

ACI SPAN指南

目錄

[簡介](#)

[背景資訊](#)

[思科ACI中的SPAN型別](#)

[限制和指導原則](#)

[組態](#)

[存取SPAN \(ERSPAN\)](#)

[示例拓撲](#)

[組態範例](#)

[存取SPAN \(本地\)](#)

[示例拓撲](#)

[組態範例](#)

[存取SPAN -使用ACL過濾器](#)

[租使用者SPAN \(ERSPAN\)](#)

[示例拓撲](#)

[組態範例](#)

[光纖SPAN \(ERSPAN\)](#)

[示例拓撲](#)

[組態範例](#)

[GUI驗證](#)

[選擇ACI SPAN型別](#)

[存取SPAN \(ERSPAN\)](#)

[案例 1.源「Leaf1 e1/11 e1/34和Leaf2 e1/11」| Dst「192.168.254.1」](#)

[案例 2.源「Leaf1 e1/11和Leaf2 e1/11」| Dst「192.168.254.1」](#)

[案例 3.Src「Leaf1 e1/11和Leaf2 e1/11和EPG1過濾器」| Dst「192.168.254.1」](#)

[案例 4.源「Leaf1-Leaf2 vPC」| Dst「192.168.254.1」](#)

[存取SPAN \(本地SPAN\)](#)

[案例 1.源「Leaf1 e1/11 e1/34」| Dst「Leaf1 e1/33」](#)

[案例 2.Src「Leaf1 e1/11 e1/34和EPG1過濾器」| Dst「Leaf1 e1/33」](#)

[案例 3.源「Leaf1 e1/11和Leaf2 e1/11」| Dst「Leaf1 e1/33」\(錯誤案例\)](#)

[案例 4.Src「Leaf1 e1/11和EPG3過濾器」| Dst「Leaf1 e1/33」\(錯誤案例\)](#)

[案例 5: 源「EPG1過濾器」| Dst「Leaf1 e1/33」\(錯誤案例\)](#)

[案例 6.源「Leaf1 - Leaf2 vPC」| Dst「Leaf1 e1/33」\(錯誤案例\)](#)

[案例 7.源「Leaf1 e1/11」| Dst「Leaf1 e1/33和e1/33屬於EPG」\(工作有故障\)](#)

[租使用者SPAN \(ERSPAN\)](#)

[案例 1.源「EPG1」| Dst「192.168.254.1」](#)

[光纖SPAN \(ERSPAN\)](#)

[案例 1.Src「Leaf1 e1/49-50」| Dst「192.168.254.1」](#)

[案例 2.Src「Leaf1 e1/49-50和VRF過濾器」| Dst「192.168.254.1」](#)

[案例 3.Src「Leaf1 e1/49-50 & BD filter」| Dst「192.168.254.1」](#)

[您在SPAN目的地裝置上需要什麼？](#)

[對於ERSPAN](#)

[本地SPAN](#)

[如何讀取ERSPAN資料](#)

[ERSPAN版本 \(型別 \)](#)

[ERSPAN型別I \(由Broadcom Trident 2使用 \)](#)

[ERSPAN型別II或III](#)

[ERSPAN資料範例](#)

[租戶SPAN/存取SPAN \(ERSPAN\)](#)

[擷取封包的詳細資訊 \(ERSPAN型別I \)](#)

[光纖SPAN \(ERSPAN\)](#)

[擷取封包的詳細資訊 \(ERSPAN型別II \)](#)

[如何解碼ERSPAN型別](#)

[如何解碼IPv4LAN報頭](#)

