Configuración del analizador de puertos conmutados en ACI

Contenido

Introducción

Este documento describe cómo configurar el Analizador de puerto conmutado (SPAN) en Cisco Application Centric Infrastructure (ACI) versión 5.x y 6.x.

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 y las diferencias entre 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.

- SPAN to CPU es capturar los paquetes que entran y salen interfaces between Leaf switches and external devices(comenzando en 6.2).

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
- SPAN a CPU está configurado 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 Troubleshooting de Cisco APIC: Herramientas y metodología de Troubleshooting > Uso de SPAN.

SPAN de acceso (ERSPAN)

Topología de ejemplo

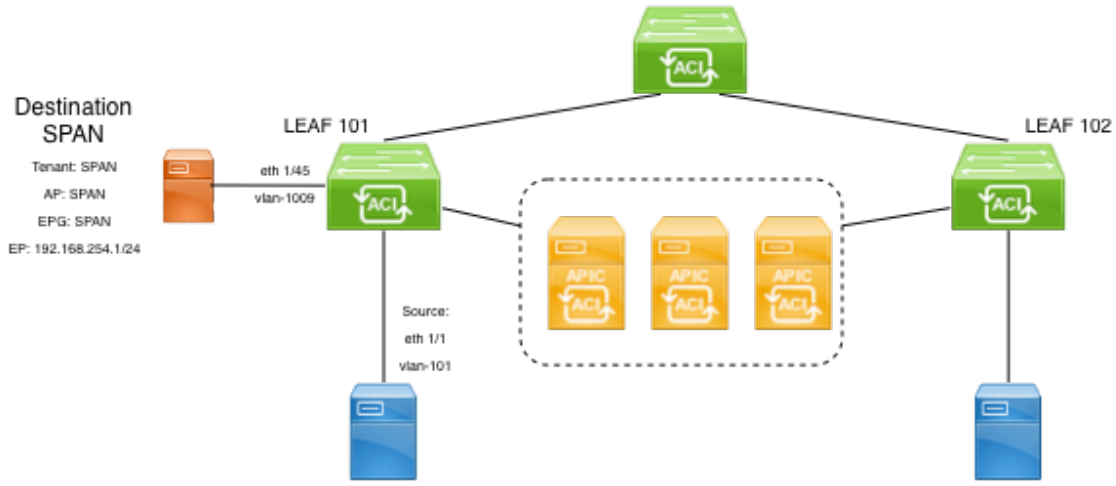

Imagen 1: Topología de ejemplo para el acceso a ERSPAN

Ejemplo de configuración

Vaya a .Fabric > Access Policies > Policies > Troubleshooting > SPAN

- Haga clic con el botón derecho en 'SPAN Destination Groups' y seleccione la opción para crear SPAN Destination Group (DST_EPG).

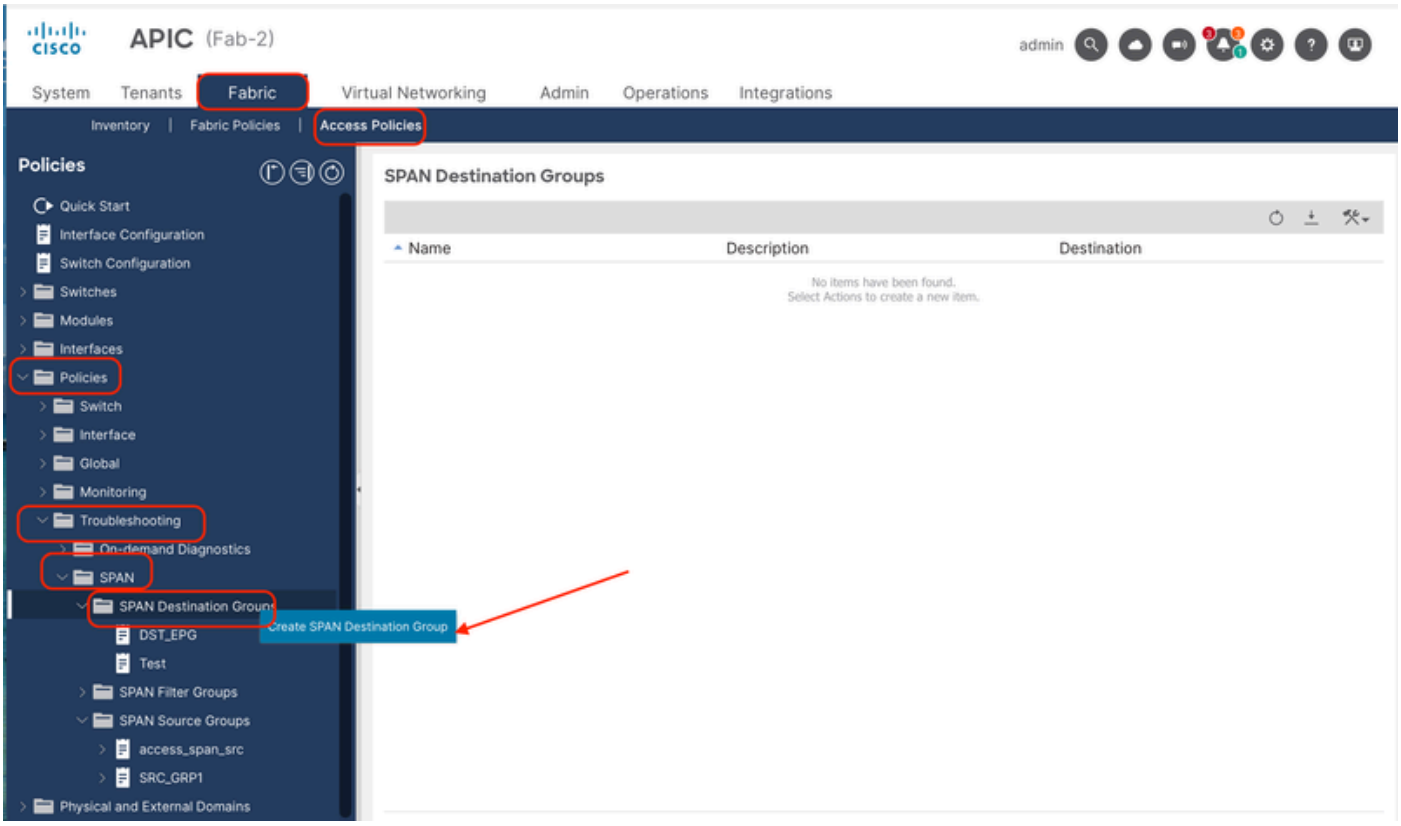

Imagen 2: Ruta para crear el grupo de destino ERSPAN de acceso

Rellene la información:

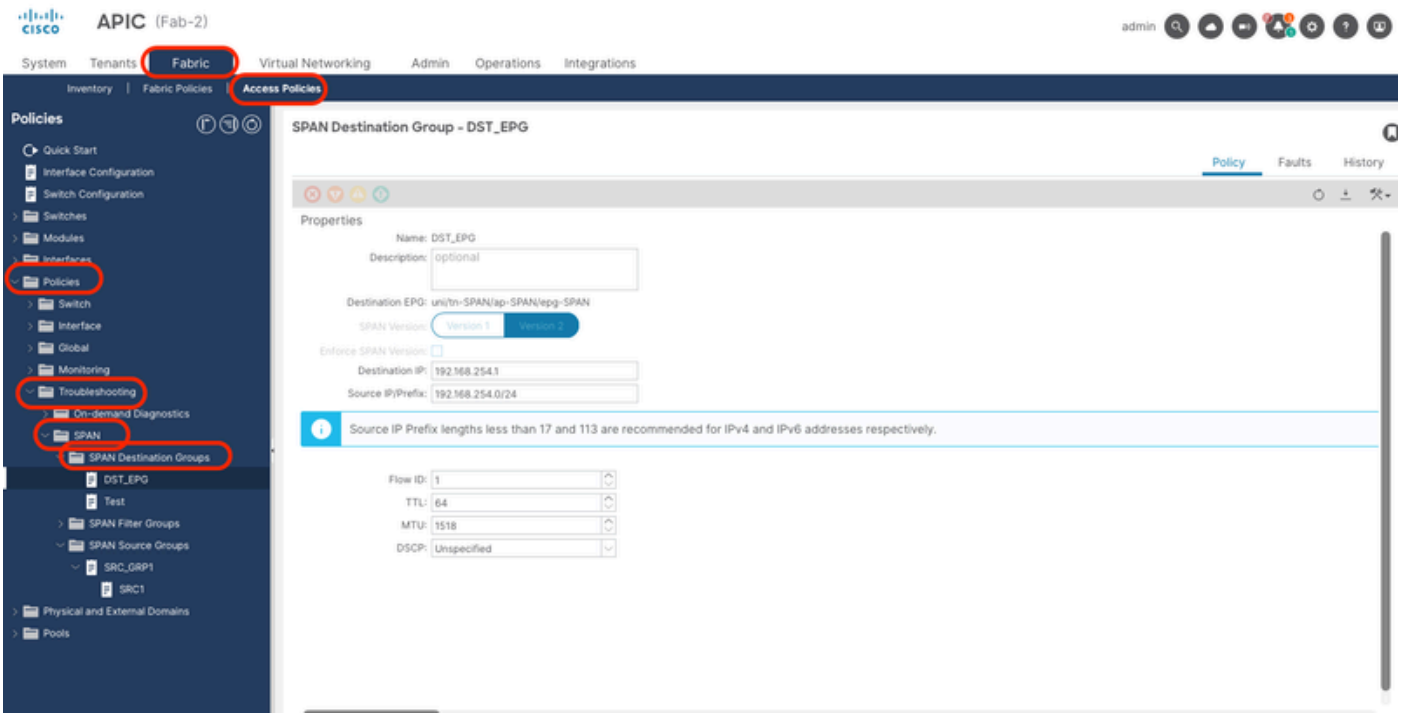

Imagen 3: Configuración de un grupo de destino ERSPAN de acceso

Where:

Tipo de destino: EPG (obligatorio para acceder a ERSPAN)

EPG de destino: Arrendatario/AP/EPG donde se aprende el terminal de destino

IP de destino: IP del punto final de destino

IP 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: 192.168.254.0/24 en node-101 => src IP 192.168.254.101

ID de flujo: De forma predeterminada se establece en 1, lo cual es útil para identificar el paquete por flujo en el encabezado ERSPAN:

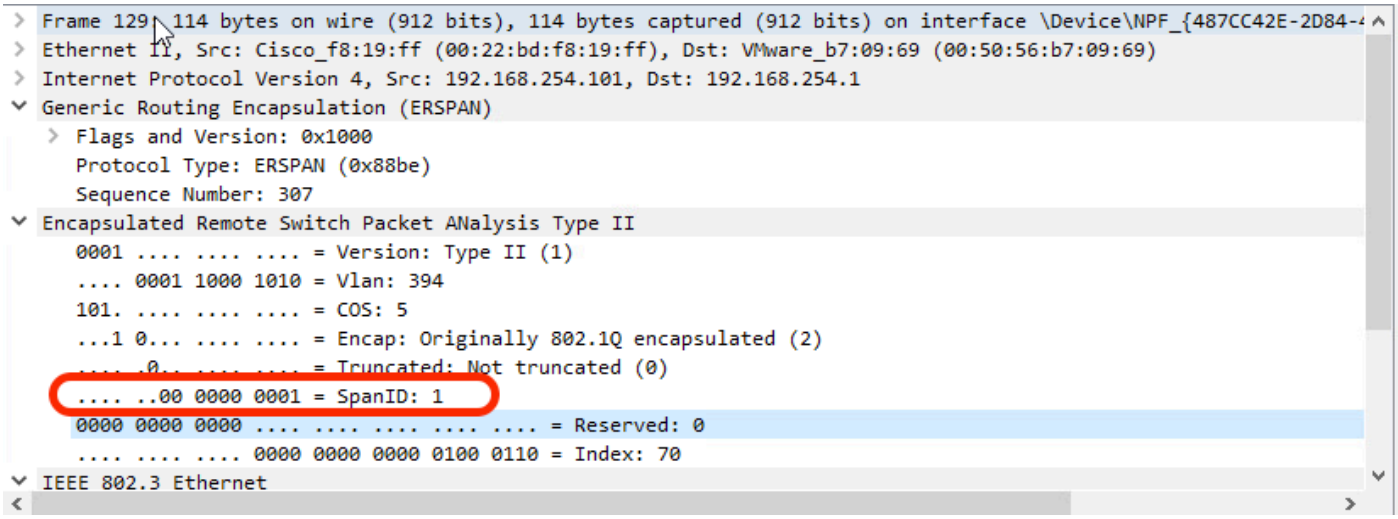

Imagen 4: Paquete en Wireshark para mostrar ID de flujo

Consejo: Para filtrar el ID de flujo, puede utilizar este filtro de Wireshark: erspan.spanid == <ID de flujo>

- Create SPAN Source Group (SRC_GRP1), haga clic con el botón derecho en 'SPAN Source Groups' y seleccione 'Create SPAN Source groups':

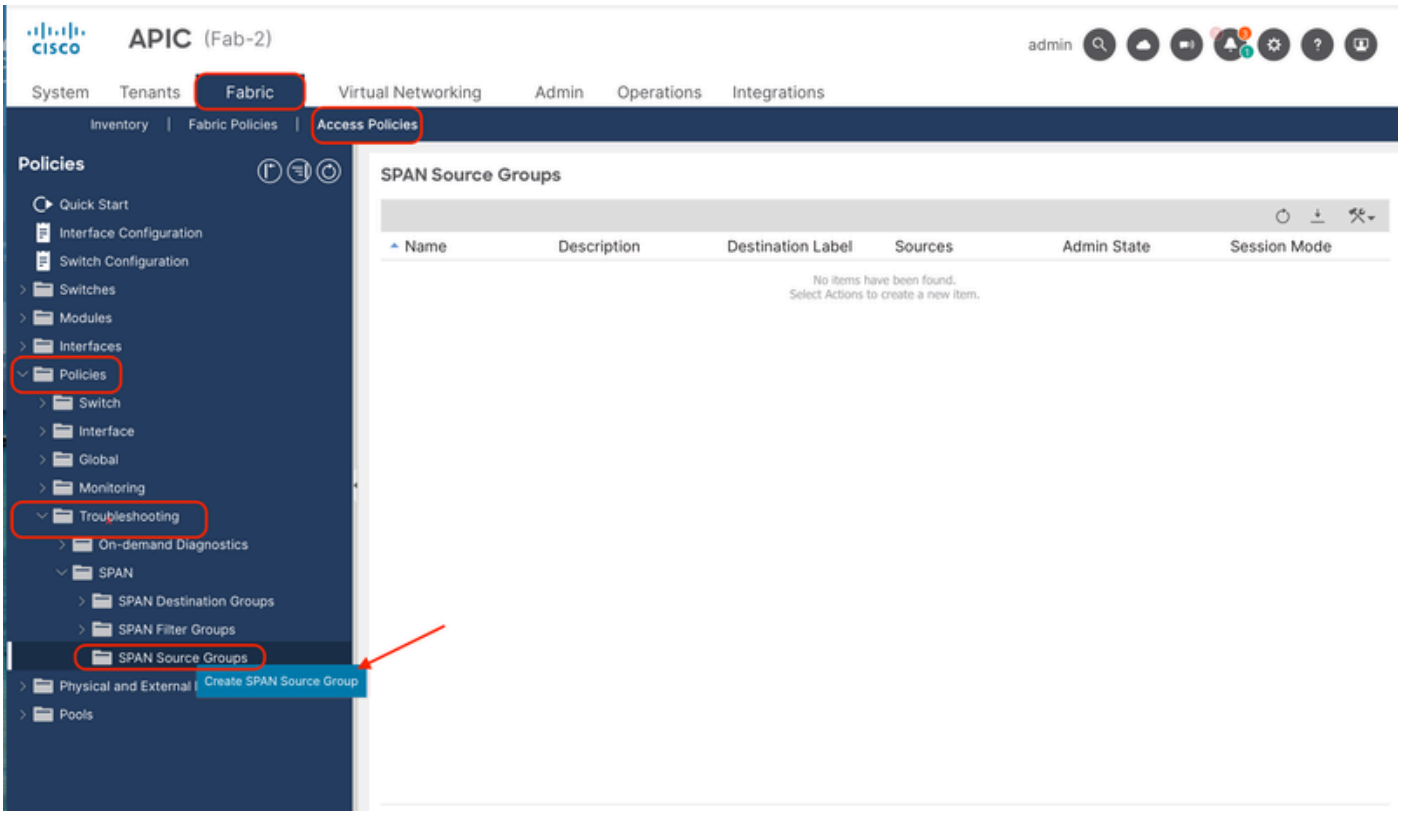

Imagen 5: Ruta para crear un grupo de origen ERSPAN de acceso

Rellene la información:

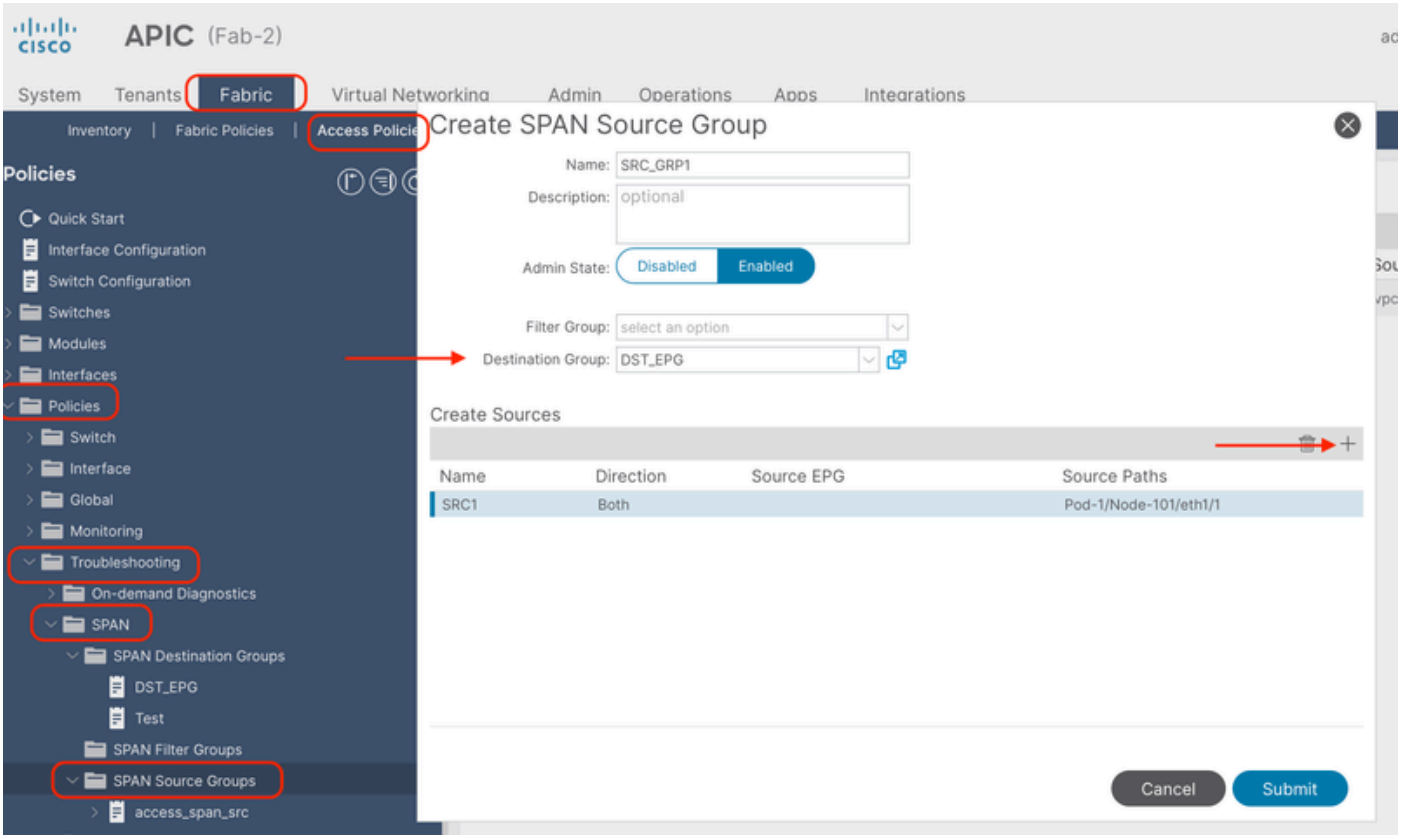

Imagen 6: Configuración de un grupo de origen ERSPAN de acceso

Where:

Estado del administrador: habilitado

Grupo de destino: Seleccione el grupo de destino creado anteriormente (DST_EPG)

- En este mismo cuadro, haga clic en el botón más (+) para agregar al menos un origen de SPAN.
- Configure estos parámetros para crear el SPAN Source (SRC1):

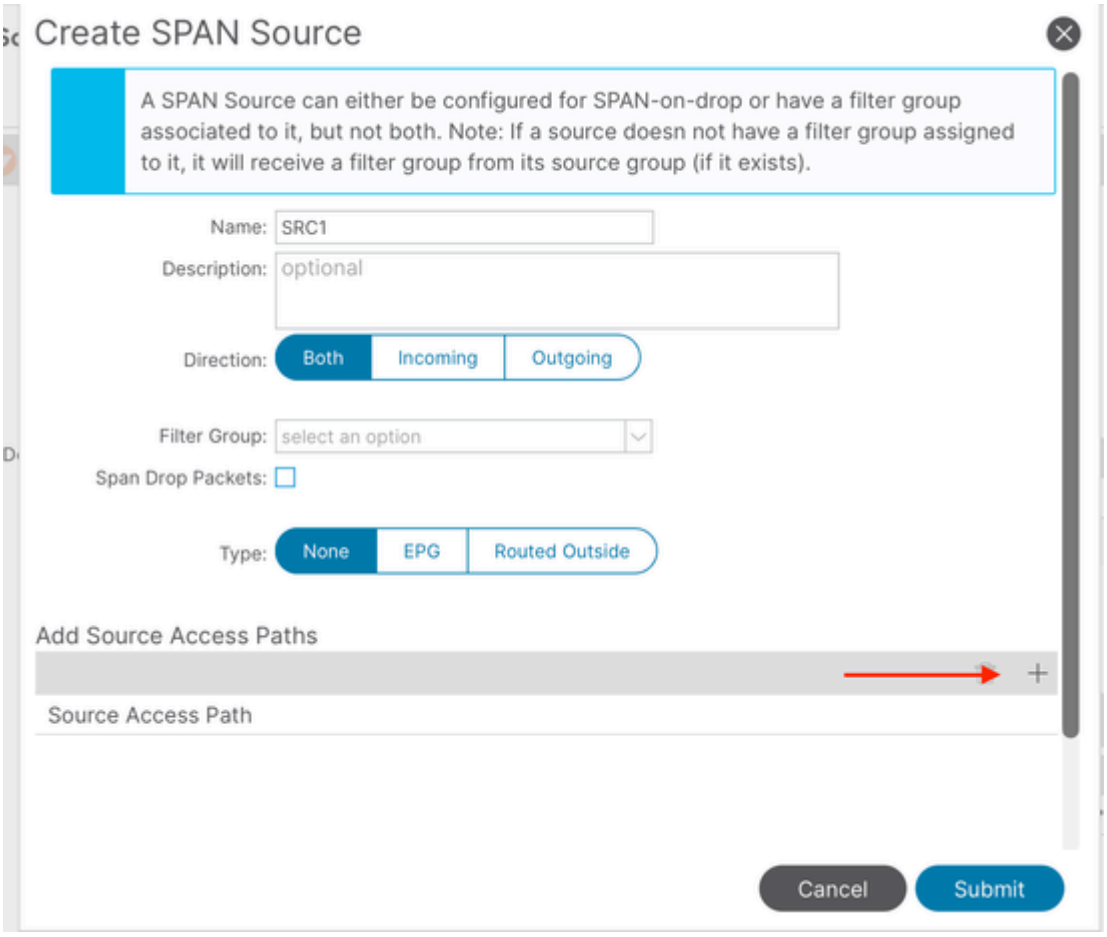

Imagen 7: Configuración de una fuente ERSPAN de acceso

Where:

Dirección: Puede elegir entre: Direcciones entrantes, salientes o ambas

Tipo: Puede elegir entre: Ninguno (un puerto frontal normal), EPG (interfaz implementada como enlace estático en un EPG y solo se duplica el tráfico de EPG) o Enrutado externo (interfaz utilizada en una salida L3).

En este ejemplo, se utiliza un puerto frontal normal.

- Haga clic en el botón más (+) para agregar una ruta de acceso de origen. Rellene la información:

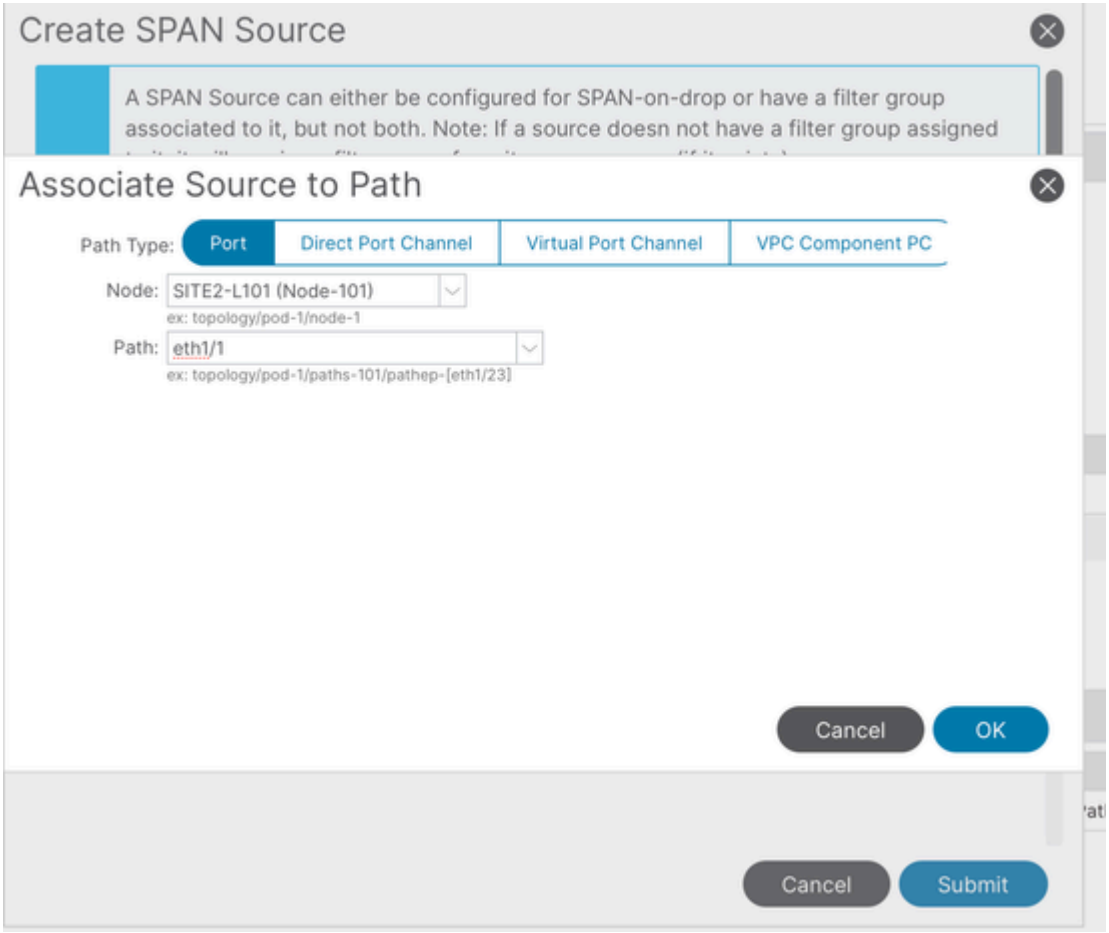

Imagen 8: Creación de una trayectoria de origen ERSPAN de acceso

Where:

Tipo de ruta: Elija entre Port (individual), Direct port-channel, Virtual port-channel (al elegir esta opción, la ruta muestra las VPC ya formadas) y VPC component PC (solo un tramo de la VPC, eligiendo el nodo específico)

Nodo: Elija el nodo de origen (nodo 101 según el ejemplo de topología)

Ruta: interfaz de origen (eth1/1 según ejemplo de topología)

Acceso a SPAN local

Topología de ejemplo

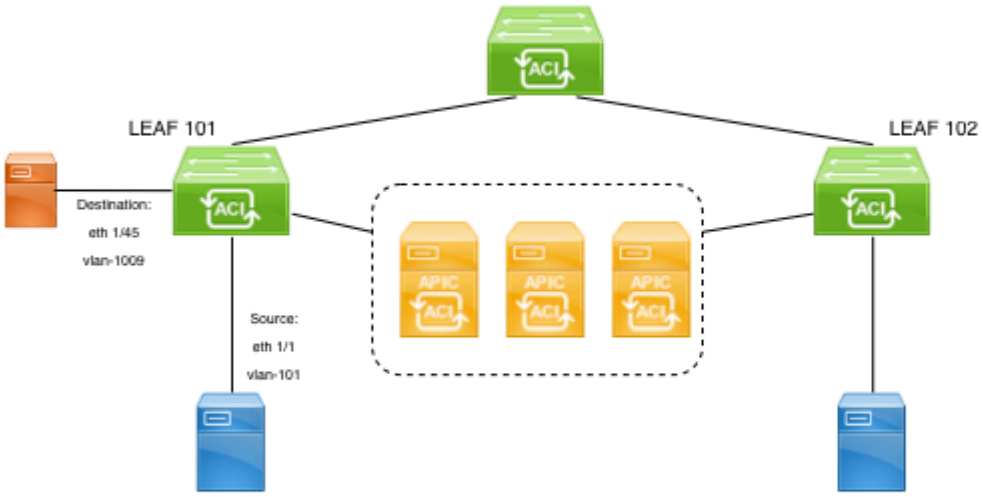

Imagen 9: Topología de ejemplo de un SPAN de acceso local

Ejemplo de configuración

Vaya a .Fabric > Access Policies > Policies > Troubleshooting > SPAN

- Haga clic con el botón derecho en 'SPAN Destination Groups' y seleccione la opción para crear SPAN Destination Group (DST_EPG).

