Guide ACI SPAN

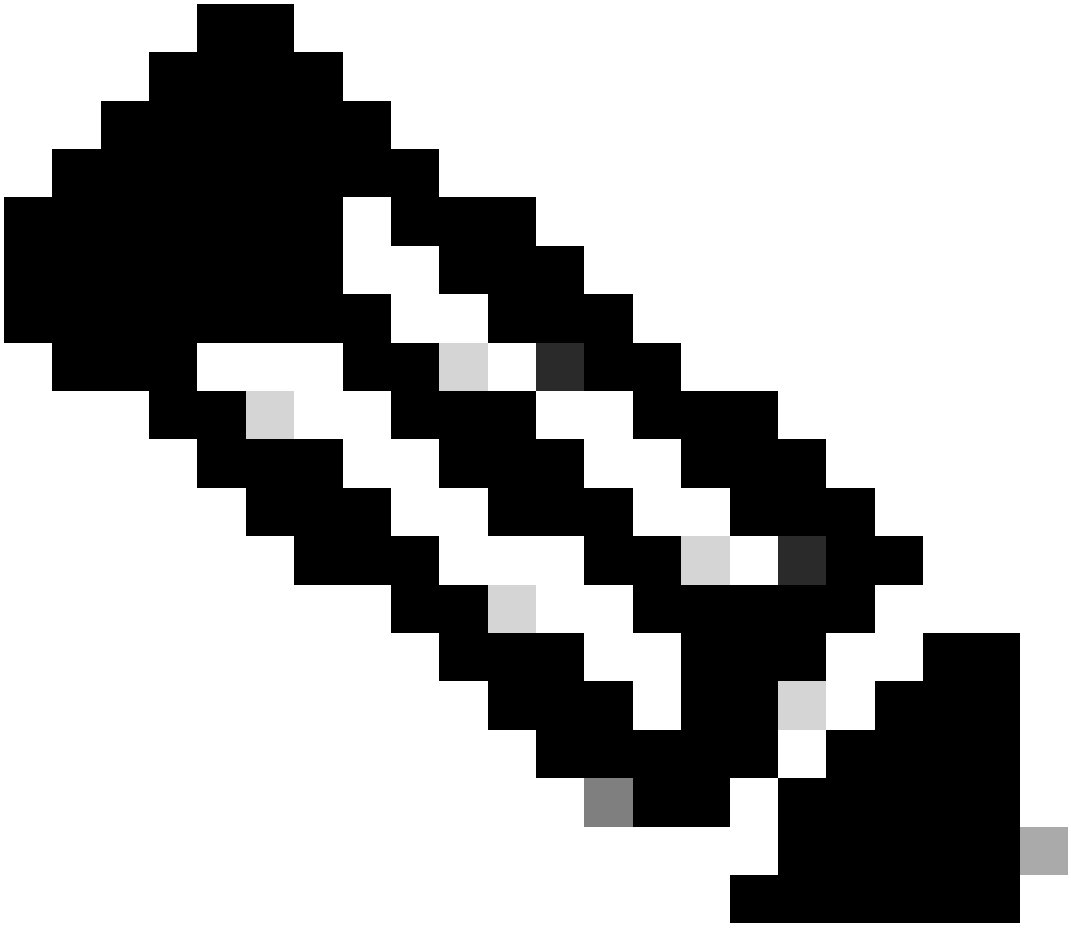
Table des matières

Introduction

Ce document décrit comment configurer l'analyseur de port commuté (SPAN) sur l'infrastructure axée sur les applications (ACI) de Cisco.

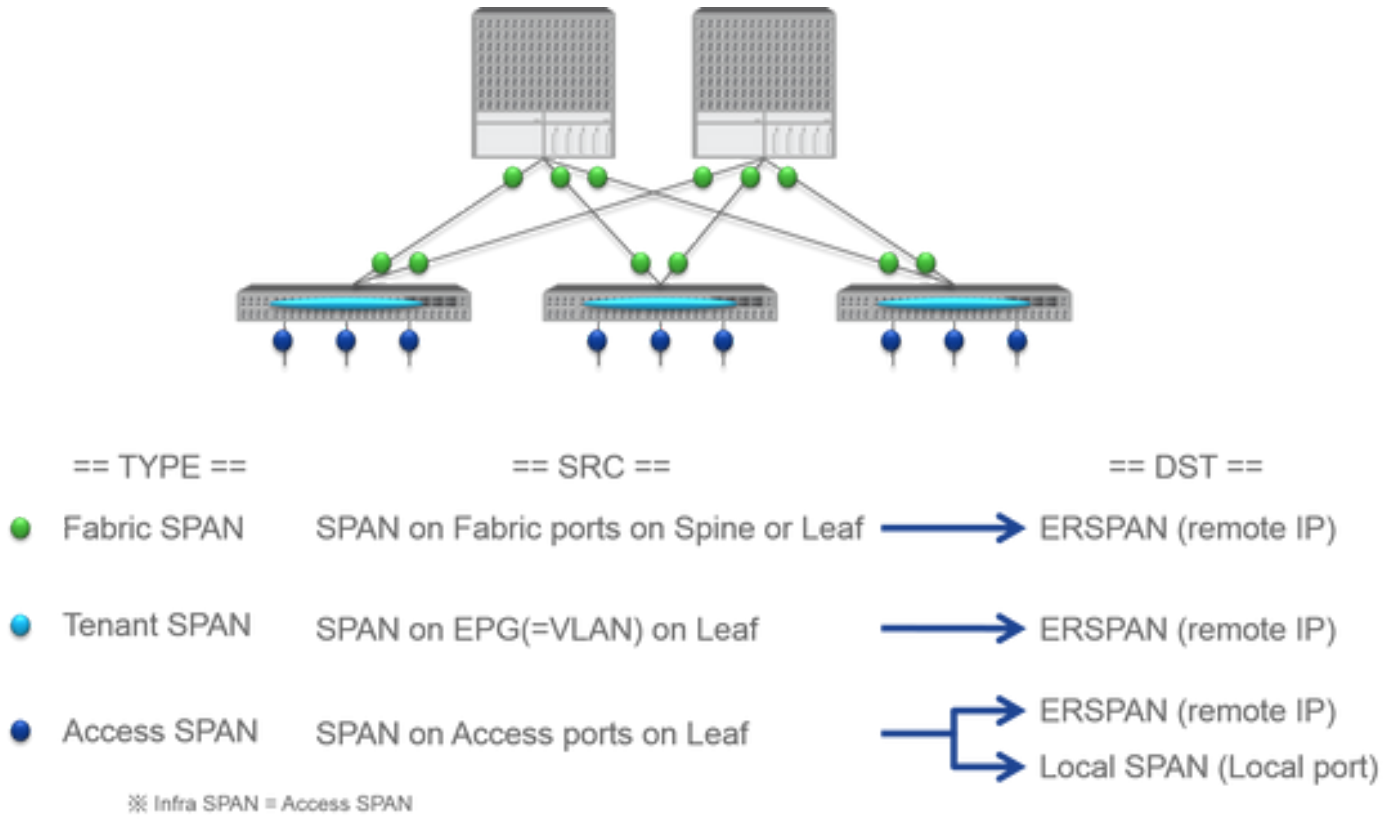
Informations générales

En général, il existe trois types de SPAN. Local SPAN, Remote SPAN (RSPAN) et Encapsulated Remote SPAN (ERSPAN). Les différences entre ces SPAN sont principalement la destination des paquets de copie. L'ACI Cisco prend en charge les fonctionnalités SPAN et ERSPAN locales.



Remarque : ce document suppose que les lecteurs connaissent déjà la fonctionnalité SPAN en général, notamment les différences entre les fonctionnalités Local SPAN et ERSPAN.

Type SPAN dans l'ACI Cisco



L'ACI Cisco propose trois types de SPAN : Fabric SPAN, Tenant SPAN et Access SPAN. La différence entre chaque SPAN est la source des paquets de copie.

Comme mentionné précédemment,

- **Fabric SPAN** est de capturer les paquets qui entrent et sortent de **interfaces between Leaf and Spine switches**.
    - Access SPAN est de capturer les paquets qui entrent et sortent de interfaces between Leaf switches and external devices.
    - Tenant SPAN est de capturer les paquets qui entrent et sortent de EndPoint Group (EPG) on ACI Leaf switches.

Ce nom SPAN correspond à l'emplacement à configurer sur l'interface utilisateur graphique de l'ACI Cisco.

- La fonctionnalité SPAN du fabric est configurée sous Fabric > Fabric Policies
    - Access SPAN est configuré sous Fabric > Access Policies

- La fonctionnalité SPAN du locataire est configurée sous Tenants > {each tenant}

En ce qui concerne la destination de chaque SPAN, seul Access SPAN est capable des deux Local SPAN et ERSPAN. Les deux autres SPAN (Fabric et Tenant) sont uniquement capables de ERSPAN.

Limites et lignes directrices

Veuillez consulter le Guide de dépannage Cisco APIC Limitations & Guidelines. Il est mentionné dans la Troubleshooting Tools and Methodology > Using SPAN.

Configuration

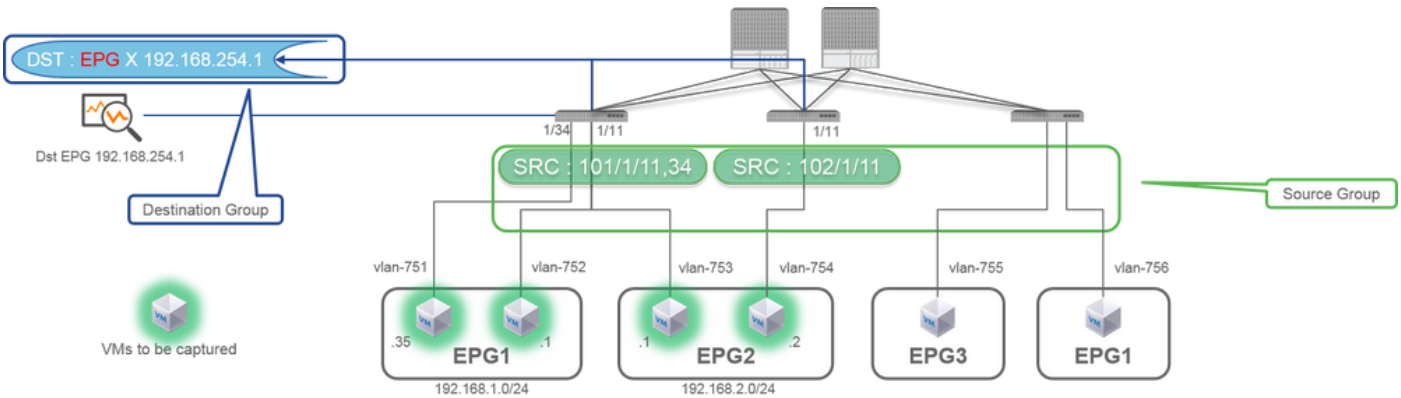
Cette section présente de brefs exemples relatifs à la configuration de chaque type de SPAN. Il existe des exemples spécifiques de sélection du type d'étendue dans la section suivante.

La configuration de la fonctionnalité SPAN est également décrite dans le Guide de dépannage du contrôleur APIC Cisco : Outils et méthodologie de dépannage > Utilisation de la fonctionnalité SPAN.

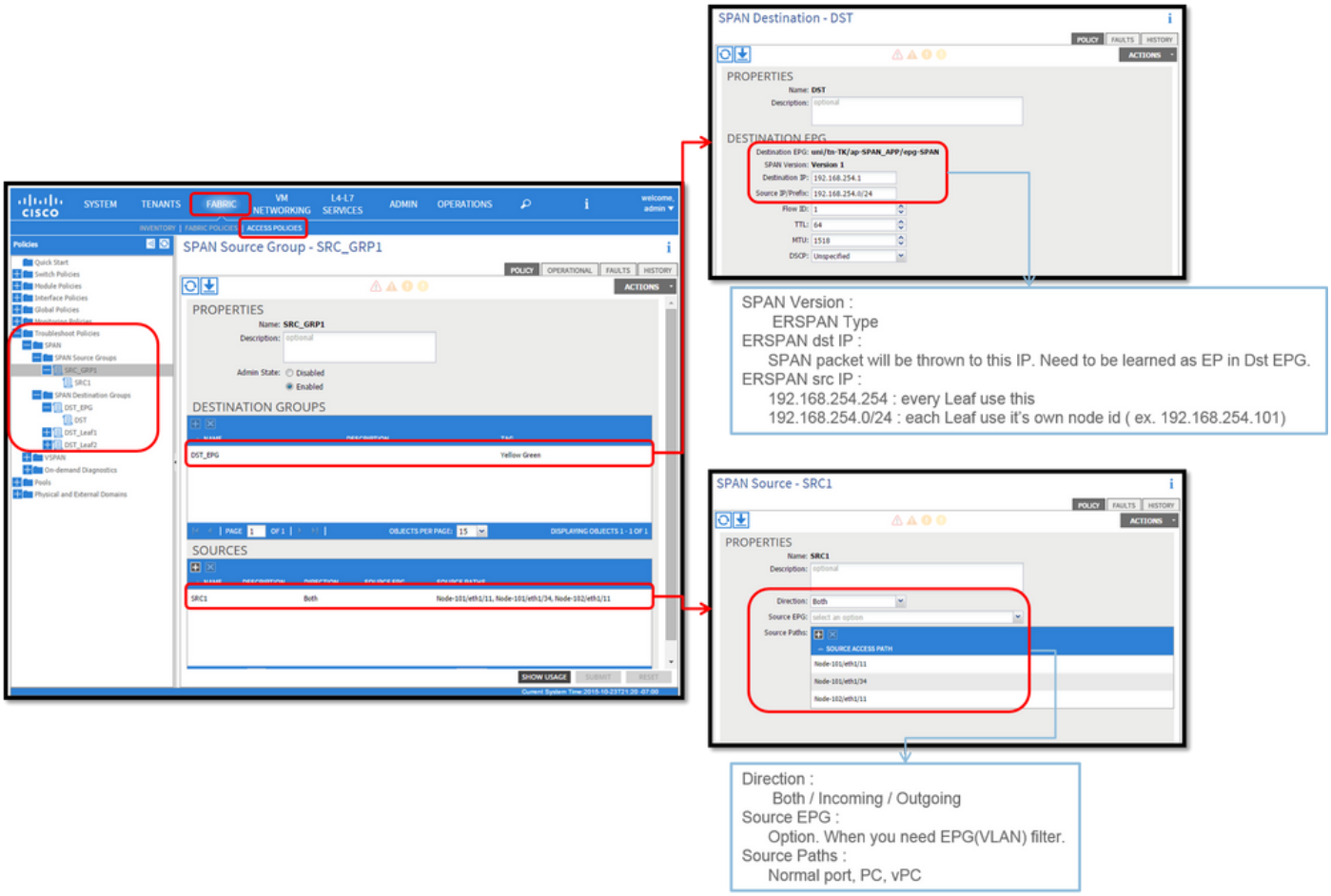
L'interface utilisateur peut être différente des versions actuelles, mais l'approche de la configuration est la même.

SPAN d'accès (ERSPAN)

Exemple de topologie



Exemple de configuration



Where:

Accédez à FABRIC > ACCESS POLICIES > Troubleshoot Policies > SPAN.

- SPAN Source Groups
    - SPAN Destination Groups

SPAN Source Group liens Destination et Sources.

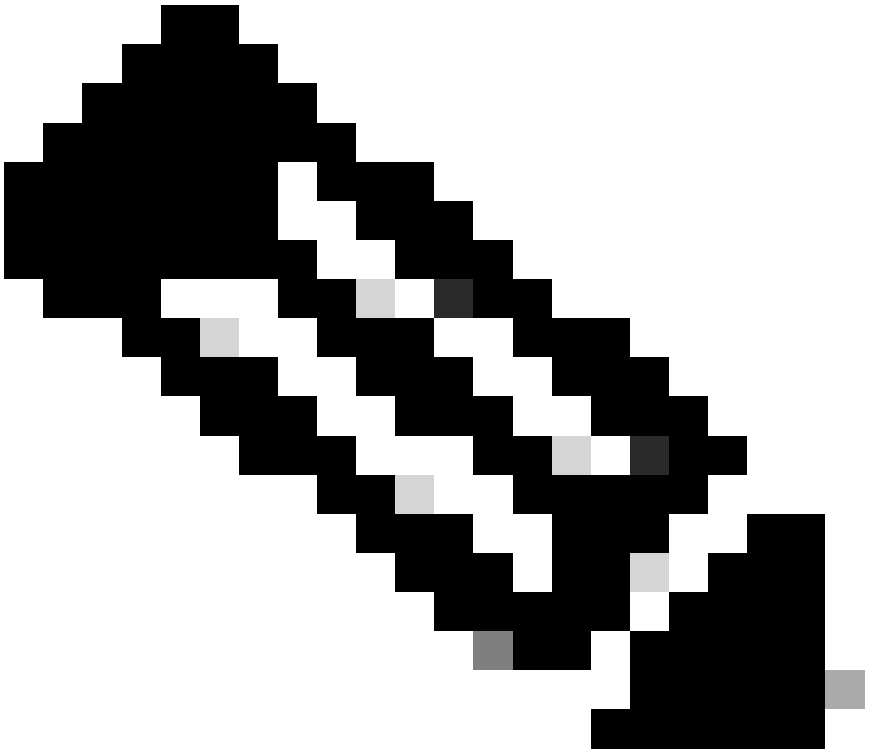
Comment :

1. Créer (SPAN Source GroupSRC_GRP1).

- Créez SPAN Source (SRC1) sous SPAN Source Group (SRC_GRP1).

- Configurez ces paramètres pour SPAN Source (SRC1).

- Direction - EPG source (option)
- Chemins source (il peut s'agir de plusieurs interfaces)



Remarque : veuillez vous reporter à l'image pour plus de détails sur chaque paramètre.

- Créer (SPAN Destination GroupDST_EPG).

- Créer (SPAN DestinationDST).