簡介

本檔案介紹如何在思科以應用程式為中心的基礎設施(ACI)上設定交換連線埠分析器(SPAN)。

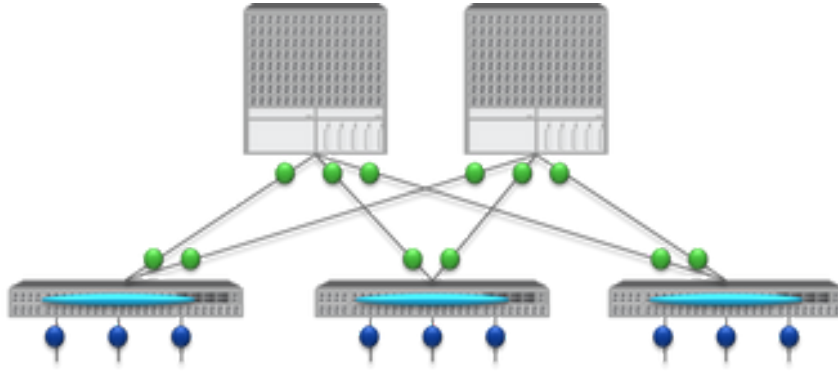
背景資訊

一般而言，SPAN有三種型別。本地SPAN、遠端SPAN (RSPAN)和封裝遠端SPAN (ERSPAN)。這些SPAN之間的差異主要是複製封包的目的地。Cisco ACI支援本地SPAN和ERSPAN。



附註：本檔案假設讀者已大致熟悉SPAN，例如本地SPAN和ERSPAN差異。

思科ACI中的SPAN型別



== TYPE ==	== SRC ==	== DST ==
● Fabric SPAN	SPAN on Fabric ports on Spine or Leaf	→ ERSPAN (remote IP)
● Tenant SPAN	SPAN on EPG(=VLAN) on Leaf	→ ERSPAN (remote IP)
● Access SPAN	SPAN on Access ports on Leaf	→ ERSPAN (remote IP) → Local SPAN (Local port)

※ Infra SPAN = Access SPAN

思科ACI有三種型別的SPAN：Fabric SPAN、Tenant SPAN和Access SPAN。每個SPAN之間的差異是複製資料包的來源。

如前所述

- **Fabric SPAN** 是捕獲從 **interfaces between Leaf and Spine switches**傳入和傳出的資料包。
- Access SPAN 是捕獲從 **interfaces between Leaf switches and external devices**傳入和傳出的資料包。
- Tenant SPAN 是捕獲從 **EndPoint Group (EPG) on ACI Leaf switches**傳入和傳出的資料包。

此SPAN名稱對應於Cisco ACI GUI上的設定位置。

- 交換矩陣SPAN配置在 Fabric > Fabric Policies
- 接入SPAN配置在 Fabric > Access Policies

- 租戶SPAN配置在 Tenants > {each tenant}

至於每個SPAN的目的地而言，只有Access SPAN可以同時使用Local SPAN和ERSPAN。其他兩個SPAN(Fabric和Tenant)只能使用ERSPAN。

限制和指導原則

請檢視[思科APIC故障排除指南](#)的限制和指導原則。在Troubleshooting Tools and Methodology > Using SPAN中提到它。

組態

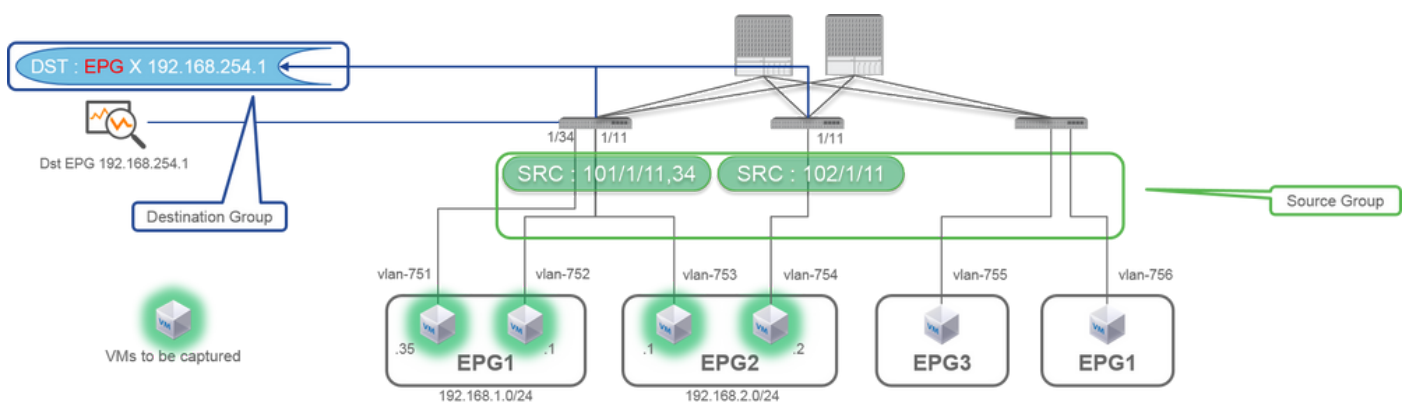
本節介紹與每個SPAN型別的設定相關的簡短範例。在後面的部分中，有關於如何選擇範圍型別的特定示例情況。