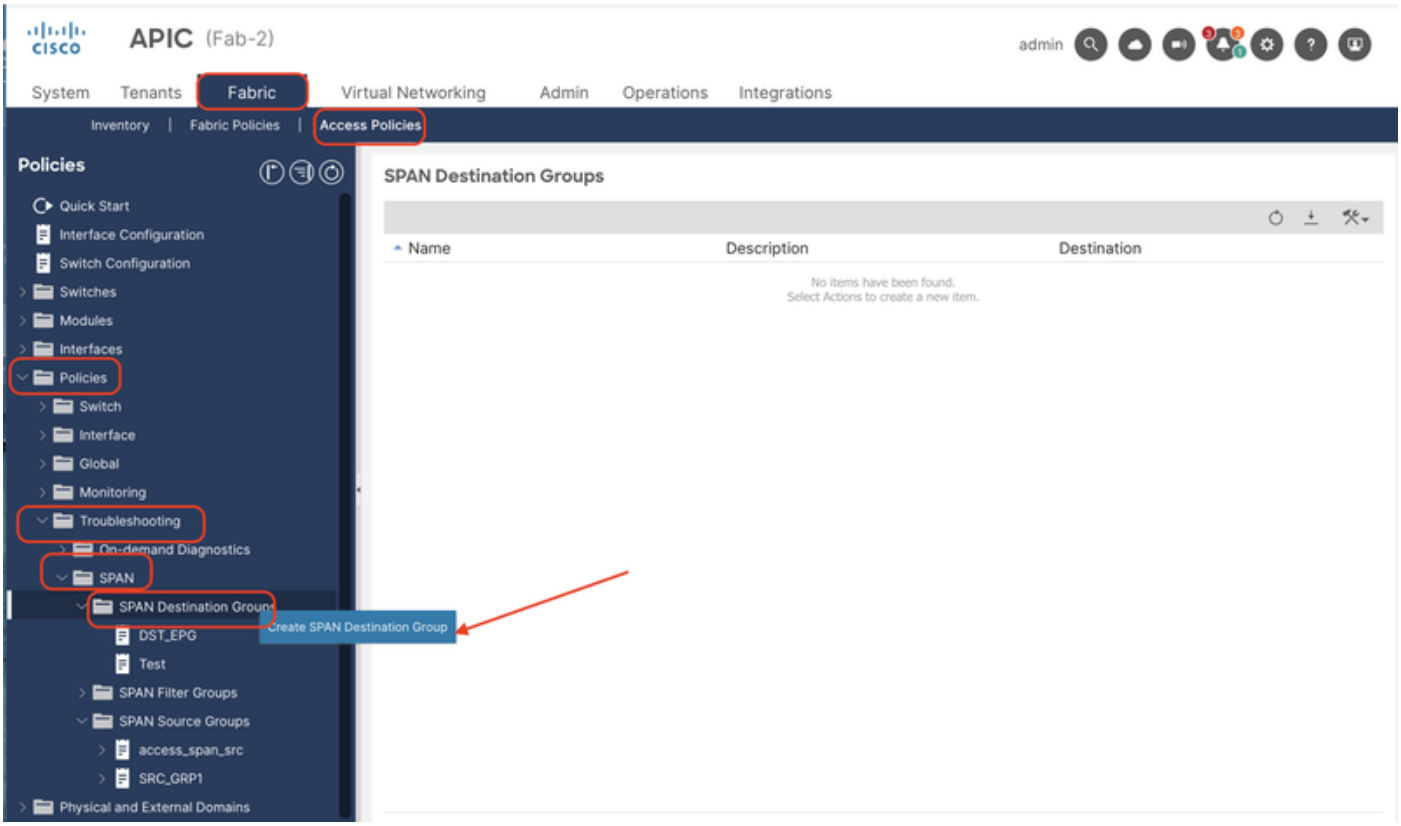

Imagen 10: Ruta para crear un grupo de destino SPAN de acceso local

Rellene la información:

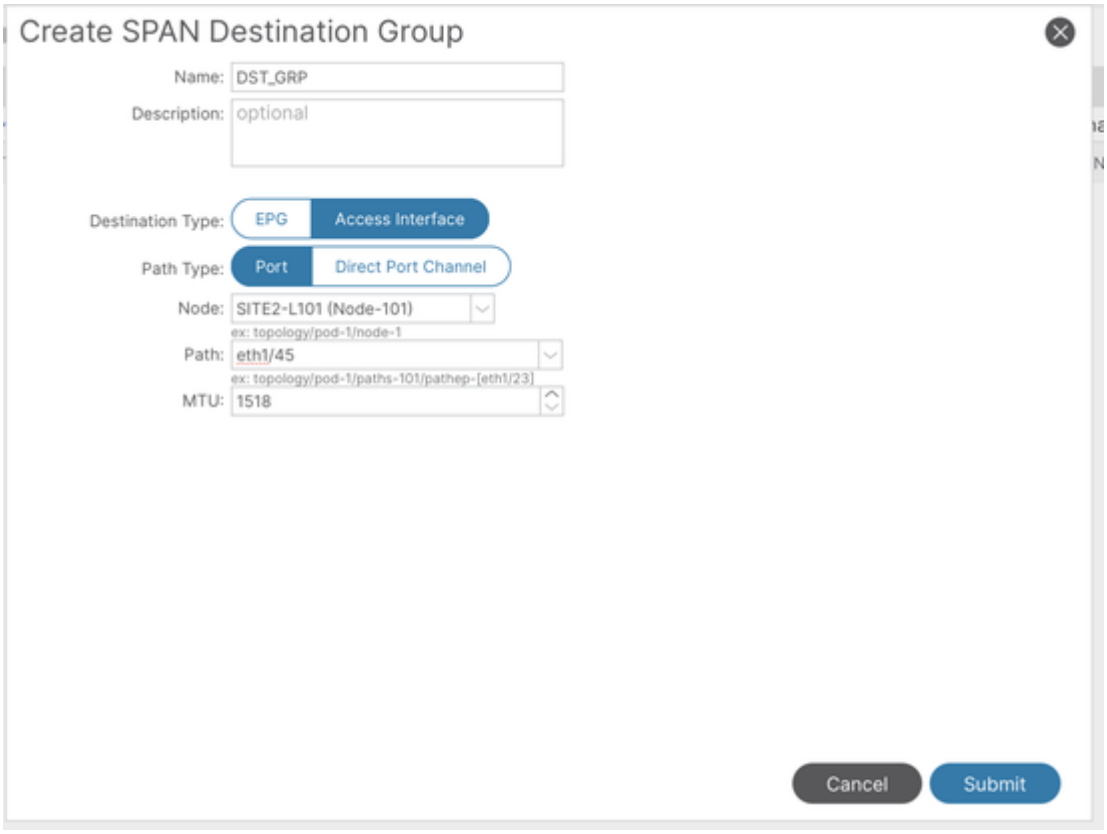

Imagen 1: Configuración de un grupo de destino SPAN de acceso local

Where:

Tipo de destino: Interfaz de acceso (obligatorio para ser SPAN local)

Tipo de ruta: Puerto

Nodo: Nodo 101 (según la topología)

Ruta: eth1/45 (según la topología)

Nota: No es necesario que el puerto de destino tenga aplicada ninguna política de arrendatarios (p. ej. EPG, L3out o infra); de lo contrario, se genera este error:

Error: F1559

Descripción: Delegado de errores: Error al configurar SPAN con destino DST_GRP del grupo de destino DST_GRP debido a puerto de destino no seguro para SPAN. El puerto ya tiene una implementación existente de Application EPG, L3Out o Infra VLAN

Si el puerto de destino es parte de un EPG, la alternativa sería cambiar a Access ERSPAN.

- Create SPAN Source Group (SRC_GRP1), haga clic con el botón derecho en 'SPAN Source Groups' y seleccione 'Create SPAN Source groups':

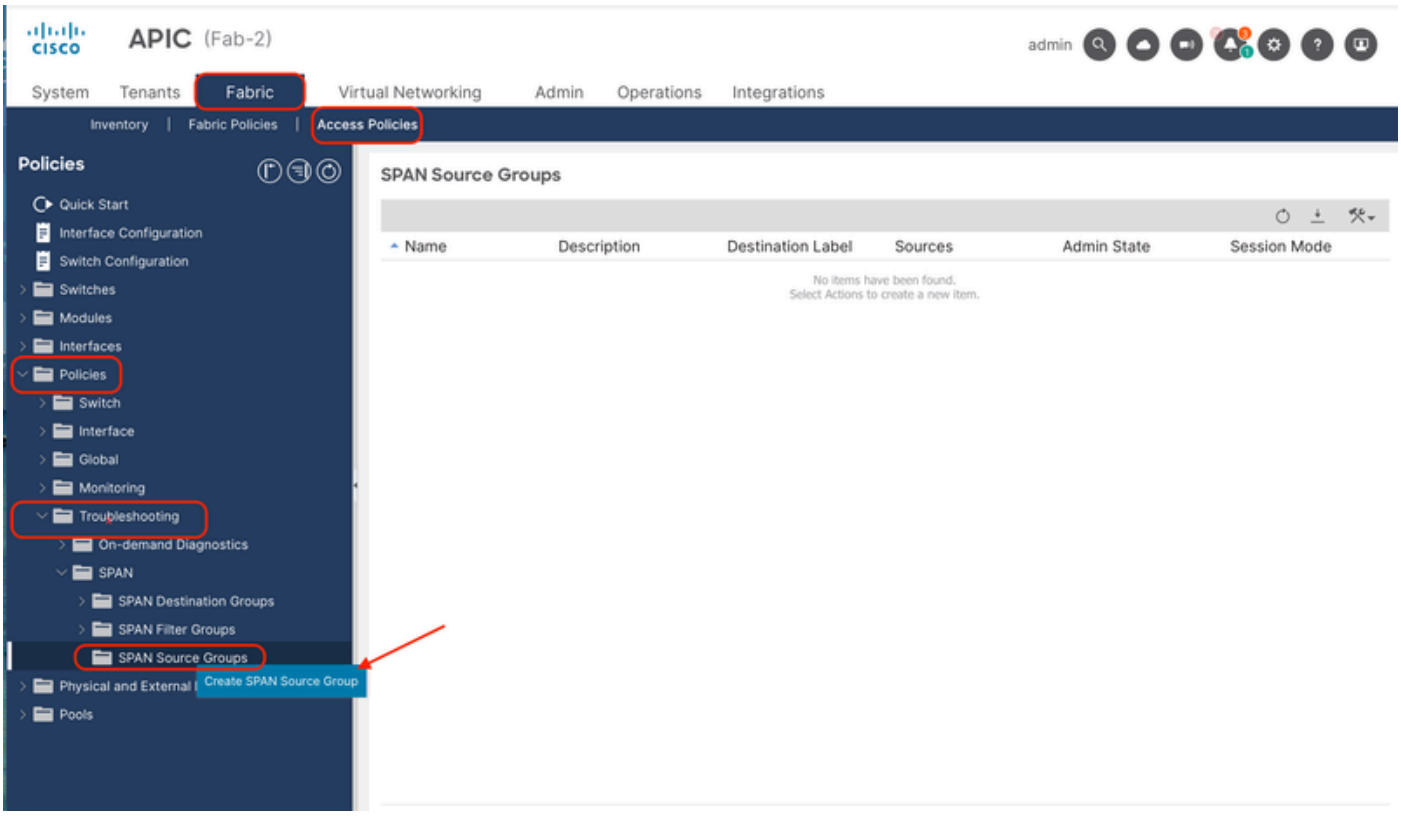

Imagen 12: Ruta para crear un grupo de origen SPAN de acceso local

Rellene la información:

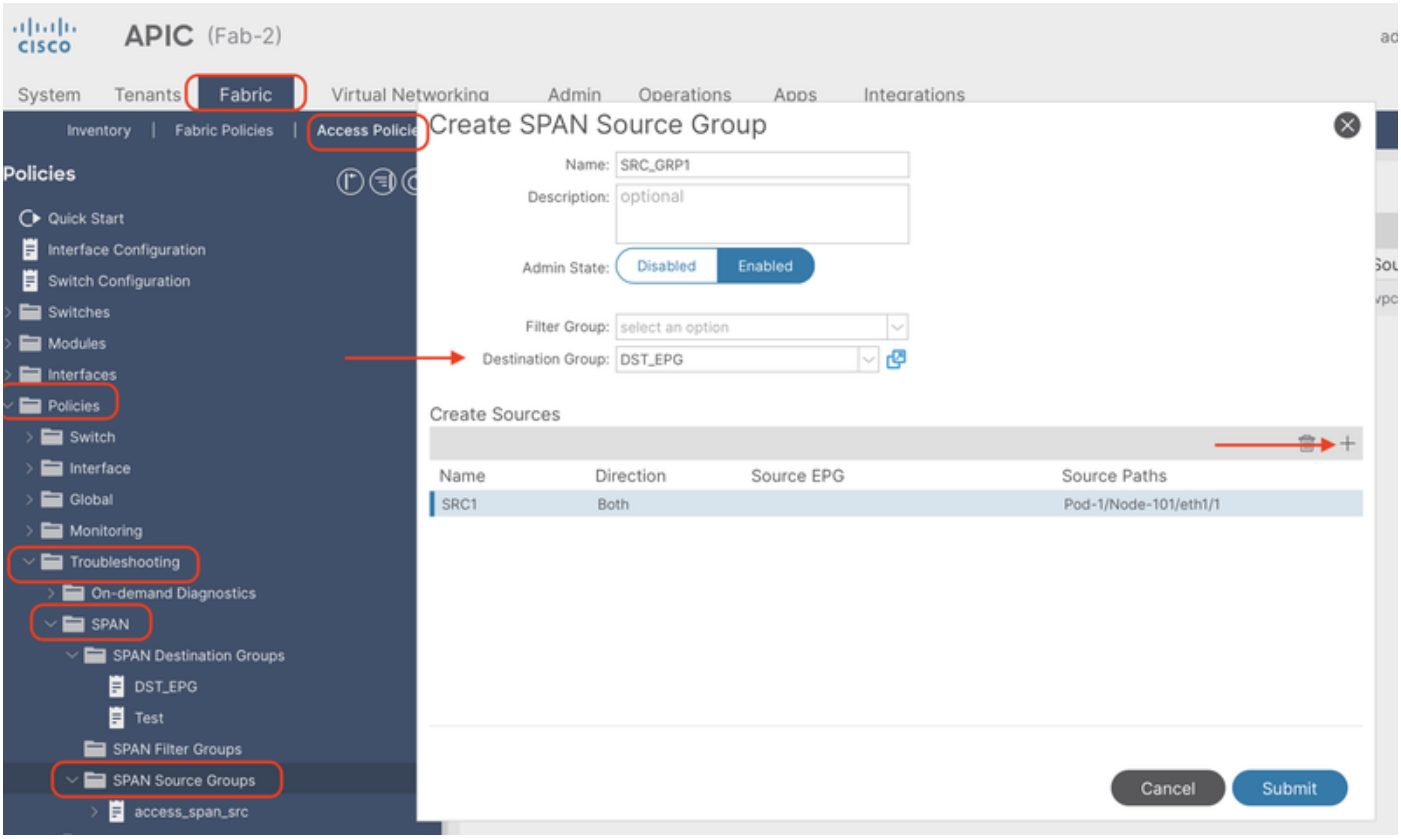

Imagen 13: Creación de un grupo de origen SPAN de acceso local

Where:

Estado del administrador: habilitado

Grupo de destino: Seleccione el grupo de destino creado anteriormente (DST_EPG)

- En este mismo cuadro, haga clic en el botón más (+) para agregar al menos un origen de SPAN.
- Configure estos parámetros para crear el SPAN Source (SRC1):

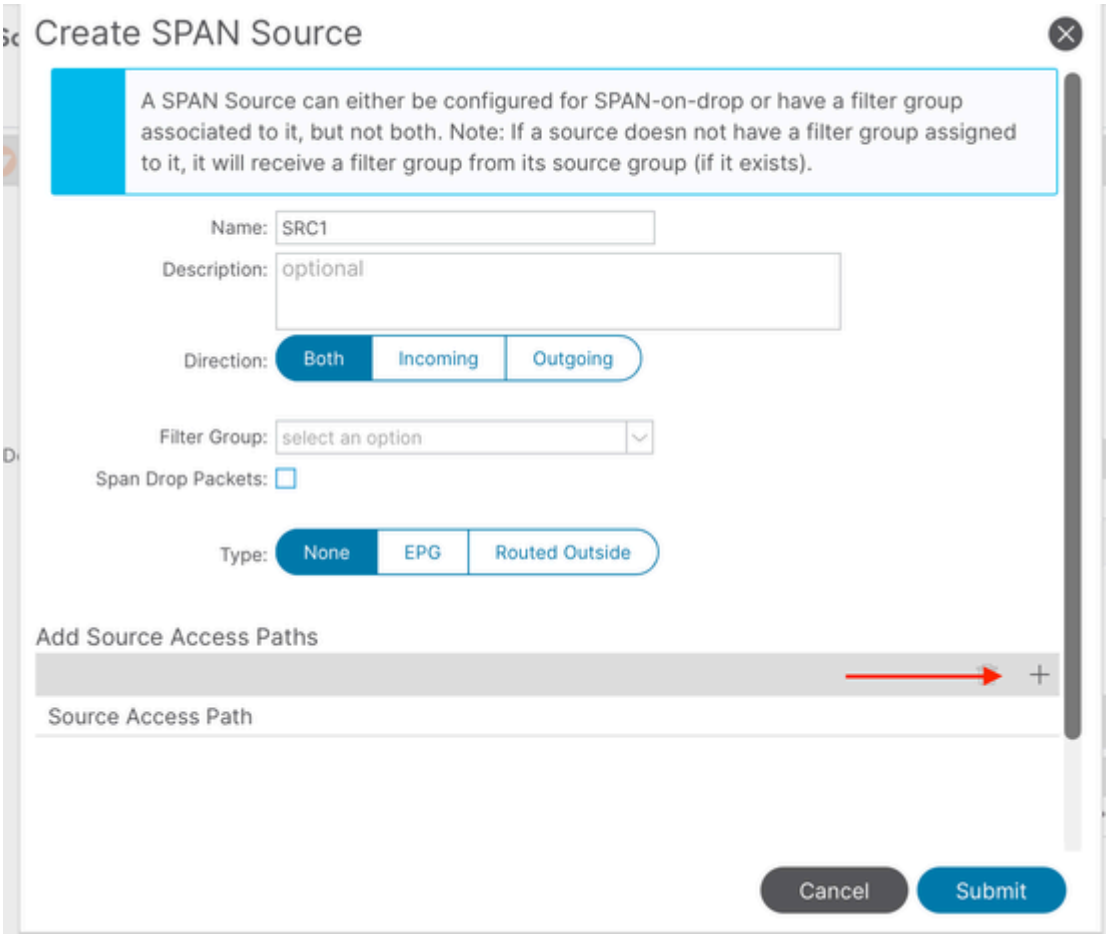

Imagen 14: pasos para la creación de un origen SPAN de acceso local

Where:

Dirección: Elija entre entrante, saliente o ambas direcciones

Tipo: Puede elegir entre: Ninguno (un puerto frontal normal), EPG (interfaz implementada como enlace estático en un EPG y solo se duplica el tráfico de EPG) o Enrutado externo (interfaz utilizada en una salida L3).

