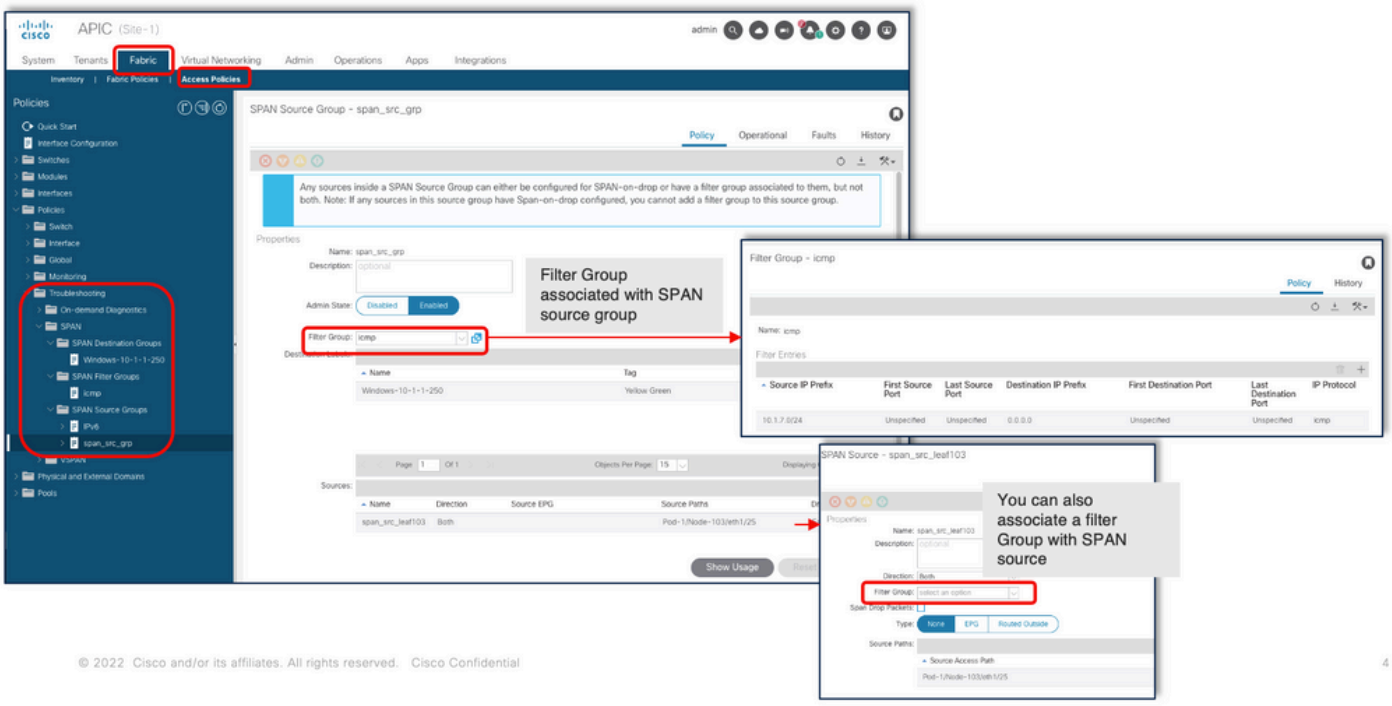
- No se pueden utilizar PC y vPC como puerto de destino para SPAN local. A partir de la versión 4.1(1), el PC se puede utilizar como puerto de destino para SPAN local.

SPAN de acceso: con filtros de ACL

Puede utilizar filtros ACL en orígenes de tramo de acceso. Esta función proporciona la capacidad de SPAN para un flujo o flujo de tráfico particular de entrada/salida de un origen de SPAN.
Los usuarios pueden aplicar las ACL de SPAN a un origen cuando sea necesario que SPAN fluya tráfico específico.
No es compatible con los grupos/orígenes de origen de Fabric SPAN y Tenant Span.
Se debe tener cuidado al agregar entradas de filtro en un grupo de filtros, ya que podría agregar entradas tcam para cada origen que utilice actualmente el grupo de filtros.

Un grupo de filtros se puede asociar a:
-Span Source: el grupo de filtros se utiliza para filtrar el tráfico en TODAS las interfaces definidas en este origen de span.
-Span Source Group: el grupo de filtros (por ejemplo, x) se utiliza para filtrar el tráfico en TODAS las interfaces definidas en cada uno de los orígenes de span de este grupo de orígenes de span.

En esta instantánea de configuración, el grupo de filtros se aplica al grupo de origen Span.

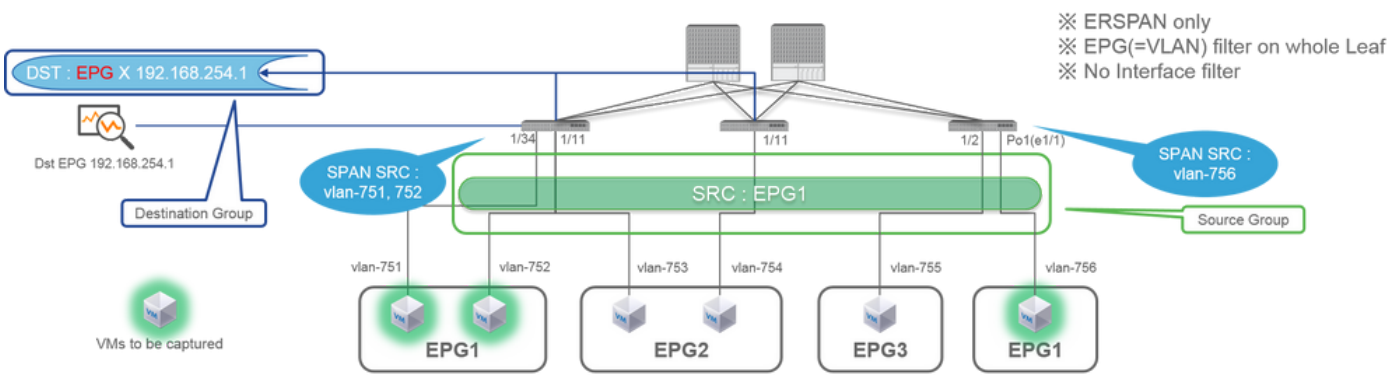


En el caso de que un origen de Span determinado ya se asocie con un grupo de filtros (por ejemplo, y), ese grupo de filtros (y) se utiliza en su lugar para filtrar el grupo en todas las interfaces bajo este origen de Span específico

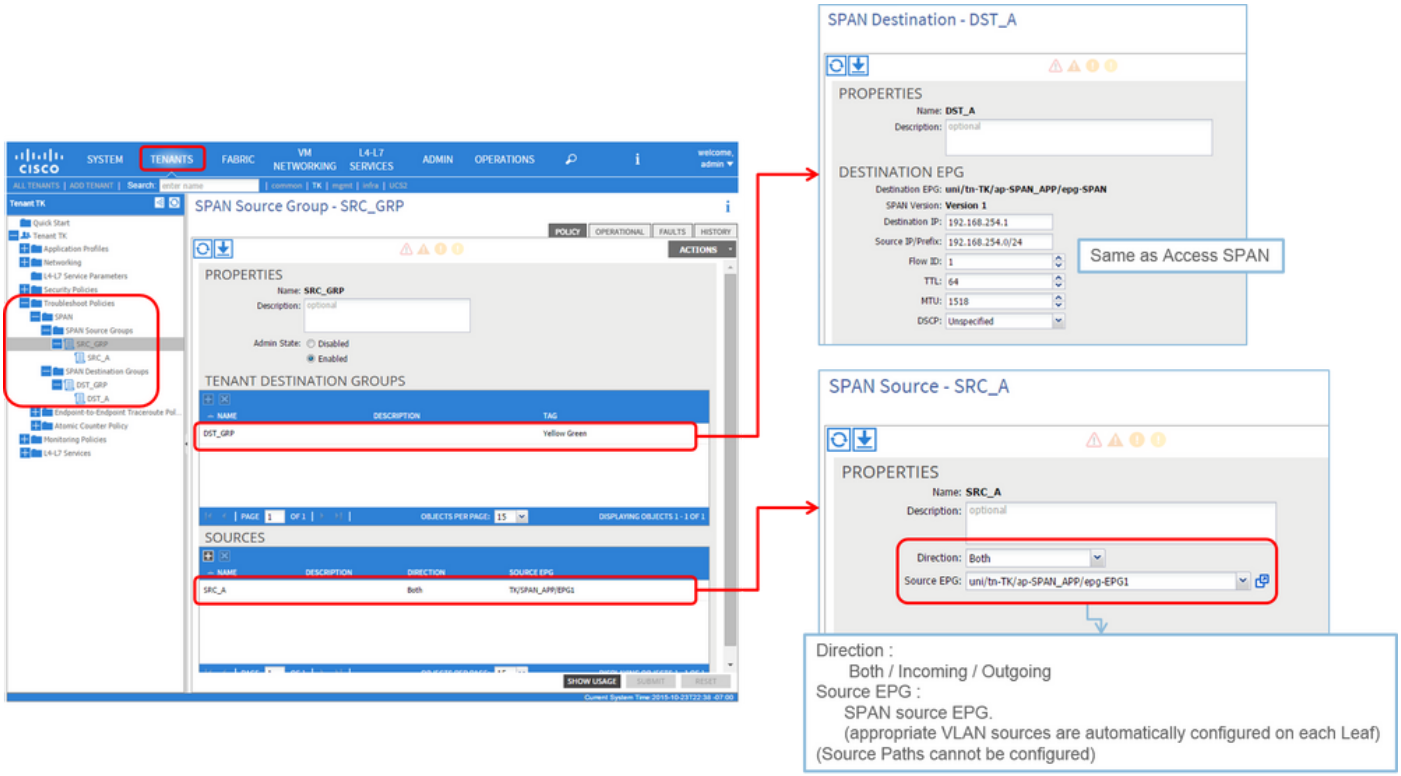
- Un grupo de filtros que se aplica a un grupo de orígenes se aplica automáticamente a todos los orígenes de ese grupo de orígenes.
- Un grupo de filtros que se aplica en un origen sólo es aplicable a ese origen.
- Si se aplica un grupo de filtros tanto al grupo de origen como a un origen de dicho grupo de origen, el grupo de filtros aplicado al origen tiene prioridad.
- Se elimina un grupo de filtros aplicado a un origen, el grupo de filtros aplicado al grupo de orígenes principal se aplica automáticamente.
- Se elimina un grupo de filtros aplicado a un grupo de origen, se elimina de todos los orígenes que heredan actualmente en ese grupo de origen.

SPAN de arrendatario (ERSPAN)

Topología de ejemplo



Ejemplo de configuración



- Where:

Tenants > {tenant name} > Troubleshoot Policies > SPAN

- SPAN Source Groups

- SPAN Destination Groups

※ Enlaces de grupos de origen SPAN Destination y Sources.

- Cómo:

1. Crear SPAN Source Group (SRC_GRP)

- Crear SPAN Source (SRC_A) en SPAN Source Group (SRC_GRP)

- Configure estos parámetros para SPAN Source (SRC_A)
  -Dirección:
  - EPG de origen

※ Consulte la imagen para obtener detalles de cada parámetro.

- Crear SPAN Destination Group (DST_GRP)

- Crear SPAN Destination (DST_A)

- Configure estos parámetros para SPAN Destination(DST_A)
  - EPG de destino
  -IP de destino
  - IP/Prefijo de origen
  - Otros parámetros se pueden dejar como predeterminados

※ Consulte la imagen para obtener detalles de cada parámetro.

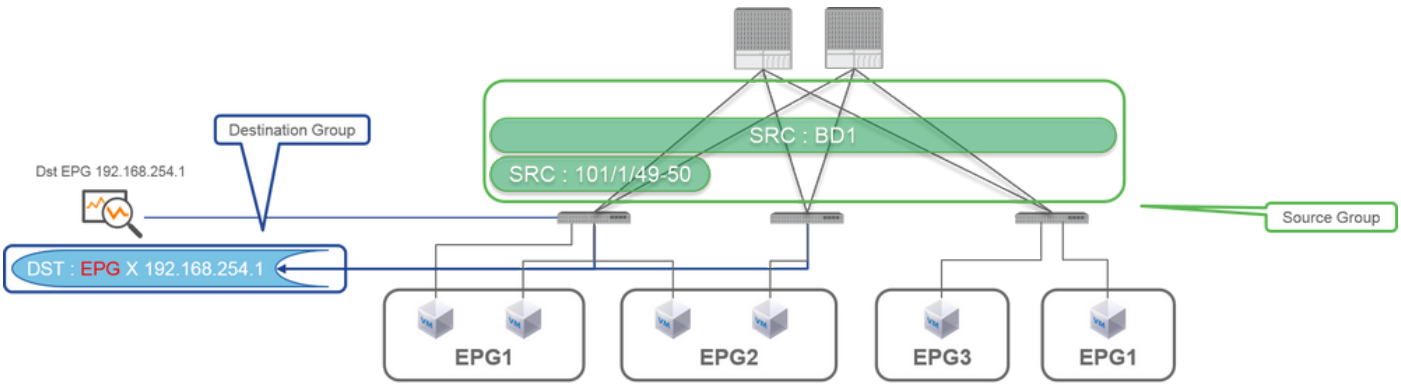
- Asegúrese SPAN Destination Group de que está vinculado a un SPAN Source Group adecuado.

- Asegúrese Admin State de que está habilitado.

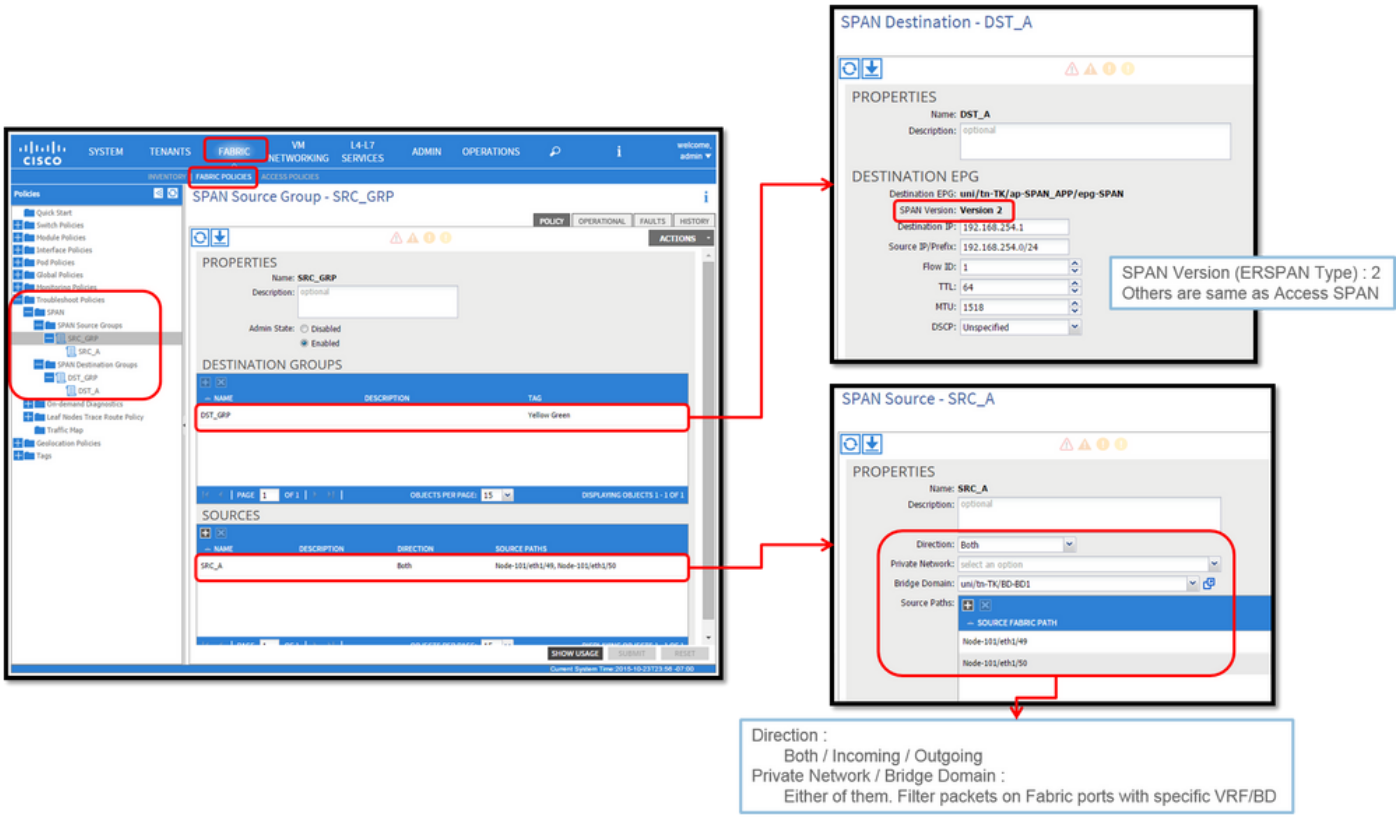
※ SPAN se detiene cuando selecciona Disabled (Desactivado) en este estado de administración. No es necesario eliminar todas las directivas si las vuelve a utilizar más adelante.