[思科APIC故障排除指南：故障排除工具和方法>使用SPAN](#) 中還對SPAN配置進行了說明。

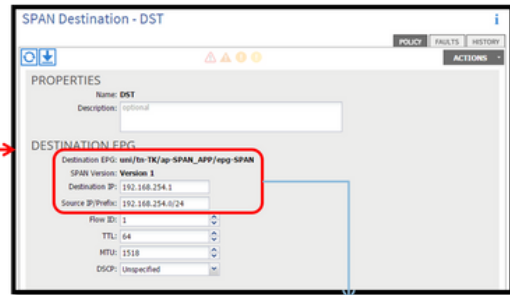
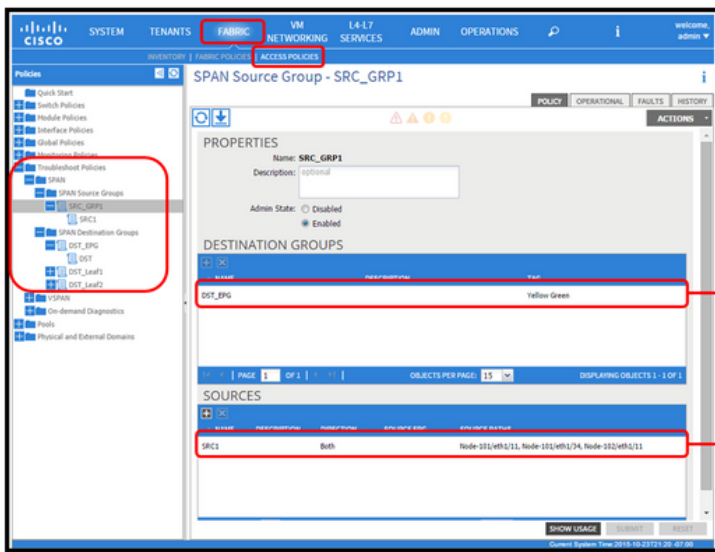
UI可能顯示不同於當前版本，但配置方法相同。

存取SPAN (ERSPAN)

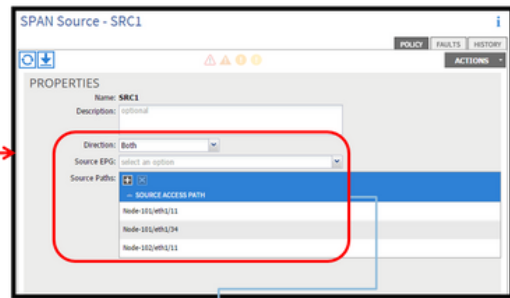
示例拓撲



組態範例



SPAN Version :
 ERSPAN Type
 ERSPAN dst IP :
 SPAN packet will be thrown to this IP. Need to be learned as EP in Dst EPG.
 ERSPAN src IP :
 192.168.254.254 : every Leaf use this
 192.168.254.0/24 : each Leaf use it's own node id (ex. 192.168.254.101)



Direction :
 Both / Incoming / Outgoing
 Source EPG :
 Option. When you need EPG(VLAN) filter.
 Source Paths :
 Normal port, PC, vPC