En este ejemplo, se utiliza un puerto frontal normal. Siempre que las rutas de acceso de origen agregadas posteriormente se implementen en el mismo nodo, se admite la configuración.

- Haga clic en el botón más (+) para agregar una ruta de acceso de origen. Rellene la información:

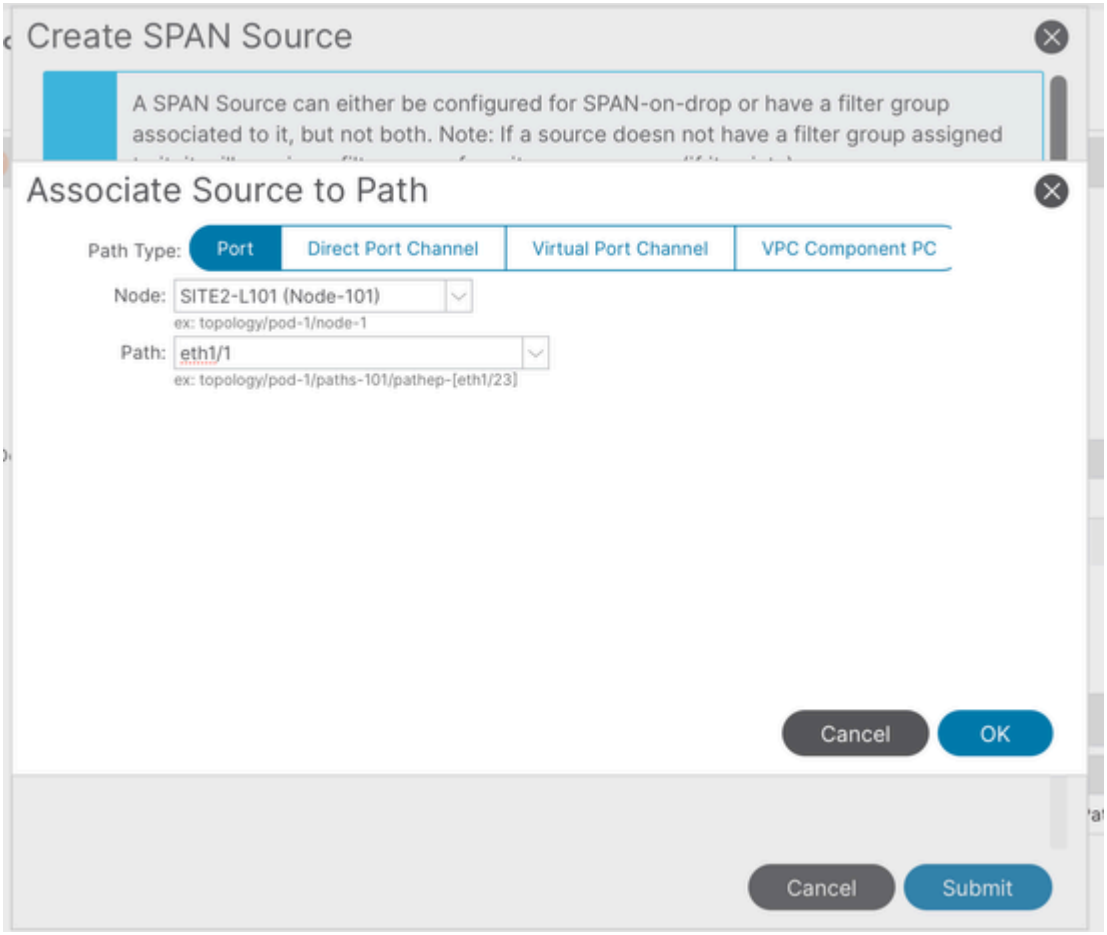

Imagen 15: Creación de una trayectoria de origen SPAN de acceso local

Where:

Tipo de ruta: Elija entre Port (individual), Direct port-channel, Virtual port-channel (al elegir esta opción, la ruta muestra las VPC ya formadas) y VPC component PC (solo un tramo de la VPC, eligiendo el nodo específico)

Nota: El canal de puerto virtual no es compatible con el SPAN de acceso local

---

Nodo: Elija el nodo de origen (nodo 101 según el ejemplo de topología)

Ruta: interfaz de origen (eth1/1 según ejemplo de topología)

Limitaciones:

Nota: 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 (Id. de error de Cisco CSCvc1053). En su lugar, se agregó soporte para SPAN en "VPC component PC" a través de la identificación de error de Cisco CSCvc44643en 2.1(2e), 2.2(2e) y adelante. 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 solamente un subconjunto de los paquetes se extienda (también debido al ID de bug de Cisco 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 arrendatario (ERSPAN)

Topología de ejemplo

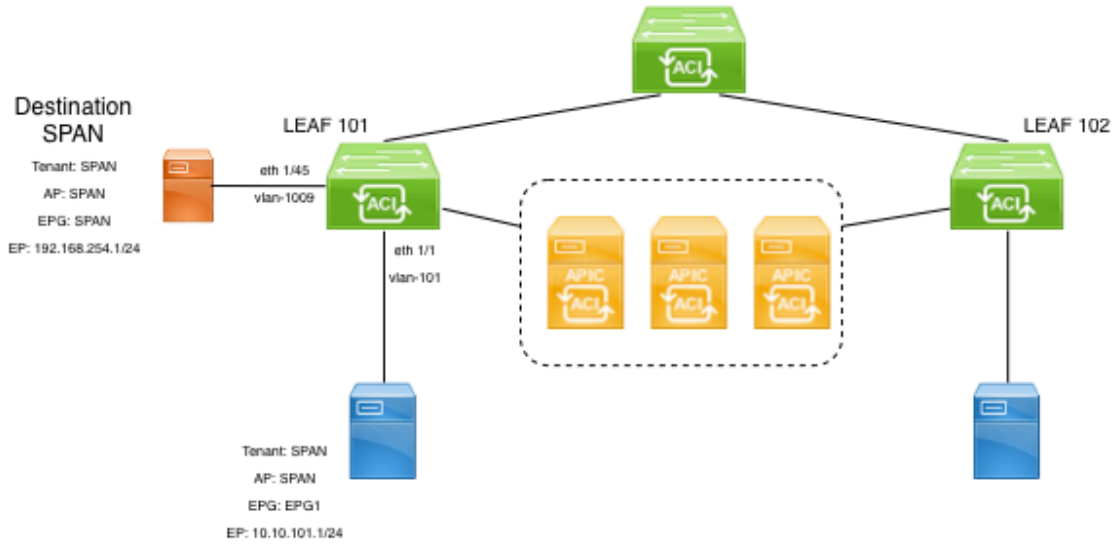

Imagen 16: Topología de ejemplo para el arrendatario ERSPAN

Ejemplo de configuración

Vaya a .Tenant >

> Policies > Troubleshooting > SPAN

- Haga clic con el botón derecho en 'SPAN Destination Groups' y seleccione la opción para crear SPAN Destination Group (DST_EPG).

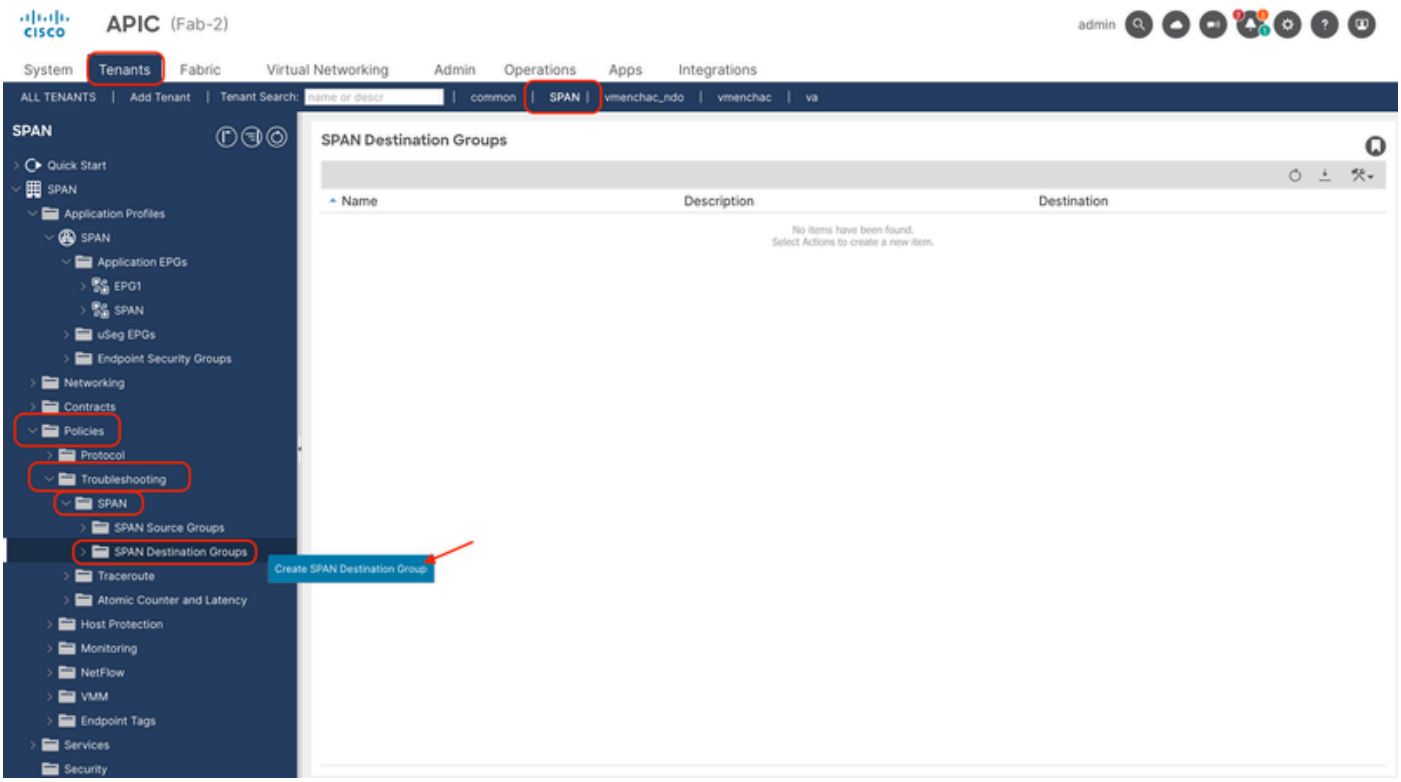

Imagen 17: ruta para crear el grupo de destino ERSPAN del arrendatario

Rellene la información:

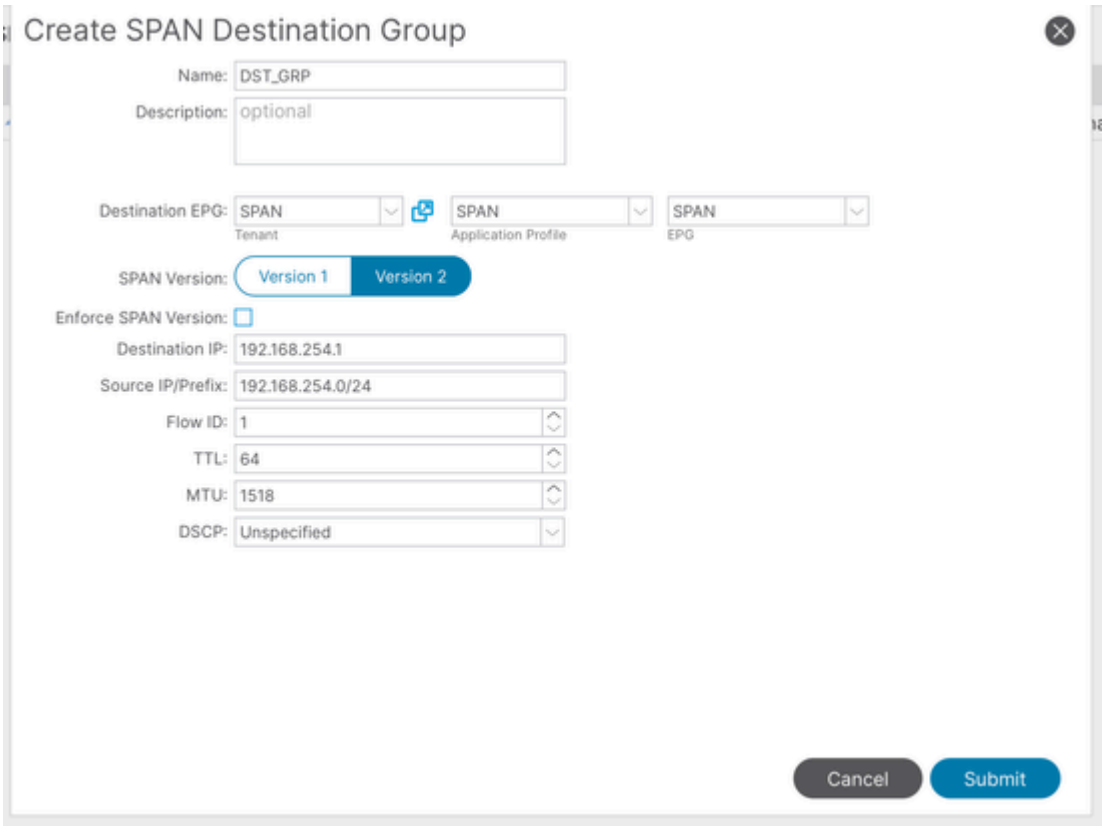

Imagen 18: Creación del grupo de destino ERSPAN del arrendatario

Where:

EPG de destino: configure el arrendatario (de forma predeterminada, lleva el mismo arrendatario donde se configura ERSPAN), el AP y el EPG donde se aprende el terminal de destino

IP de destino: IP del punto final de destino

IP 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: 192.168.254.0/24 en node-101 => src IP 192.168.254.101

ID de flujo: De forma predeterminada, se establece en 1, lo que resulta útil para identificar el paquete por flujo en el encabezado ERSPAN. Utilice la sugerencia que se muestra en Access ERSPAN para filtrar capturas cuando se personaliza este ID de flujo.