Fabric SPAN (ERSPAN)

Topología de ejemplo



Ejemplo de configuración



- Where:

Fabric > FABRIC POLICIES > Troubleshoot Policies > SPAN

- Fabric

- SPAN Destination Groups

※ SPAN Source Group lazos Destination y Sources

- Cómo:

1. Crear SPAN Source Group (SRC_GRP)

- Crear SPAN Source (SRC_A) en SPAN Source Group (SRC_GRP)

- Configure estos parámetros para SPAN Source (SRC_A)
  -Dirección:
  - Red privada (opción)
  - Dominio de puente (opción)
  - Rutas de origen (pueden ser interfaces múltiples)

※ consulte la imagen para obtener detalles de cada parámetro.

- Crear SPAN Destination Group (DST_GRP)

- Crear SPAN Destination (DST_A)

- Configure estos parámetros para SPAN Destination (DST_A)
  - EPG de destino
  -IP de destino
  - IP/Prefijo de origen
  - Otros parámetros se pueden dejar como predeterminados

※ consulte la imagen para obtener detalles de cada parámetro.

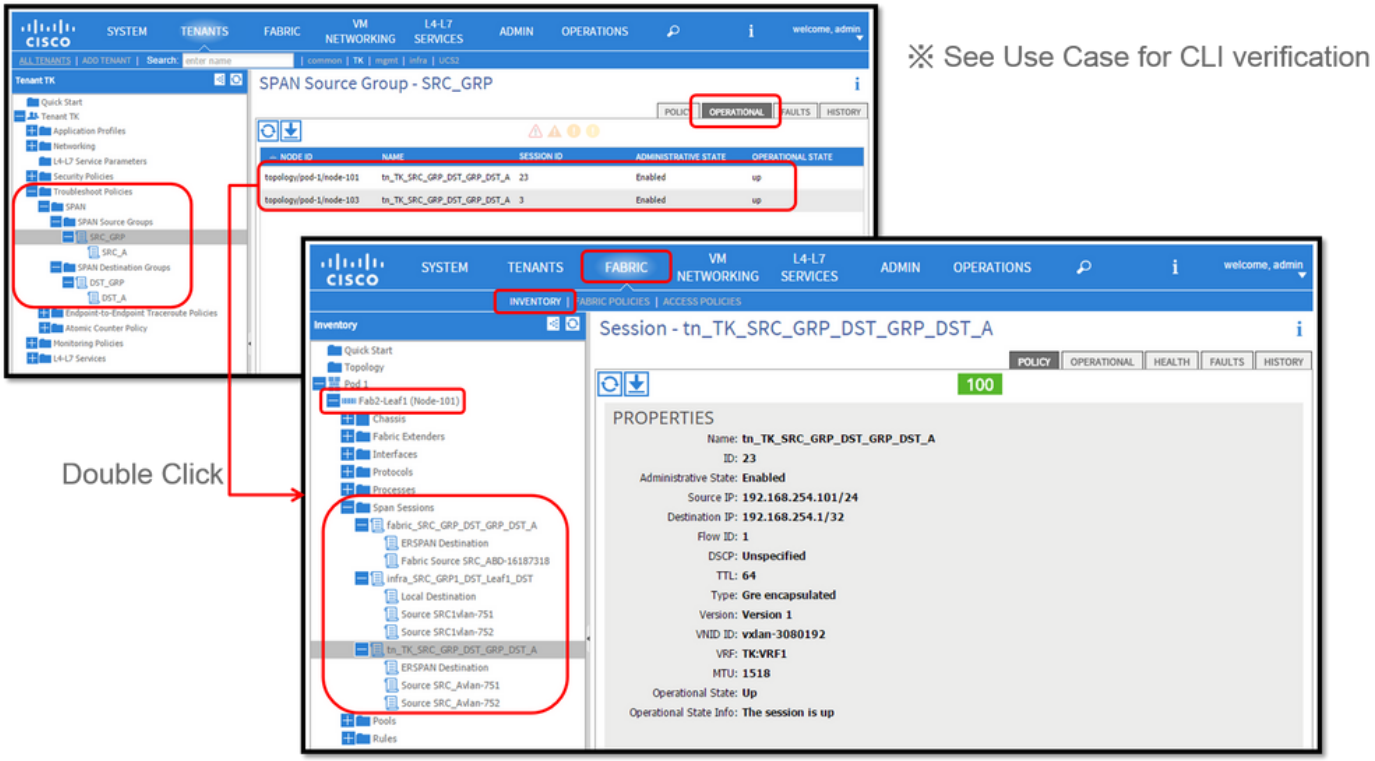
- Asegúrese SPAN Destination Group de que está vinculado a un SPAN Source Group adecuado.

- Asegúrese Admin State de que está habilitado.

※ SPAN se detiene cuando se selecciona Disabled (Desactivado) en este Admin State campo. No es necesario eliminar todas las directivas si las vuelve a utilizar más adelante.

Aunque se describe en una sección posterior "Versión ERSPAN (tipo)", puede decir que la versión ERSPAN II se utiliza para Fabric SPAN y la versión I se utiliza para Tenant y Access SPAN.

Verificación de GUI



- Verificación de la Política de Configuración de SPAN

1. Fabric > ACCESS POLICIES > Troubleshoot Policies > SPAN > SPAN Source Groups > Operational tab

   - Fabric > FABRIC POLICIES > Troubleshoot Policies > SPAN > SPAN Source Groups > Operational tab
   - Tenants > {tenant name} > Troubleshoot Policies > SPAN > SPAN Source Groups > Operational tab

Asegúrese de que el estado operativo está activado.

- Verificación en la Sesión SPAN en el propio nodo

1. Haga doble clic en cada sesión de SPAN Configuration Policyo Fabric > INVENTORY > Node > Span Sessions > { SPAN session name }

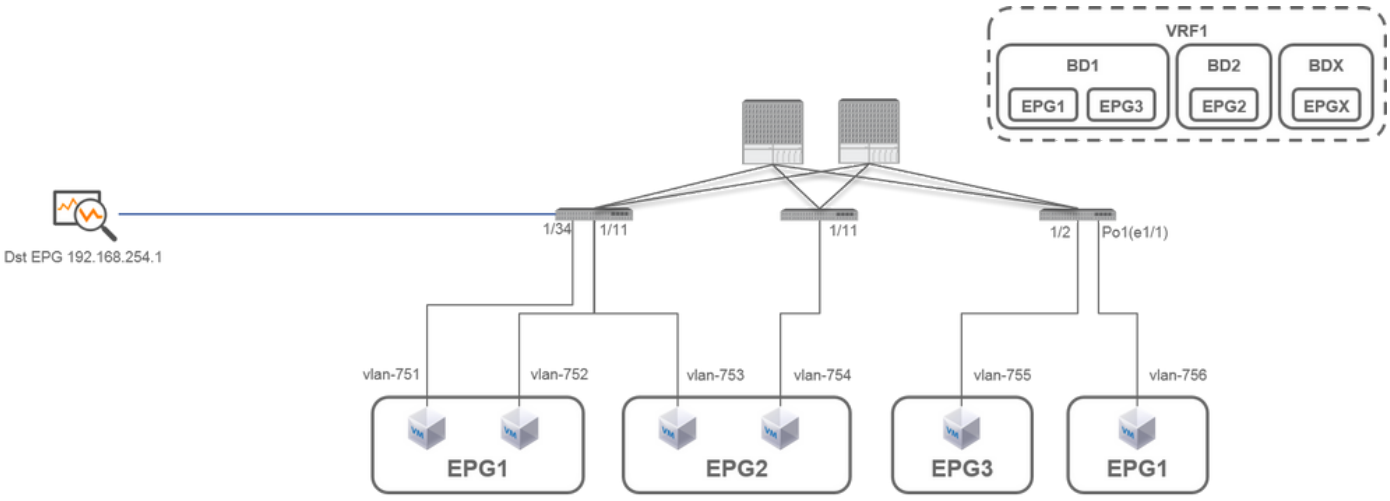
Asegúrese de que el estado operativo está activado.

Convención de denominación de sesiones SPAN:

- SPAN de fabric: fabric_xxxx

- SPAN de acceso: infra_xxxx
- SPAN de arrendatario: tn_xxxx

Seleccione el tipo de SPAN de ACI



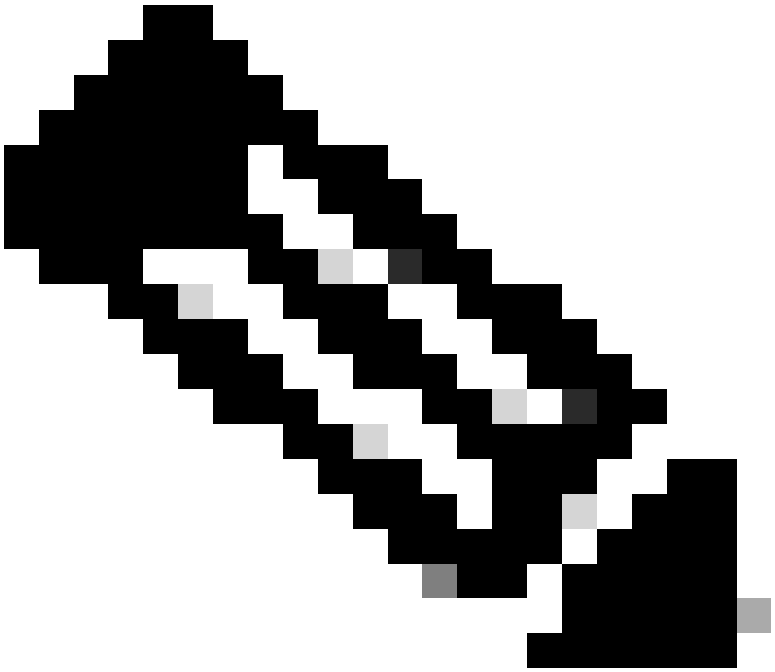
En esta sección, se describen escenarios detallados para cada tipo de SPAN de ACI (Access, Tenant, Fabric). La topología base para cada escenario se menciona en la sección anterior.

Si comprende estos escenarios, puede seleccionar el tipo de SPAN de ACI adecuado para sus necesidades, como por ejemplo, los paquetes en interfaces específicas solamente deben ser capturados o todos los paquetes en un EPG específico, independientemente de las interfaces, deben ser capturados, y más.

En Cisco ACI, SPAN se configura con el source group y destination group. El grupo Origen contiene varios factores de origen como interfaces o

EPG. El grupo de destino contiene información de destino como la interfaz de destino para SPAN local o la IP de destino para ESPAN.

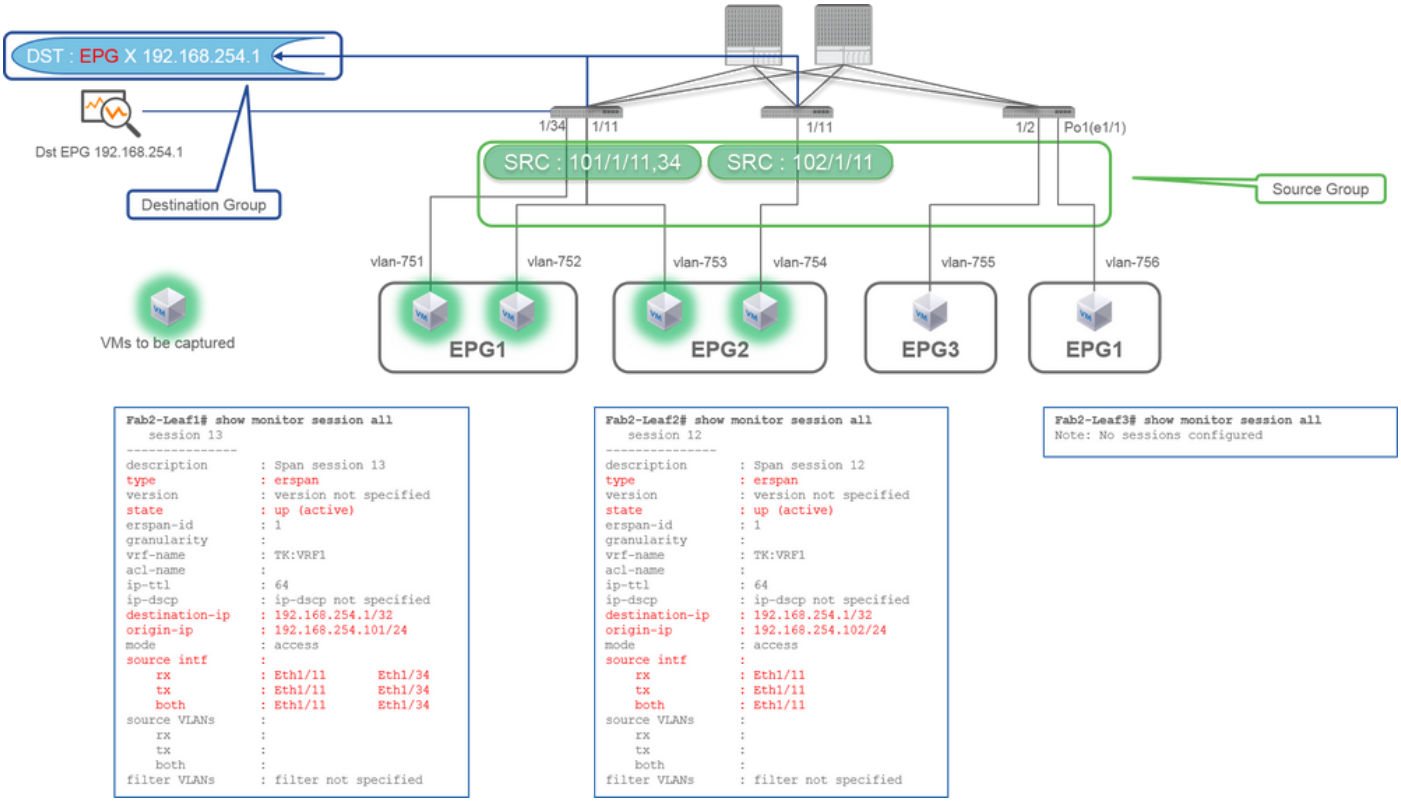
Una vez capturados los paquetes, consulte la sección "Cómo leer datos SPAN" para descodificar los paquetes capturados.



Nota: céntrese en las VM resaltadas con una luz verde en cada topología. Cada escenario consiste en capturar paquetes de estas VM resaltadas.

SPAN de acceso (ERSPAN)

Caso 1. Src "Leaf1 e1/11 e1/34 & Leaf2 e1/11" | Dst "192.168.254.1"



- Source Group
  - Hoja1 e1/11
  - Hoja1 e1/34
  - Hoja2 e1/11
- Destination Group
  - 192.168.254.1 en EPG X

Access SPAN puede especificar varias interfaces para una sola sesión SPAN. Puede capturar todos los paquetes que entran o salen de interfaces especificadas independientemente de su EPG.