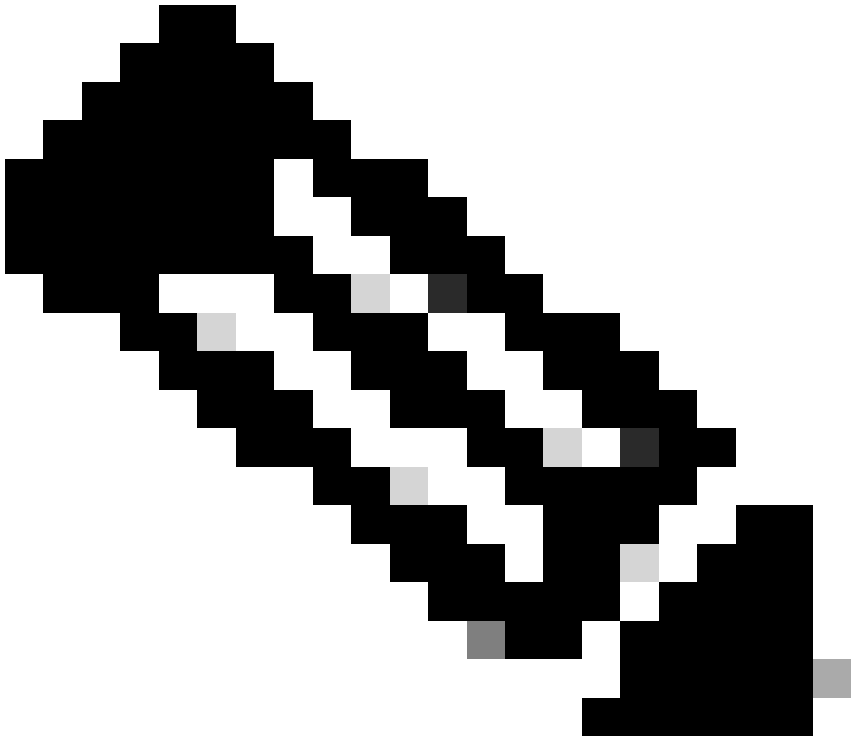
- Configurez ces paramètres pour SPAN Destination (DST)

- EPG de destination

-Adresse IP de destination

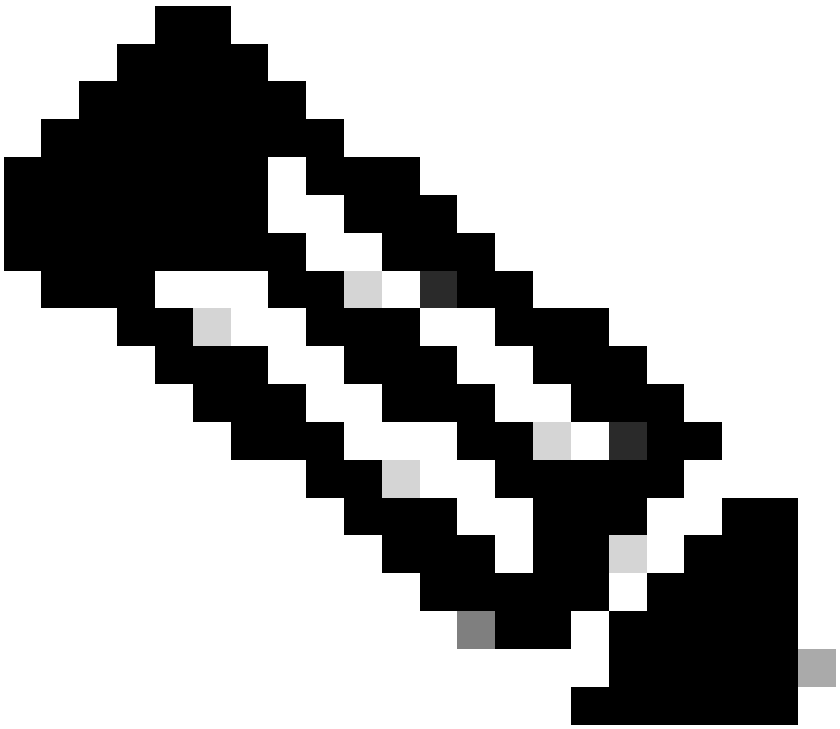
- Adresse IP/préfixe source (il peut s'agir de n'importe quelle adresse IP. Si le préfixe est utilisé, node-id du noeud source est utilisé pour les bits non définis. Par exemple, préfixe : 1.0.0.0/8 sur node-101 => src (IP 1.0.0.101)

- D'autres paramètres peuvent être laissés par défaut



Remarque : veuillez vous reporter à l'image pour plus de détails sur chaque paramètre.

- Assurez-vous que le SPAN Destination Group est lié à un SPAN Source Group approprié.
- Assurez-vous Admin Stateque est activé.

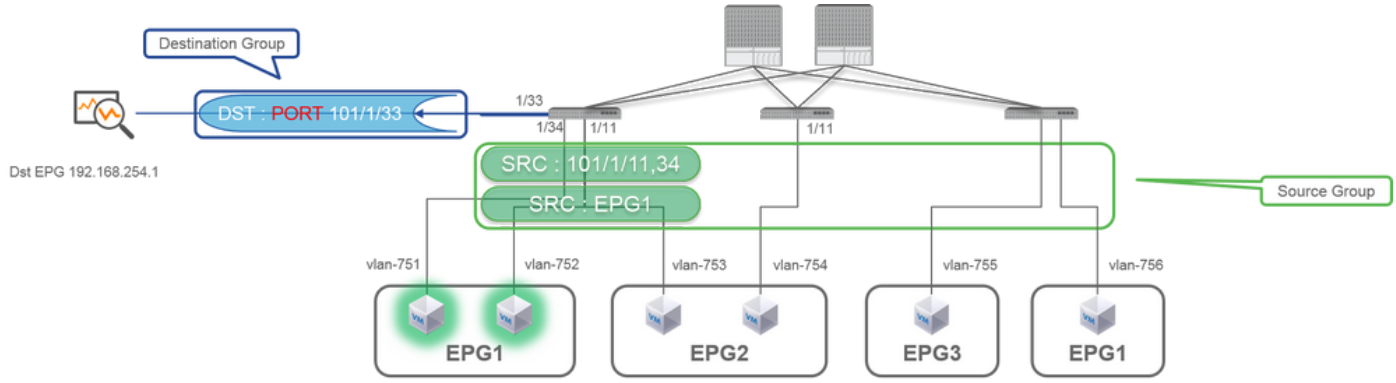


Remarque : la fonctionnalité SPAN s'arrête lorsque vous sélectionnez Disabled (Désactivé) dans cet état Admin. Il n'est pas nécessaire de supprimer toutes les stratégies si vous les réutilisez ultérieurement.

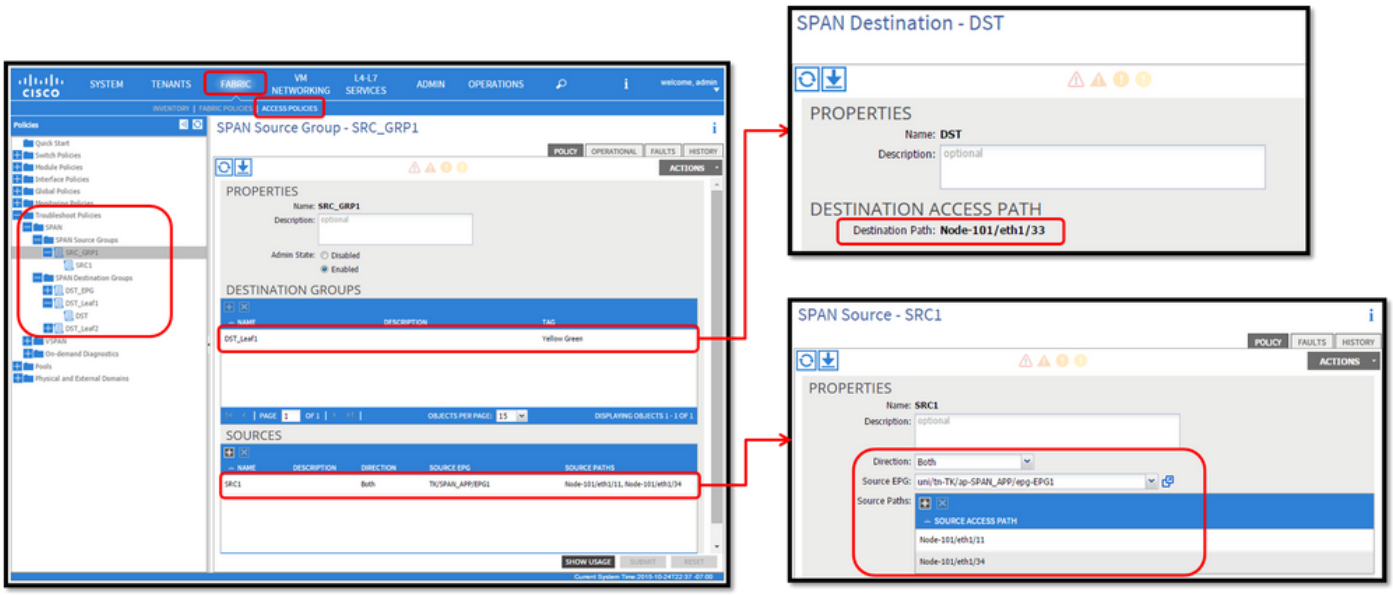
Assurez-vous également que l'adresse IP de destination pour ERSPAN est apprise en tant que point de terminaison sous l'EPG de destination spécifié. Dans l'exemple mentionné précédemment, 192.168.254.1 doit être appris sous Tenant TK > Application profile SPAN_APP > EPG SPAN. Ou l'adresse IP de destination peut être configurée comme un point d'extrémité statique sous cet EPG si le périphérique de destination est un hôte silencieux.

Accès SPAN (local)

Exemple de topologie



Exemple de configuration



- Where:

Fabric > ACCESS POLICIES > Troubleshoot Policies > SPAN

- SPAN Source Groups

- SPAN Destination Groups

SPAN Source Group liens Destination et Sources.

- Comment :

1. Créer SPAN Source Group (SRC_GRP1)

   - Créer (SPAN SourceSRC1) sous SPAN Source Group (SRC_GRP1)

   - Configurez ces paramètres pour SPAN Source (SRC1)
   -Direction
   - EPG source (option)
   - Chemins source (il peut s'agir de plusieurs interfaces)
   ※ veuillez vous reporter à l'image pour plus de détails sur chaque paramètre.

   - Créer (SPAN Destination GroupDST_Leaf1)

   - Créer (SPAN DestinationDST)

   - Configurez ces paramètres pour SPAN Destination (DST)
   - Interface et noeud de destination.

   - Assurez-vous que le SPAN Destination Group est lié à un SPAN Source Group approprié.

   -

   Assurez-vous que Admin State est activé.
   ※ La fonctionnalité SPAN s'arrête lorsque vous sélectionnez Désactivé dans cet état Admin. Il n'est pas nécessaire de supprimer toutes les stratégies si vous les réutilisez ultérieurement.

L'interface de destination ne nécessite aucune configuration par les groupes de stratégies d'interface. Il fonctionne lorsque vous branchez un câble sur l'interface de l'ACI Leaf.

Limites:

- Pour la fonctionnalité SPAN locale, une interface de destination et des interfaces source doivent être configurées sur le même leaf.

- L'interface de destination ne nécessite pas qu'elle soit sur un EPG tant qu'elle est UP.

- Lorsque l'interface vPC (Virtual Port-Channel) est spécifiée comme port source, la fonctionnalité SPAN locale ne peut pas être utilisée Cependant, il existe une solution de contournement. Sur un leaf de première génération, un port physique individuel membre de vPC ou PC peut être configuré comme source SPAN. Avec cette fonctionnalité, la fonctionnalité SPAN locale peut être utilisée pour le trafic sur les ports vPC.
  Cette option n'est toutefois pas disponible sur un leaf de deuxième génération (CSCvc11053). Au lieu de cela, la prise en charge de la fonctionnalité SPAN sur le « PC de composant VPC » a été ajoutée viaCSCvc44643 dans les versions 2.1(2e), 2.2(2e) et ultérieures. Avec cela, n'importe quel leaf de génération peut configurer un canal de port, qui est un membre de vPC, comme source SPAN. Cela permet à n'importe quel leaf de génération d'utiliser la fonctionnalité SPAN locale pour le trafic sur les ports vPC.

- Si vous spécifiez les ports individuels d'un canal de port sur des feuilles de deuxième génération, seul un sous-ensemble des paquets sera étendu (également en raison de CSCvc11053).

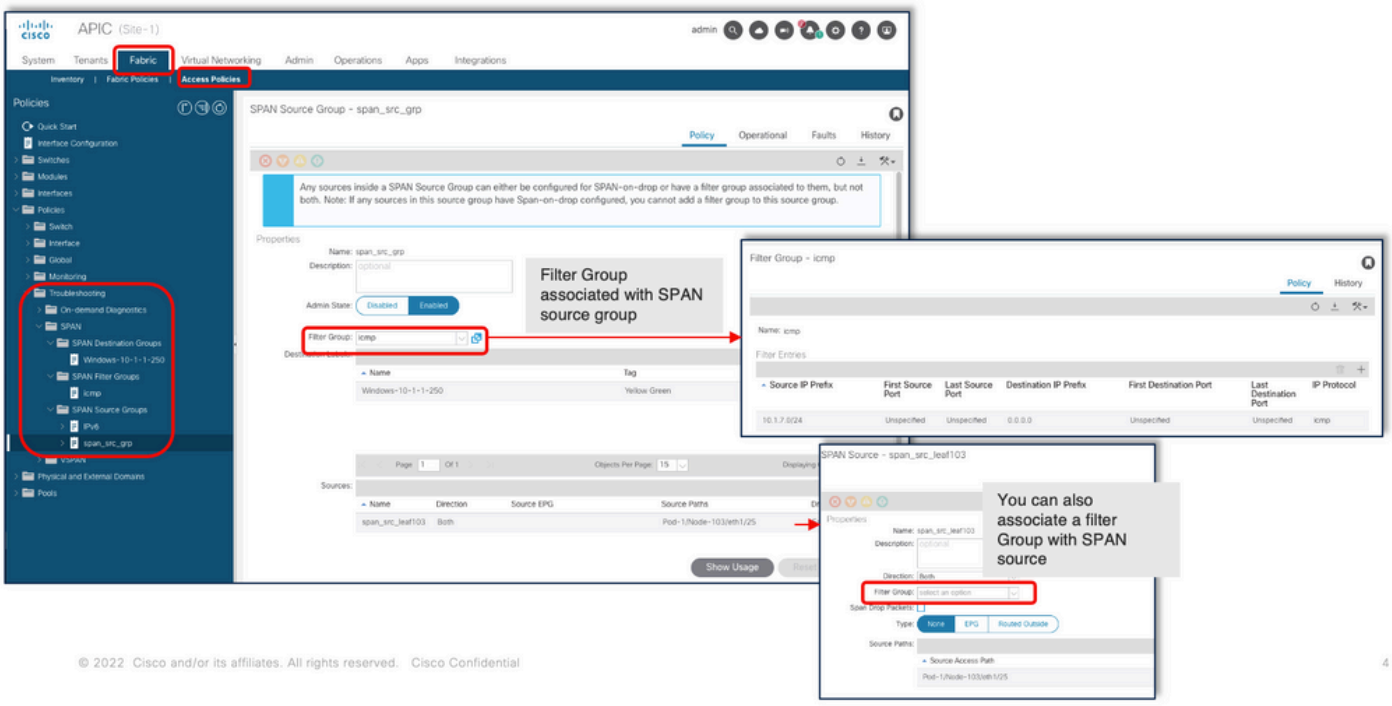
- PC et vPC ne peuvent pas être utilisés comme port de destination pour la fonctionnalité SPAN locale. À partir de la version 4.1(1), le PC peut être utilisé comme port de destination pour la fonctionnalité SPAN locale.

SPAN d'accès - Avec filtres ACL

Vous pouvez utiliser des filtres ACL sur les sources d'étendue d'accès. Cette fonctionnalité permet d'effectuer une analyse SPAN d'un flux particulier ou d'un flux de trafic entrant/sortant d'une source SPAN.
Les utilisateurs peuvent appliquer la ou les listes de contrôle d'accès SPAN à une source lorsqu'il est nécessaire de faire circuler le trafic spécifique de la fonctionnalité SPAN.
Il n'est pas pris en charge dans les groupes/sources source Fabric SPAN et Tenant Span.
Vous devez être prudent lorsque vous ajoutez des entrées de filtre dans un groupe de filtres, car il peut ajouter des entrées tcam pour chaque source qui utilise actuellement le groupe de filtres.

Un groupe de filtres peut être associé à :
-Span Source : le groupe de filtres est utilisé pour filtrer le trafic sur TOUTES les interfaces définies sous ce Span Source.
-Span Source Group : le groupe de filtres (par exemple x) est utilisé pour filtrer le trafic sur TOUTES les interfaces définies sous chaque source de span de ce groupe de sources de span.

Dans cet instantané de configuration, le groupe de filtres est appliqué au groupe source Span.