- Create SPAN Source Group (SRC_GRP1), haga clic con el botón derecho en 'SPAN Source Groups' y seleccione 'Create SPAN Source groups':

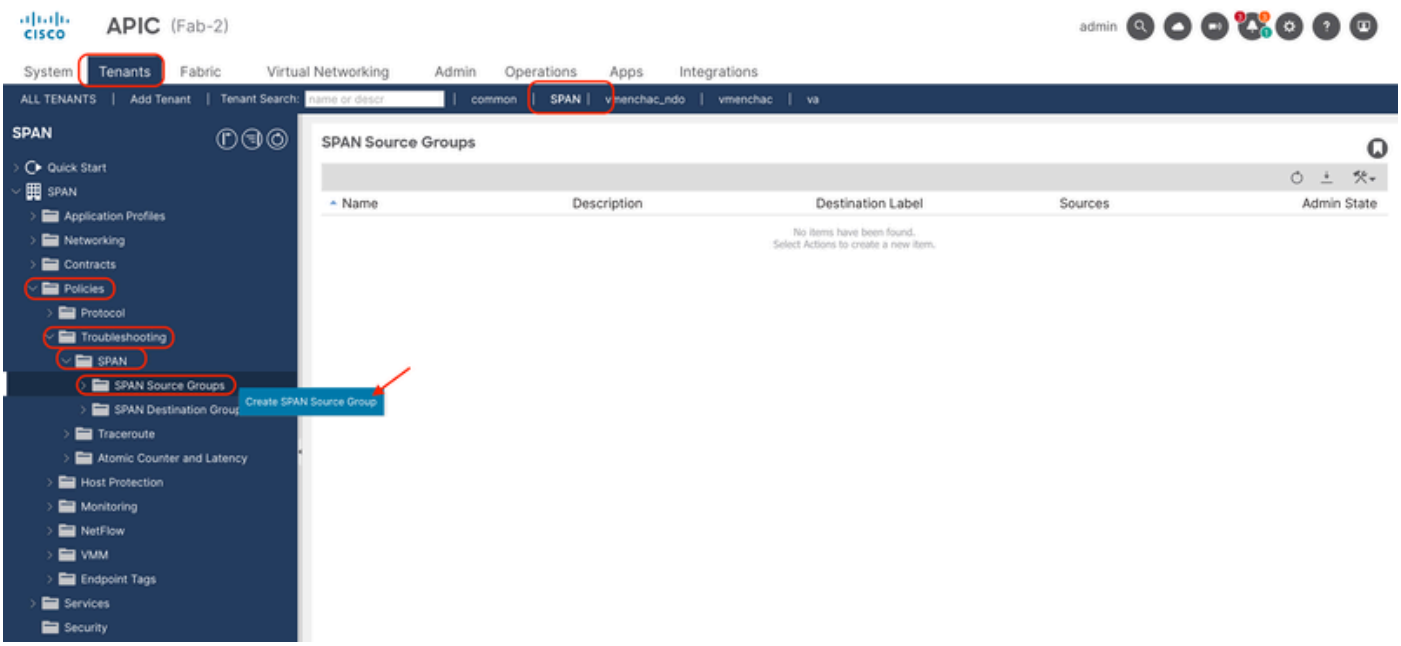

Imagen 19: ruta para crear el grupo de origen ERSPAN del arrendatario

Rellene la información:

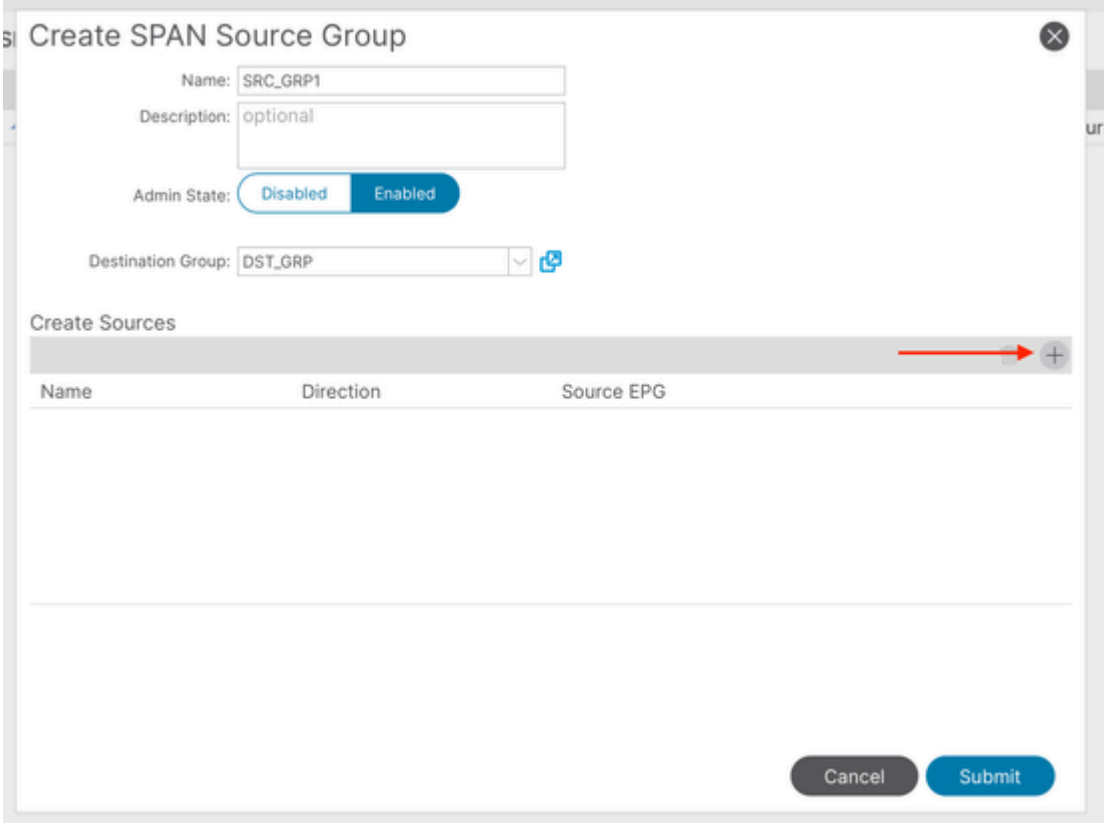

Imagen 20: Creación del grupo de origen ERSPAN del arrendatario

Where:

Estado del administrador: habilitado

Grupo de destino: Seleccione el grupo de destino creado anteriormente (DST_EPG)

- En este mismo cuadro, haga clic en el botón más (+) para agregar al menos un origen de SPAN.
- Configure estos parámetros para crear el SPAN Source (SRC1):

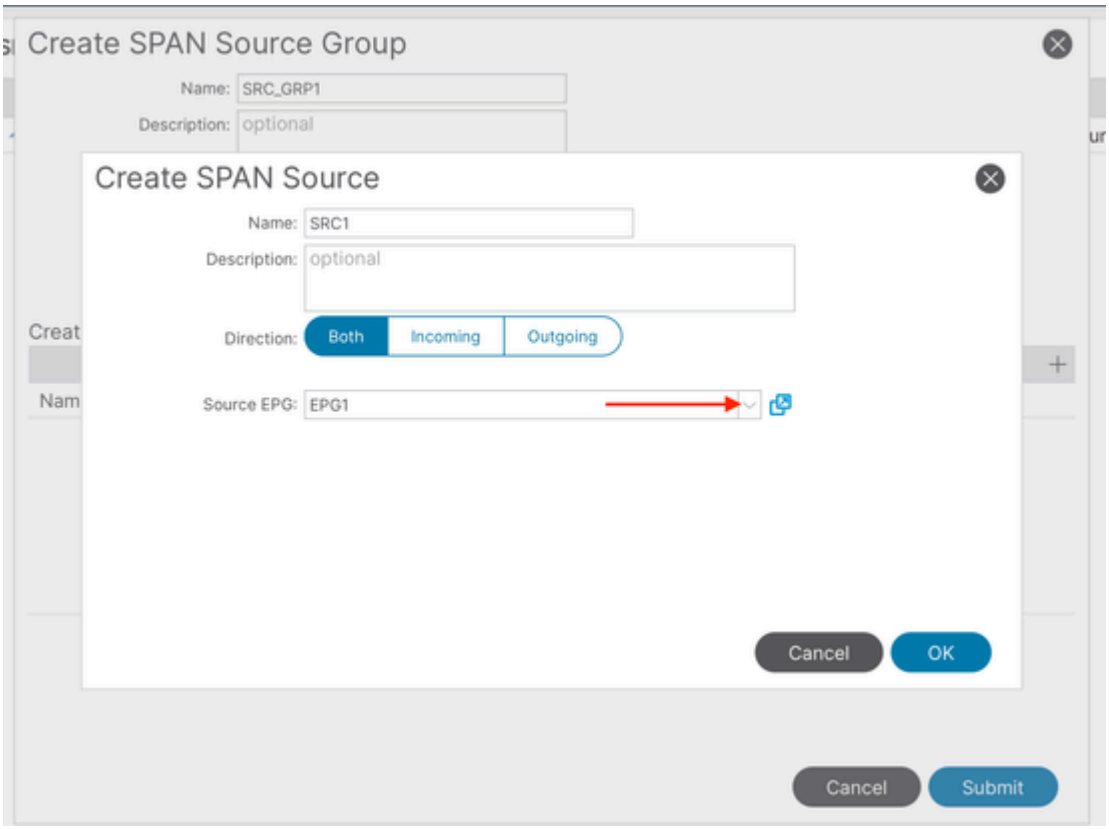

Imagen 21: creación de EPG de origen de ERSPAN de arrendatario

Where:

Dirección: Elija entre entrante, saliente o ambas direcciones

Origen de EPG: se puede elegir entre todos los EPG del mismo arrendatario. (EPG1 según el ejemplo de topología)

Fabric SPAN (ERSPAN)

Topología de ejemplo

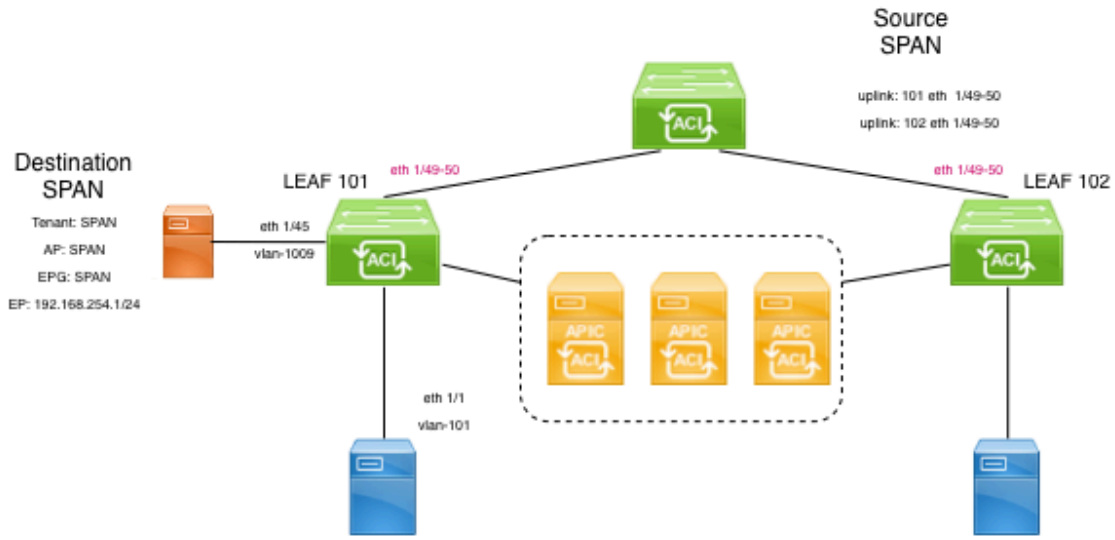

Imagen 2: Topología de ejemplo para Fabric ERSPAN

Ejemplo de configuración

Vaya a .Fabric > Fabric Policies > Policies > Troubleshooting > SPAN

- Haga clic con el botón derecho en 'SPAN Destination Groups' y seleccione la opción para crear SPAN Destination Group (DST_EPG).

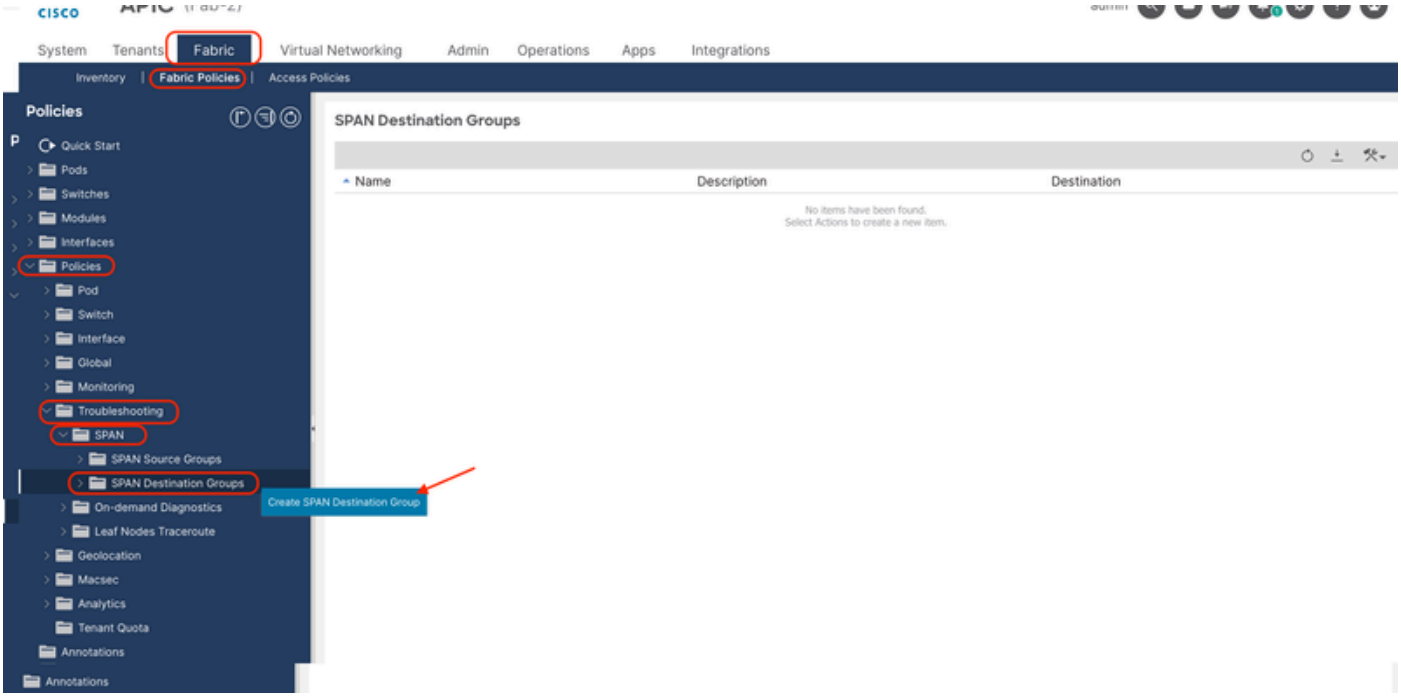

Imagen 23: Ruta para crear un grupo de destino ERSPAN de fabric

Rellene la información:

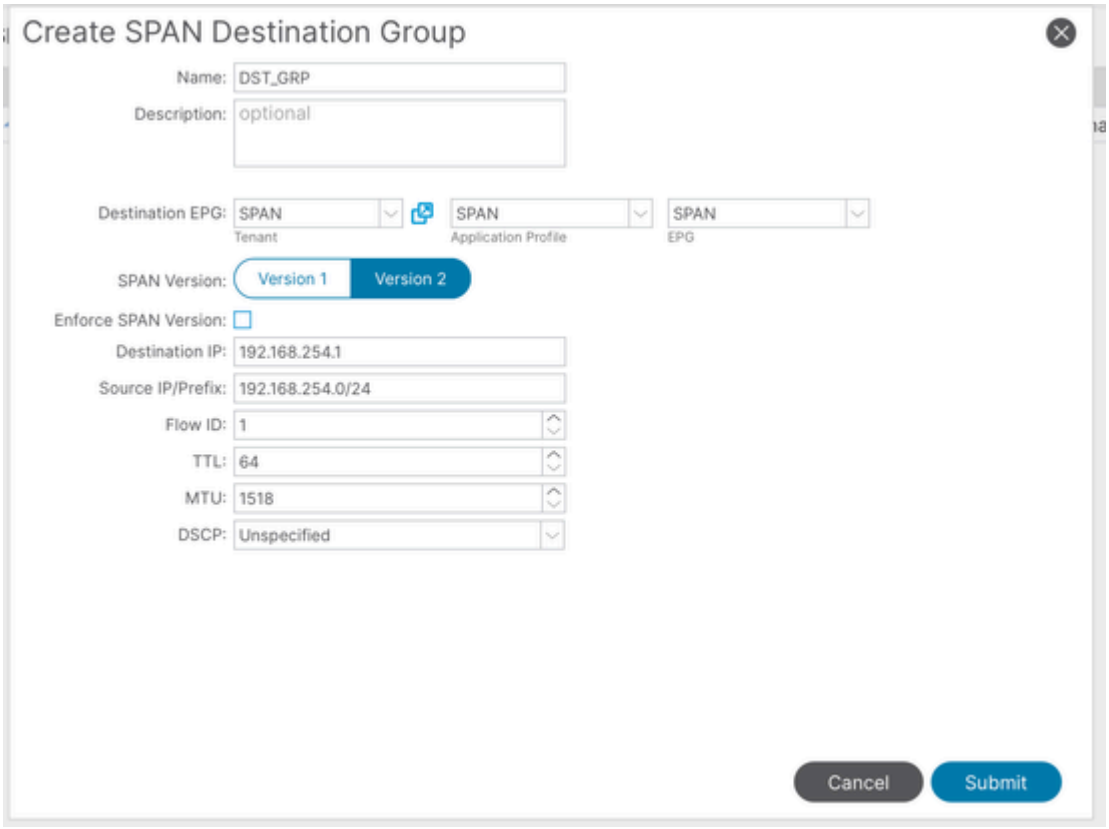

Imagen 24: Creación del grupo de destino ERSPAN de fabric

Where:

EPG de destino: configure el arrendatario, el AP y el EPG donde se aprende el terminal de destino

IP de destino: IP del punto final de destino

IP 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: 192.168.254.0/24 en node-101 => src IP 192.168.254.101

ID de flujo: De forma predeterminada, se establece en 1, lo que resulta útil para identificar el paquete por flujo en el encabezado ERSPAN. Utilice la sugerencia que se muestra en Access ERSPAN para filtrar capturas cuando se personaliza este ID de flujo.