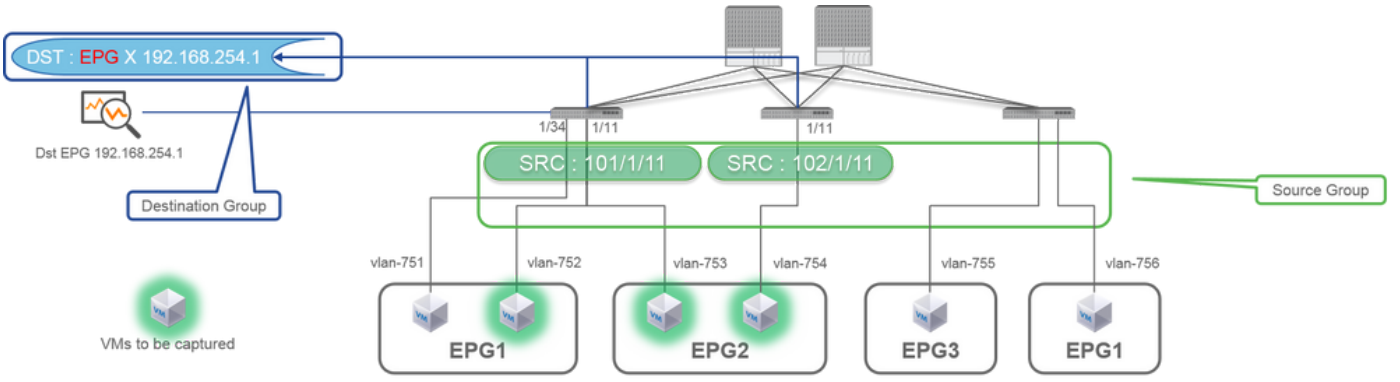
Cuando se especifican varias interfaces como un grupo de origen de varios switches de hoja, el grupo de destino debe ser ERSPAN, no SPAN local.

En este ejemplo, copia paquetes de todas las VM en EPG1 y EPG2.

Punto de control CLI

- Asegúrese de que el estado es "activo (activo)"
- "destination-ip" es la IP de destino de ERSPAN
    - "origin-ip" es IP de origen para ERSPAN

Caso 2. Src "Leaf1 e1/11 & Leaf2 e1/11" | Dst "192.168.254.1"




```
Fab2-Leaf1# show monitor session all
   session 2
---------------
description       : Span session 2
type              : erspan
version           : version not specified
state             : up (active)
erspan-id         : 1
granularity       :
vrf-name          : TK:VRF1
acl-name          :
ip-ttl            : 64
ip-dscp           : ip-dscp not specified
destination-ip    : 192.168.254.1/32
origin-ip         : 192.168.254.101/24
mode              : access
source intf       :
    rx            : Eth1/11
    tx            : Eth1/11
    both          : Eth1/11
source VLANs      :
    rx            :
    tx            :
    both          :
filter VLANs      : filter not specified
```

```
Fab2-Leaf2# show monitor session all
   session 3
---------------
description       : Span session 3
type              : erspan
version           : version not specified
state             : up (active)
erspan-id         : 1
granularity       :
vrf-name          : TK:VRF1
acl-name          :
ip-ttl            : 64
ip-dscp           : ip-dscp not specified
destination-ip    : 192.168.254.1/32
origin-ip         : 192.168.254.102/24
mode              : access
source intf       :
    rx            : Eth1/11
    tx            : Eth1/11
    both          : Eth1/11
source VLANs      :
    rx            :
    tx            :
    both          :
filter VLANs      : filter not specified
```

```
Fab2-Leaf3# show monitor session all
Note: No sessions configured
```

- **Grupo de origen**
    - Hoja1 e1/11
    - Hoja2 e1/11
- **Grupo de destino**
    - 192.168.254.1 en EPG X

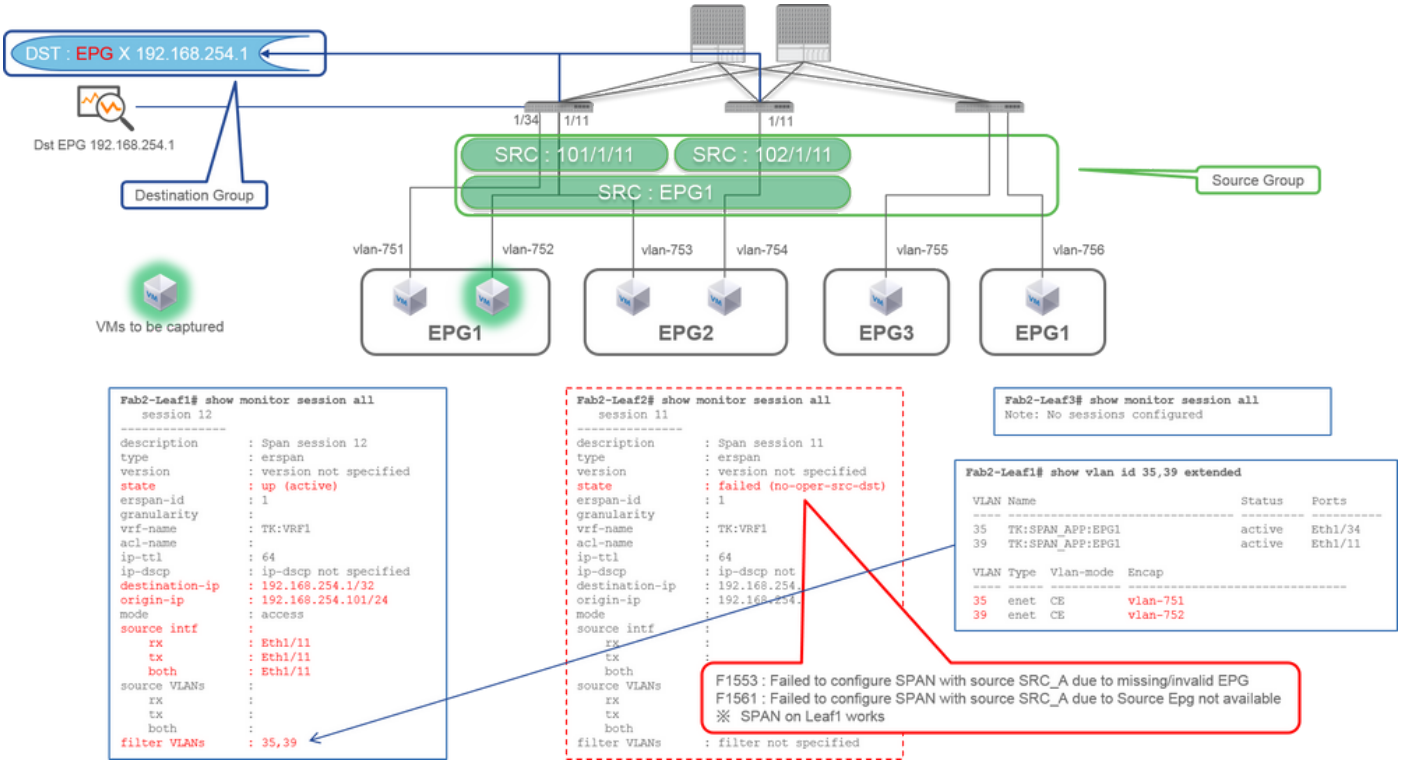
En este ejemplo, Leaf1 e1/34 se elimina del Grupo de Origen SPAN configurado en Case1 anterior.

El punto clave en este ejemplo es que Access SPAN puede especificar interfaces de origen independientemente de EPG.

Punto de control CLI

- La interfaz de origen en Leaf1 se cambia a "Eth1/11" de "Eth1/11 Eth1/34"

Caso 3. Src "Leaf1 e1/11 & Leaf2 e1/11 & EPG1 filter" | Dst "192.168.254.1"



- **Grupo de origen**
    - Hoja1 e1/11
    - Hoja2 e1/11
    - Filtrar EPG1
- **Grupo de destino**
    - 192.168.254.1 en EPG X

Este ejemplo muestra que Access SPAN también puede especificar un EPG específico en los puertos de origen. Esto es útil cuando varios EPG fluyen en una sola interfaz y se requiere capturar el tráfico solamente para EPG1 en esta interfaz.

Dado que EPG1 no se implementa en Leaf2, SPAN para Leaf2 falla con los fallos F1553 y F1561. Sin embargo, SPAN en Leaf1 aún funciona.

Además, se agregan automáticamente dos filtros VLAN para la sesión SPAN en Leaf1 porque EPG1 utiliza dos VLAN (VLAN-751,752) en Leaf1.

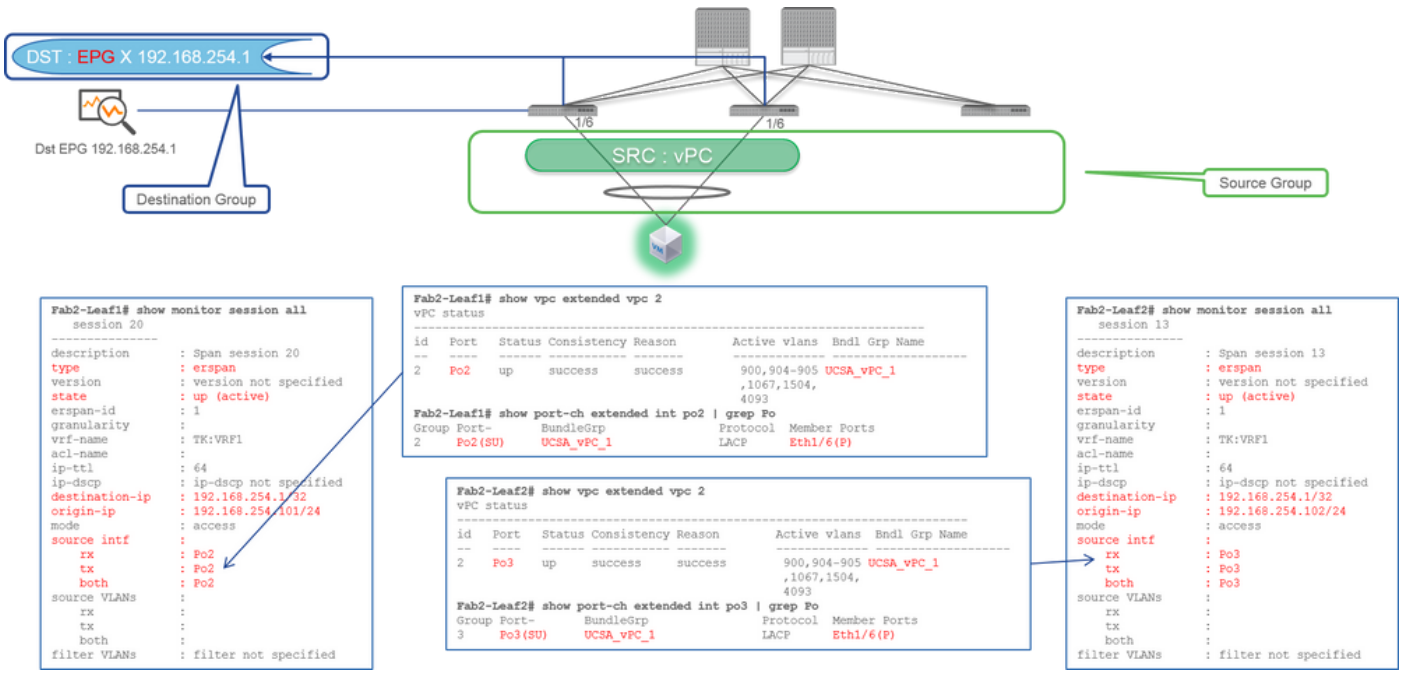
Tenga en cuenta que el ID de VLAN en CLI (35, 39) es la VLAN interna denominada PI-VLAN (VLAN independiente de la plataforma), que no es el ID real en el cable. Como se muestra en la imagen, el comando **show vlan extended** muestra la asignación del ID de VLAN de encapsulamiento real y PI-VLAN.

Esta sesión SPAN nos permite capturar paquetes solo para EPG1 (VLAN-752) en Leaf1 e1/11, incluso aunque EPG2 (VLAN-753) fluya en la misma interfaz.

Punto de control CLI

- Las VLAN de filtro se agregan según los EPG que se utilizan para el filtro.
- Si no hay EPG correspondientes en la hoja, la sesión SPAN en esa hoja falla.

Caso 4. Src "vPC de hoja 1-hoja 2" | Dst "192.168.254.1"

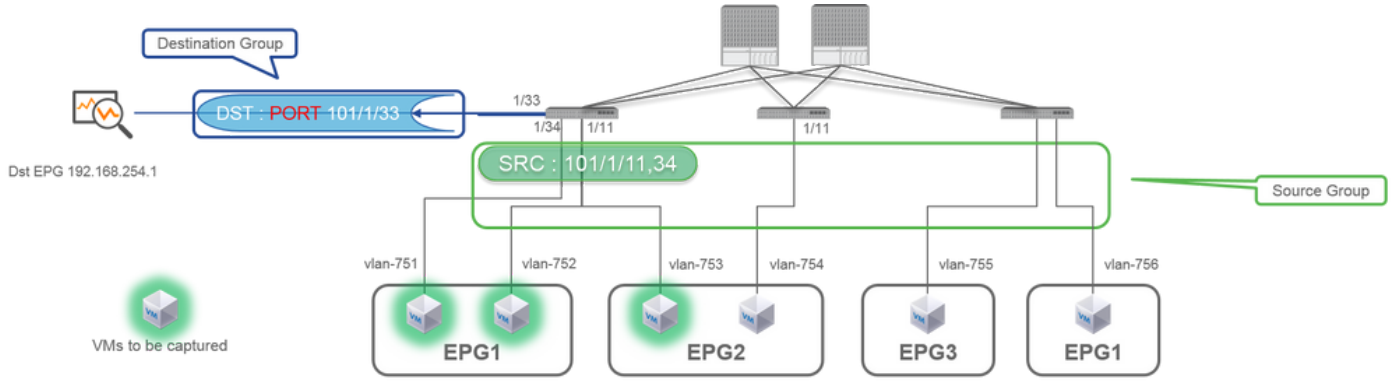


- **Grupo de origen**
    - Hoja1 - 2e1/11
- **Grupo de destino**
    - 192.168.254.1 en EPG X

Cuando la interfaz vPC se configura como origen, un destino debe ser una IP remota (ERSPAN) y no la interfaz (SPAN local)

SPAN de acceso (SPAN local)

Caso 1. Src "Leaf1 e1/11 e1/34" | Dst "Leaf1 e1/33"




```
Fab2-Leaf1# show monitor session all
    session 14
---------------
description       : Span session 14
type              : local
state             : up (active)
mode              : access
source intf       :
    rx            : Eth1/11       Eth1/34
    tx            : Eth1/11       Eth1/34
    both          : Eth1/11       Eth1/34
source VLANs      :
    rx            :
    tx            :
    both          :
filter VLANs      : filter not specified
destination ports : Eth1/33
```

```
Fab2-Leaf2# show monitor session all
Note: No sessions configured
```

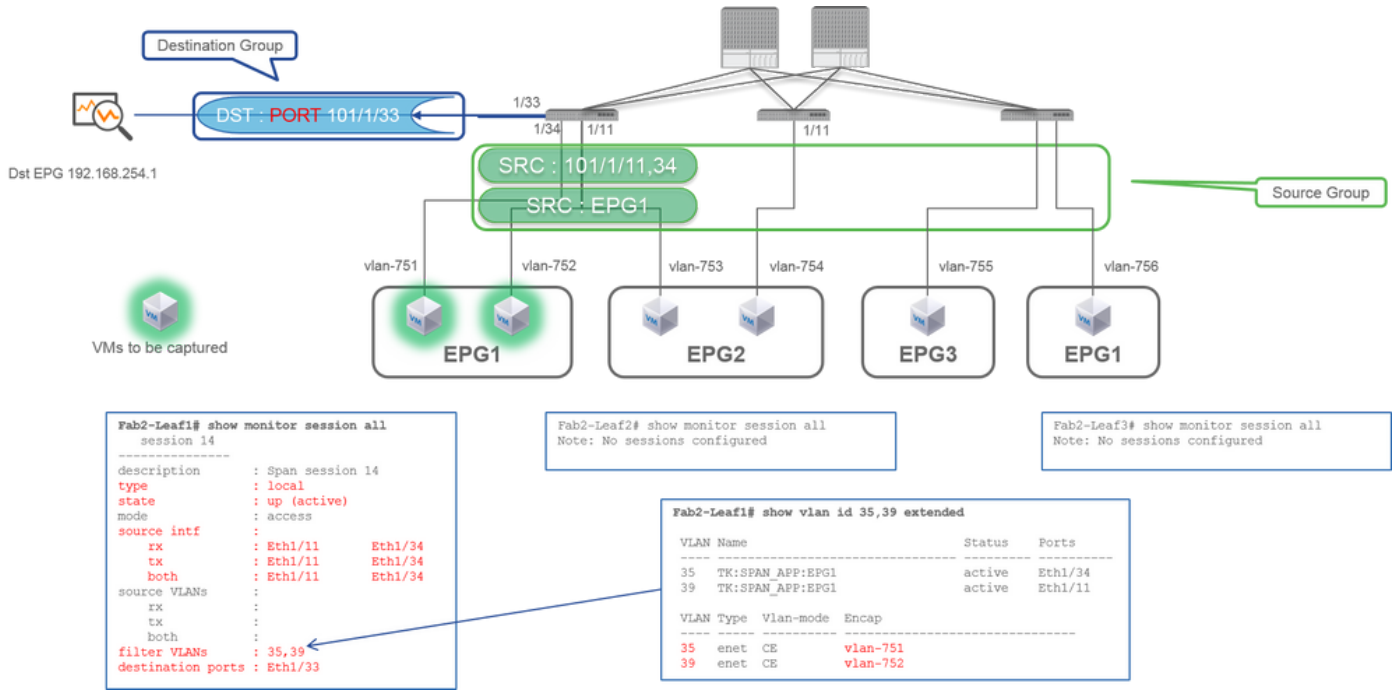
```
Fab2-Leaf3# show monitor session all
Note: No sessions configured
```

- **Grupo de origen**
    - Hoja1 e1/11
    - Hoja1 e1/34
- **Grupo de destino**
    - Hoja1 e1/33

El SPAN de acceso también puede utilizar el SPAN local (es decir, una interfaz específica como destino)

Sin embargo, en este caso, las interfaces de origen deben estar en la misma hoja que la interfaz de destino.