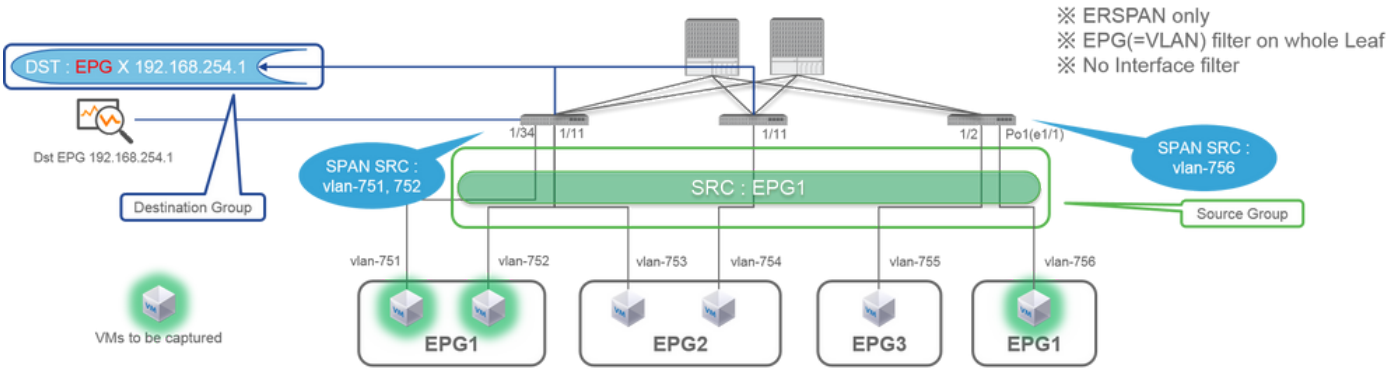


Dans le cas où une source étendue particulière est déjà associée à un groupe de filtres (par exemple, y), ce groupe de filtres (y) est utilisé à la place pour filtrer le groupe sur toutes les interfaces sous cette source étendue spécifique

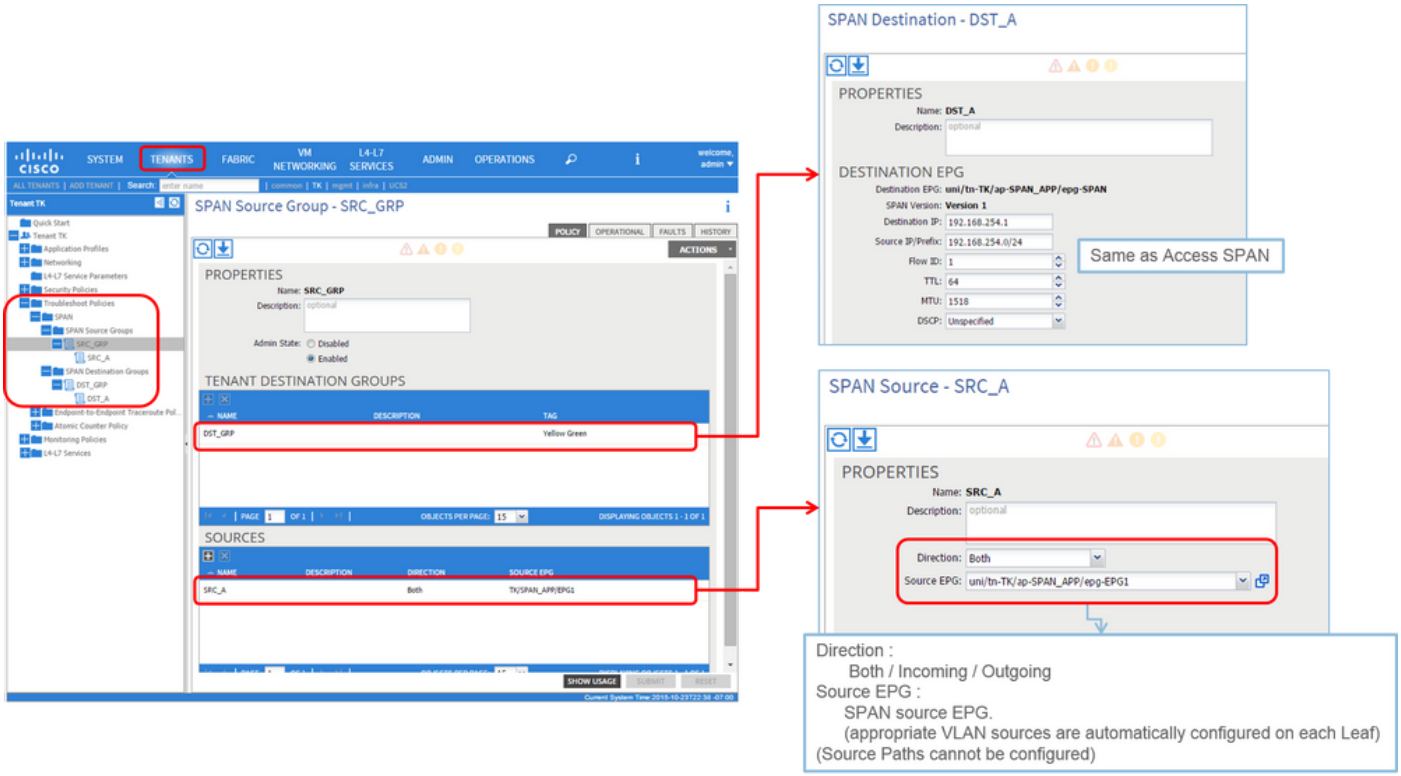
- Un groupe de filtres appliqué à un groupe source s'applique automatiquement à toutes les sources de ce groupe source.
- Un groupe de filtres appliqué à une source ne s'applique qu'à cette source.
- Un groupe de filtres est appliqué à la fois au groupe source et à une source dans ce groupe source, le groupe de filtres appliqué à la source est prioritaire.
- Un groupe de filtres appliqué à une source est supprimé, le groupe de filtres appliqué au groupe source parent est automatiquement appliqué.
- Un groupe de filtres appliqué à un groupe source est supprimé, il est supprimé de toutes les sources qui héritent actuellement de ce groupe source.

SPAN du locataire (ERSPAN)

Exemple de topologie



Exemple de configuration



- Where:

Tenants > {tenant name} > Troubleshoot Policies > SPAN

- SPAN Source Groups

- SPAN Destination Groups

※ Liens du groupe source SPAN Destination et Sources.

- Comment :

1. Créer SPAN Source Group (SRC_GRP)

- Créer SPAN Source (SRC_A) sous SPAN Source Group (SRC_GRP)

- Configurez ces paramètres pour SPAN Source (SRC_A)
  -Direction
  - EPG source

※ Reportez-vous à l'image pour plus de détails sur chaque paramètre.

- Créer SPAN Destination Group (DST_GRP)

- Créer SPAN Destination (DST_A)

- Configurez ces paramètres pour (SPAN DestinationDST_A)
  - EPG de destination
  -Adresse IP de destination
  - IP/préfixe source
  - D'autres paramètres peuvent être laissés par défaut

※ Reportez-vous à l'image pour plus de détails sur chaque paramètre.

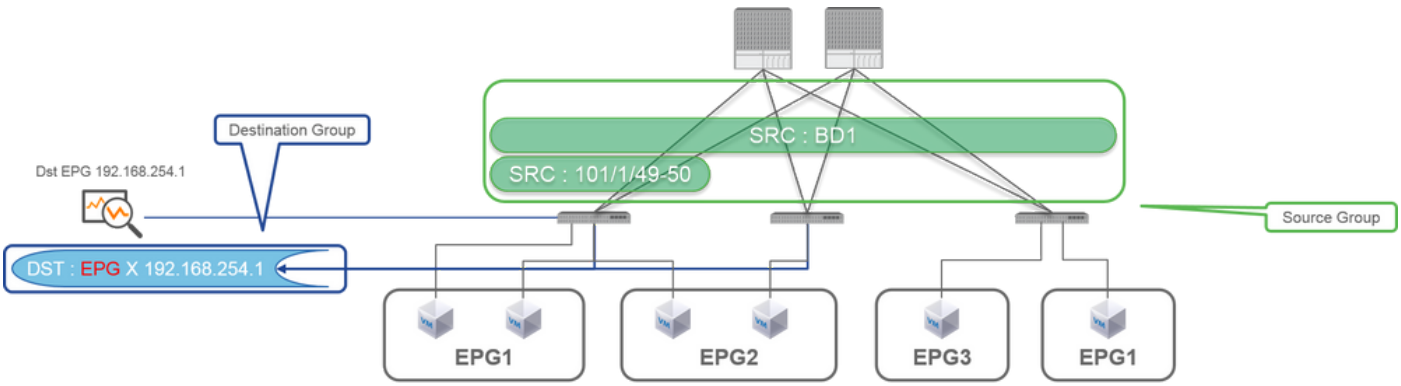
- Assurez-vous queSPAN Destination Group est lié à un SPAN Source Group.

- Assurez-vous que Admin State est activé.

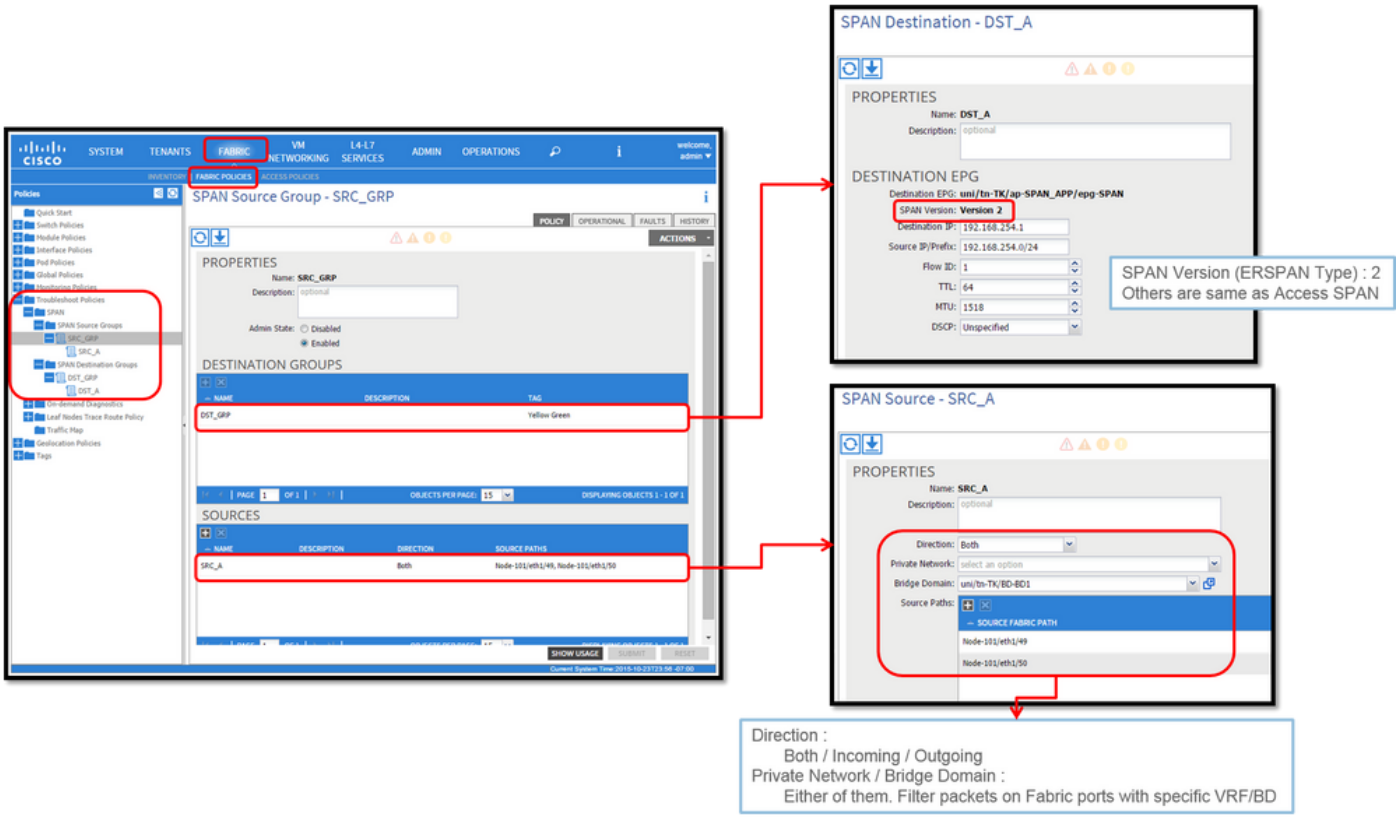
※ La fonctionnalité SPAN s'arrête lorsque vous sélectionnez Désactivé dans cet état Admin. Il n'est pas nécessaire de supprimer toutes les stratégies si vous les réutilisez ultérieurement.

Fabric SPAN (ERSPAN)

Exemple de topologie



Exemple de configuration



- Where:

Fabric > FABRIC POLICIES > Troubleshoot Policies > SPAN

- Fabric

- SPAN Destination Groups

※ SPAN Source Group liens Destination et Sources

- Comment :

1. Créer SPAN Source Group (SRC_GRP)

- Créer SPAN Source (SRC_A) sous SPAN Source Group (SRC_GRP)

- Configurez ces paramètres pour SPAN Source (SRC_A)
  -Direction
  - Réseau privé (option)
  - Domaine du pont (option)
  - Chemins source (il peut s'agir de plusieurs interfaces)

※ veuillez vous reporter à l'image pour plus de détails sur chaque paramètre.

- Créer SPAN Destination Group (DST_GRP)

- Créer SPAN Destination (DST_A)

- Configurez ces paramètres pour SPAN Destination (DST_A)
  - EPG de destination
  -Adresse IP de destination
  - IP/préfixe source
  - D'autres paramètres peuvent être laissés par défaut

※ veuillez vous reporter à l'image pour plus de détails sur chaque paramètre.

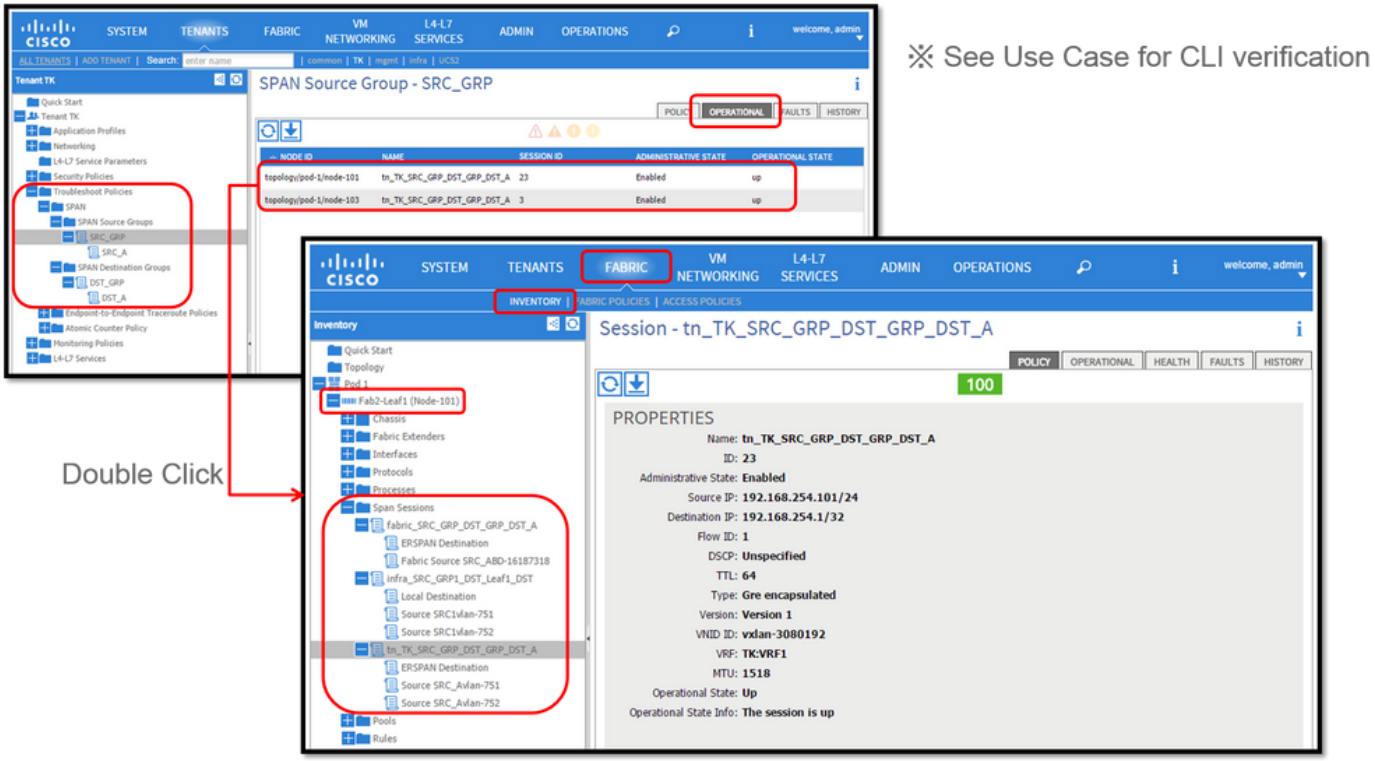
- Assurez-vous queSPAN Destination Group est lié à un SPAN Source Group.

- Assurez-vous Admin State que est activé.

※ La fonctionnalité SPAN s'arrête lorsque vous sélectionnez Désactivé sur cette Admin State. Il n'est pas nécessaire de supprimer toutes les stratégies si vous les réutilisez ultérieurement.

Bien qu'elle soit décrite dans une section ultérieure « Version (type) d'ERSPAN », vous pouvez savoir que la version II d'ERSPAN est utilisée pour Fabric SPAN et que la version I est utilisée pour Tenant et Access SPAN.

Vérification GUI



- Vérification de la stratégie de configuration 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

Assurez-vous que l'état opérationnel est activé.

- Vérification sur la session SPAN sur le noeud lui-même

1. Double-cliquez sur chaque session à partir de SPAN Configuration Policyou Fabric > INVENTORY > Node > Span Sessions > { SPAN session name }

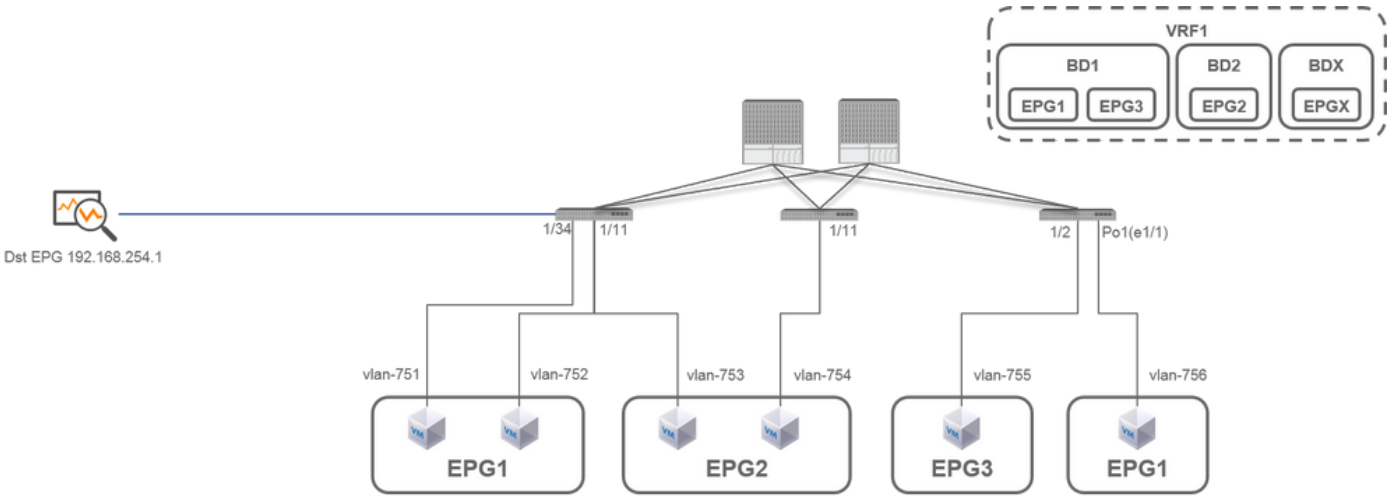
Assurez-vous que l'état opérationnel est activé.