- Create SPAN Source Group (SRC_GRP1), haga clic con el botón derecho en 'SPAN Source Groups' y seleccione 'Create SPAN Source groups':

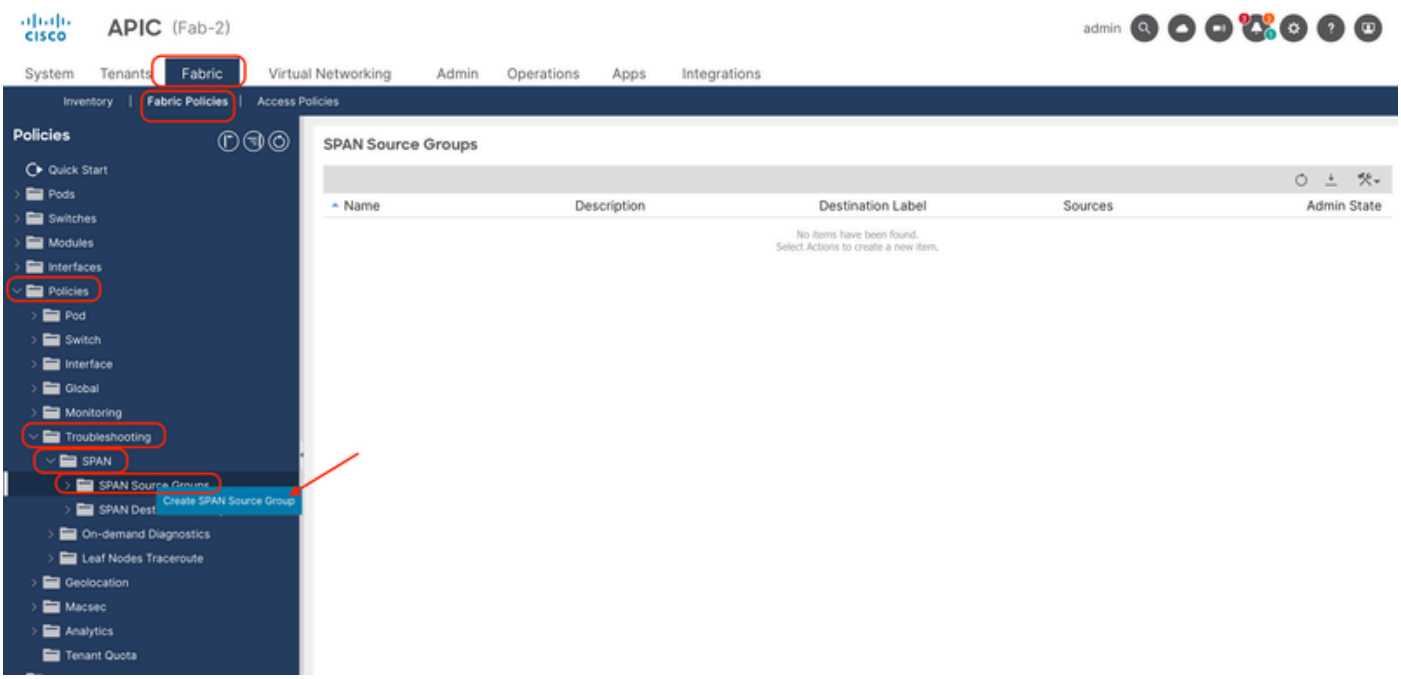

Imagen 25: ruta para crear grupos de origen de ERSPAN de fabric

Rellene la información:

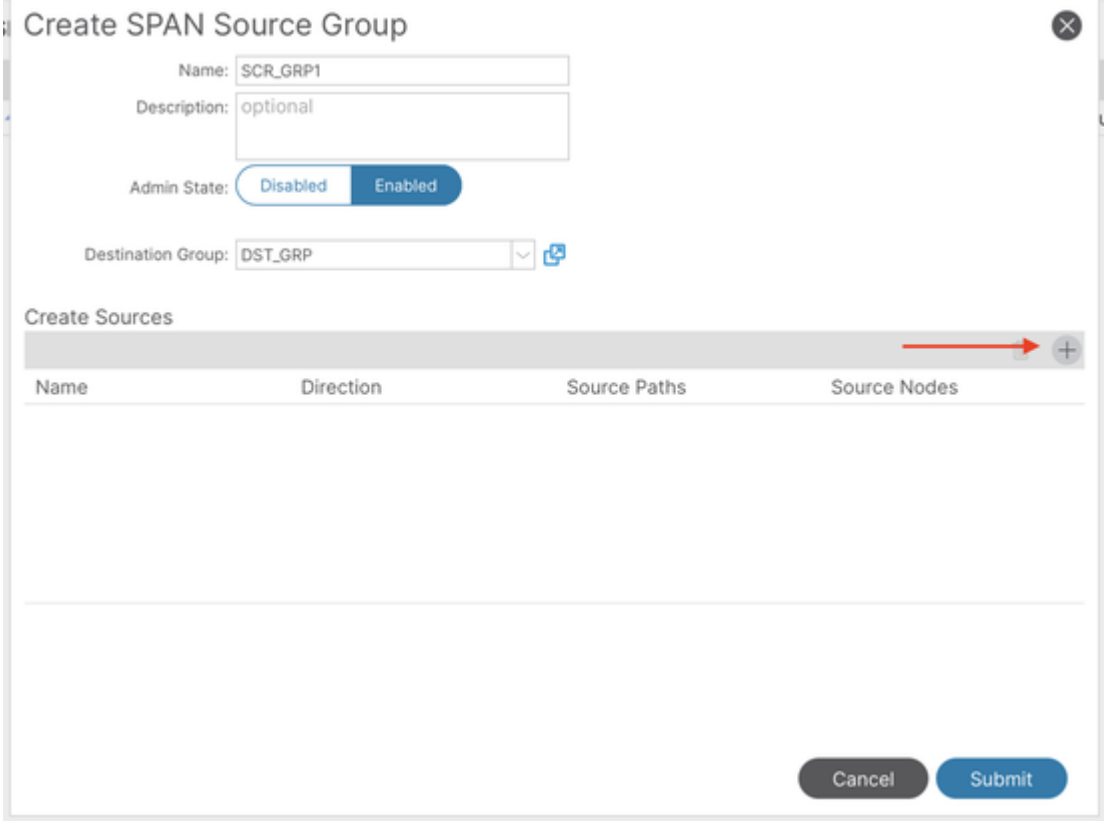

Imagen 26: Creación del grupo de origen ERSPAN de fabric

Where:

Estado del administrador: habilitado

Grupo de destino: Seleccione el grupo de destino creado anteriormente (DST_EPG)

- En este mismo cuadro, haga clic en el botón más (+) para agregar al menos en Origen.
- Configure estos parámetros para crear Source (SRC1):

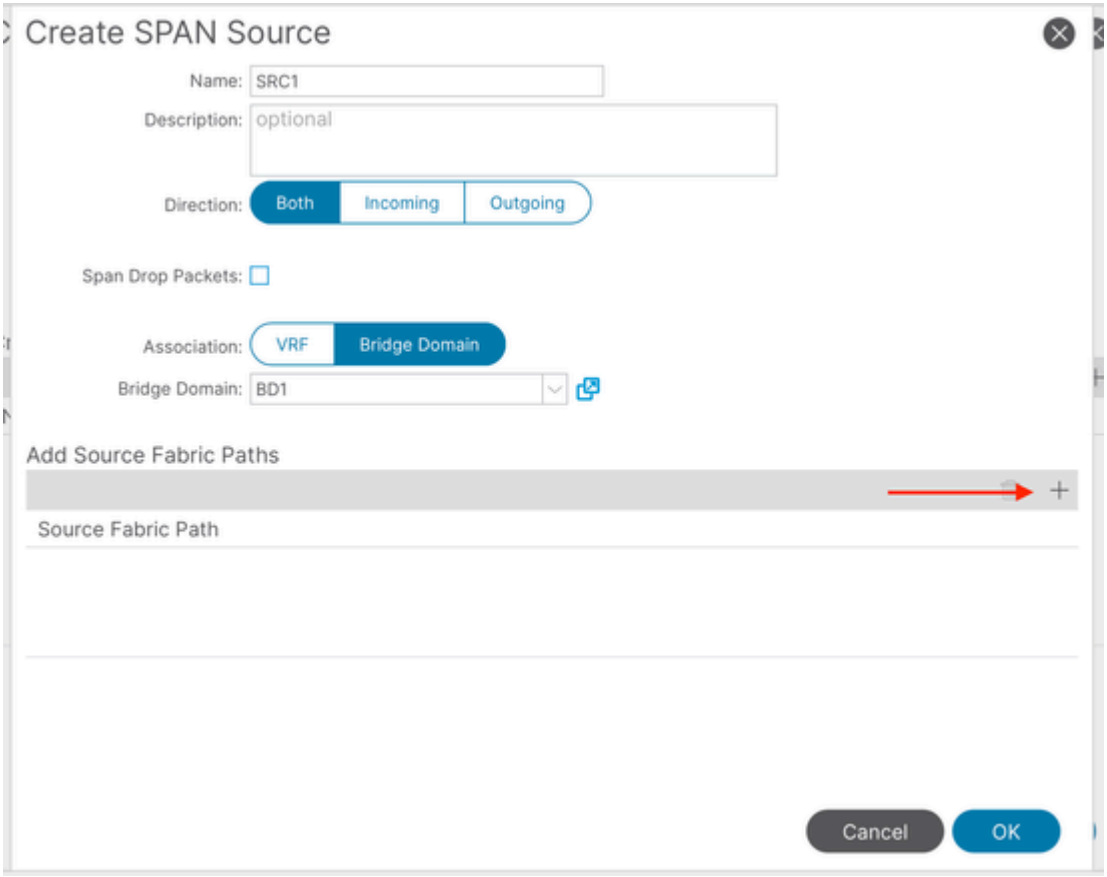

Imagen 27: creación de la ruta de fabric ERSPAN de arrendatario

Where:

Dirección: Elija entre entrante, saliente o ambas direcciones

Asociación: Elija entre VRF o Dominio de Bridge (en este ejemplo, se ha elegido un BD específico para capturar)

- Haga clic en el botón más (+) para agregar una ruta de fabric de origen. Rellene la información:

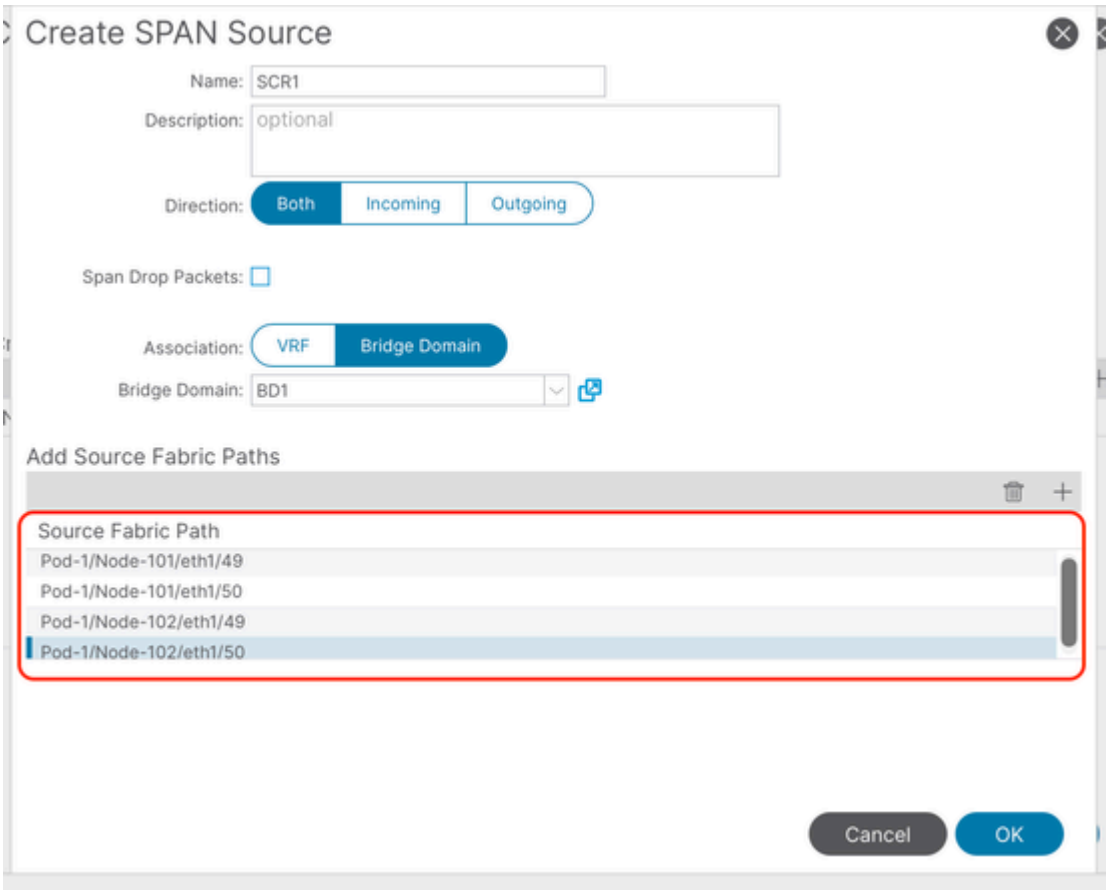

Imagen 28: Creación de rutas de origen para el fabric ERSPAN

Where:

Nodo: nodo de origen

Interfaz: El menú desplegable muestra solo los enlaces ascendentes del nodo seleccionado (en este ejemplo, se mostraron los 4 enlaces ascendentes de la topología ya agregada)

Extensión a CPU

Antes de ACI 6.2.1, los switches de hoja de ACI no admitían el envío de una sesión SPAN local (analizador de puerto conmutado) directamente al puerto de CPU del switch (`sup-eth0`), lo que dificultaba considerablemente la captura y el análisis integrados.

Topología de ejemplo

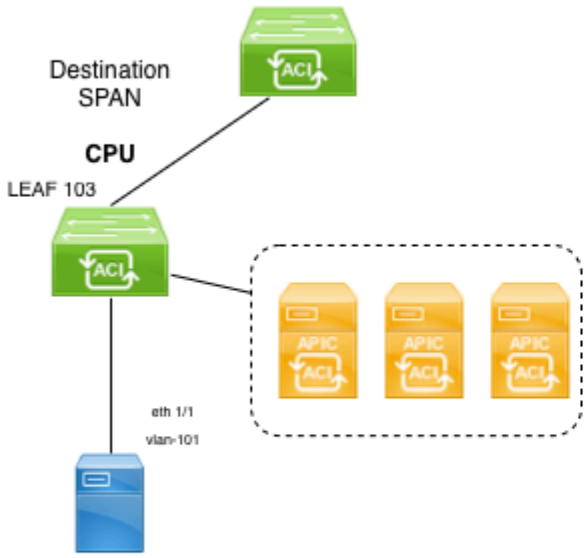

Imagen 29: Topología de ejemplo para SPAN a CPU

Ejemplo de configuración

Vaya a .Fabric > Access Policies > Policies > Troubleshooting > SPAN

- Haga clic con el botón derecho del ratón en 'SPAN Destination Groups' y seleccione la opción para crear SPAN Destination Group.