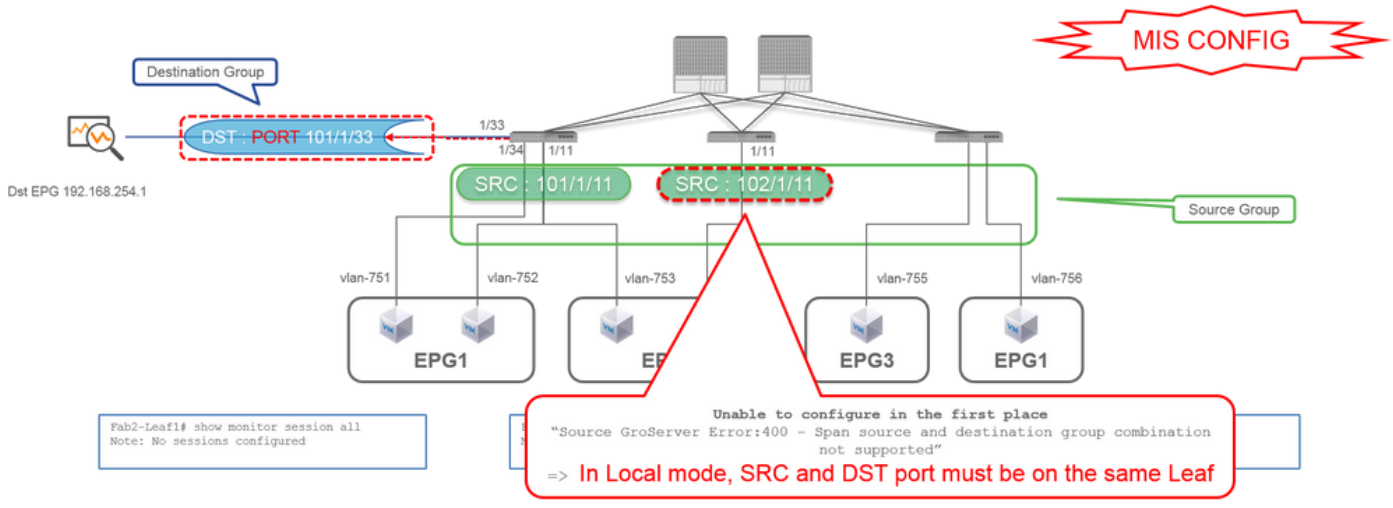
Caso 2. Src "Leaf1 e1/11 e1/34 & EPG1 filter | Dst " Leaf1 e1/33"



- **Grupo de origen**
    - Hoja1 e1/11
    - Hoja1 e1/34
    - Filtro EPG1
- **Grupo de destino**
    - Hoja1 e1/33

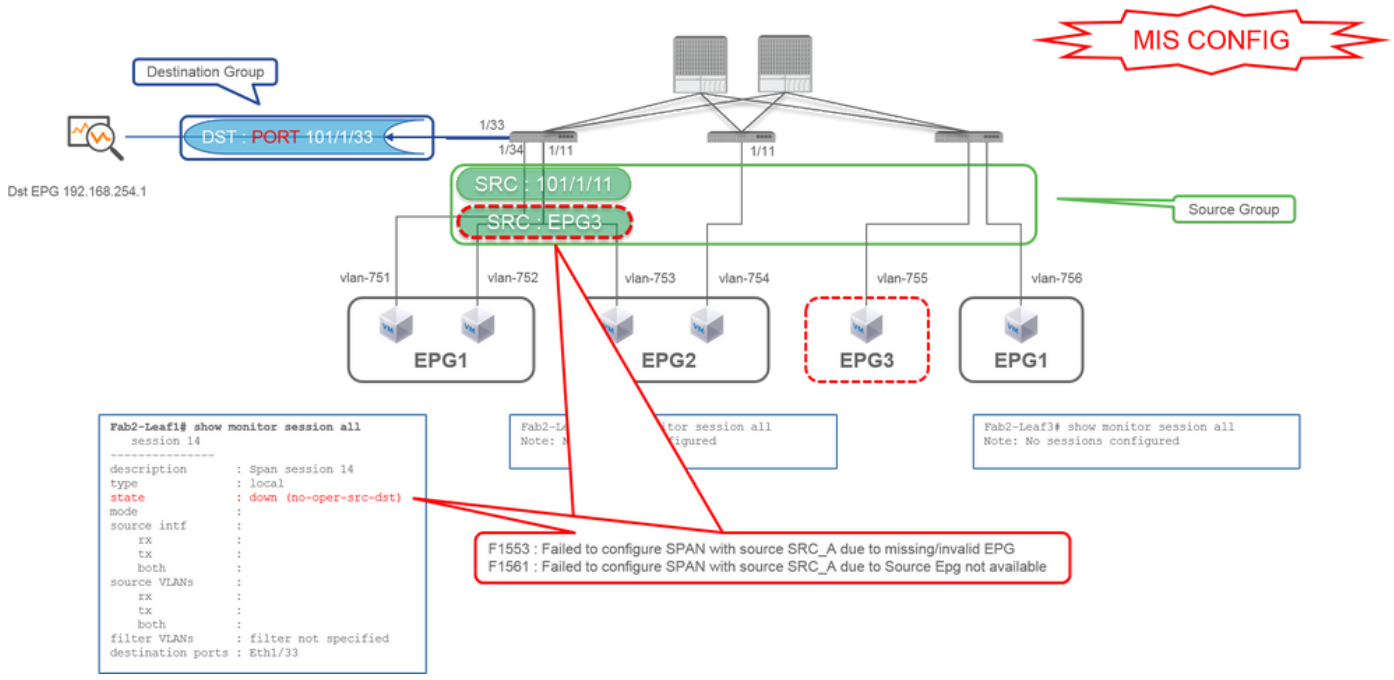
El SPAN de acceso con SPAN local también puede utilizar el filtro EPG así como ERSPAN.

Caso 3. Src "Leaf1 e1/11 & Leaf2 e/11" | Dst "Leaf1 e1/33" (bad case)



- **Grupo de origen**
    - Hoja1 e1/11
    - Hoja2 e1/11
- **Grupo de destino**
    - Hoja1 e1/33

Caso 4. Src "Leaf1 e1/11 & EPG3 filter" | Dst "Leaf1 e1/33" (bad case)



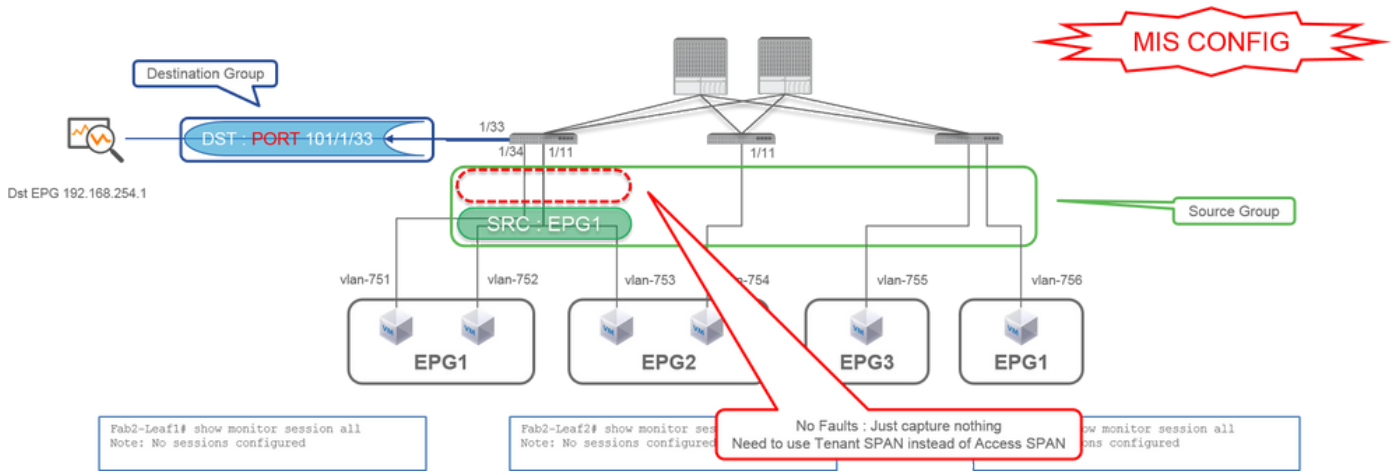
- **Grupo de origen**

- Hoja1 e1/11
- Filtro EPG3

- **Grupo de destino**
  - Hoja1 e1/33

Es similar al caso 3 en Access SPAN (ERSPAN), pero en este ejemplo, la única sesión SPAN en Leaf1 falla porque EPG3 no existe en Leaf1. Por lo tanto, SPAN no funciona en absoluto.

Caso 5: Src "EPG1 filter" | Dst "Leaf1 e1/33" (bad case)

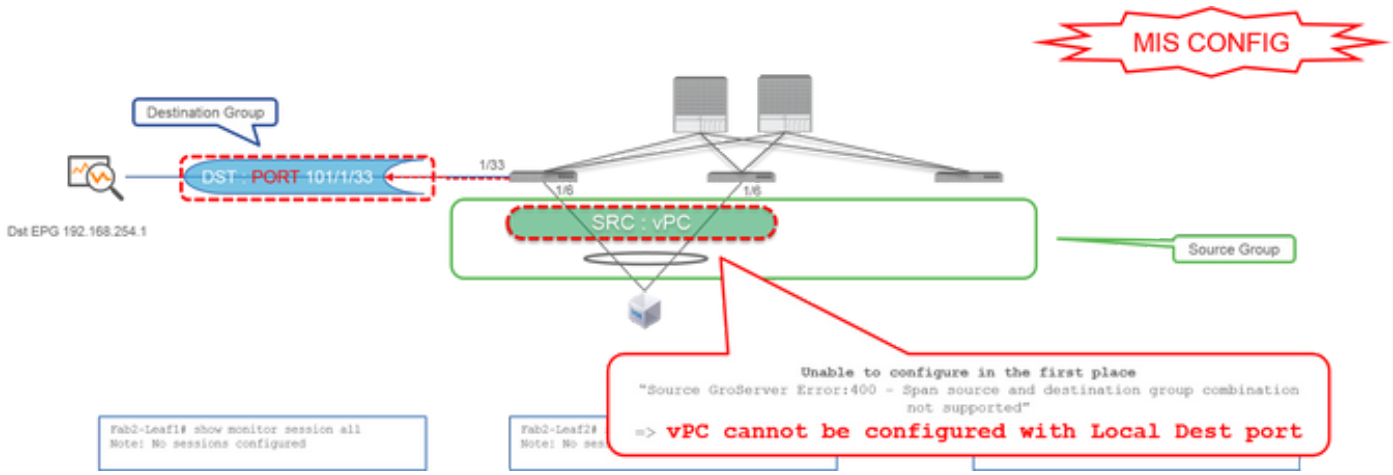


- **Grupo de origen**
  - Filtro EPG1

- **Grupo de destino**
    - Hoja1 e1/33

El filtro EPG en el SPAN de acceso funciona solamente cuando los puertos de origen están configurados. Si EPG es el único origen que se debe especificar, se debe utilizar SPAN de arrendatario en lugar de SPAN de acceso.

Caso 6. Src "Leaf1 - Leaf2 vPC" | Dst "Leaf1 e1/33" (bad case)

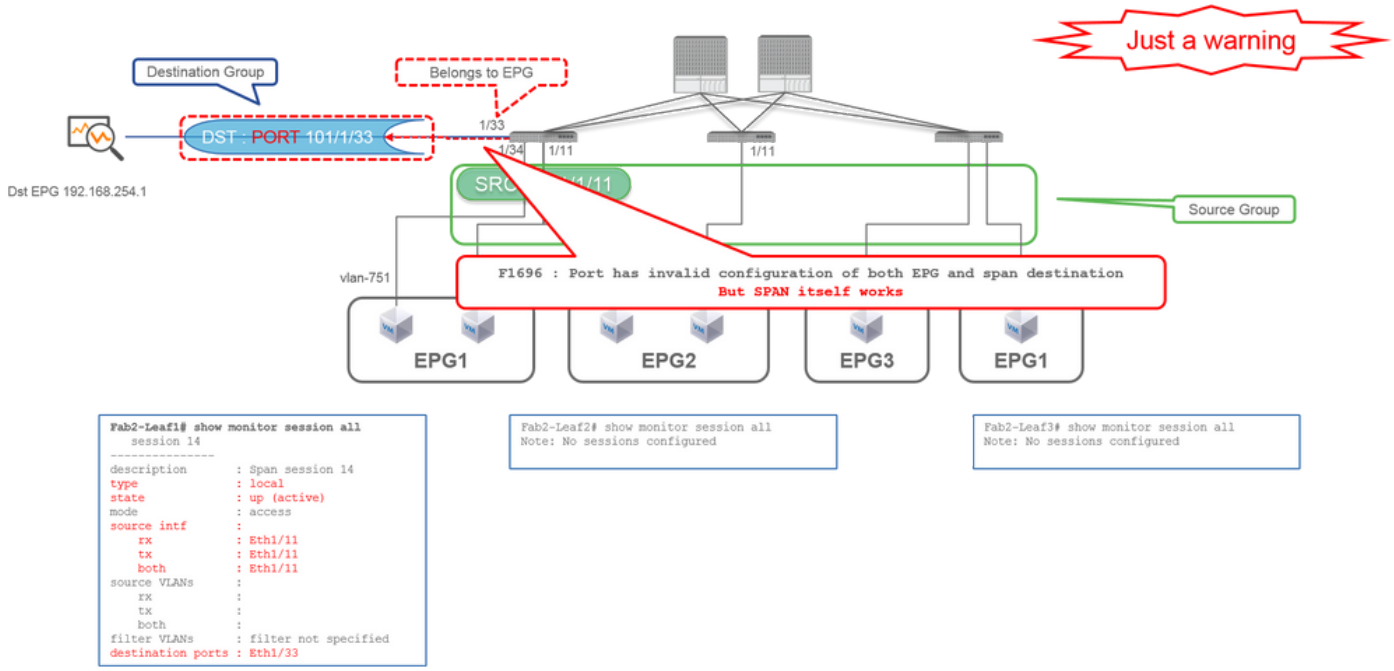


- **Grupo de origen**
    - vPC hoja1-2

- **Grupo de destino**
    - Hoja1 e1/33

Una interfaz vPC no se puede configurar como origen con SPAN local. Utilice ERSPAN. Consulte el caso 4 para obtener información sobre el SPAN de acceso (ERSPAN).