Convention d'attribution de noms de session SPAN :

- SPAN du fabric : fabric_xxxx

- SPAN d'accès : infra_xxxx
- SPAN du locataire : tn_xxxx

Sélectionnez le type de SPAN ACI



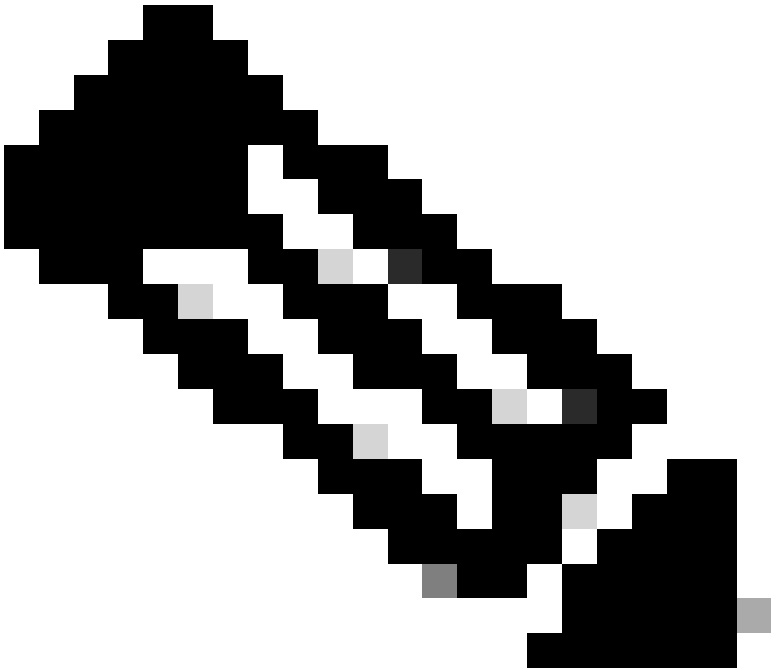
Dans cette section, des scénarios détaillés sont décrits pour chaque type de SPAN ACI (Access, Tenant, Fabric). La topologie de base de chaque scénario est mentionnée dans la section précédente.

Si vous comprenez ces scénarios, vous pouvez sélectionner le type de SPAN ACI approprié à votre besoin, par exemple les paquets sur des interfaces spécifiques uniquement doivent être capturés ou tous les paquets sur un EPG spécifique indépendamment des interfaces doivent être capturés, et plus encore.

Dans l'ACI Cisco, la fonctionnalité SPAN est configurée avec les source group et destination group. Le groupe Source contient plusieurs

facteurs source, tels que des interfaces ou des EPG. Le groupe de destinations contient des informations de destination telles que l'interface de destination pour la fonctionnalité SPAN locale ou l'adresse IP de destination pour la fonctionnalité ESPAN.

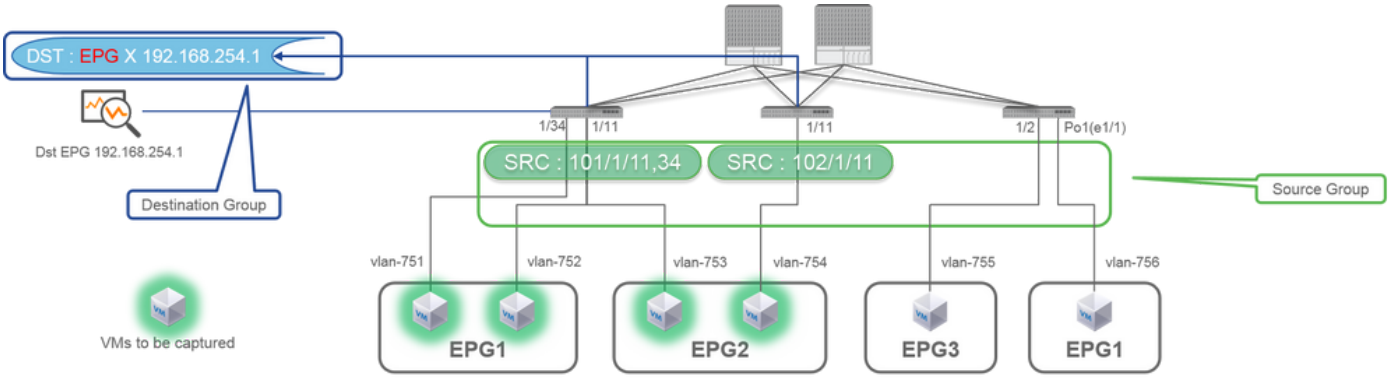
Une fois les paquets capturés, reportez-vous à la section « Comment lire les données SPAN » pour décoder les paquets capturés.



Remarque : concentrez-vous sur les machines virtuelles signalées par un voyant vert dans chaque topologie. Chaque scénario consiste à capturer des paquets à partir de ces machines virtuelles mises en évidence.

SPAN d'accès (ERSPAN)

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




```
Fab2-Leaf1# show monitor session all
   session 13
---------------
description       : Span session 13
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       Eth1/34
    tx            : Eth1/11       Eth1/34
    both          : Eth1/11       Eth1/34
source VLANs      :
    rx            :
    tx            :
    both          :
filter VLANs      : filter not specified
```

```
Fab2-Leaf2# show monitor session all
   session 12
---------------
description       : Span session 12
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
```

- Source Group
  - Leaf1 e1/1
  - Leaf1 e1/34
  - Leaf2 e1/1
- Destination Group
  - 192.168.254.1 sur EPG X

Access SPAN peut spécifier plusieurs interfaces pour une seule session SPAN. Il peut capturer tous les paquets qui entrent ou sortent des interfaces spécifiées, quel que soit leur EPG.

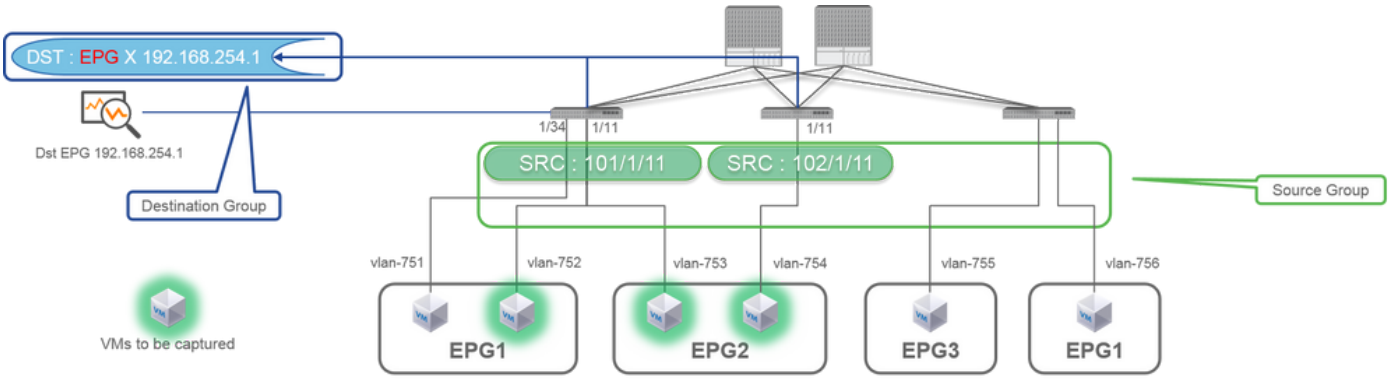
Lorsque plusieurs interfaces sont spécifiées en tant que groupe source à partir de plusieurs commutateurs Leaf, le groupe de destination doit être ERSPAN et non Local SPAN.

Dans cet exemple, il copie les paquets de toutes les machines virtuelles sur EPG1 et EPG2.

Point de contrôle CLI

- Vérifiez que l'état est « up (active) »
- "destination-ip" est l'adresse IP de destination pour ERSPAN
    - "origin-ip" est l'adresse IP source pour ERSPAN

Cas 2 . Src "Leaf1 e1/11 et 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
```

- **Groupe source**
    - Leaf1 e1/1
    - Leaf2 e1/1
- **Groupe de destinations**
    - 192.168.254.1 sur EPG X

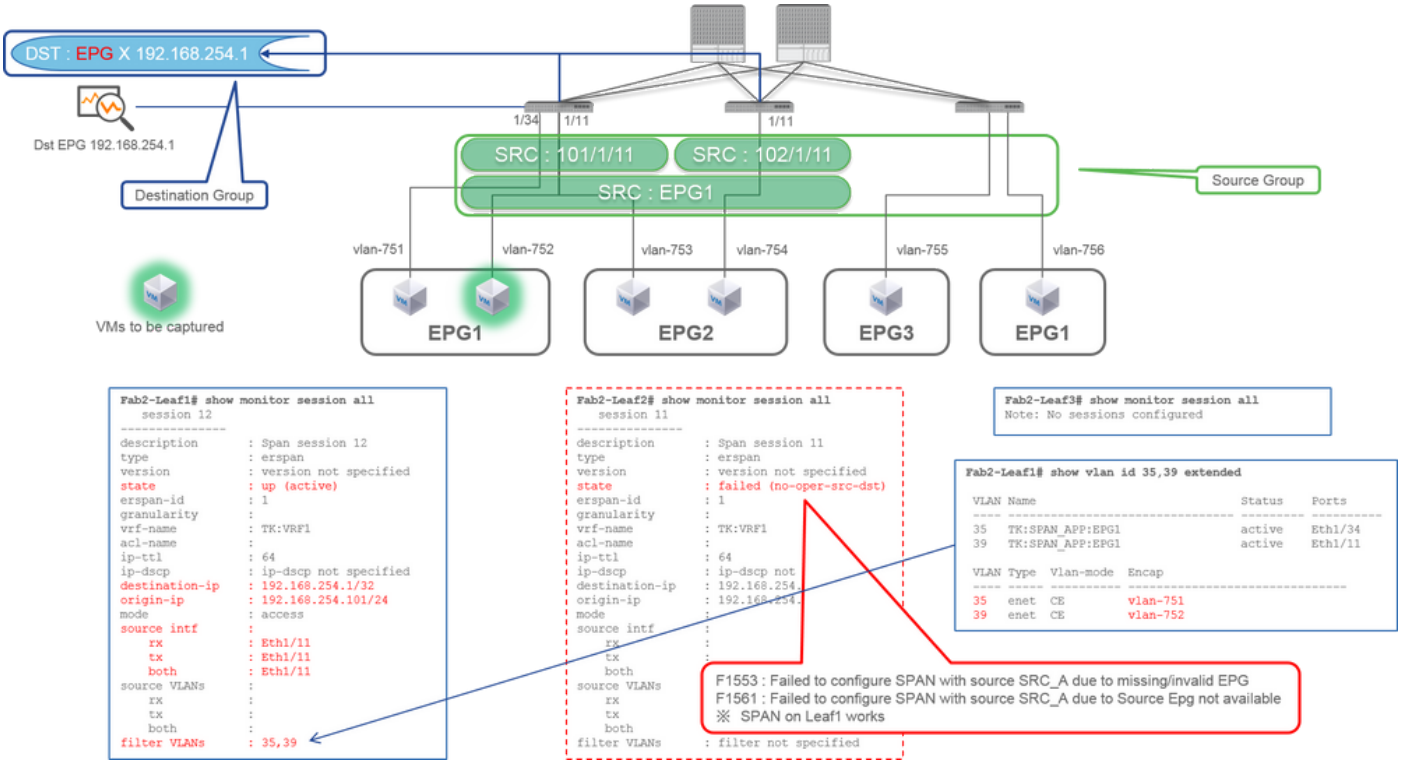
Dans cet exemple, Leaf1 e1/34 est supprimé du groupe source SPAN configuré dans le cas précédent Case1.

Le point clé de cet exemple est qu'Access SPAN peut spécifier des interfaces source indépendamment de l'EPG.

Point de contrôle CLI

- L'interface source sur Leaf1 est remplacée par "Eth1/11" et non par "Eth1/11 Eth1/34"

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



- **Groupe source**
  - Leaf1 e1/1
  - Leaf2 e1/1
  - Filtre EPG1
- **Groupe de destinations**
  - 192.168.254.1 sur EPG X

Cet exemple montre qu'Access SPAN peut également spécifier un EPG spécifique sur les ports source. Ceci est utile lorsque plusieurs EPG circulent sur une seule interface et qu'il est nécessaire de capturer le trafic uniquement pour EPG1 sur cette interface.

Comme EPG1 n'est pas déployé sur Leaf2, la fonctionnalité SPAN pour Leaf2 échoue avec les défaillances F1553 et F1561. Cependant, la fonctionnalité SPAN sur Leaf1 fonctionne toujours.

En outre, deux filtres VLAN sont automatiquement ajoutés pour la session SPAN sur Leaf1, car EPG1 utilise deux VLAN (VLAN-751,752) sur Leaf1.

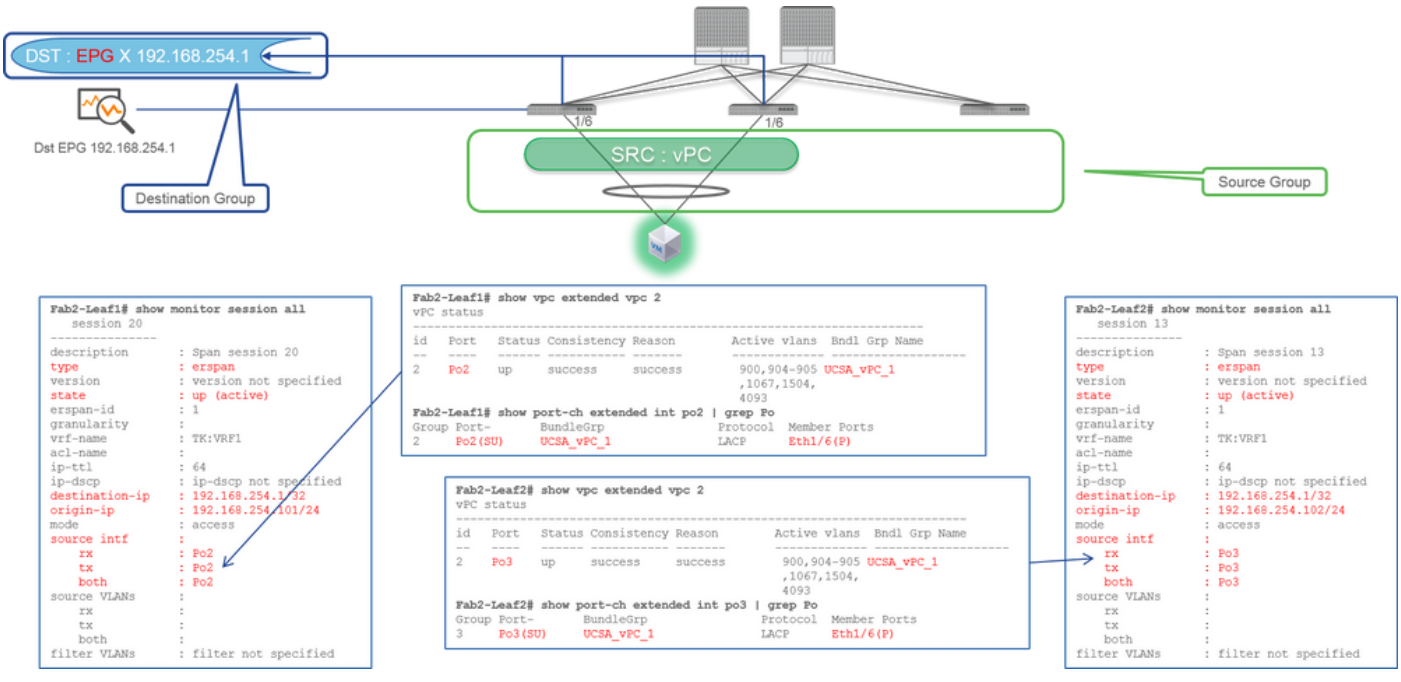
Notez que l'ID de VLAN sur l'interface de ligne de commande (35, 39) est le VLAN interne appelé PI-VLAN (Platform Independent VLAN) qui n'est pas l'ID réel sur le câble. Comme le montre l'image, la commande **show vlan extended** montre le mappage de l'ID de VLAN d'encapsulation et du PI-VLAN.

Cette session SPAN nous permet de capturer des paquets uniquement pour EPG1 (VLAN-752) sur Leaf1 e1/11 même si EPG2 (VLAN-753) circule sur la même interface.

Point de contrôle CLI

- Les VLAN de filtre sont ajoutés conformément aux groupes de terminaux utilisés pour le filtre.
- S'il n'y a aucun EPG correspondant sur ce Leaf, la session SPAN sur ce Leaf échoue.

Cas 4 . Src "Leaf1-Leaf2 vPC" | Dst "192.168.254.1"

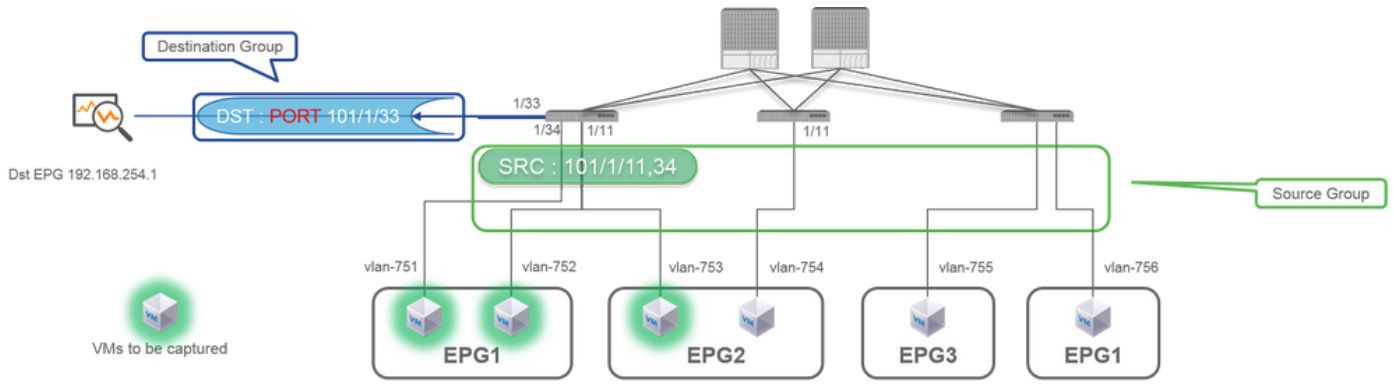


- **Groupe source**
    - Leaf1 - 2e1/11
- **Groupe de destinations**
    - 192.168.254.1 sur EPG X

Lorsque l'interface vPC est configurée en tant que source, une destination doit être une adresse IP distante (ERSPAN) et non l'interface (SPAN local)

Access SPAN (Local SPAN)

Cas 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
```

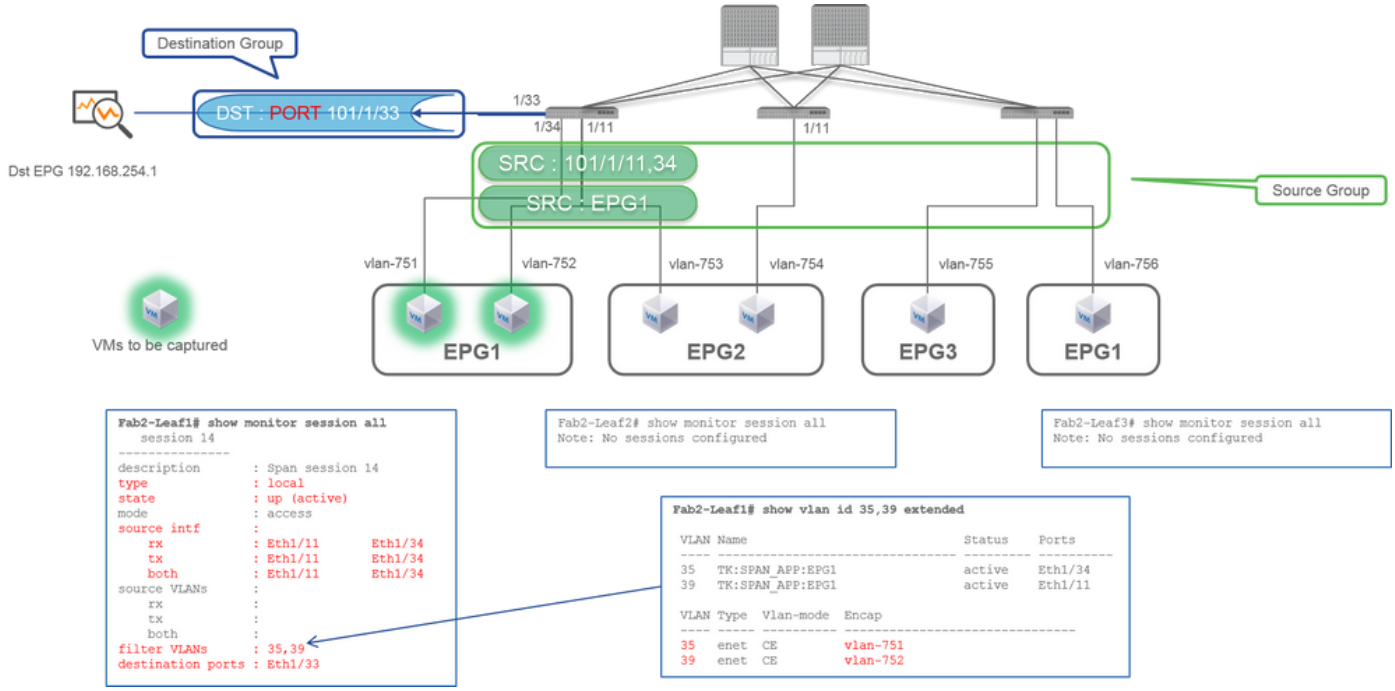
```
Fab2-Leaf3# show monitor session all
Note: No sessions configured
```

- **Groupe source**
    - Leaf1 e1/1
    - Leaf1 e1/34
- **Groupe de destinations**
    - Leaf1 e1/3

Access SPAN peut également utiliser Local SPAN (c'est-à-dire une interface spécifique comme destination)

Cependant, dans ce cas, les interfaces source doivent se trouver sur le même leaf que l'interface de destination.