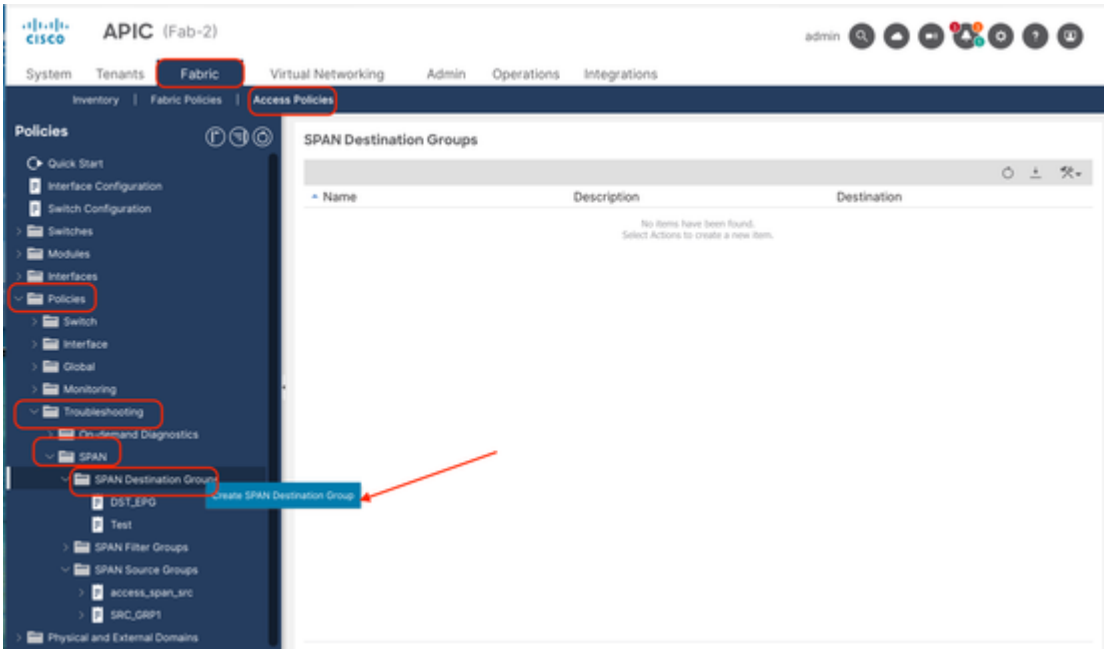

Imagen 30: Ruta para crear un SPAN para el grupo de destino CPU

Rellene la información:

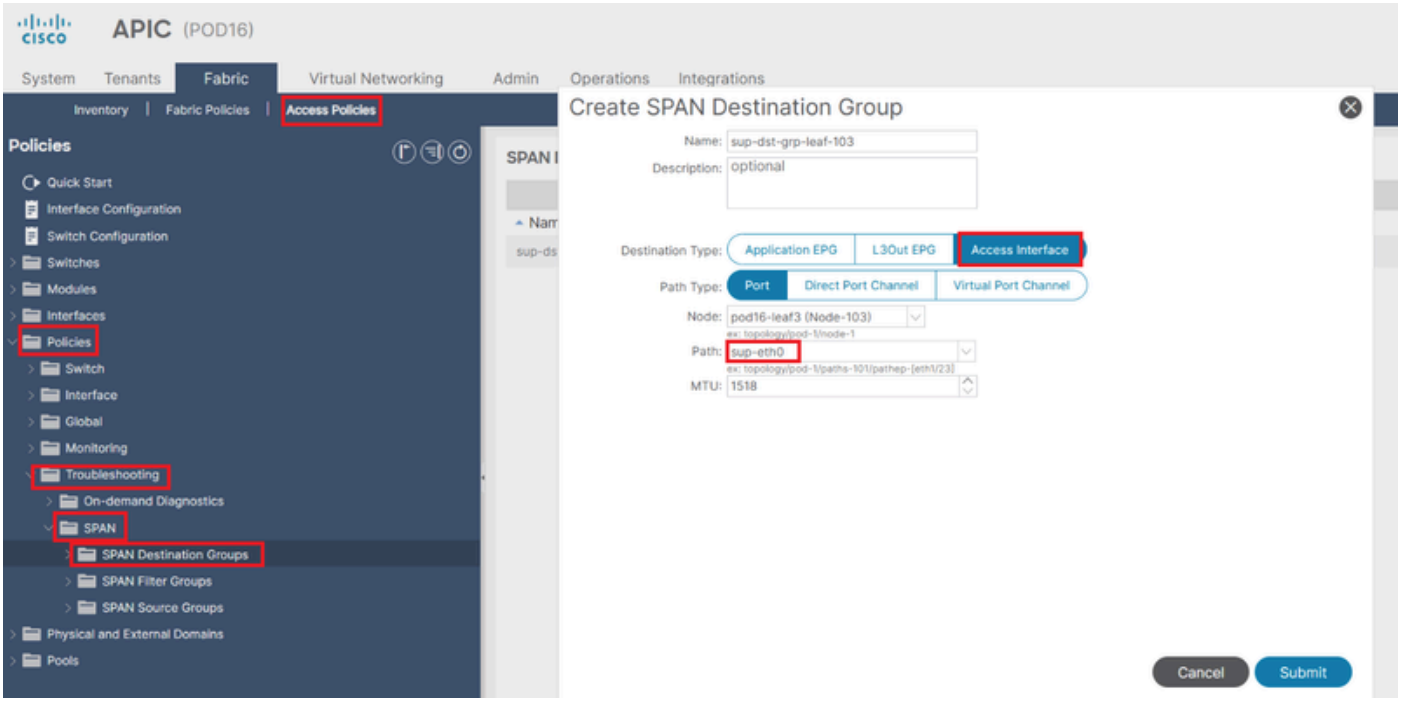

Imagen 31: creación de SPAN a grupo de destino de CPU

Where:

Tipo de destino: interfaz de acceso

Tipo de pieza: Puerto

Ruta: seleccione sup-eth0.

- Continúe con la configuración como se muestra en la sección Acceso al SPAN Local.

Los pasos de configuración también se muestran en este vídeo:

https://video.cisco.com/detail/video/6389779606112

Limitaciones:

SPAN a CPU sólo se admite en las siguientes plataformas:

- FX2 (CELESTIAL)
- FX3 (Sundown)
- GX (Wolfridge)
- GX2 (Cuadrápicos)
- HX (Ararat)

Filtros/ACL

El SPAN de acceso tiene la capacidad de utilizar filtros ACL en orígenes SPAN 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.

Un grupo de filtros se puede asociar a:

-Origen de extensión: el grupo de filtros se utiliza para filtrar el tráfico en TODAS las interfaces definidas en este origen de extensión.

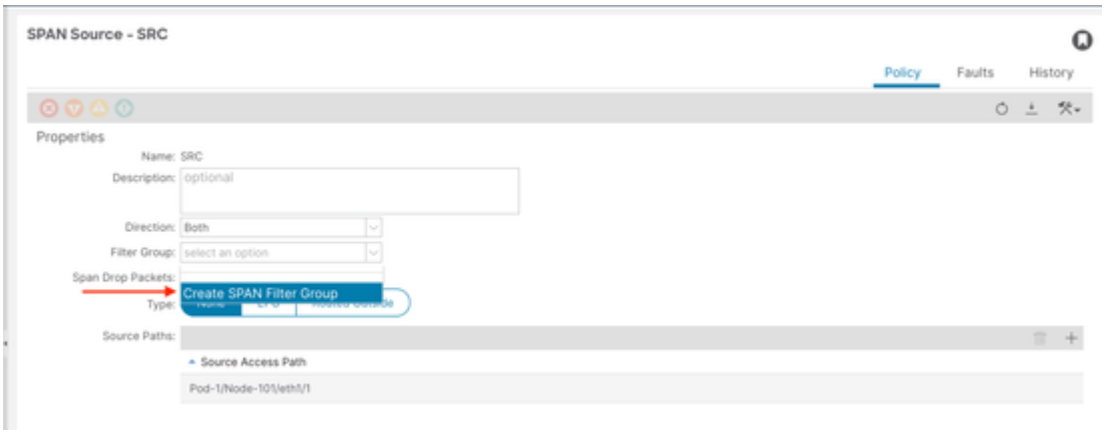

Imagen 32: Opción para agregar un filtro en el origen de acceso

-Grupo de origen de extensión: 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 expansión de este grupo de orígenes de expansión.

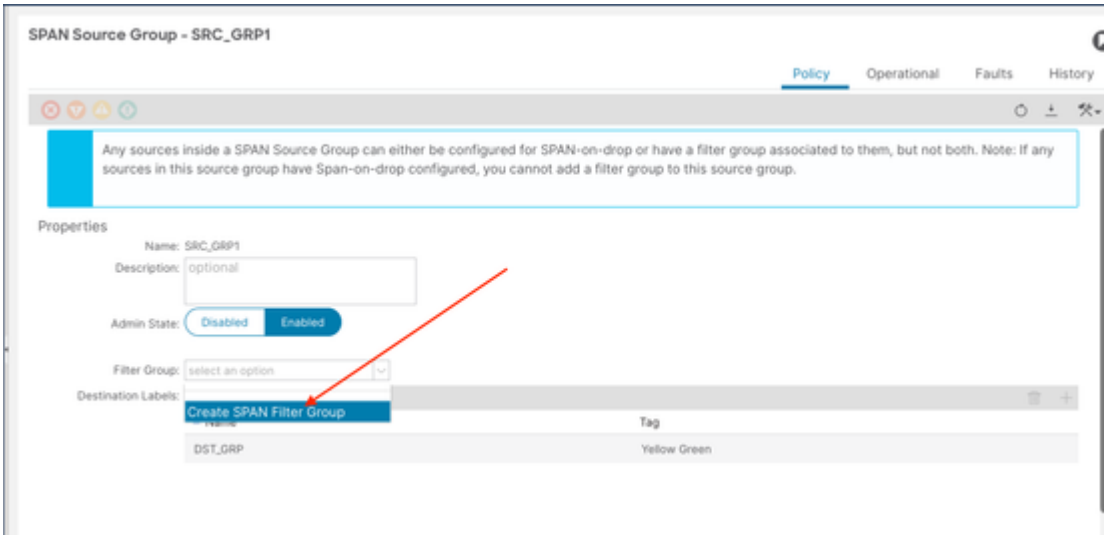

Imagen 3: Opción para agregar un filtro en el grupo de origen de acceso

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.

Para crear un filtro, están disponibles estas opciones:

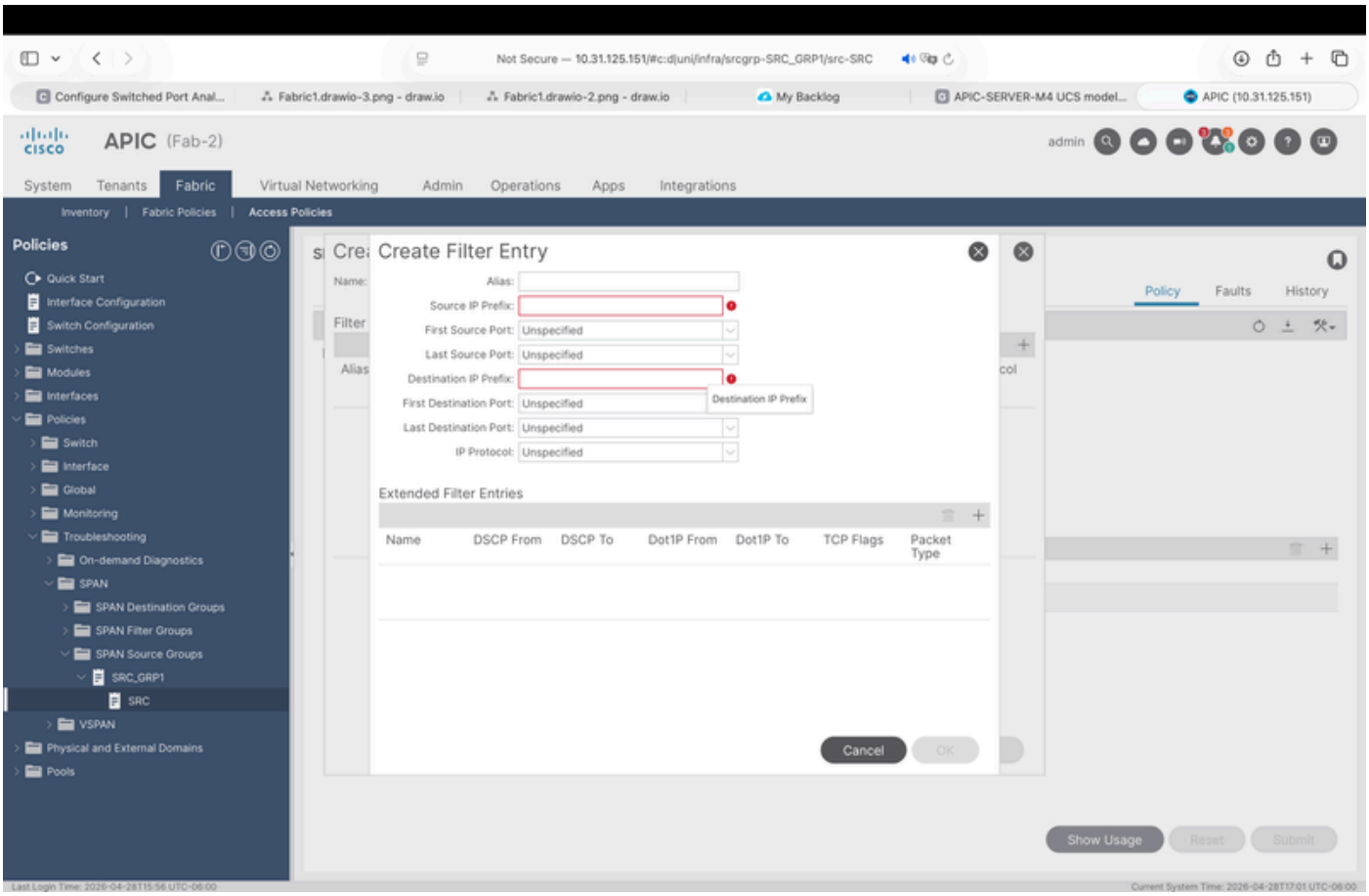

Imagen 34: opciones de entrada de filtro

- Prefijos de origen y destino.

- Rangos de puertos de origen/destino.

- Protocolo IP.

- Filtros extendidos como: Indicadores DCSP, Dot1P, TCP.