Caso 7. Src "Hoja1 e1/11 | Dst "Leaf1 e1/33 & e1/33 pertenece a EPG" (funciona con fallo)

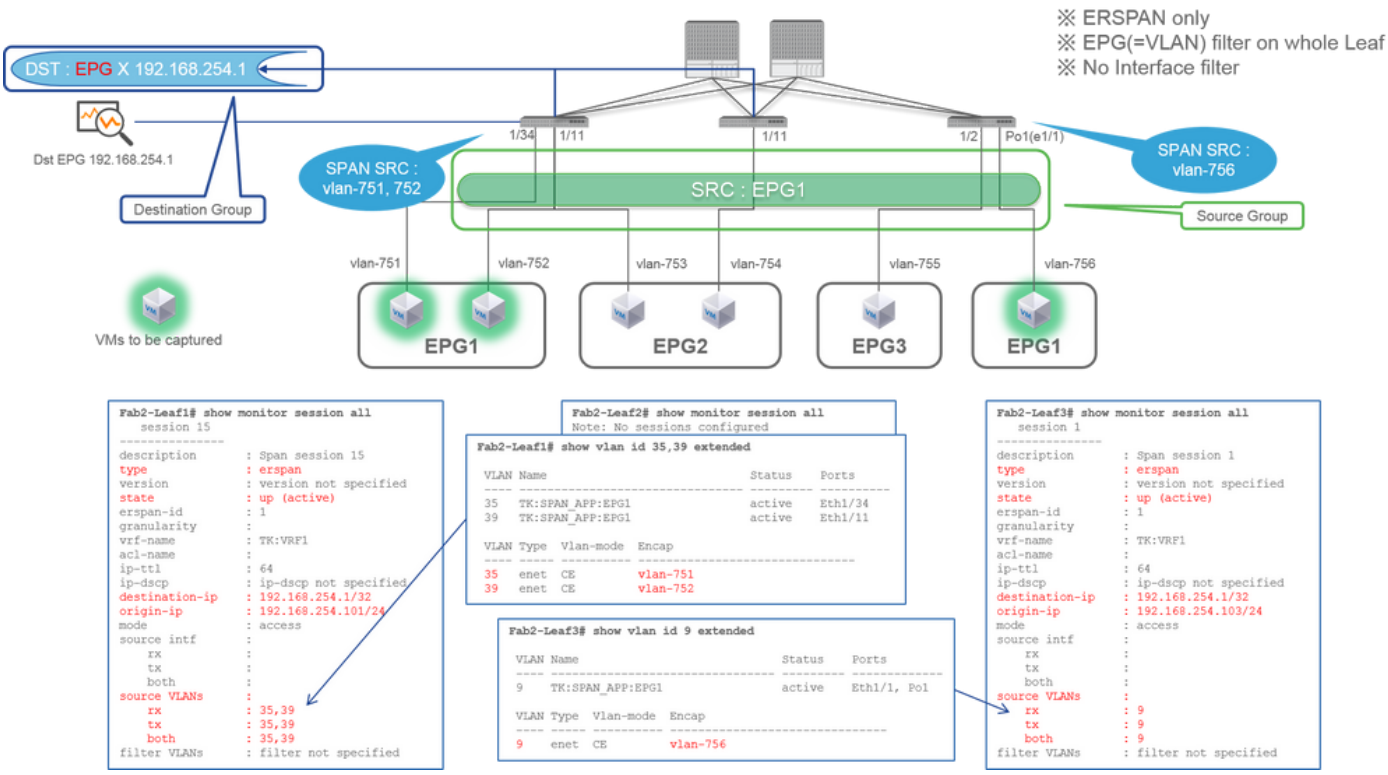


Si una I/F de destino para SPAN ya pertenece a EPG, se genera un error "F1696: el puerto tiene una configuración no válida de EPG y destino de tramo" bajo la I/F física.

Pero incluso con esta falla, SPAN funciona sin ningún problema. Este fallo es solo una advertencia sobre el tráfico adicional causado por SPAN, ya que puede afectar el tráfico EPG normal de los clientes en la misma I/F.

SPAN de arrendatario (ERSPAN)

Caso 1. Src "EPG1" | Dst "192.168.254.1"



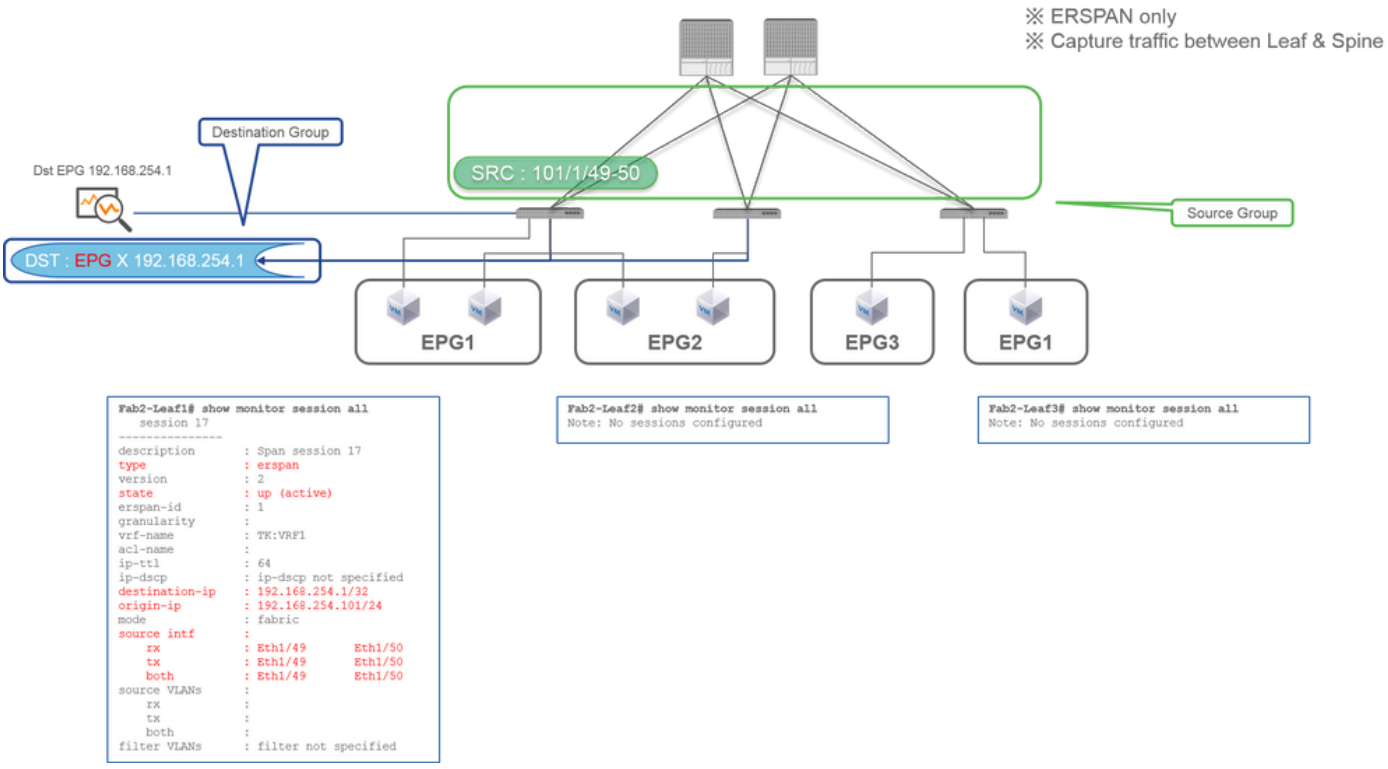
- **Grupo de origen**
  - EPG1 (sin filtro)
- **Grupo de destino**
  - 192.168.254.1 en EPG X

El SPAN del arrendatario utiliza el EPG como origen, mientras que el SPAN de acceso utiliza el EPG solo para un filtro.

El punto clave de SPAN de arrendatario es que no tiene que especificar cada puerto individual y ACI detecta automáticamente las VLAN apropiadas en cada switch de hoja. Esto sería útil cuando todos los paquetes para un EPG específico deben ser monitoreados y los puntos finales para ese EPG pertenecen a múltiples interfaces a través de los switches de hoja.

Fabric SPAN (ERSPAN)

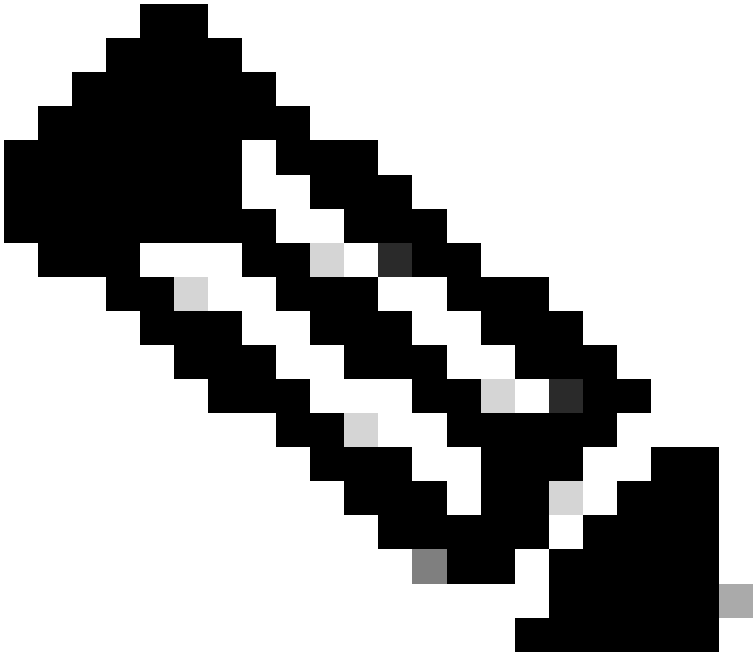
Caso 1. Src "Leaf1 e1/49-50" | Dst "192.168.254.1"



- **Grupo de origen**
  - Hoja1 e1/49-50
- **Grupo de destino**
  - 192.168.254.1 en EPG X

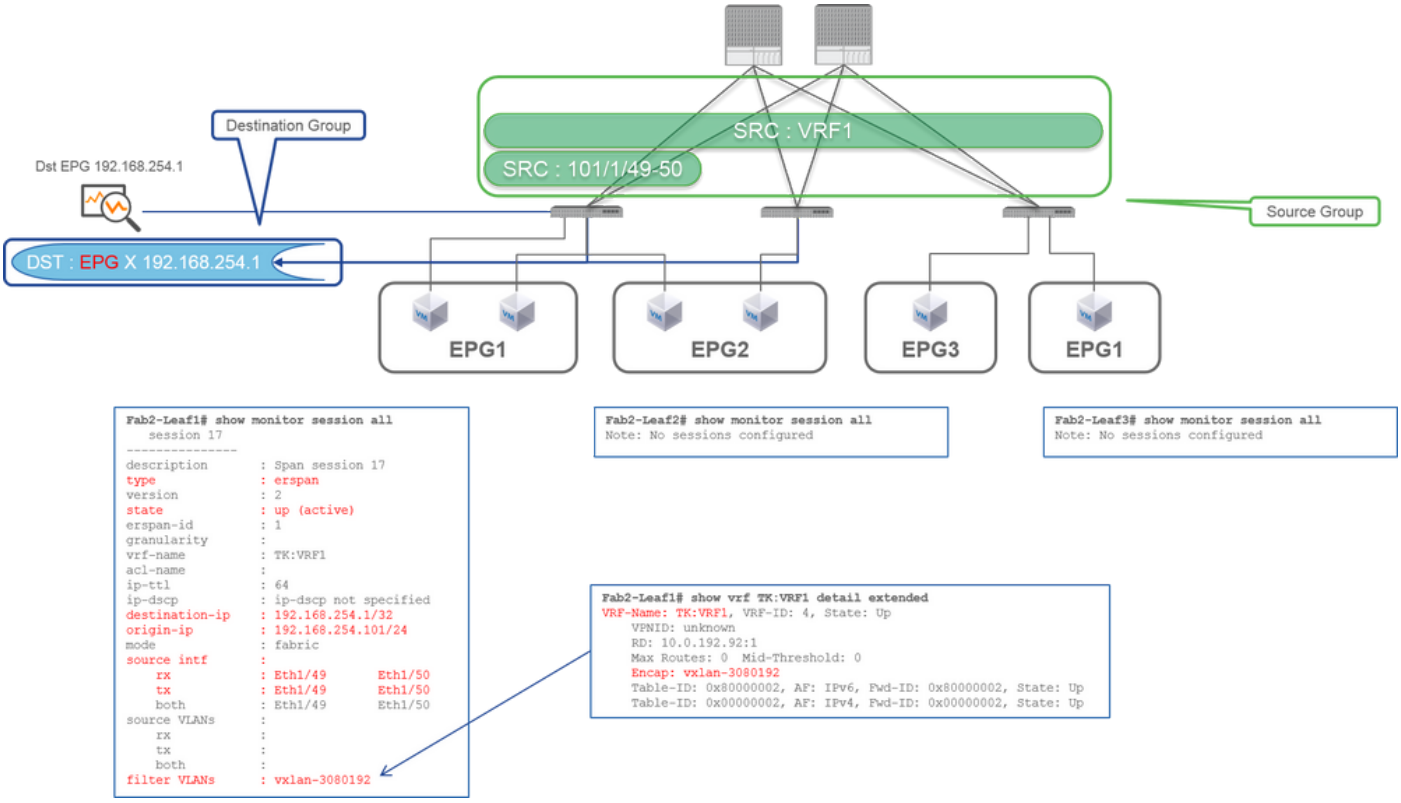
SPAN de fabric especifica los puertos de fabric como origen en los que los puertos de fabric son interfaces entre los switches de hoja y de columna.

Este SPAN es útil cuando se requiere copiar paquetes entre los switches de hoja y columna. Sin embargo, los paquetes entre los switches Leaf y Spine se encapsulan con el encabezado VxLAN. Así que se requiere un poco de un truco para leerlo. Consulte "Cómo leer los datos de SPAN".



Nota: el encabezado VxLAN es un encabezado VxLAN mejorado solo para uso interno del fabric ACI.