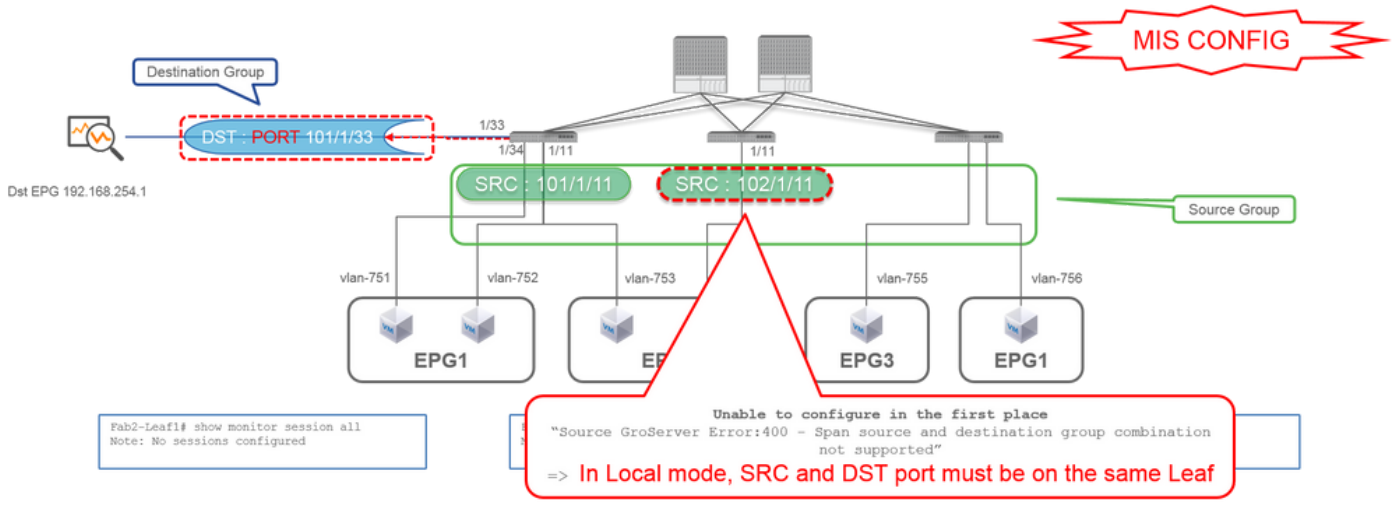
Cas 2 . Src "Leaf1 e1/11 e1/34 et filtre EPG1 | Dst " Leaf1 e1/33"



- **Groupe source**
    - Leaf1 e1/1
    - Leaf1 e1/34
    - Filtre EPG1
- **Groupe de destinations**
    - Leaf1 e1/3

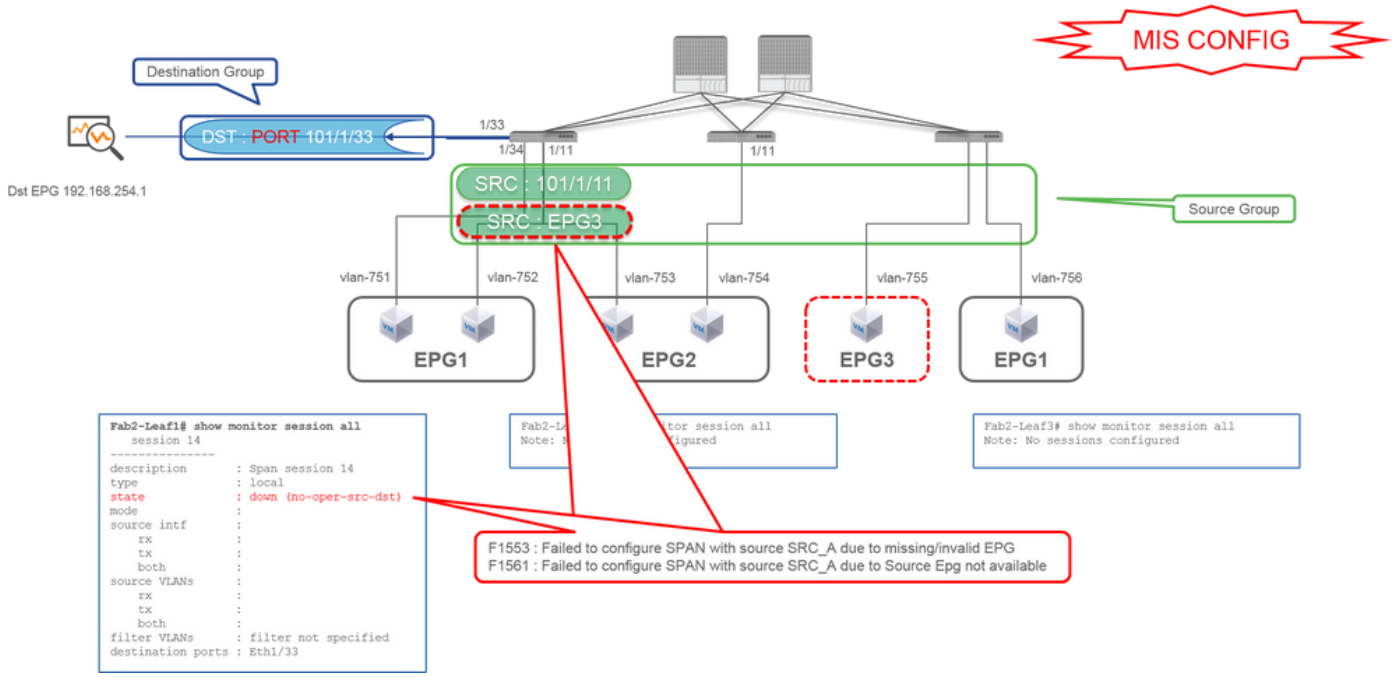
Access SPAN avec Local SPAN peut également utiliser EPG Filter ainsi qu'ERSPAN.

Cas 3 . Src "Leaf1 e1/11 et Leaf2 e/11" | Dst "Leaf1 e1/33" (casse non respectée)



- **Groupe source**
  - Leaf1 e1/1
  - Leaf2 e1/1
- **Groupe de destinations**
  - Leaf1 e1/3

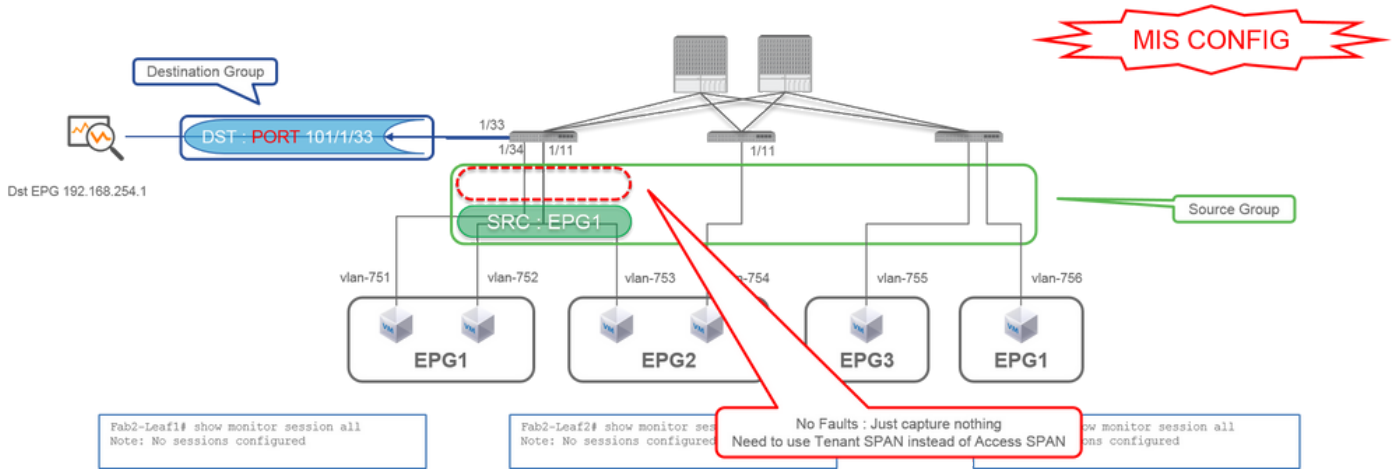
Cas 4 . Src "Filtre Leaf1 e1/11 et EPG3" | Dst "Leaf1 e1/33" (casse non respectée)



- **Groupe source**
    - Leaf1 e1/1
    - Filtre EPG3
- **Groupe de destinations**
    - Leaf1 e1/3

Il est similaire au cas 3 sur la fonctionnalité Access SPAN (ERSPAN), mais dans cet exemple, la seule et unique session SPAN sur Leaf1 échoue car EPG3 n'existe pas sur Leaf1. La fonctionnalité SPAN ne fonctionne donc pas du tout.

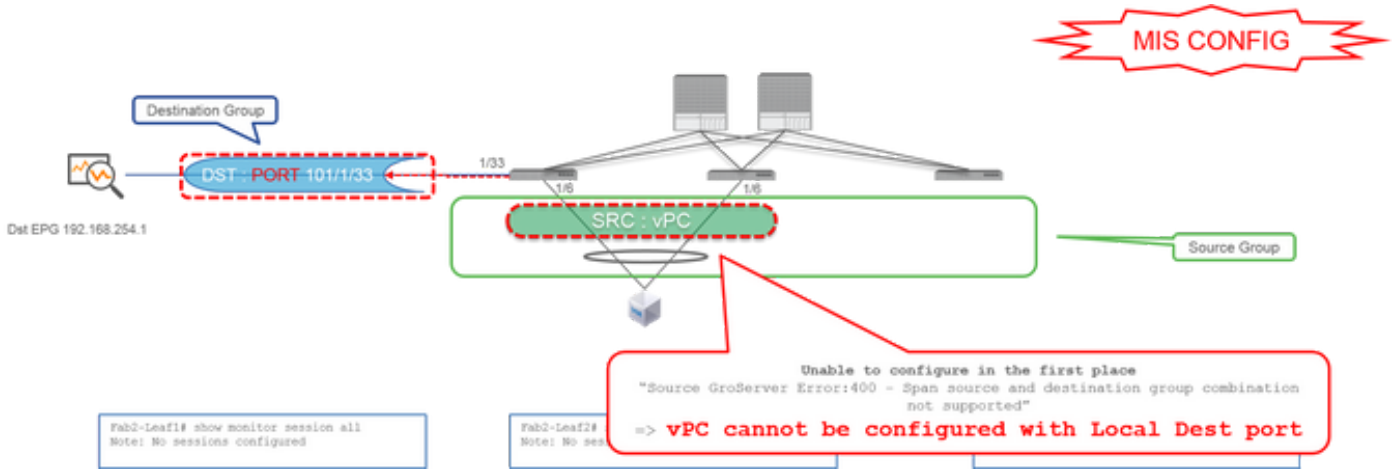
Cas 5 : Src "EPG1 filter" | Dst "Leaf1 e1/33" (casse non respectée)



- **Groupe source**
    - Filtre EPG1
- **Groupe de destinations**
    - Leaf1 e1/3

Le filtre EPG sur Access SPAN fonctionne uniquement lorsque les ports sources sont configurés. Si EPG est la seule source à spécifier, la fonctionnalité SPAN du locataire doit être utilisée à la place de la fonctionnalité SPAN d'accès.

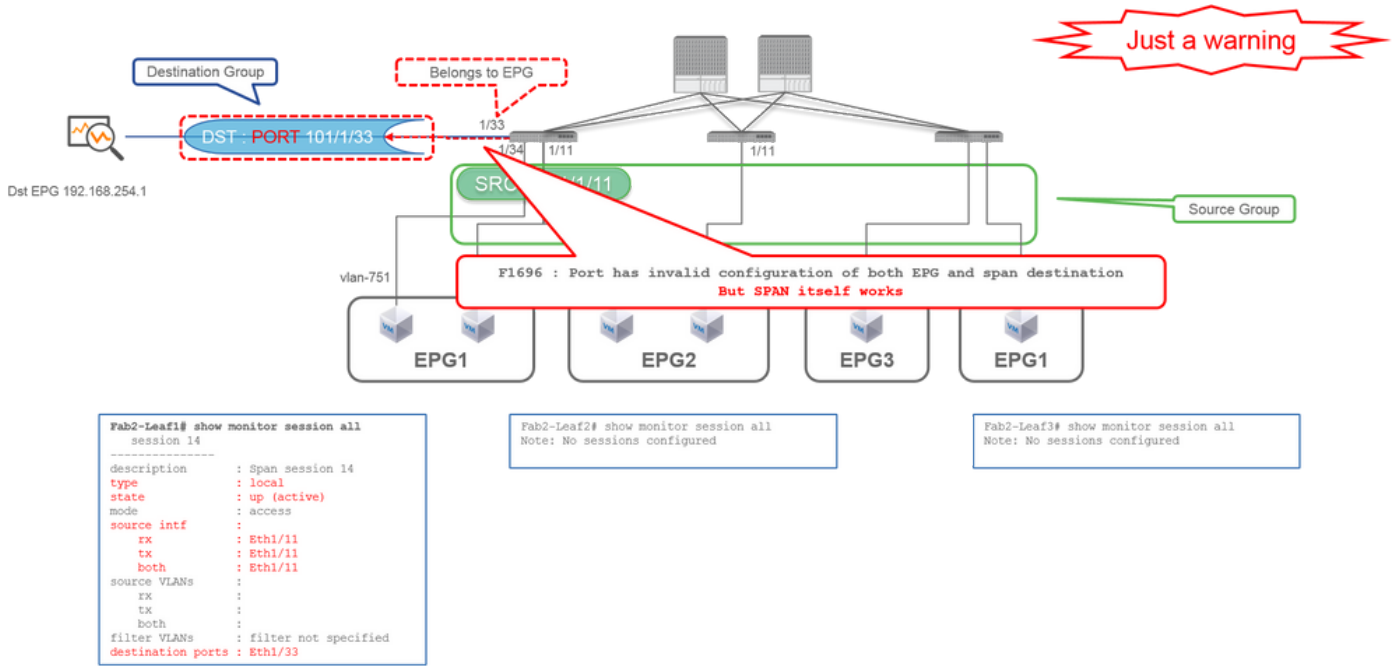
Cas 6 . Src "Leaf1 - Leaf2 vPC" | Dst "Leaf1 e1/33" (casse non respectée)



- **Groupe source**
  - vPC Leaf1-2
- **Groupe de destinations**
  - Leaf1 e1/3

Une interface vPC ne peut pas être configurée en tant que source avec la fonctionnalité SPAN locale. Veuillez utiliser ERSPAN. Reportez-vous au cas4 pour la fonctionnalité Access SPAN (ERSPAN).