Validación

- En GUI, vaya al grupo de origen de interés, haga clic en él y vaya a la pestaña Operativo:

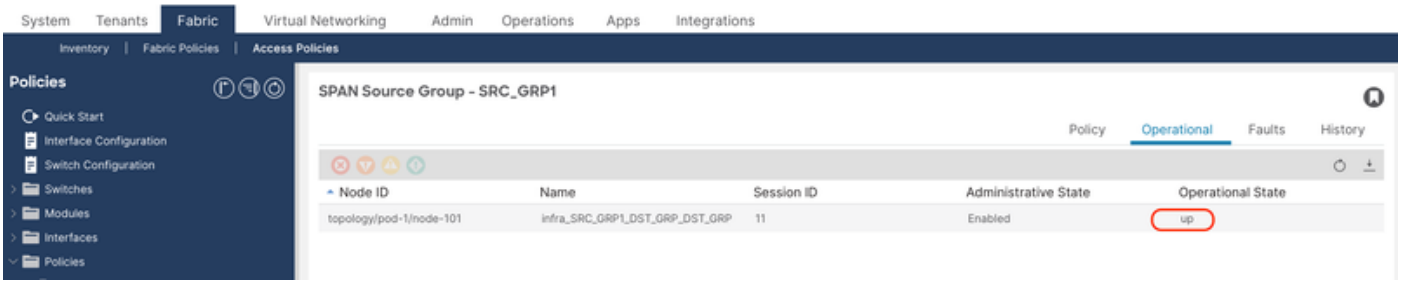

Imagen 35: Validación de sesión en GUI

- EN CLI APIC:

Muestra todas las SPAN/sesiones configuradas en el fabric

```
show monitor summary
```

Para filtrar sesiones por tipo:

```
show monitor access session all

show monitor tenant session all

show monitor fabric session all
```

- En el switch de origen CLI:

```
show monitor session all
```

Ejemplo:

```
SITE2-L101# show monitor session all
session 11
---------------
name : SRC_GRP1
description : Span session 11
type : erspan
scale-mode : filter
version : 2
oper version : 2
state : up (active)
erspan-id : 1
granularity :
```

```
vrf-name : SPAN:SPAN
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.  >>>> node ID 101
mode : access
Filter Group : None
source intf :
rx : [Eth1/1]
tx : [Eth1/1]
both : [Eth1/1]
source VLANs :
rx :
tx :
both :
filter VLANs : filter not specified
filter L3Outs : filter not specified
```

Esta salida es útil para confirmar si la sesión está habilitada, así como el origen, los encabezados de destino y las interfaces de origen (si se enumera en rx y tx, la dirección se estableció en ambos)
Para confirmar que esto está configurado correctamente, tome el ID de sesión de span de la descripción y ejecute el siguiente comando:

Ejemplo:

```
SITE2-L101# show system internal span-mgr session 11

SSN id 11 name "infra_SRC_GRP1_DST_GRP_DST_GRP" ptr 0x562a21a24b70 Admin UP nSrcsUP 1 Dst ERSPAN UP
         Scale mode FILTER
         vrfName SPAN:SPAN vnid 2752515 SrcIP 192.168.254.101/24 DstIP 192.168.254.1/32 flowId 1 ttl 64
         vrf_id 5 table_id 0x5 vrf_vnid 2752515 (0x2a0003) slot 0 urib_nh_reg 1 epm_registered 1
         Spine Proxy NH: RESOLVED nh_is_fabric 1 nh_dtep_ip 0xa00e042 nh_flag 1 nh_if_idx 0x1a031009 nh
         Local NH: NOT Resolved ep_valid 0 ep_mac 00:00:00:00:00:00 ep_vlan 0 ep_if_idx 0x0
                   ep_flags 0 ep_tun_if_idx 0x0 ep_nh_mac 00:00:00:00:00:00 ep_nh_dtep_ip 0x0 ep_nh_ifid
         COOP NH: NOT Resolved coop_valid 0 coop_tep_ip 0x0
         Span Offset 255
         Filter Group ID: 0
         (src-name, flt-grp-id) associations:
         Src name: "SRC" Filter Group ID: 0
                SRC: id 17 ptr 0x562a21a22170 ssn_id 11 mode Access type Port dir ING-EGR vlan 0 if_idx
                    vlan_type INVALID hw_vlan 0 hw_vlan_up DOWN if_up UP is_fex 0 is_pc 0 slot -1 pc_mb
Per SSN Summary: SSN 11 n_srcs_per_ssn 1 srcs UP 1

Summary: nSSNs: 1 nSSNs UP: 1 nSrcs 1 nSrcs UP 1
```

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)

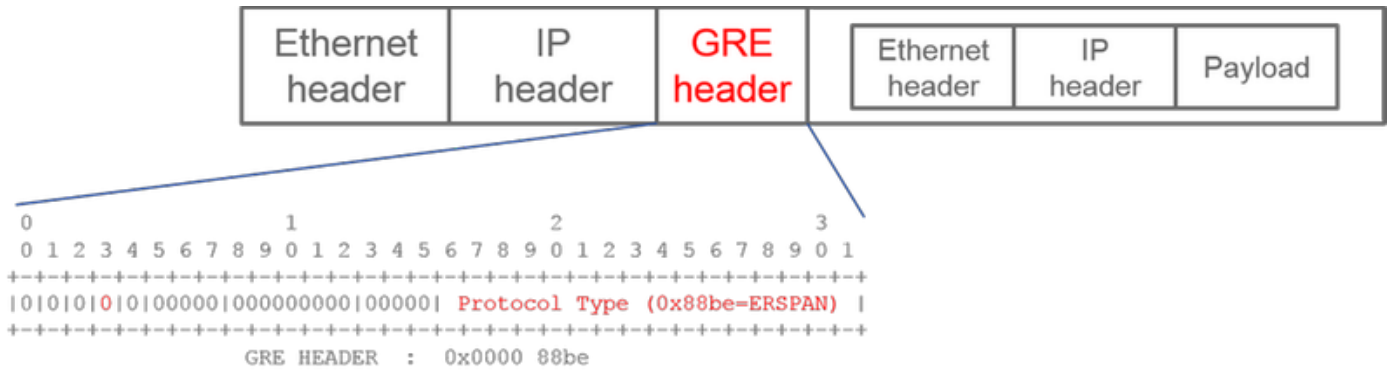

Imagen 36: Encabezado GRE para ERSPAN versión I

Para proporcionar un ejemplo, wireshark muestra este tipo de protocolo:

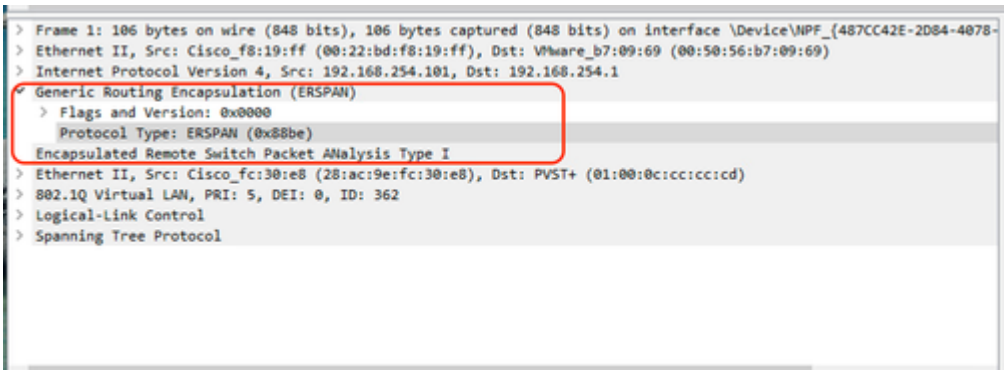

Imagen 37: validación de versión en wireshark

El tipo I no utiliza el campo de secuencia del encabezado GRE. Ni siquiera utiliza el encabezado ERSPAN que debe suceder 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

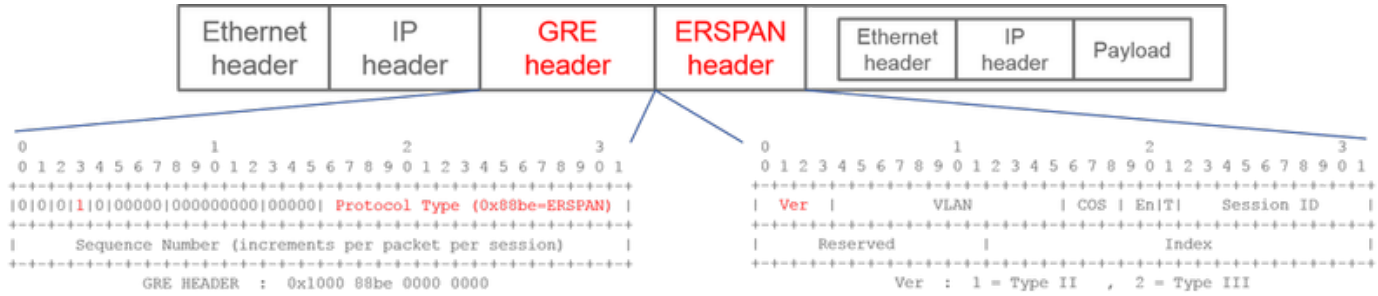

Imagen 38: Encabezado GRE para ERSPAN versión II

El ejemplo de Wireshark es:

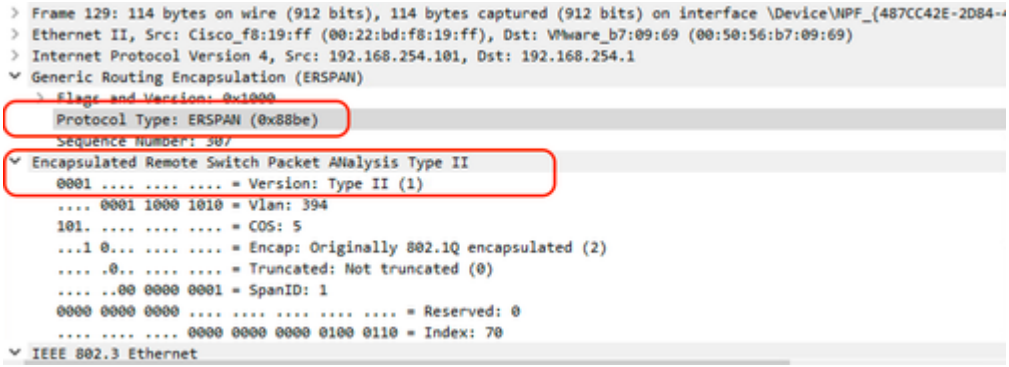

Imagen 39: validación de versión en wireshark

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 30/04/2026.

Tipo de ERSPAN y tipo de ACI SPAN

En los nodos de columna y de hojas de primera generación, cada SPAN de ACI (fabric, acceso y arrendatario) funciona en chips diferentes en cada nodo.

- El SPAN de acceso y el SPAN de arrendatario se utilizan en el chip Broadcom (T2:Trident2) en hoja
- El Fabric SPAN funciona con el chip NS (NorthStar) en Leaf o con el chip ALP (Alpine) en Spine.

Por lo tanto, debido a las limitaciones del chip Broadcom,

- SPAN de acceso y SPAN de arrendatario utilizan ERSPAN tipo I

Por otro lado, los chips NS y ALP soportan el tipo II. Por lo tanto,

- Fabric SPAN utiliza ERSPAN tipo II

En los nodos de segunda generación o posteriores, todos los SPAN de ACI utilizan ERSPAN de tipo II de forma predeterminada.

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.

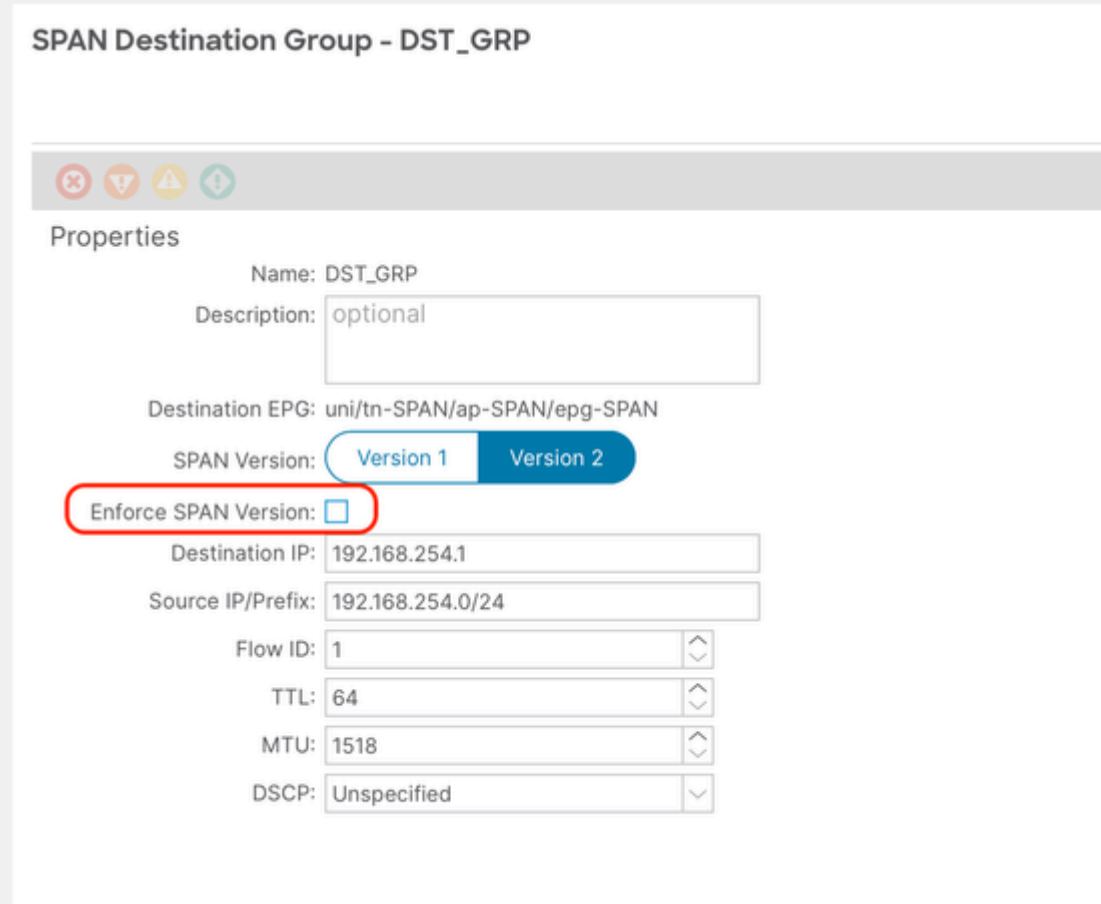

Imagen 40: Opción para aplicar la versión de SPAN

- Versión de SPAN (Versión 1 o Versión 2): Se refiere al ERSPAN de tipo I o II
- Aplicar versión de SPAN (activado o desactivado): Esto decide si la sesión SPAN debe fallar en caso de que el tipo 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	Aplicar versión	nodo de origen de 1ª generación	Nodo de origen de 2ª generación

de SPAN	de SPAN		
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

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. Vaya a .Edit > Preferences > Protocols > VxLAN
3. Agregue el puerto 48879 al final de los puertos:
4. Y luego Apply.

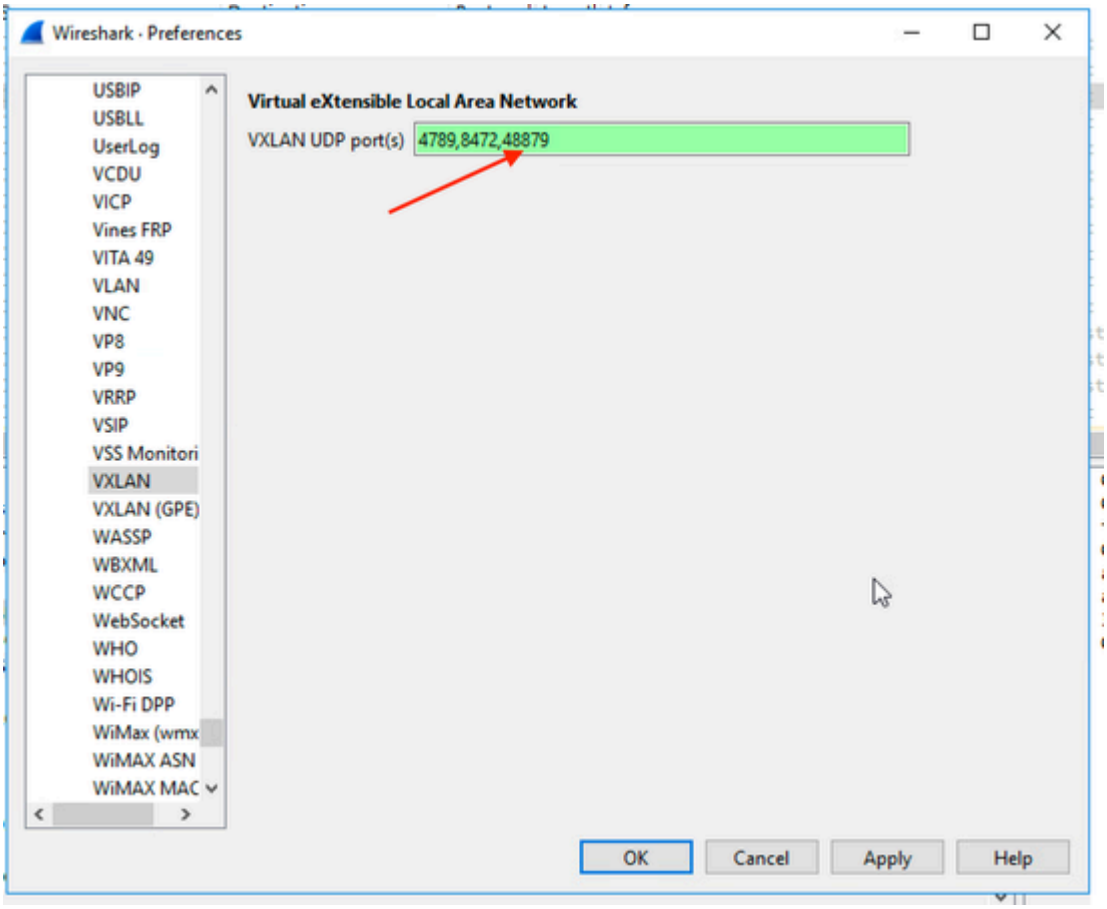

Imagen 41: Cómo agregar un puerto personalizado para decodificar el encabezado iVXLAN

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

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).