其中：

導航到FABRIC > ACCESS POLICIES > Troubleshoot Policies > SPAN。

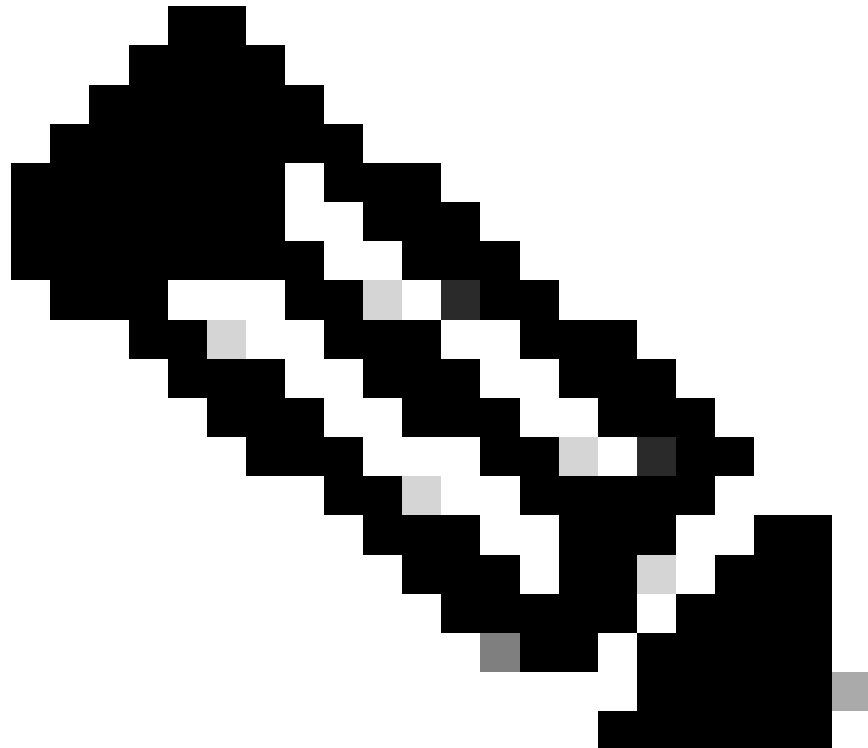
- SPAN Source Groups
- SPAN Destination Groups

SPAN Source Group 領帶Destination和Sources。

方式：

1. Create SPAN Source Group (SRC_GRP1)。

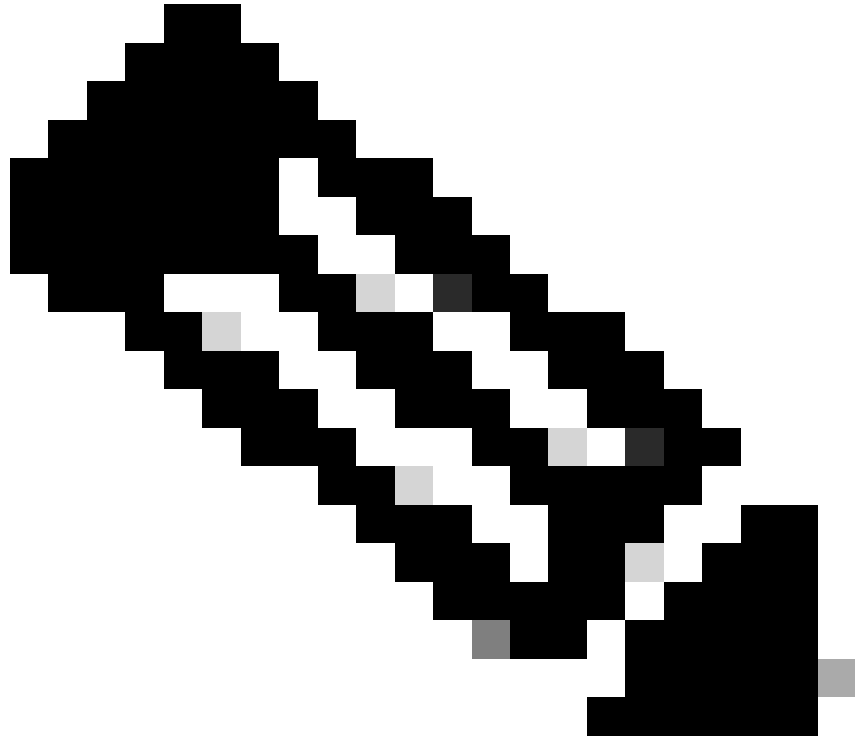
- 在SPAN Source Group (SRC_GRP1)下建立SPAN Source(SRC1)。
 - 為SPAN Source(SRC1)配置這些引數。
 - 方向-源EPG (選項)
 - 源路徑 (可以是多個介面)
-