Cas 7 . Src "Leaf1 e1/11 | Dst "Leaf1 e1/33 & e1/33 appartient à EPG" (fonctionne avec défaut)

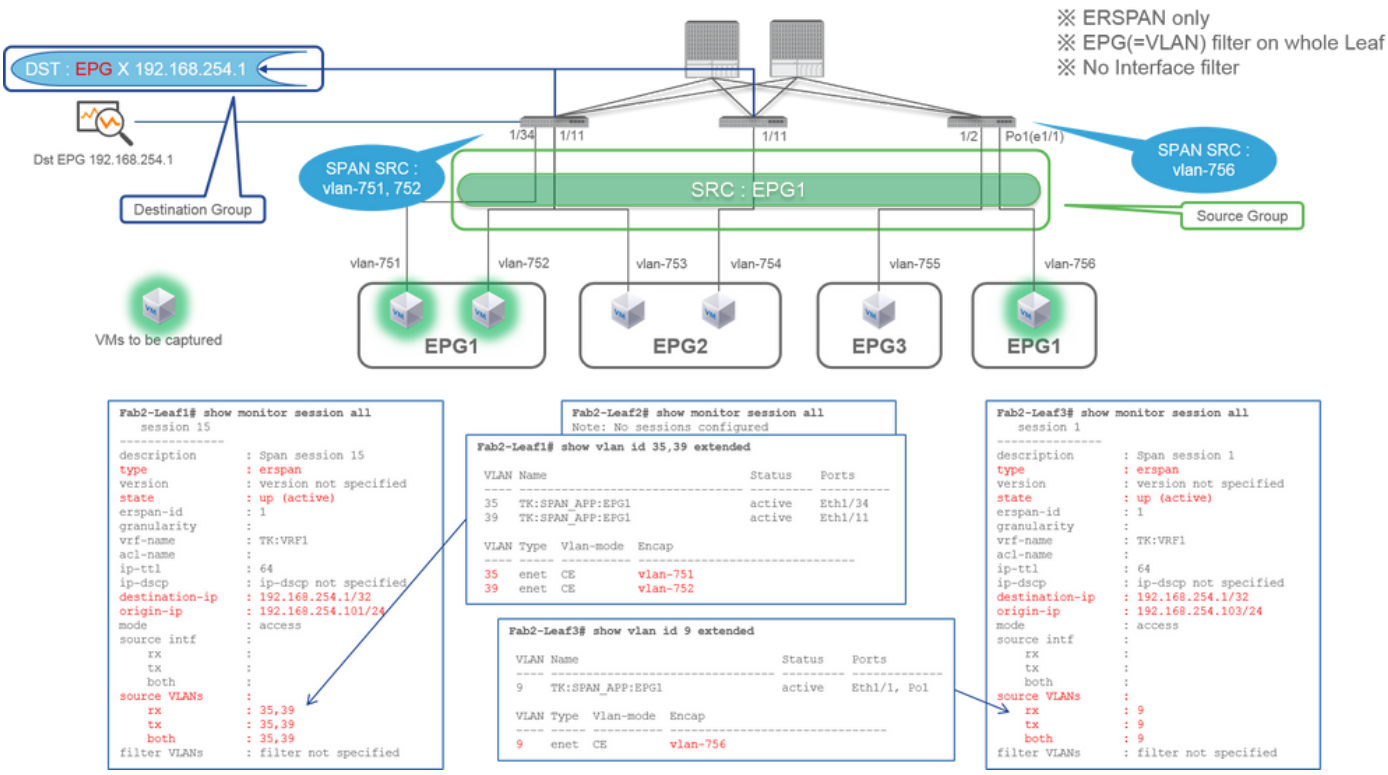


Si une I/F de destination pour SPAN appartient déjà à l'EPG, une erreur « F1696 : Port has an invalid configuration of EPG and span destination » est générée sous l'I/F physique.

Mais même avec cette faille, SPAN fonctionne sans aucun problème. Cette erreur n'est qu'un avertissement sur le trafic supplémentaire causé par la fonctionnalité SPAN, car il peut avoir un impact sur le trafic EPG normal des clients sur la même I/F.

SPAN du locataire (ERSPAN)

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



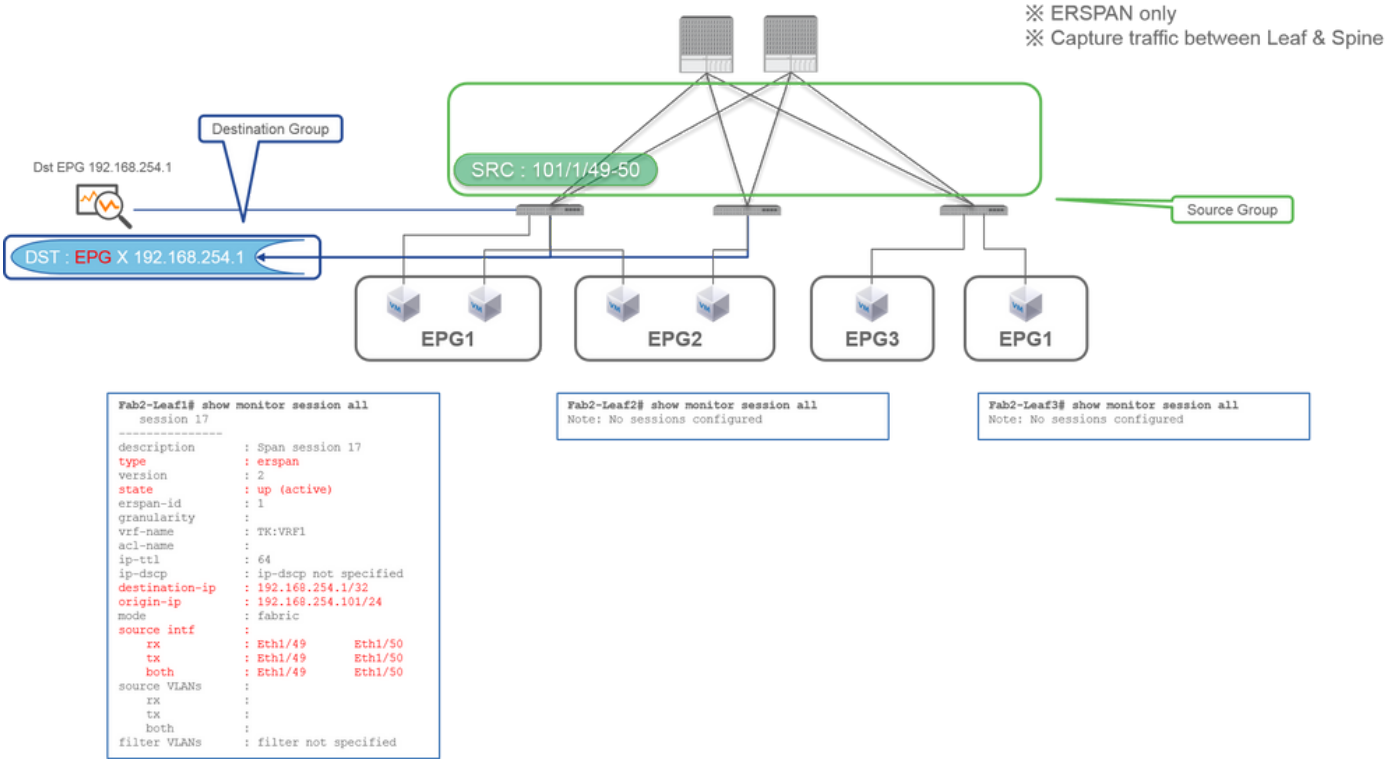
- **Groupe source**
  - EPG1 (pas de filtre)
- **Groupe de destinations**
  - 192.168.254.1 sur EPG X

La fonctionnalité SPAN du locataire utilise l'EPG lui-même comme source, tandis que la fonctionnalité Access SPAN utilise l'EPG uniquement pour un filtre.

Le point clé de la fonctionnalité SPAN du locataire est que vous n'avez pas besoin de spécifier chaque port individuel et que l'ACI détecte automatiquement les VLAN appropriés sur chaque commutateur Leaf. Cela serait donc utile lorsque tous les paquets pour un EPG spécifique doivent être surveillés et que les terminaux pour cet EPG appartiennent à plusieurs interfaces sur des commutateurs Leaf.

Fabric SPAN (ERSPAN)

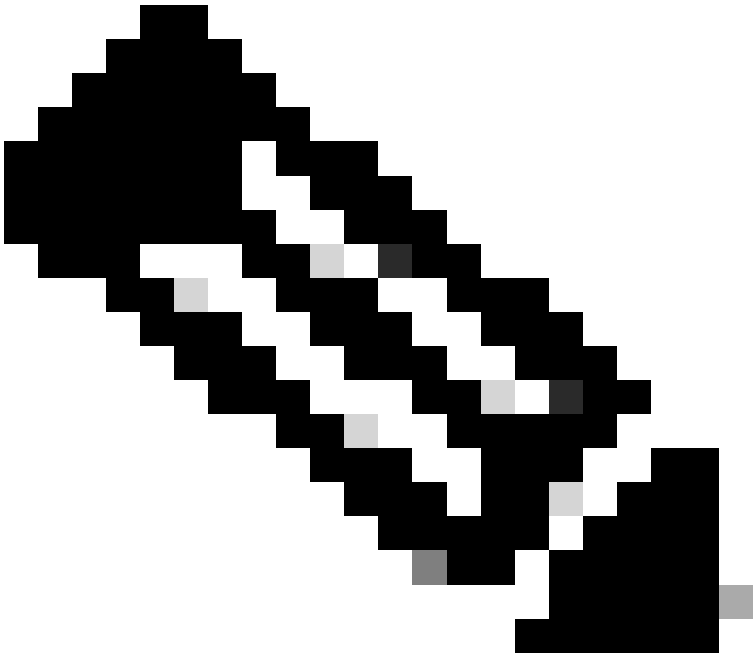
Cas 1 . Src "Leaf1 e1/49-50" | Dst "192.168.254.1"



- **Groupe source**
    - Leaf1 e1/49-50
- **Groupe de destinations**
    - 192.168.254.1 sur EPG X

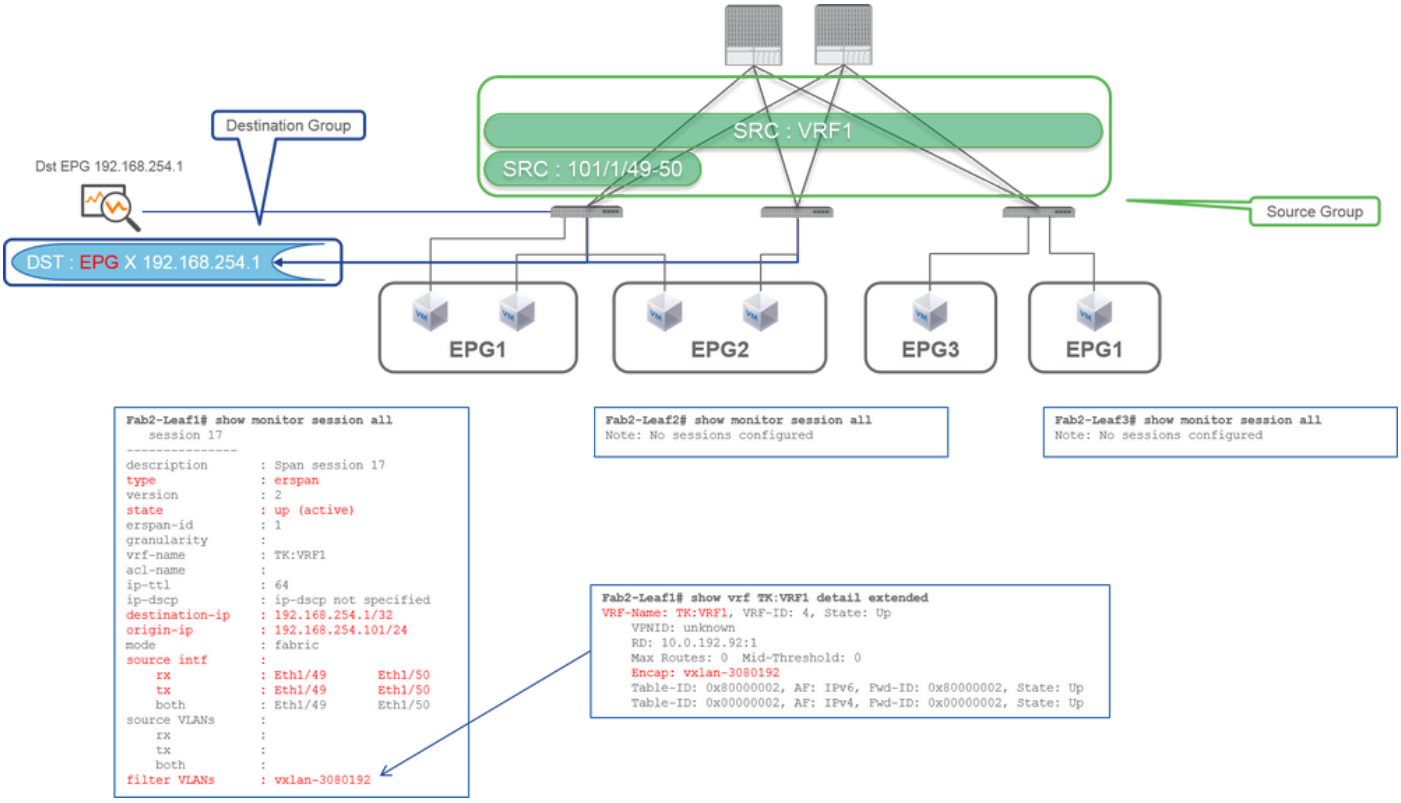
La fonctionnalité SPAN du fabric spécifie les ports du fabric comme source où les ports du fabric sont des interfaces entre les commutateurs Leaf et Spine.

Cette fonctionnalité SPAN est utile lorsqu'il est nécessaire de copier des paquets entre des commutateurs Leaf et Spine. Cependant, les paquets entre les commutateurs Leaf et Spine sont encapsulés avec un en-tête iVxLAN. Il faut donc un peu de piège pour le lire. Reportez-vous à la section « Lecture des données SPAN ».



Remarque : l'en-tête VxLAN est un en-tête VxLAN amélioré uniquement pour une utilisation interne du fabric ACI.

Cas 2 . Src "Leaf1 e1/49-50 et filtre VRF" | Dst "192.168.254.1"



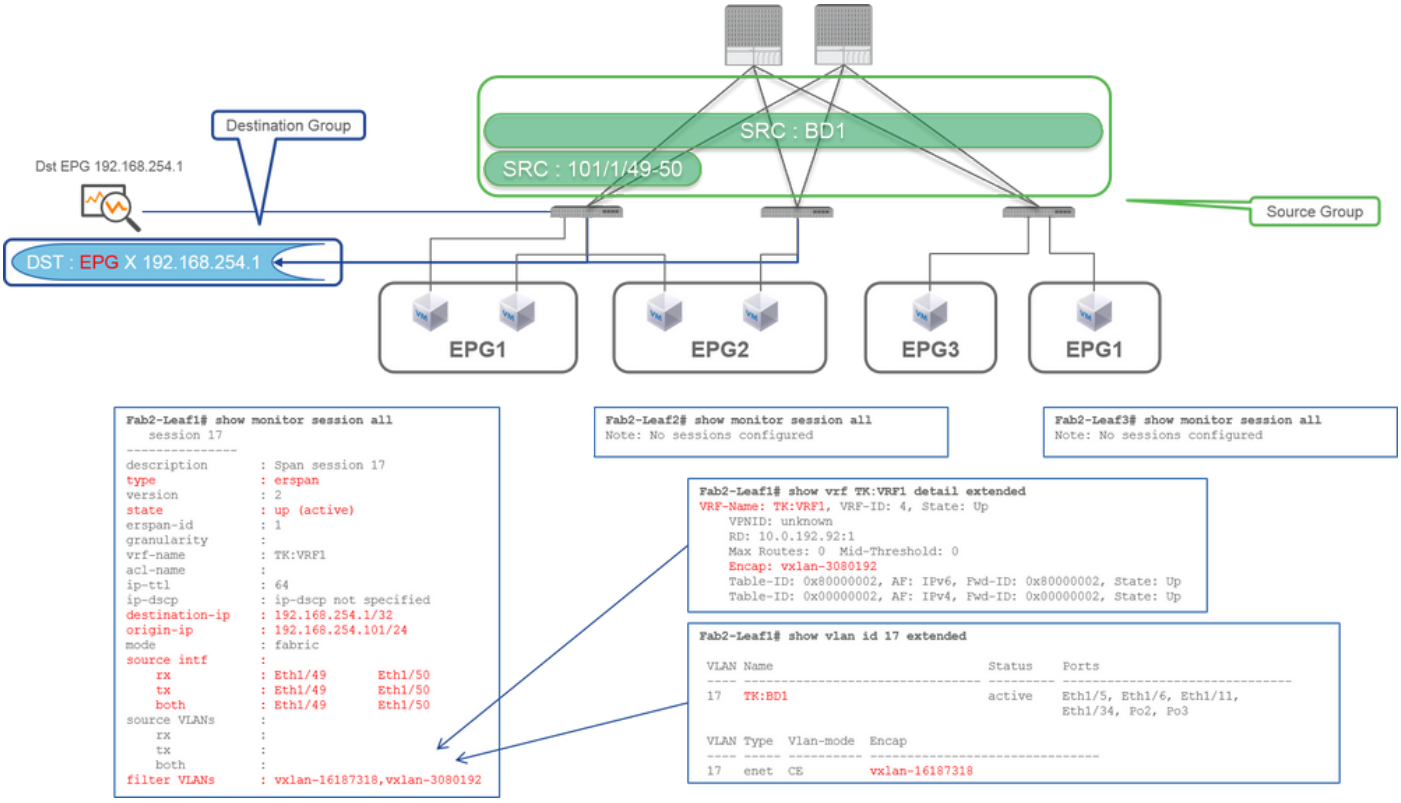
- **Groupe source**
  - Leaf1 e1/49-50
  - Filtre VRF
- **Groupe de destinations**
  - 192.168.254.1 sur EPG X

La fonctionnalité SPAN du fabric peut utiliser des filtres ainsi que la fonctionnalité SPAN d'accès. Mais le type de filtre est différent. La fonctionnalité SPAN du fabric utilise le VRF (Virtual Routing and Forwarding) ou BD comme filtre.

Dans l'ACI Cisco, comme décrit précédemment, les paquets qui passent par les ports de fabric sont encapsulés avec un en-tête iVxLAN. Cet en-tête iVxLAN contient des informations VRF ou BD en tant qu'identificateur de réseau virtuel (VNID). Lorsque les paquets sont transférés en tant que couche 2 (L2), iVxLAN VNID est l'acronyme de BD. Lorsque les paquets sont transférés en tant que couche 3 (L3), iVxLAN VNID est l'acronyme de VRF.

Par conséquent, lorsqu'il est nécessaire de capturer le trafic routé sur les ports du fabric, utilisez VRF comme filtre.