Caso 2. Src "Leaf1 e1/49-50 & VRF filter" | Dst "192.168.254.1"



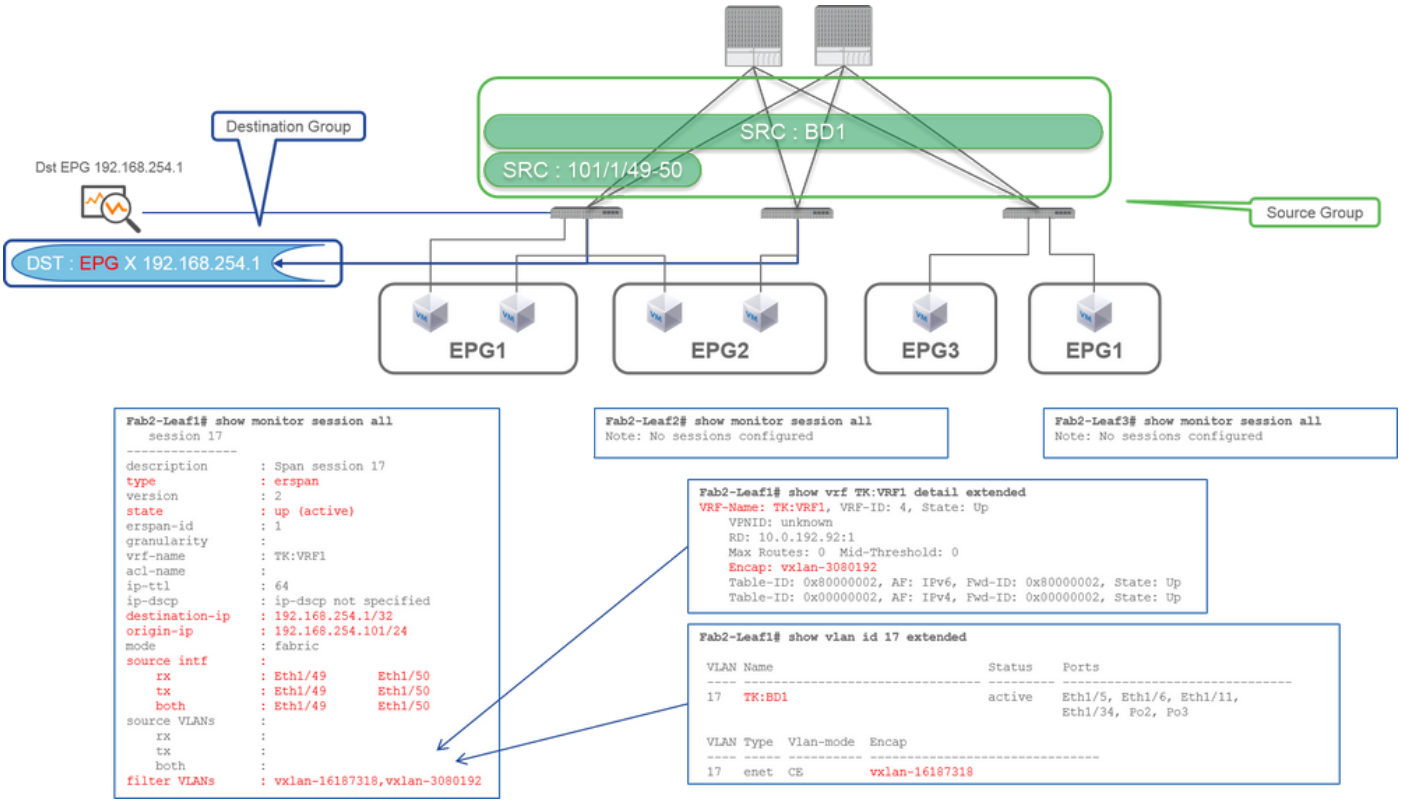
- **Grupo de origen**
  - Hoja1 e1/49-50
  - Filtro VRF
- **Grupo de destino**
  - 192.168.254.1 en EPG X

El Fabric SPAN puede utilizar filtros, así como el Access SPAN. Pero el tipo de filtro es diferente. Fabric SPAN utiliza Virtual Routing and Forwarding (VRF) o BD como filtro.

En Cisco ACI, como se ha descrito anteriormente, los paquetes que pasan a través de los puertos de fabric se encapsulan con el encabezado iVxLAN. Este encabezado iVxLAN tiene información VRF o BD como identificador de red virtual (VNID). Cuando los paquetes se reenvían como capa 2 (L2), VNID de iVxLAN significa BD. Cuando los paquetes se reenvían como capa 3 (L3), VNID de iVxLAN significa VRF.

Por lo tanto, cuando sea necesario capturar el tráfico ruteado en los puertos de fabric, utilice VRF como filtro.

Caso 3. Src "Leaf1 e1/49-50 & BD filter" | Dst "192.168.254.1"

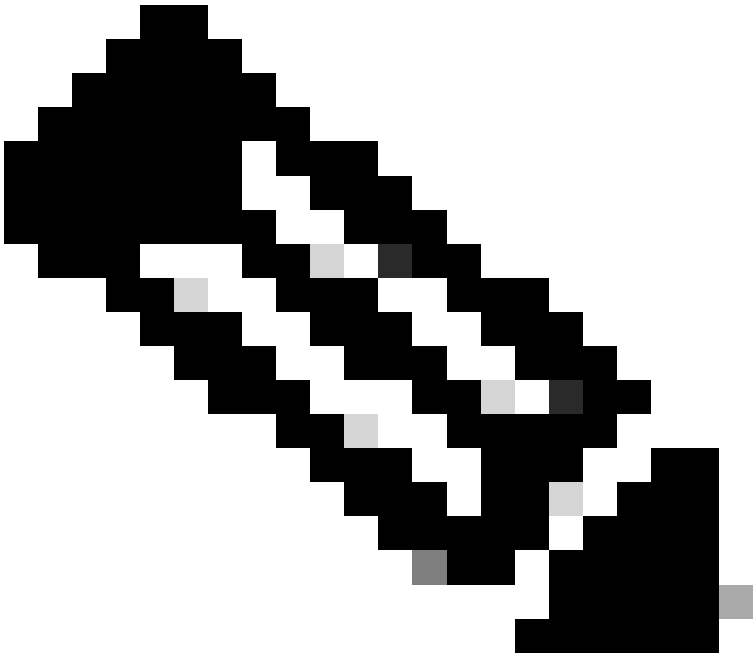


- **Grupo de origen**
  - Hoja1 e1/49-50
  - Filtro BD
- **Grupo de destino**

- 192.168.254.1 en EPG X

Como se describe en el caso anterior 2, Fabric SPAN puede utilizar BD como filtro.

Cuando sea necesario capturar el tráfico puenteado en los puertos de fabric, utilice BD como filtro.



Nota: Solo se puede configurar un solo filtro de BD o VRF a la vez.

¿Qué necesita en el dispositivo de destino SPAN?

Simplemente ejecute una aplicación de captura de paquetes como tcpdump, wireshark en ella. No es necesario configurar la sesión de destino de ERSPAN ni nada parecido.

Para ERSPAN

Asegúrese de ejecutar una herramienta de captura en la interfaz con la IP de destino para ERSPAN, ya que los paquetes SPAN se reenvían a la IP de destino.

El paquete recibido se encapsula con un encabezado GRE. Consulte esta sección "Cómo leer datos ERSPAN" para obtener información sobre cómo descodificar el encabezado ERSPAN GRE.

Para SPAN local

Asegúrese de ejecutar una herramienta de captura en la interfaz que se conecta a la interfaz de destino SPAN en la hoja ACI.

Los paquetes sin procesar se reciben en esta interfaz. No es necesario tratar con el encabezado ERSPAN.

Cómo leer datos ERSPAN

Versión de ERSPAN (tipo)

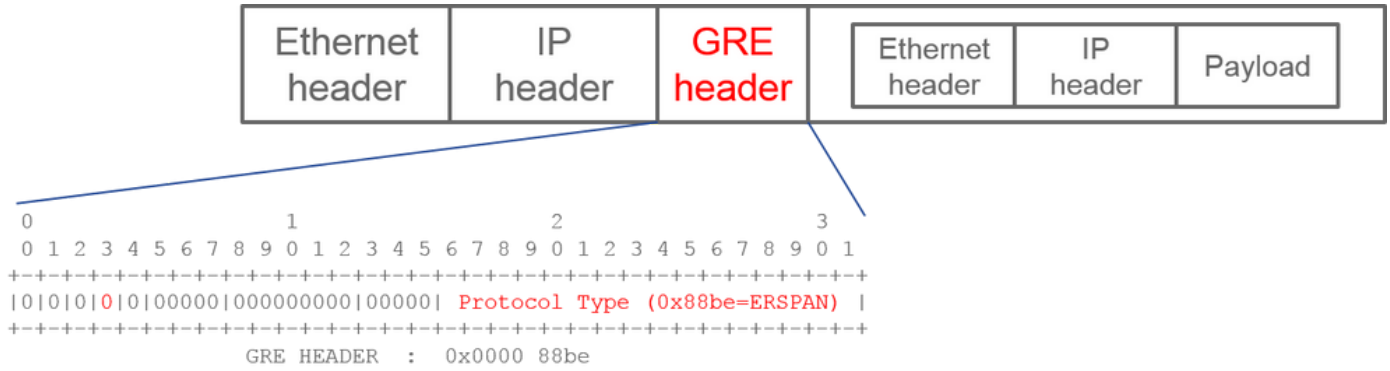
ERSPAN encapsula los paquetes copiados para reenviarlos al destino remoto. GRE se utiliza para esta encapsulación. El tipo de protocolo para ERSPAN en el encabezado GRE es 0x88be.

En el documento del Grupo de trabajo de ingeniería de Internet (IETF), la versión de ERSPAN se describe como tipo en lugar de versión.

Hay tres tipos de ERSPAN. I, II y III. El tipo ERSPAN se menciona en este borrador RFC. Además, este GRE RFC1701 puede ser útil para comprender también cada tipo de ERSPAN.

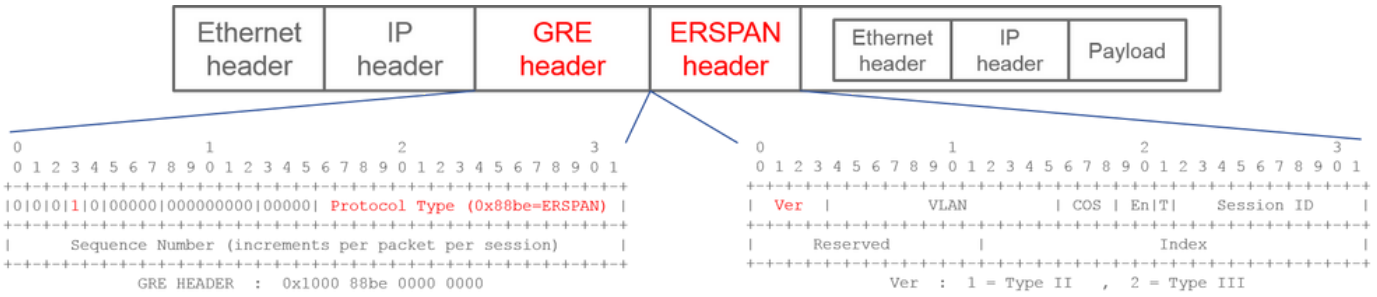
Este es el formato de paquete de cada tipo:

ERSPAN tipo I (utilizado por Broadcom Trident 2)



El tipo I no utiliza el campo de secuencia del encabezado GRE. Ni siquiera utiliza el encabezado ERSPAN que debe seguir al encabezado GRE si era ERSPAN tipo II y III. Broadcom Trident 2 solo es compatible con este ERSPAN tipo I.

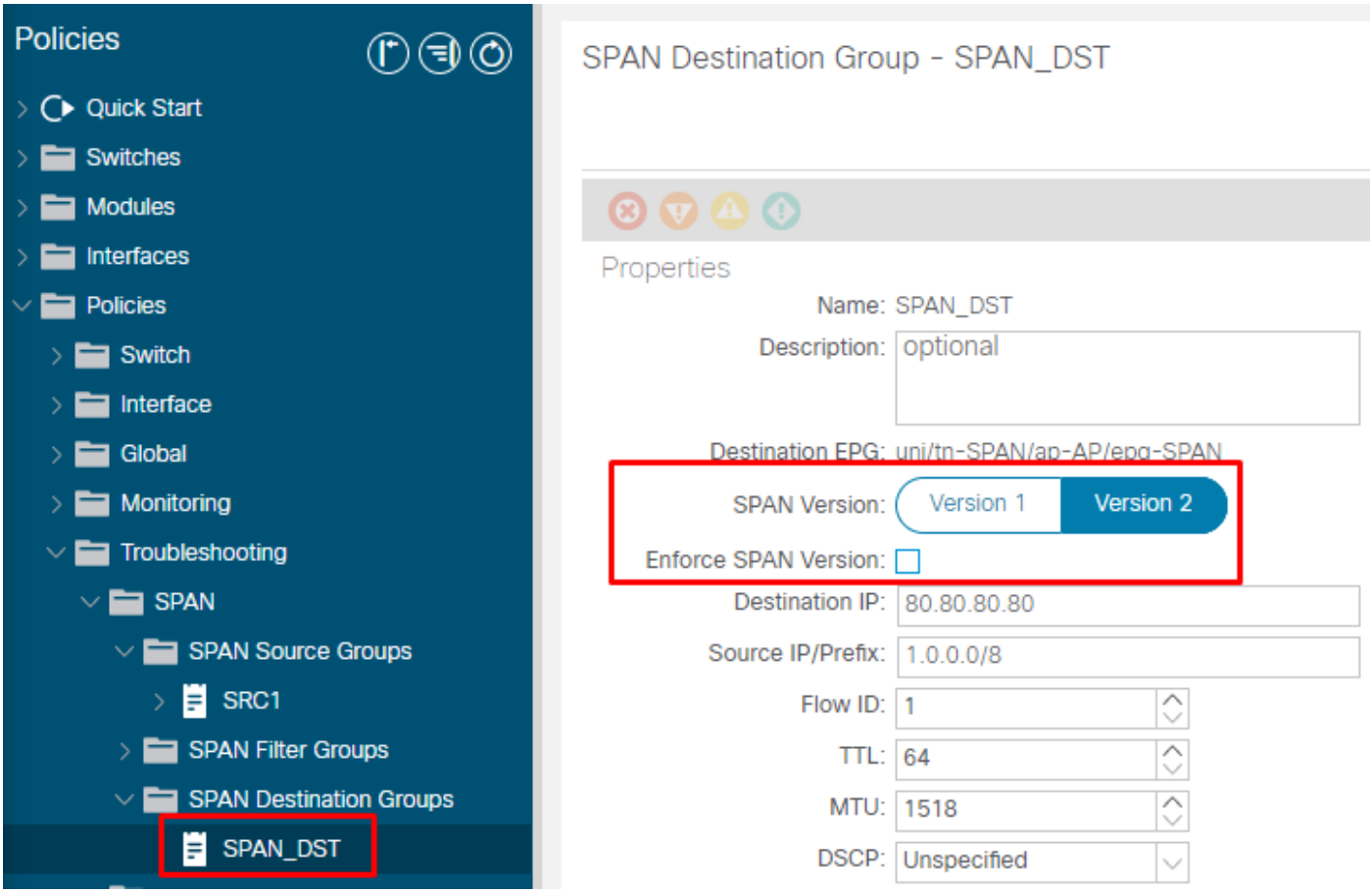
ERSPAN tipo II o III



Si el campo de secuencia es activado por el bit S, éste debe ser ERSPAN tipo II o III. El campo de versión del encabezado ERSPAN identifica el tipo de ERSPAN. En ACI, el tipo III no es compatible a partir del 20/03/16.

Si un grupo de origen de SPAN para Access o SPAN de arrendatario tiene orígenes en los nodos de 1ª y 2ª generación, el destino de ERSPAN recibe los paquetes ERSPAN de tipo I y II de cada generación de nodos. Sin embargo, Wireshark puede decodificar sólo uno de los tipos ERSPAN a la vez. Por defecto, sólo decodifica ERSPAN tipo II. Si activa la descodificación de ERSPAN tipo I, Wireshark no descodifica ERSPAN tipo II. Consulte la sección posterior sobre cómo descodificar ERSPAN tipo I en Wireshark.

Para evitar este tipo de problema, puede configurar el tipo de ERSPAN en un grupo de destino de SPAN.



- Versión de SPAN (Versión 1 o Versión 2): se refiere al ERSPAN de tipo I o II

- Aplicar versión de SPAN (activada o desactivada): se decide si la sesión de SPAN debe fallar en caso de que el tipo de ERSPAN configurado no sea compatible con el hardware del nodo de origen.