注意：請參閱圖片瞭解每個引數的詳細資訊。

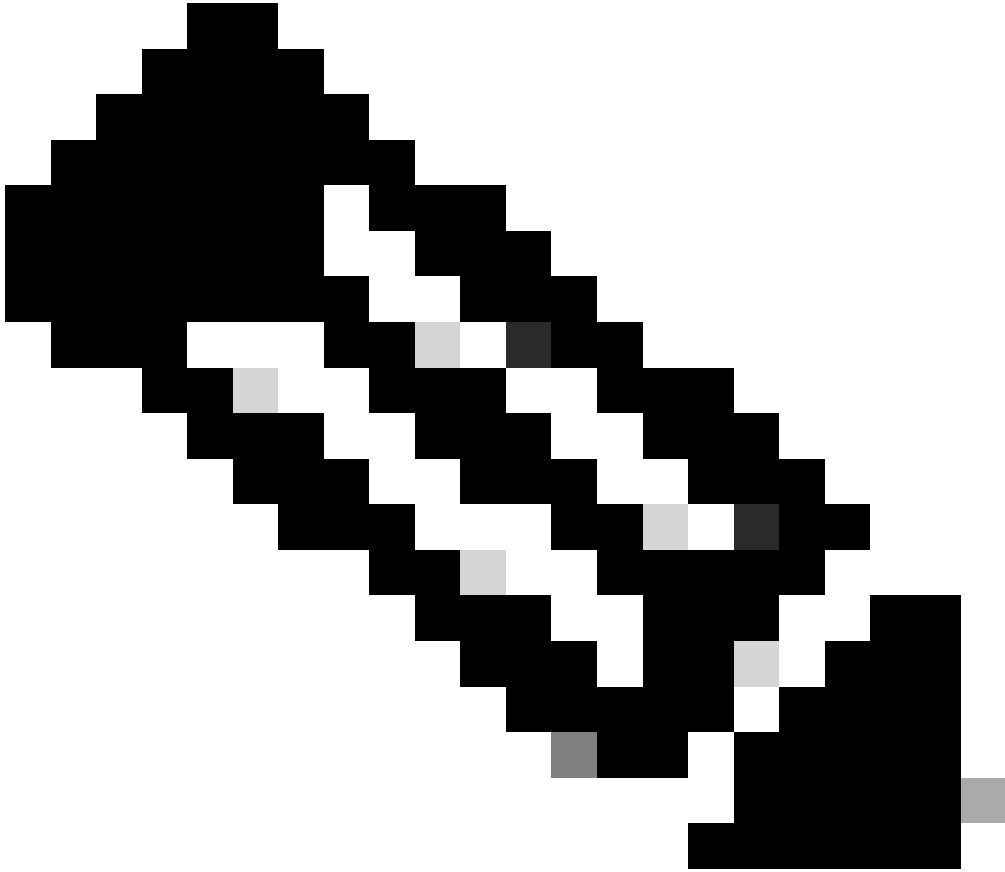
-
- 建立SPAN Destination Group(DST_EPG)。
 - 建立SPAN Destination (DST)。
 - 為SPAN Destination(DST)配置這些引數

- 目標EPG
 - 目的地 IP
 - 來源IP/首碼(可以是任何IP。如果使用字首，則源節點的節點ID用於未定義的位。例如，字首：節點101上的1.0.0.0/8 => src IP 1.0.0.101)
 - 其他引數可以保留為預設值
-