Cas 3 . Src "Leaf1 e1/49-50 & filtre BD" | Dst "192.168.254.1"

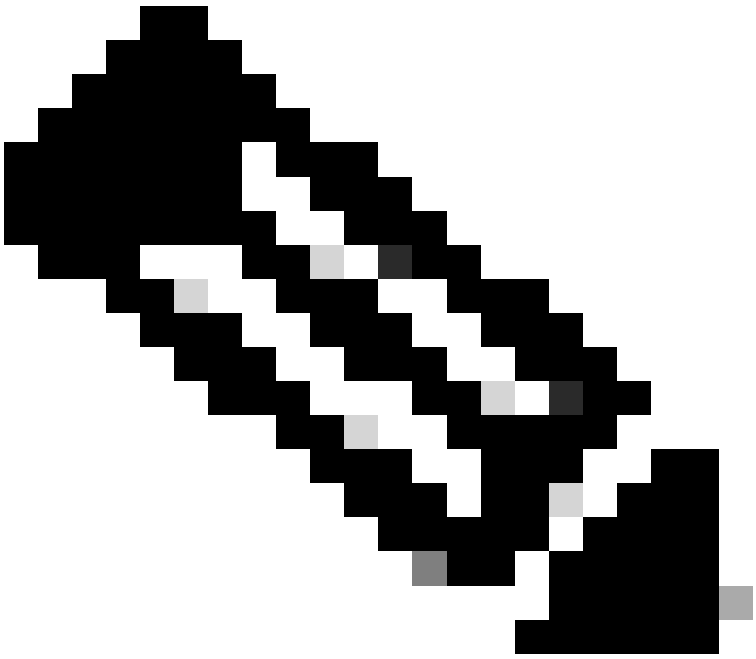


- **Groupe source**
  - Leaf1 e1/49-50
  - Filtre BD
- **Groupe de destinations**

- 192.168.254.1 sur EPG X

Comme décrit dans le cas précédent 2, la fonctionnalité Fabric SPAN peut utiliser BD comme filtre.

Lorsqu'il est nécessaire de capturer le trafic ponté sur les ports du fabric, utilisez BD comme filtre.



Remarque : un seul filtre de BD ou VRF peut être configuré à la fois.

De quoi avez-vous besoin sur le périphérique de destination SPAN ?

Il vous suffit d'exécuter une application de capture de paquets telle que tcpdump, wireshark sur elle. Il n'est pas nécessaire de configurer la session de destination ERSPAN ou autre.

Pour ERSPAN

Assurez-vous d'exécuter un outil de capture sur l'interface avec l'adresse IP de destination pour ERSPAN puisque les paquets SPAN sont transférés vers l'adresse IP de destination.

Le paquet reçu est encapsulé avec un en-tête GRE. Reportez-vous à cette section « Lecture des données ERSPAN » pour savoir comment décoder l'en-tête ERSPAN GRE.

Pour SPAN local

Assurez-vous d'exécuter un outil de capture sur l'interface qui se connecte à l'interface de destination SPAN sur le leaf ACI.

Des paquets bruts sont reçus dans cette interface. Il n'est pas nécessaire de traiter l'en-tête ERSPAN.

Lecture des données ERSPAN

Version ERSPAN (type)

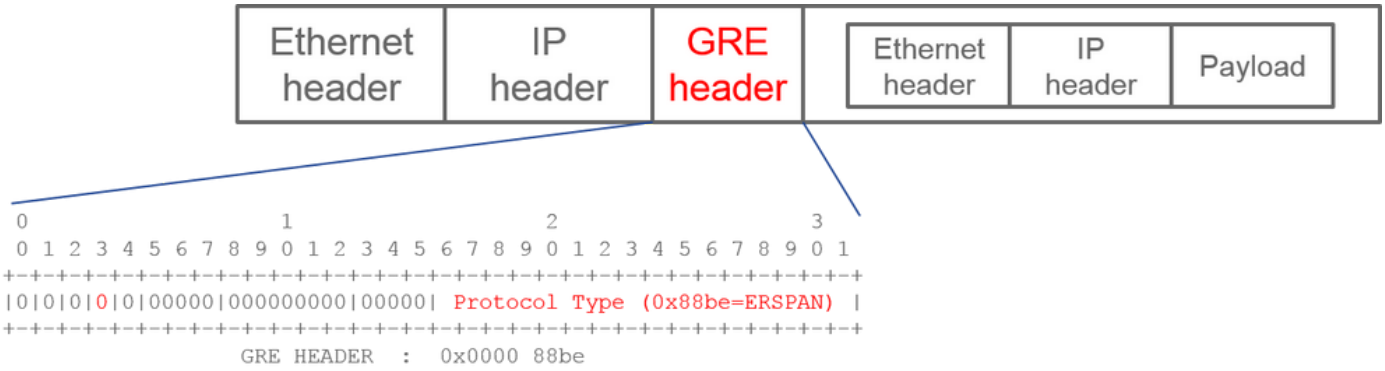
ERSPAN encapsule les paquets copiés pour les transférer vers la destination distante. GRE est utilisé pour cette encapsulation. Le type de protocole pour ERSPAN sur l'en-tête GRE est 0x88be.

Dans le document IETF (Internet Engineering Task Force), la version d'ERSPAN est décrite comme type et non comme version.

Il existe trois types d'ERSPAN. I, II et III. Le type ERSPAN est mentionné dans ce projet de RFC. En outre, ce GRE RFC1701 peut être utile pour comprendre également chaque type ERSPAN.

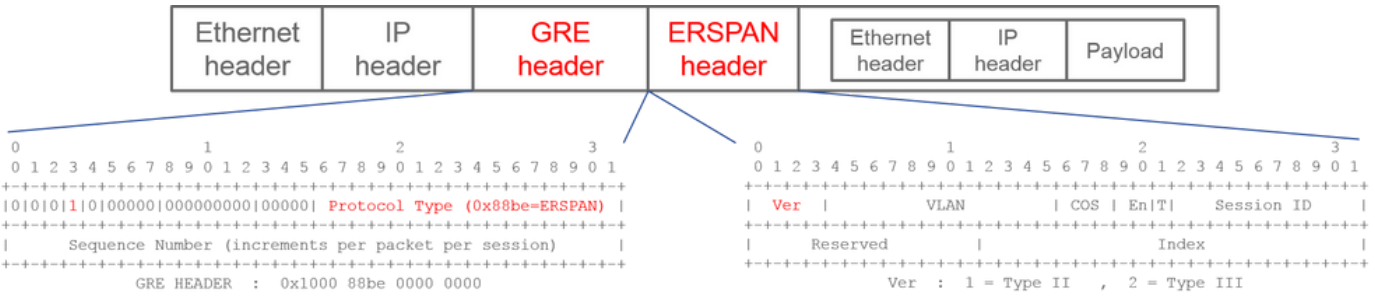
Voici le format de paquet de chaque type :

ERSPAN Type I (utilisé par Broadcom Trident 2)



Le type I n'utilise pas le champ de séquence de l'en-tête GRE. Il n'utilise même pas l'en-tête ERSPAN qui doit suivre l'en-tête GRE s'il s'agissait d'ERSPAN de type II et III. Broadcom Trident 2 prend uniquement en charge cette fonctionnalité ERSPAN de type I.

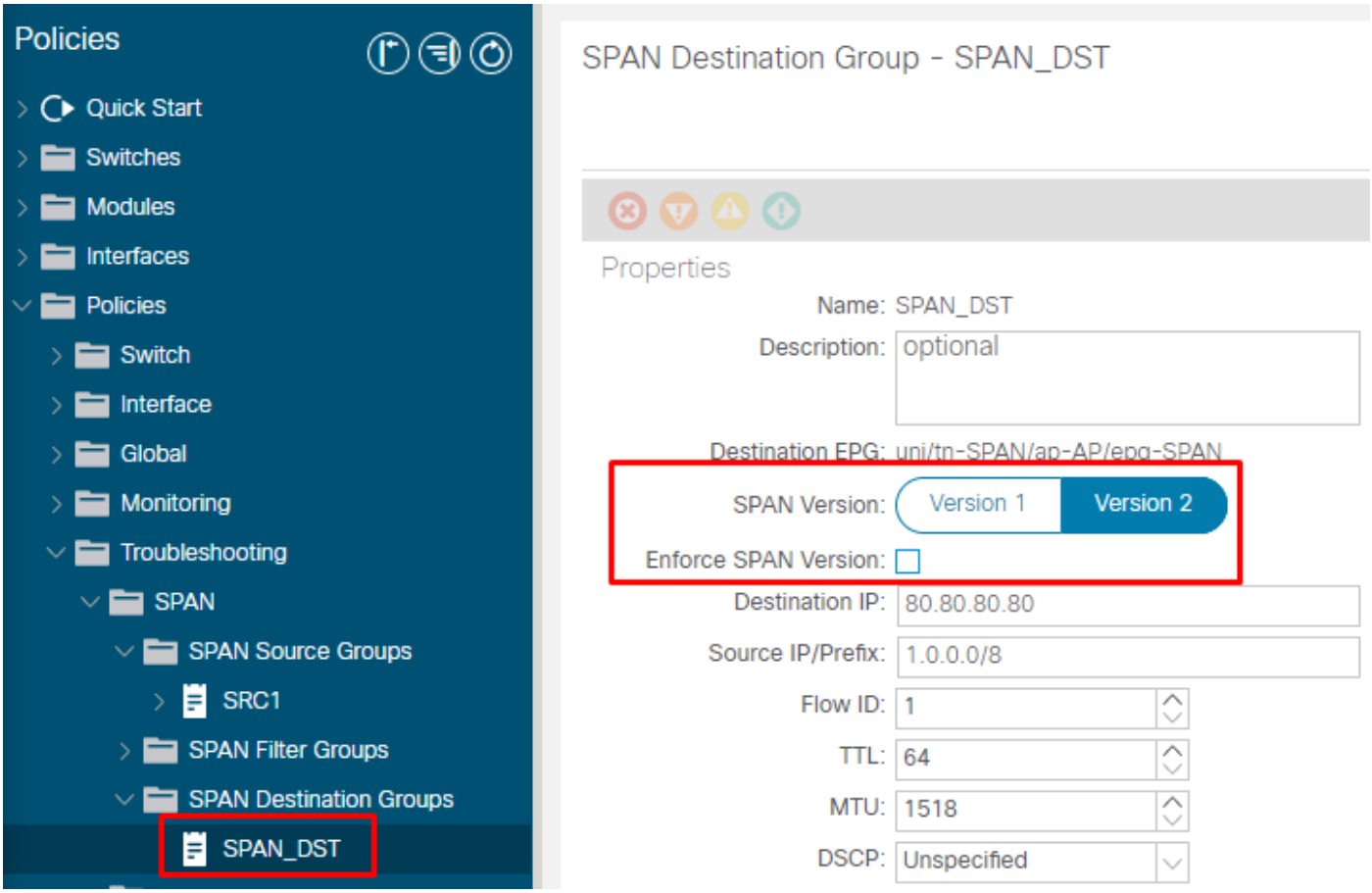
ERSPAN de type II ou III



Si le champ de séquence est activé par le bit S, il doit s'agir d'ERSPAN de type II ou III. Le champ version de l'en-tête ERSPAN identifie le type ERSPAN. Dans l'ACI, le type III n'est pas pris en charge à partir du 20/03/2016.

Si un groupe de sources SPAN pour l'accès ou le SPAN du locataire a des sources sur les noeuds de 1re et de 2e génération, la destination ERSPAN reçoit les paquets ERSPAN de type I et II de chaque génération de noeuds. Cependant, Wireshark ne peut décoder qu'un seul des types ERSPAN à la fois. Par défaut, il décode uniquement ERSPAN Type II. Si vous activez le décodage d'ERSPAN Type I, Wireshark ne décode pas ERSPAN Type II. Reportez-vous à la section suivante pour savoir comment décoder ERSPAN Type I sur Wireshark.

Pour éviter ce type de problème, vous pouvez configurer le type ERSPAN sur un groupe de destinations SPAN.



- SPAN Version (Version 1 ou Version 2) : fait référence à ERSPAN Type I ou II

- Enforce SPAN Version (activé ou non activé) : cette option détermine si la session SPAN doit échouer au cas où le type ERSPAN configuré n'est pas pris en charge sur le matériel du noeud source.

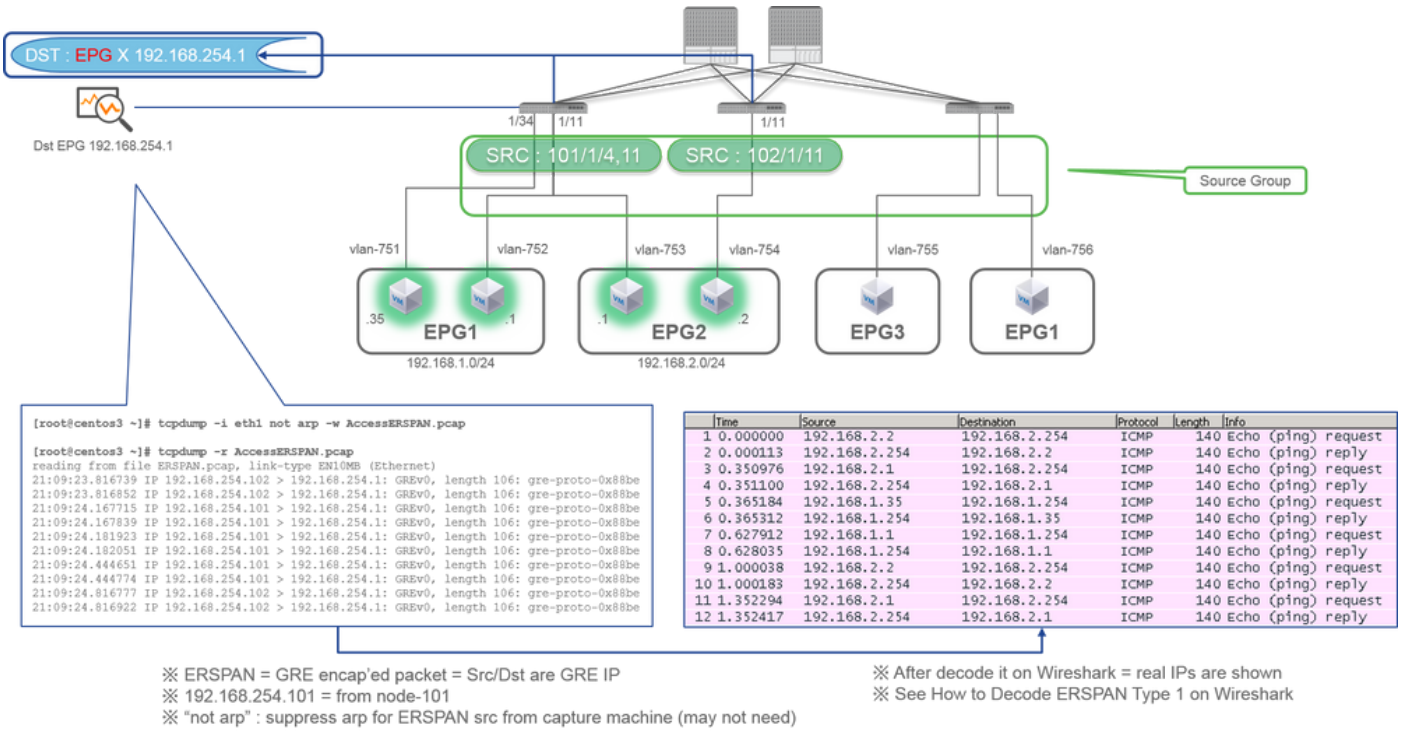
Par défaut, Version SPAN est Version 2 et l'option Appliquer la version SPAN est désactivée. Cela signifie que si le noeud source est de 2e génération ou ultérieure qui prend en charge ERSPAN Type II, il génère ERSPAN avec Type II. Si le noeud source est de 1ère génération et ne prend pas en charge la fonctionnalité ERSPAN de type II (sauf pour la fonctionnalité Fabric SPAN), il revient au type I, car l'option Enforce SPAN Version n'est pas cochée. Par conséquent, la destination ERSPAN reçoit un type mixte d'ERSPAN.

Ce tableau explique chaque combinaison pour la fonctionnalité SPAN d'accès et de service partagé.

Version SPAN	**Appliquer la version SPAN**	**Noeud source 1re génération**	**Noeud source de 2e génération**
Version 2	Décoché	Utilise le type I	Utilise le type II
Version 2	Coché	Échecs	Utilise le type II
Version 1	Décoché	Utilise le type I	Utilise le type I
Version 1	Coché	Utilise le type I	Utilise le type I

Exemple de données ERSPAN

SPAN/SPAN d'accès du locataire (ERSPAN)



Les paquets doivent être décodés car ils sont encapsulés par ERSPAN Type I. Cela peut être fait avec Wireshark. Reportez-vous à la section « Comment décoder ERSPAN Type 1 ».