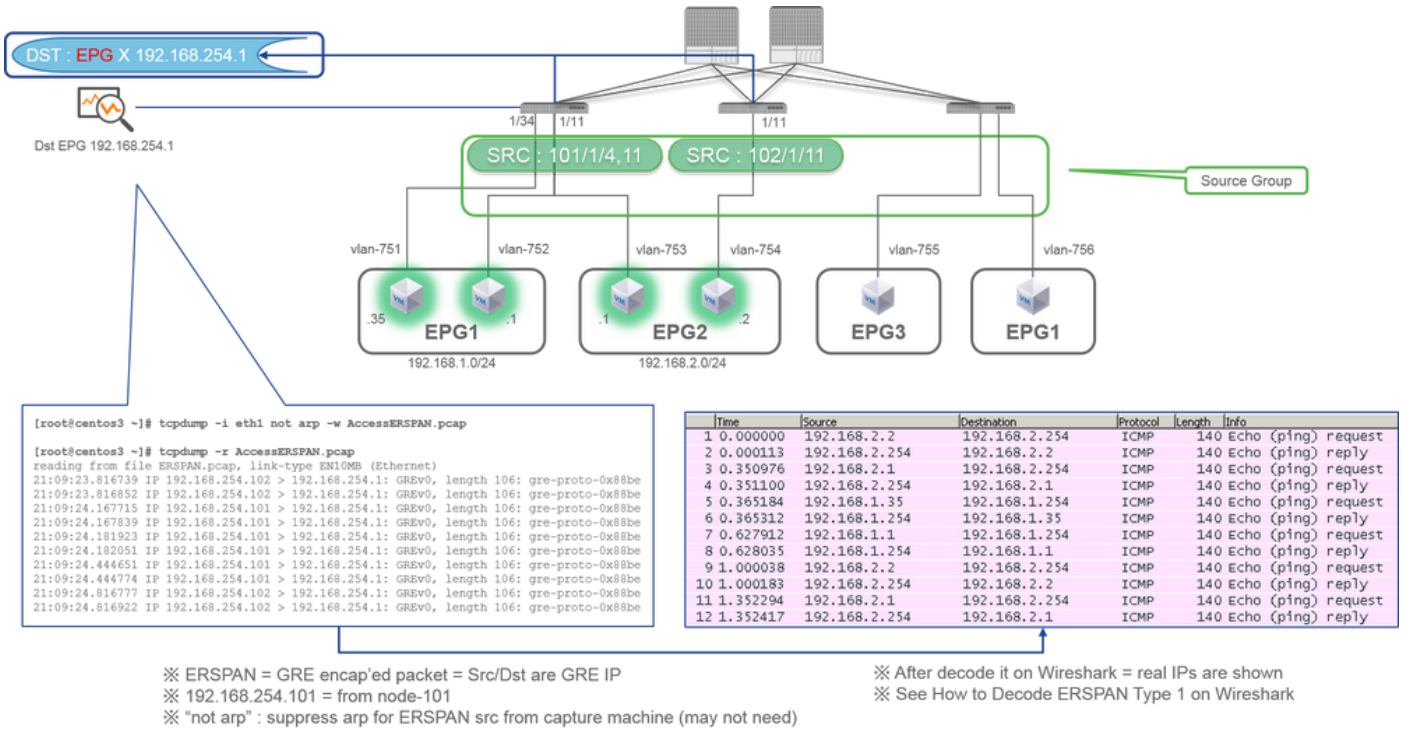
De forma predeterminada, SPAN Version es Version 2 y Enforce SPAN Version no está marcado. Esto significa que si el nodo de origen es de 2ª generación o posterior que soporta ERSPAN Tipo II, genera ERSPAN con Tipo II. Si el nodo de origen es de 1ª generación que no admite ERSPAN de tipo II (excepto para Fabric SPAN), vuelve al tipo I, ya que la opción Aplicar versión de SPAN no está activada. Como resultado, el destino de ERSPAN recibe un tipo mixto de ERSPAN.

En esta tabla se explica cada combinación para Access y SPAN de arrendatario.

Versión de SPAN	**Aplicar versión de SPAN**	**nodo de origen de 1ª generación**	**Nodo de origen de 2ª generación**
Versión 2	Desactivado	Utiliza el tipo I	Utiliza el tipo II
Versión 2	Activado	Fallos	Utiliza el tipo II
Versión 1	Desactivado	Utiliza el tipo I	Utiliza el tipo I
Versión 1	Activado	Utiliza el tipo I	Utiliza el tipo I

Ejemplo de Datos ERSPAN

SPAN de arrendatario/SPAN de acceso (ERSPAN)



Los paquetes deben ser decodificados ya que ERSPAN tipo I los encapsula. Esto se puede hacer con Wireshark. Consulte la sección "Cómo descodificar ERSPAN tipo 1".

Detalles del paquete capturado (ERSPAN tipo I)

```
[root@centos3 ~]# tcpdump -xxr AccessERSPAN.pcap -c 1
reading from file AccessERSPAN.pcap, link-type EN10MB (Ethernet)
21:09:23.816739 IP 192.168.254.102 > 192.168.254.1: GREv0, length 106: gre-proto-0x88be
        0x0000:  0050 56bb 3096 0022 bdf8 19ff 0800 4500
        0x0010:  007e 0000 0000 3d2f ff97 c0a8 fe66 c0a8                ESPAN Ethernet header         : Dst 0050.56bb.3096 , Src 0022.bdf8.19.ff
        0x0020:  fe01 0000 88be 0022 bdf8 19ff 0050 56bb                ERSPAN IP header              : Dst 192.168.254.1  , Src 192.168.254.102
        0x0030:  d6c2 8100 02f2 0800 4500 0054 0000 4000                GRE header (= ERSPAN Type I)  : 0x88be = ERSPAN (S bit off 0x0000)
        0x0040:  4001 b458 c0a8 0202 c0a8 02fe 0800 34cc                Ethernet header               : Dst 0022.bdf8.19ff , Src 0050.56bb.d6c2
        0x0050:  c847 0115 7404 2b56 0000 0000 8da9 0e00                Dot1Q header                  : VLAN 754
        0x0060:  0000 0000 1011 1213 1415 1617 1819 1a1b                IP header                     : Dst 192.168.2.254  , Src 192.168.2.2
        0x0070:  1c1d 1e1f 2021 2223 2425 2627 2829 2a2b
        0x0080:  2c2d 2e2f 3031 3233 3435 3637
```

Fabric SPAN (ERSPAN)

```
[root@centos3 ~]# tcpdump -r FabricERSPAN.pcap
reading from file FabricERSPAN.pcap, link-type EN10MB (Ethernet)
23:25:00.777331 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 54227, length 127: gre-proto-0x88be
23:25:00.777445 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 53328, length 82: gre-proto-0x88be
23:25:00.777567 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 54228, length 187: gre-proto-0x88be
23:25:00.777580 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 53329, length 82: gre-proto-0x88be
23:25:00.778068 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 53330, length 127: gre-proto-0x88be
23:25:00.817915 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 54229, length 82: gre-proto-0x88be
23:25:00.829676 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 54230, length 82: gre-proto-0x88be
23:25:00.829691 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 53331, length 82: gre-proto-0x88be
23:25:00.873953 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 54231, length 82: gre-proto-0x88be
23:25:00.873968 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 53332, length 82: gre-proto-0x88be
```

ERSPAN Type 2 is automatically decoded by Wireshark
※ be noted that this is still iVxLAN header

Filter: ip.addr==10.0.192.92 Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
26	0.184754	10.0.192.92	10.0.32.66	UDP	198	Source port: 7248 Destination port: 48879
27	0.184893	10.0.192.95	10.0.192.92	UDP	198	Source port: 25168 Destination port: 48879
32	0.262735	10.0.192.92	10.0.32.65	UDP	160	Source port: 62672 Destination port: 48879
34	0.262855	10.0.192.92	239.255.255.255	UDP	156	Source port: 38745 Destination port: 48879
35	0.262868	10.0.192.92	239.255.255.255	UDP	156	Source port: 38745 Destination port: 48879
38	0.263458	10.0.192.92	225.0.213.250	UDP	160	Source port: 43738 Destination port: 48879
148	0.768367	10.0.0.1	10.0.192.92	TCP	116	56210-12151 [ACK] Seq=1 Ack=1 Win=770 Len=0
149	0.768486	10.0.192.92	10.0.0.1	TCP	116	[TCP ACKed unseen segment] 12151-56210 [ACK]
152	0.856142	10.0.192.92	225.0.213.248	UDP	164	Source port: 45334 Destination port: 48879
175	0.875130	10.0.192.92	10.0.0.1	TCP	116	[TCP Keep-Alive] [TCP ACKed unseen segment]
176	0.875252	10.0.0.1	10.0.192.92	TCP	116	[TCP Previous segment not captured] 56210-12
234	1.185477	10.0.192.92	10.0.32.66	UDP	198	Source port: 7248 Destination port: 48879
235	1.185606	10.0.192.95	10.0.192.92	UDP	198	Source port: 25168 Destination port: 48879
253	1.259119	10.0.192.92	10.0.0.1	TCP	116	57294-12375 [ACK] Seq=1 Ack=1 Win=270 Len=0

Wireshark descodifica automáticamente ERSPAN tipo II. Sin embargo, todavía está encapsulado por el encabezado iVxLAN.

De forma predeterminada, Wireshark no entiende el encabezado iVxLAN porque es el encabezado interno de ACI. Consulte "Cómo descodificar el encabezado de VxLAN".

Detalles del paquete capturado (ERSPAN tipo II)

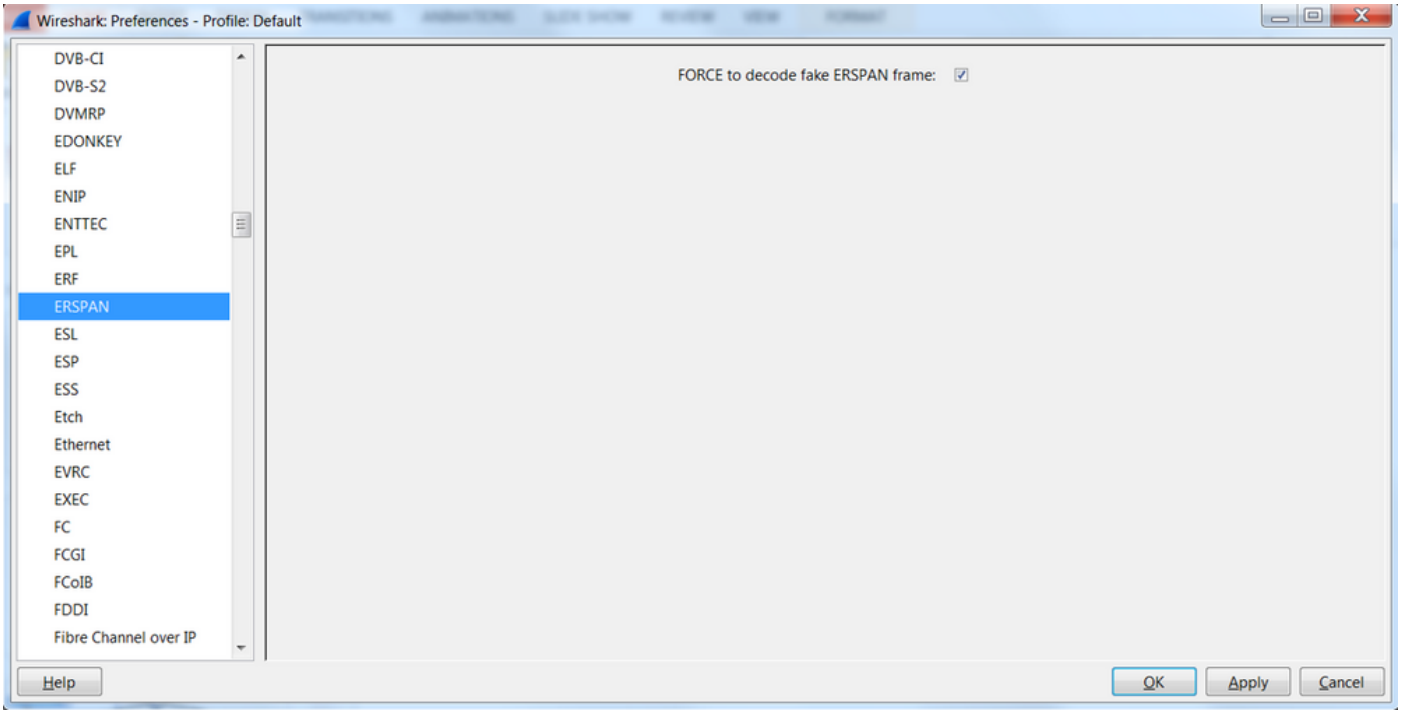
```
[root@centos3 ~]# tcpdump -xxr FabricERSPAN.pcap -c 1
reading from file FabricERSPAN.pcap, link-type EN10MB (Ethernet)
23:25:00.962224 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 53341, length 164: gre-proto-0x88be
        0x0000:  0050 56bb 3096 0022 bdf8 19ff 0800 4500
        0x0010:  00b8 0580 0000 3e2f f8de c0a8 fe65 c0a8
        0x0020:  fe01 1000 88be 0000 d05d 1002 1001 0001
        0x0030:  abcb 000c 0c0c 0c0c 0000 0000 0000 0800
        0x0040:  4500 0086 55aa 0000 1f11 b101 0a00 c05f
        0x0050:  0a00 c05c 6250 beef 0072 0000 c8a0 c007
        0x0060:  fd7f 8200 0050 56bb d95f 0050 56bb d6c2
        0x0070:  0800 4500 0054 799b 0000 4001 7bba c0a8
        0x0080:  0202 c0a8 0201 0000 4f21 b749 0027 3d24
        0x0090:  2b56 0000 0000 c720 0b00 0000 0000 1011
        0x00a0:  1213 1415 1617 1819 1a1b 1c1d 1e1f 2021
        0x00b0:  2223 2425 2627 2829 2a2b 2c2d 2e2f 3031
        0x00c0:  3233 3435 3637

ESPAN Ethernet header         : Dst 0050.56bb.3096 , Src 0022.bdf8.19.ff
ERSPAN IP header              : Dst 192.168.254.1  , Src 192.168.254.101
GRE header (= ERSPAN Type II) : 0x88be = ERSPAN (S bit on 0x1000)
ERSPAN Type II header         : VLAN 2, ERSPAN ID 1
Ethernet header               : Dst 0022.bdf8.19ff , Src 0050.56bb.d6c2
IP header                     : Dst 10.0.192.95    , Src 10.0.192.92
UDP header                    : Dst 0xbeef(48879)  , Src 0x6250(25168)
iVXLAN header                 : sclass 0xc007 , VNID 0xfd7f82
Ethernet header               : Dst 0050.56bb.d95f , Src 0050.56bb.d6c2
IP header                     : Dst 192.168.2.254  , Src 192.168.2.2
```

Cómo Decodificar ERSPAN Tipo I

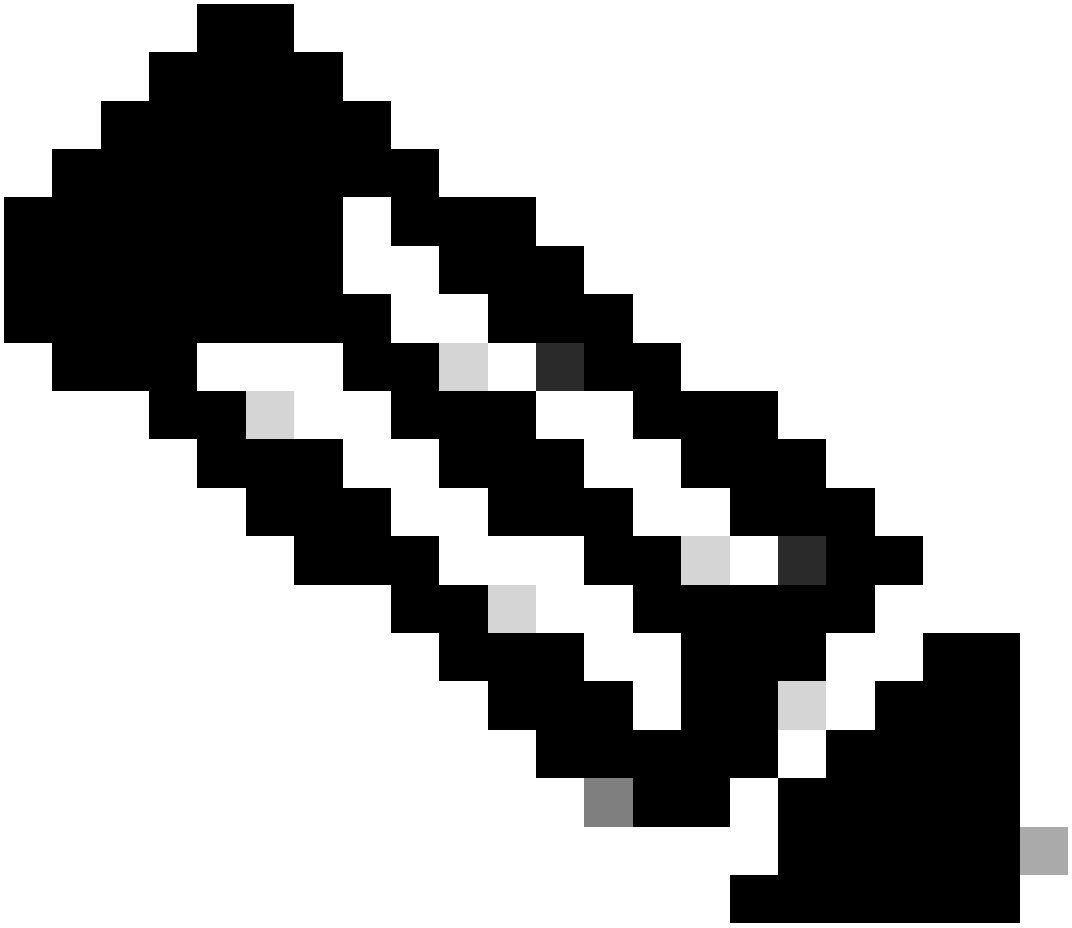
Opción 1. Desplácese hasta Edit > Preference > Protocols > ERSPAN FORCE y marque esta opción para decodificar la trama ERSPAN falsa.