Détails du paquet capturé (ERSPAN Type 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
        0x0020:  fe01 0000 88be 0022 bdf8 19ff 0050 56bb
        0x0030:  d6c2 8100 02f2 0800 4500 0054 0000 4000
        0x0040:  4001 b458 c0a8 0202 c0a8 02fe 0800 34cc
        0x0050:  c847 0115 7404 2b56 0000 0000 8da9 0e00
        0x0060:  0000 0000 1011 1213 1415 1617 1819 1a1b
        0x0070:  1c1d 1e1f 2021 2223 2425 2627 2829 2a2b
        0x0080:  2c2d 2e2f 3031 3233 3435 3637

ESPAN Ethernet header          : Dst 0050.56bb.3096 , Src 0022.bdf8.19.ff
ERSPAN IP header               : Dst 192.168.254.1  , Src 192.168.254.102
GRE header (= ERSPAN Type I)   : 0x88be = ERSPAN (S bit off 0x0000)
Ethernet header                : Dst 0022.bdf8.19ff , Src 0050.56bb.d6c2
Dot1Q header                   : VLAN 754
IP header                      : Dst 192.168.2.254  , Src 192.168.2.2
```

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 décode automatiquement ERSPAN Type II. Cependant, il est toujours encapsulé par l'en-tête iVxLAN.

Par défaut, Wireshark ne comprend pas l'en-tête iVxLAN, car il s'agit d'un en-tête interne ACI. Reportez-vous à « Comment décoder l'en-tête iVxLAN ».

Détails du paquet capturé (ERSPAN Type II)

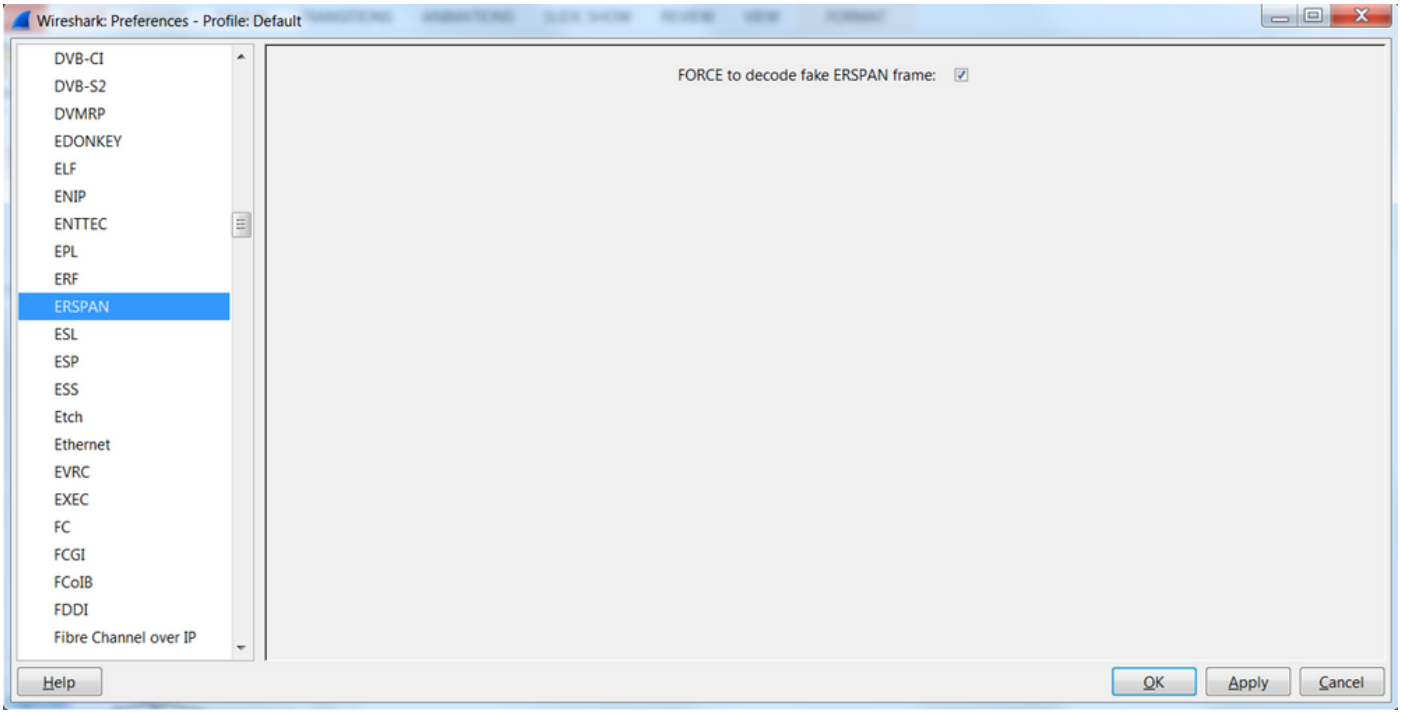
```
[root@centos3 ~]# tcpdump -xxr FabricERSPAN.pcap -c 1
reading from file FabricERSPAN.pcap, link-type EN10MB (Ethernet)
23:25:00.962224 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 53341, length 164: gre-proto-0x88be
        0x0000:  0050 56bb 3096 0022 bdf8 19ff 0800 4500
        0x0010:  00b8 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
```

Comment décoder ERSPAN Type I

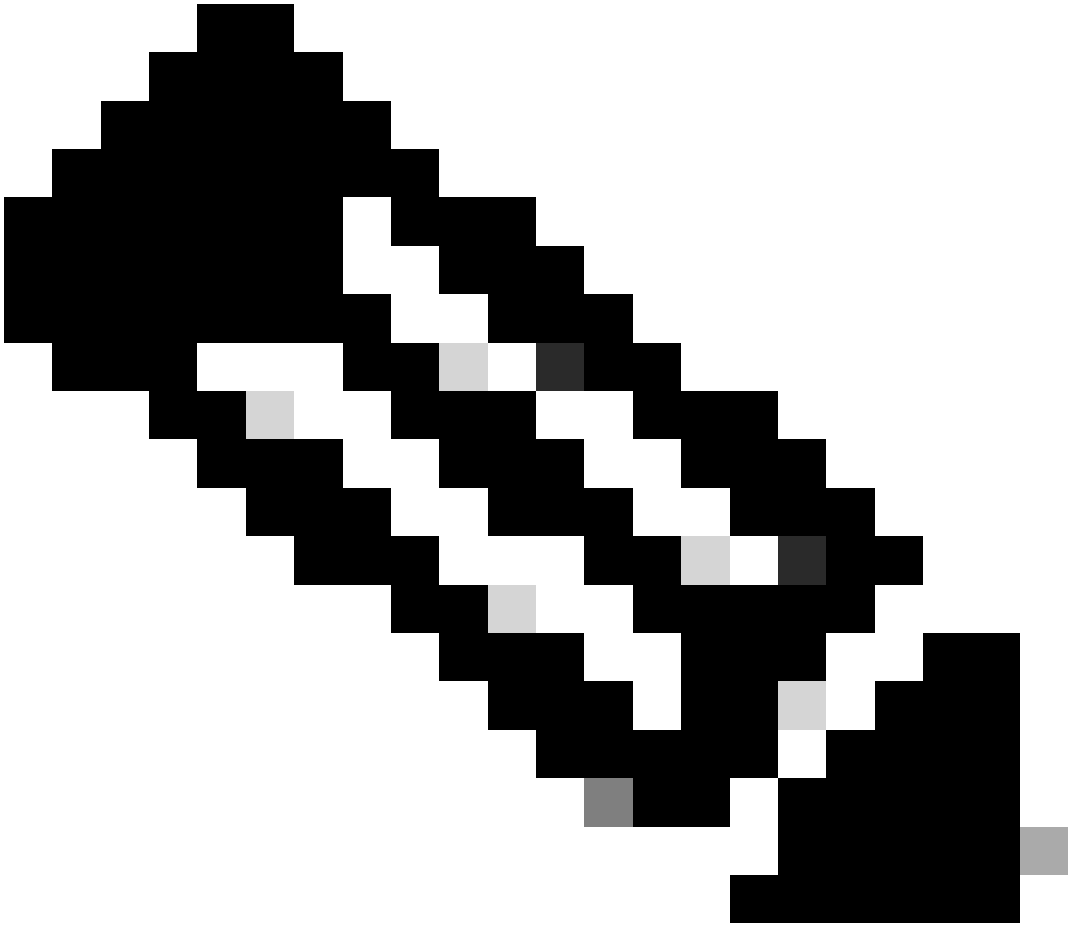
Option 1. Accédez à la trame ERSPAN et cochezEdit > Preference > Protocols > ERSPAN FORCE pour la décoder.

- Wireshark (GUI)



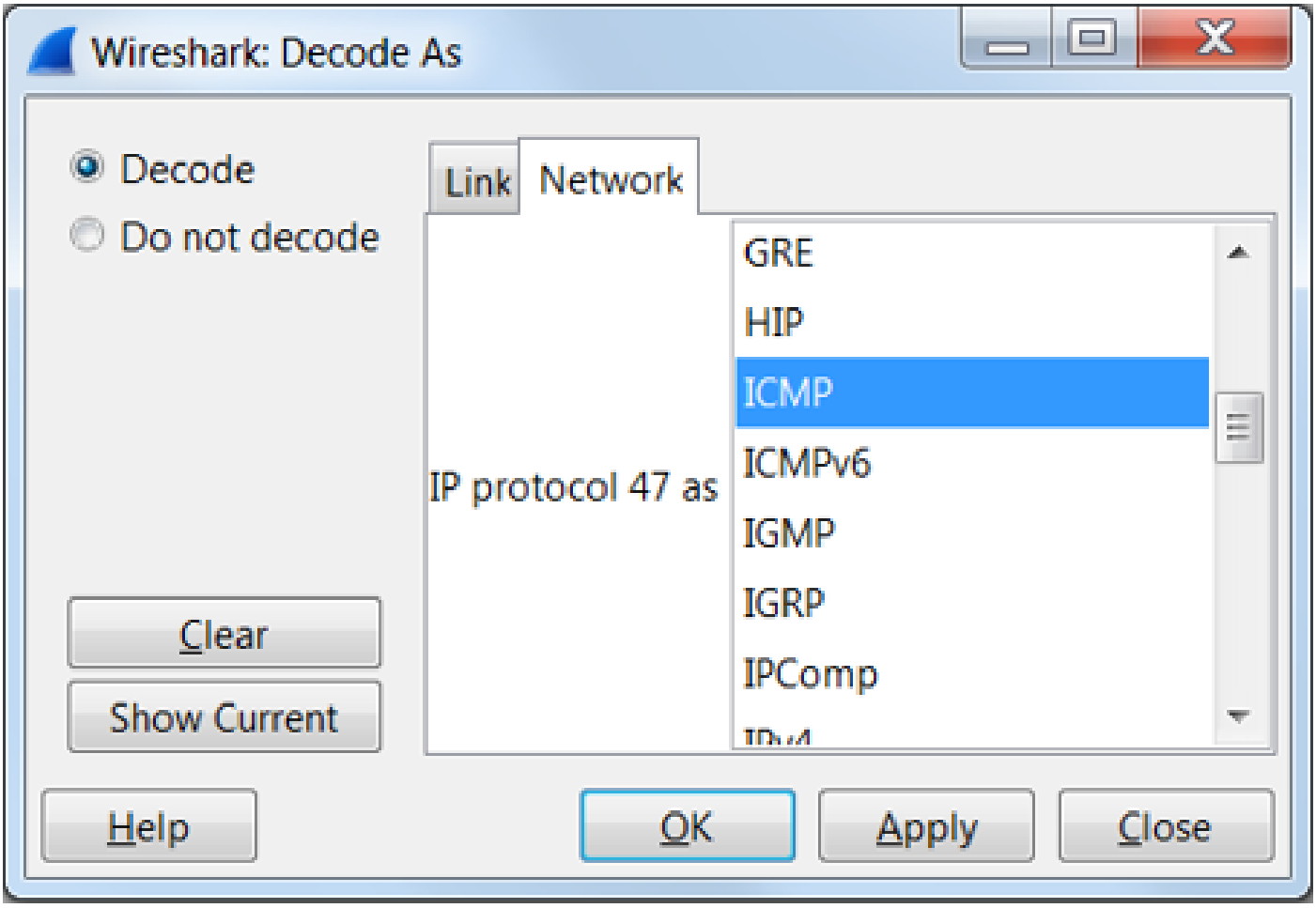
- Tshark (version CLI de Wireshark) :

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

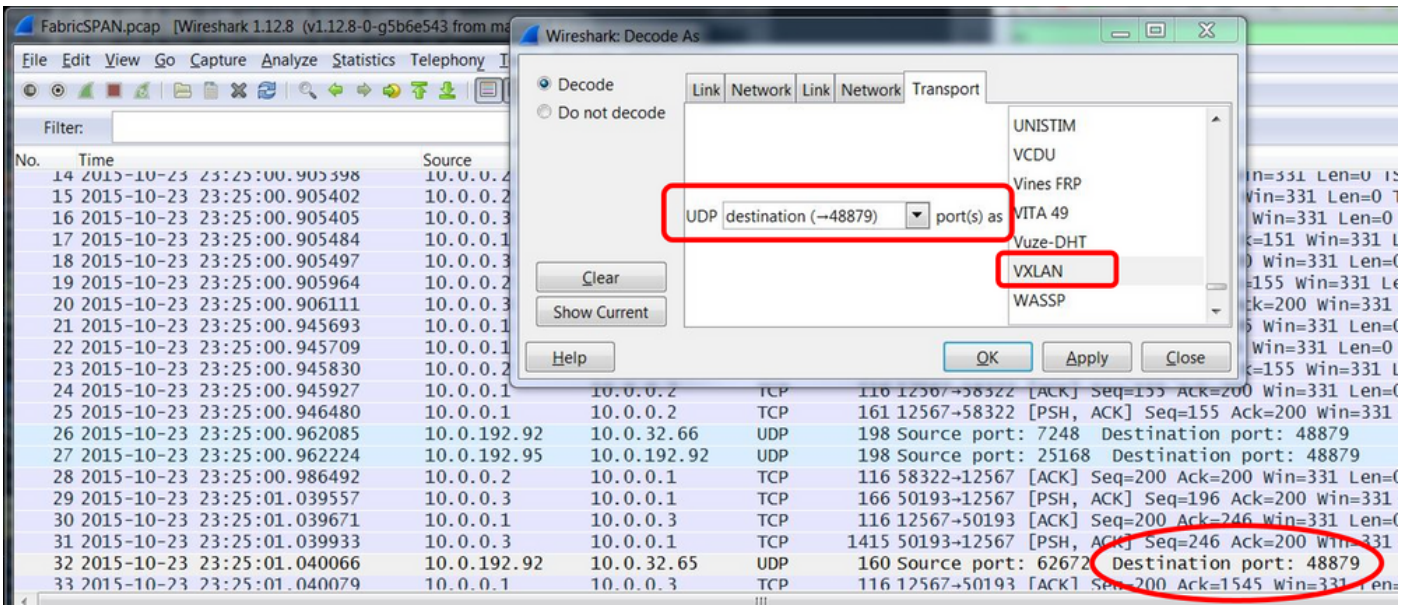


Remarque : veillez à désactiver cette option lorsque vous lisez ERSPAN de type II ou III.

Option 2. Naviguez jusqu'à Decode As > Network > ICMP (if it’s ICMP).



Comment décoder l'en-tête iVxLAN

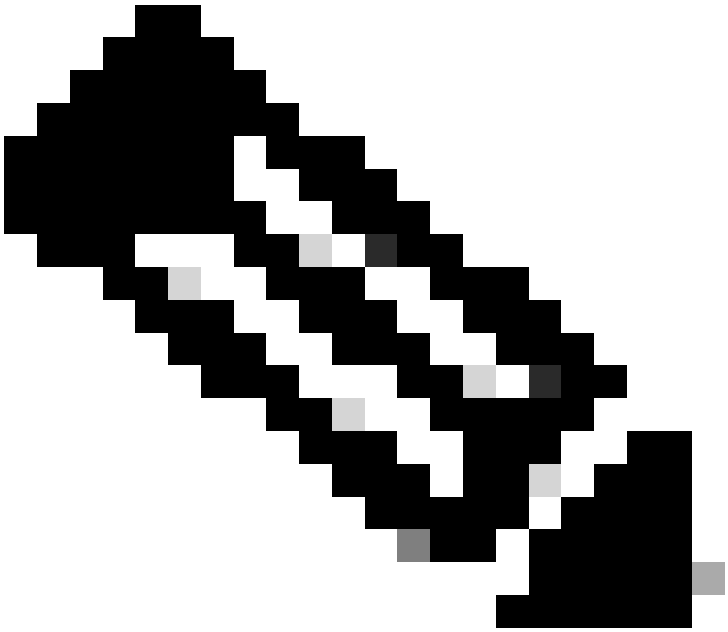


L'en-tête VxLAN utilise le port de destination 48879. Ainsi, vous pouvez décoder l'en-tête iVxLAN ainsi que VxLAN si vous configurez le port de destination UDP 48879 comme VxLAN sur Wireshark.

1. Assurez-vous de sélectionner d'abord les paquets encapsulés iVxLAN.

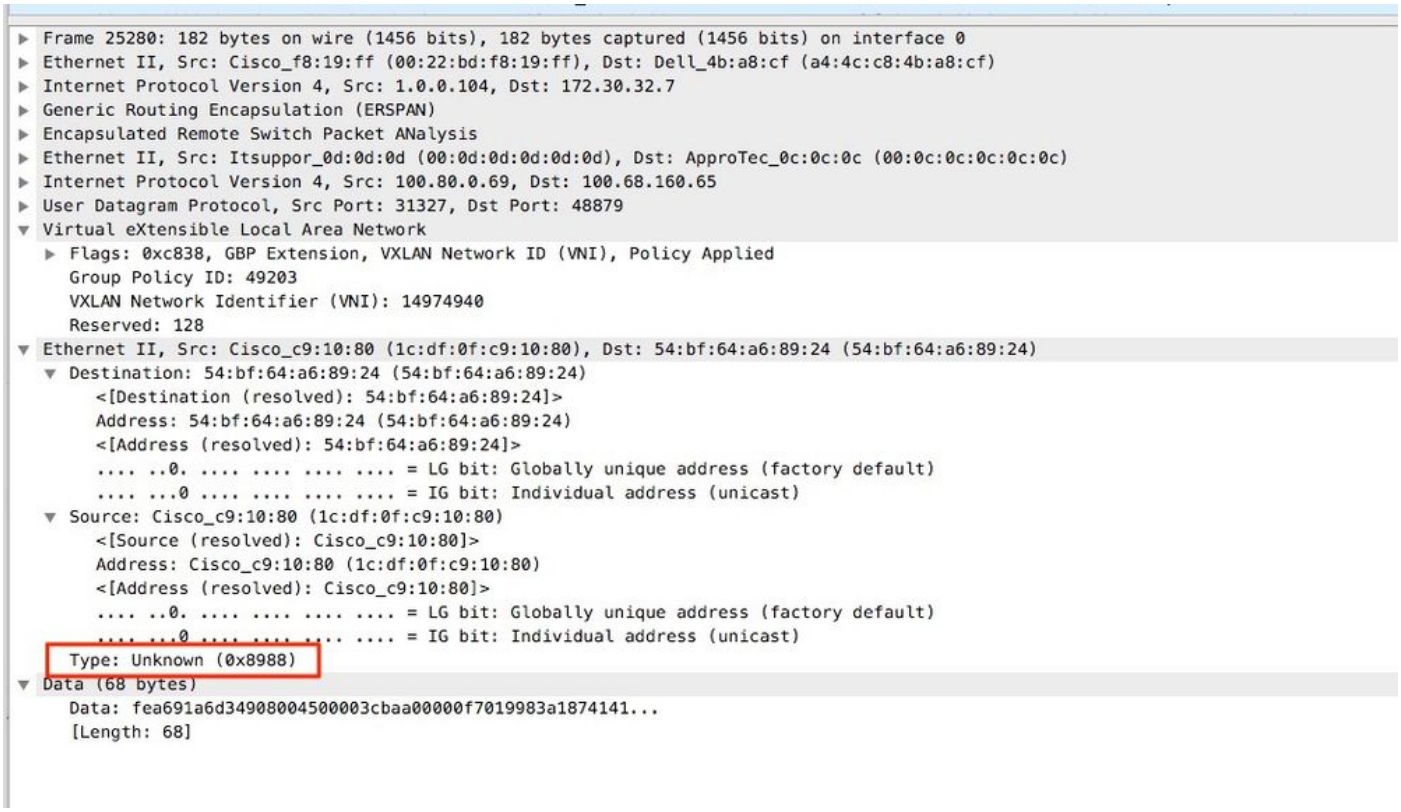
2. Accédez à Analyze > Decode As > Transport > UDP destination (48879) > VxLAN.

   - Et puis Apply.



Remarque : il existe des paquets de communication entre les cartes APIC sur les ports du fabric. Ces paquets ne sont pas encapsulés par l'en-tête iVxLAN.

Lorsque vous effectuez une capture Erspan sur un réseau utilisateur qui exécute le protocole PTP (Precision Time Protocol), il arrive que Wireshark n’interprète pas les données en raison d’un ethertype inconnu dans l’encapsulation GRE (0x8988). 0x8988 est l’ethertype de la balise time qui est insérée dans les paquets du plan de données lorsque le protocole PTP est activé. Décodez l'ethertype 0x8988 en tant que « balise Cisco » pour exposer les détails du paquet.


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]

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.