- Wireshark (GUI)



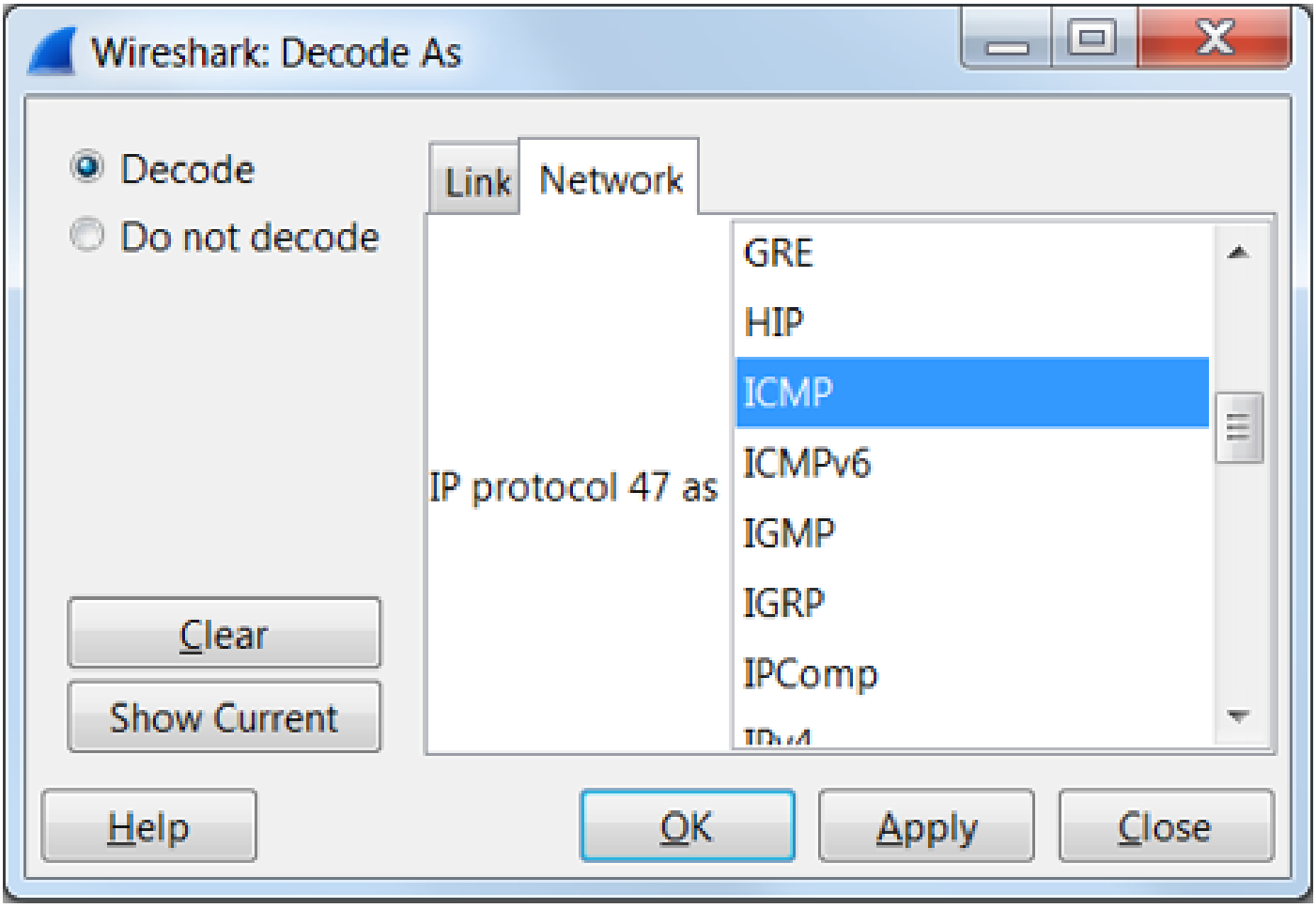
- Tshark (versión CLI de Wireshark):

```
user1@linux# tshark -f 'proto GRE' -nV -i eth0 -o erspan.fake_erspan:true
```

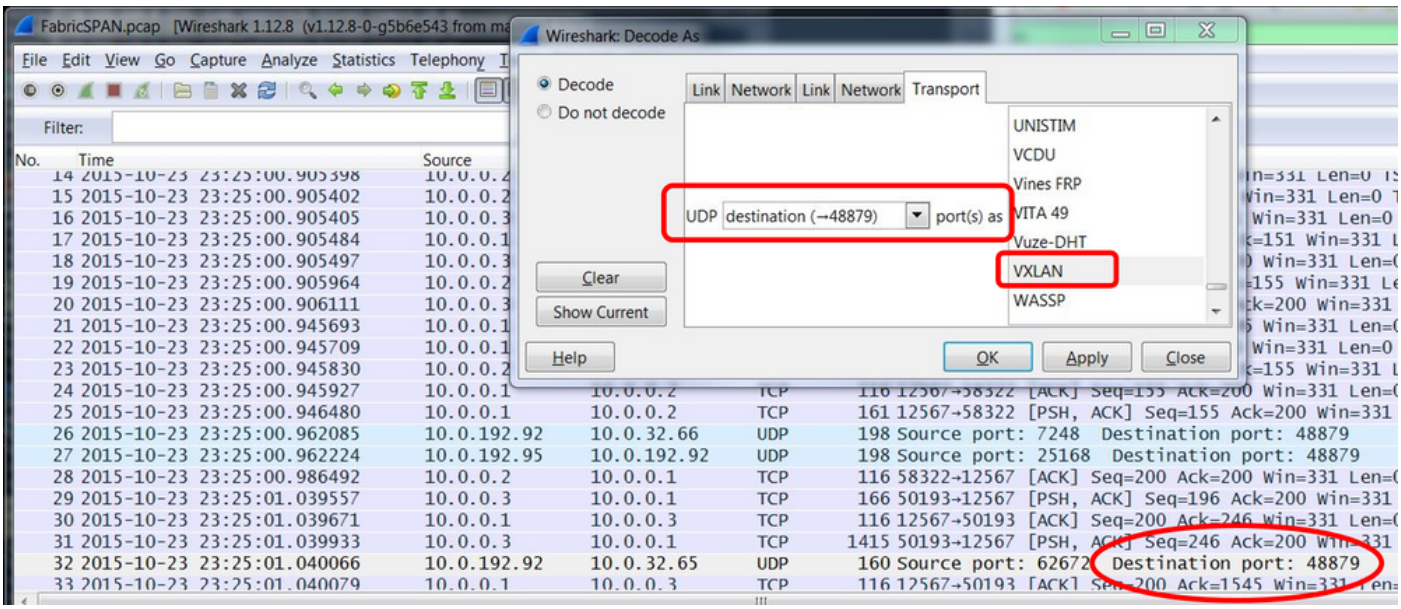


Nota: Asegúrese de desactivar esta opción cuando lea ERSPAN tipo II o III.

Opción 2. Desplácese hasta Decode As > Network > ICMP (if it’s ICMP).



Cómo descodificar el encabezado iVxLAN

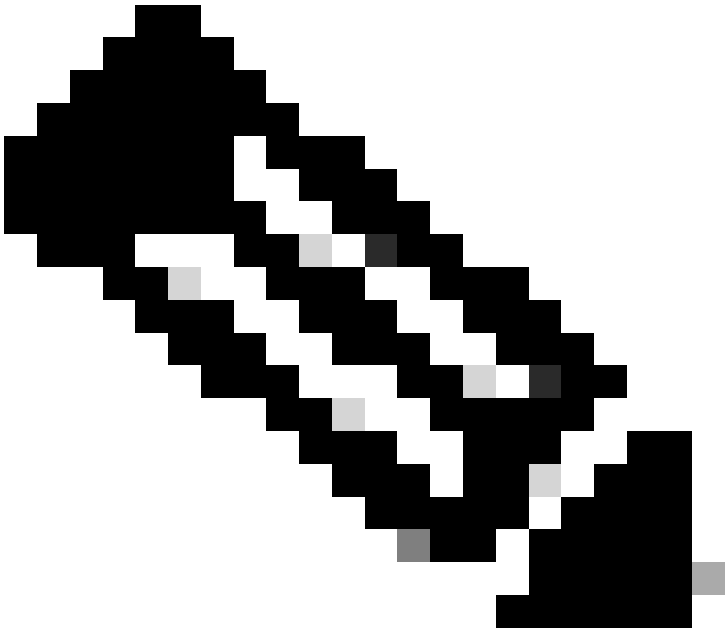


El encabezado iVxLAN utiliza el puerto de destino 48879. Por lo tanto, puede decodificar el encabezado iVxLAN y VxLAN si configura el puerto de destino UDP 48879 como VxLAN en Wireshark.

1. Asegúrese de seleccionar primero los paquetes encapsulados de VxLAN.

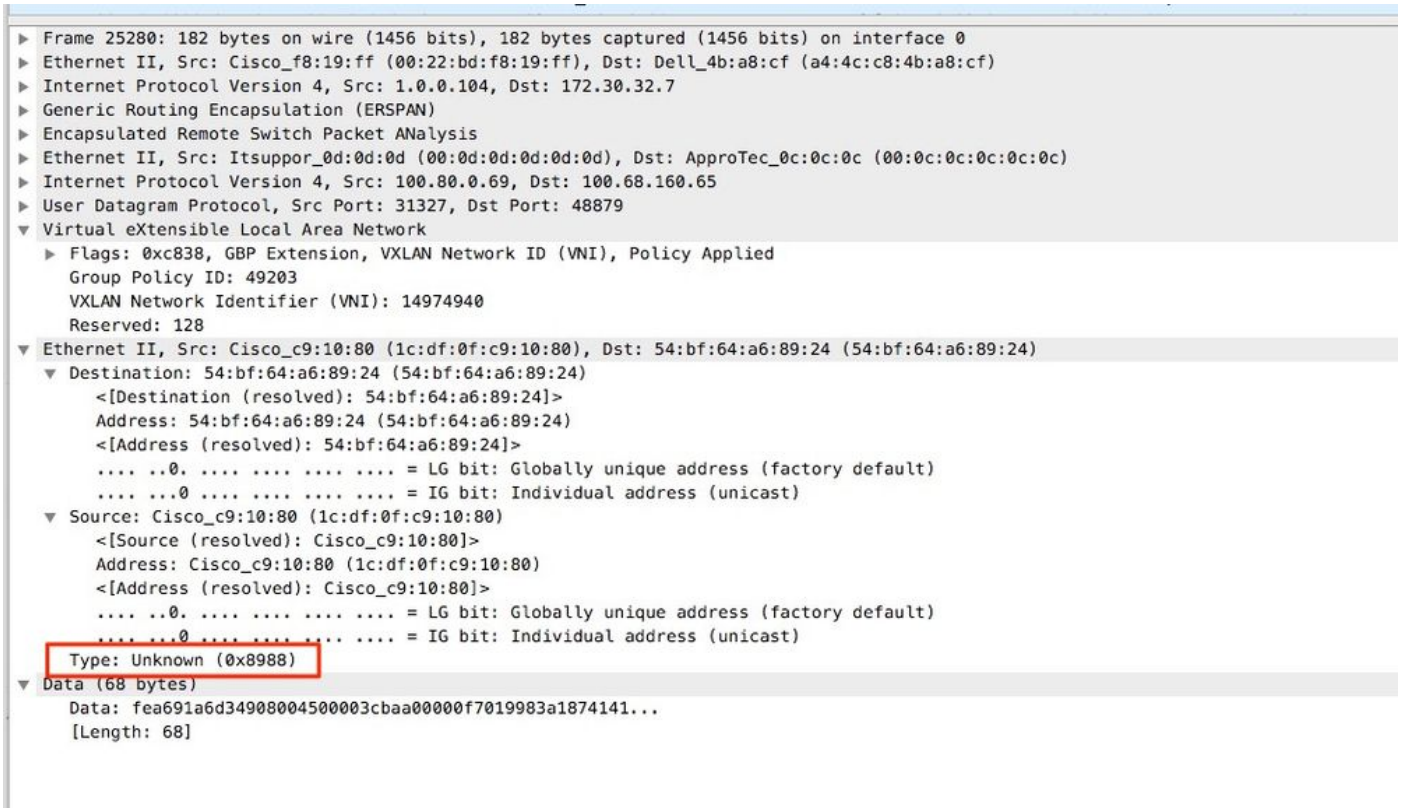
2. Desplácese hasta Analyze > Decode As > Transport > UDP destination (48879) > VxLAN.

   - Y luegoApply.



Nota: hay paquetes de comunicación entre los APIC en los puertos de fabric. Esos paquetes no están encapsulados por el encabezado iVxLAN.

Cuando se realiza una captura erspan en una red de usuario que ejecuta el protocolo de tiempo de precisión (PTP), a veces se observa que Wireshark no interpreta los datos debido a un ethertype desconocido dentro de la encapsulación GRE (0x8988). 0x8988 es el ethertype para la etiqueta de tiempo que se inserta en los paquetes del plano de datos cuando PTP está habilitado. Decodificar el ethertype 0x8988 como "etiqueta de Cisco" para exponer los detalles del paquete.


Frame 25280: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits) on interface 0
Ethernet II, Src: Cisco_f8:19:ff (00:22:bd:f8:19:ff), Dst: Dell_4b:a8:cf (a4:4c:c8:4b:a8:cf)
Internet Protocol Version 4, Src: 1.0.0.104, Dst: 172.30.32.7
Generic Routing Encapsulation (ERSPAN)
Encapsulated Remote Switch Packet ANalysis
Ethernet II, Src: Itsuppor_0d:0d:0d (00:0d:0d:0d:0d:0d), Dst: ApproTec_0c:0c:0c (00:0c:0c:0c:0c:0c)
Internet Protocol Version 4, Src: 100.80.0.69, Dst: 100.68.160.65
User Datagram Protocol, Src Port: 31327, Dst Port: 48879
Virtual eXtensible Local Area Network
Flags: 0xc838, GBP Extension, VXLAN Network ID (VNI), Policy Applied
Group Policy ID: 49203
VXLAN Network Identifier (VNI): 14974940
Reserved: 128
Ethernet II, Src: Cisco_c9:10:80 (1c:df:0f:c9:10:80), Dst: 54:bf:64:a6:89:24 (54:bf:64:a6:89:24)
Destination: 54:bf:64:a6:89:24 (54:bf:64:a6:89:24)
<[Destination (resolved): 54:bf:64:a6:89:24]>
Address: 54:bf:64:a6:89:24 (54:bf:64:a6:89:24)
<[Address (resolved): 54:bf:64:a6:89:24]>
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: Cisco_c9:10:80 (1c:df:0f:c9:10:80)
<[Source (resolved): Cisco_c9:10:80]>
Address: Cisco_c9:10:80 (1c:df:0f:c9:10:80)
<[Address (resolved): Cisco_c9:10:80]>
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: Unknown (0x8988)
Data (68 bytes)
Data: fea691a6d34908004500003cbaa00000f7019983a1874141...
[Length: 68]

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).