注意：請參閱圖片瞭解每個引數的詳細資訊。

-
- 確保SPAN Destination Group繫結到適當的SPAN Source Group。
 - 確定Admin State已啟用。
-
-

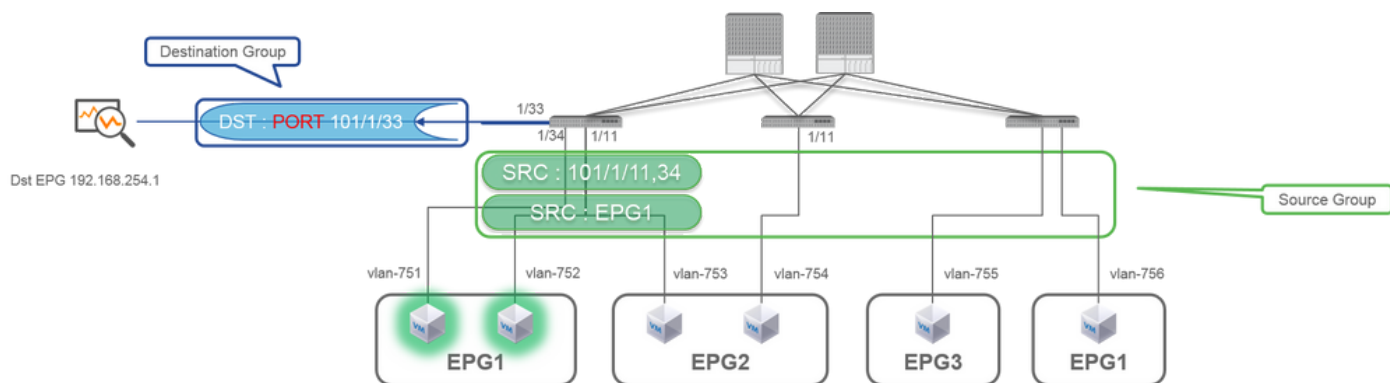


注意：當您在此管理狀態上選擇已停用時，SPAN將停止。如果以後重複使用這些策略，則不需要刪除所有策略。

另外，請確保將ERSPAN的目標IP獲知為指定目標EPG下的終端。在前面的示例中，必須在Tenant TK > Application profile SPAN_APP > EPG SPAN下獲取192.168.254.1。或者，如果目標裝置是靜默式主機，則可以在此EPG下將目標IP配置為靜態終端。

存取SPAN (本地)

示例拓撲



組態範例

Configuration screenshots for a SPAN Source Group:

SPAN Source Group - SRC_GRP1

PROPERTIES

Name: SRC_GRP1

Description: optional

Admin State: Disabled

DESTINATION GROUPS

ID	NAME	DESCRIPTION	TAG
1	DST_Leaf1		Yellow Green

SOURCES

ID	NAME	DESCRIPTION	DIRECTION	SOURCE EPG	SOURCE PATHS
1	SRC1		Both	TSPAN_APP/EPG1	Node-101/eth1/11, Node-101/eth1/24

SPAN Destination - DST

PROPERTIES

Name: DST

Description: optional

DESTINATION ACCESS PATH

Destination Path: Node-101/eth1/33

SPAN Source - SRC1

PROPERTIES

Name: SRC1

Description: optional

Direction: Both

Source EPG: uni/tn-TK/ap-SPAN_APP/epg-EPG1

Source Paths

SOURCE ACCESS PATH

Node-101/eth1/11

Node-101/eth1/24

• 其中：

Fabric > ACCESS POLICIES > Troubleshoot Policies > SPAN

- SPAN Source Groups

- SPAN Destination Groups

SPAN Source Group 領帶Destination 和 Sources.

- 方式：

1. 建立SPAN Source Group(SRC_GRP1)

- 在SPAN Source Group (SRC_GRP1)下建立(SPAN SourceSRC1)
- 為SPAN Source(SRC1)配置這些引數
 - 方向
 - 源EPG (選項)
 - 源路徑 (可以是多個介面)※請參閱圖片以瞭解每個引數的詳細資訊。
- 建立SPAN Destination Group(DST_Leaf1)
- 建立SPAN Destination(DST)
- 為SPAN Destination(DST)配置這些引數
 - 目標介面和節點。
- 確保SPAN Destination Group繫結到適當的SPAN Source Group。
-

確保Admin State已啟用。

當您在此管理狀態上選取停用※，SPAN便會停止。如果以後重複使用這些策略，則不需要刪除所有策略。

目標介面不需要按介面策略組進行任何配置。當您將電纜插入ACI枝葉上的介面時，它可以正常工作。

限制：

- 對於本地SPAN，必須在同一枝葉上配置目標介面和源介面。
- 只要目標介面處於UP狀態，它就不要求它位於EPG上。
- 將虛擬連線埠通道(vPC)介面指定為來源連線埠時，無法使用本地SPAN
但是，有一個解決方法。在第一代枝葉交換機上，作為vPC或PC成員的單個物理埠可以配置為SPAN源。透過此本地SPAN，可用於vPC埠上的流量。
但是，此選項在第二代枝葉([CSCvc11053](#))上不可用。相反，在2.1(2e)、2.2(2e)和轉發版本中，增加了[viaCSCvc44643](#)對「VPC元件PC」上SPAN的支援。這樣，任何世代枝葉都可以將作為vPC成員的埠通道配置為SPAN源。這允許任何世代枝葉對vPC埠上的流量使用本地SPAN。
- 在第二代枝葉上指定埠通道的各個埠僅導致資料包的子集被跨接(也由[於CSCvc11053](#))。
- PC和vPC不能用作本地SPAN的目的埠。從4.1(1)開始，PC可作為本地SPAN的目的埠連線埠。

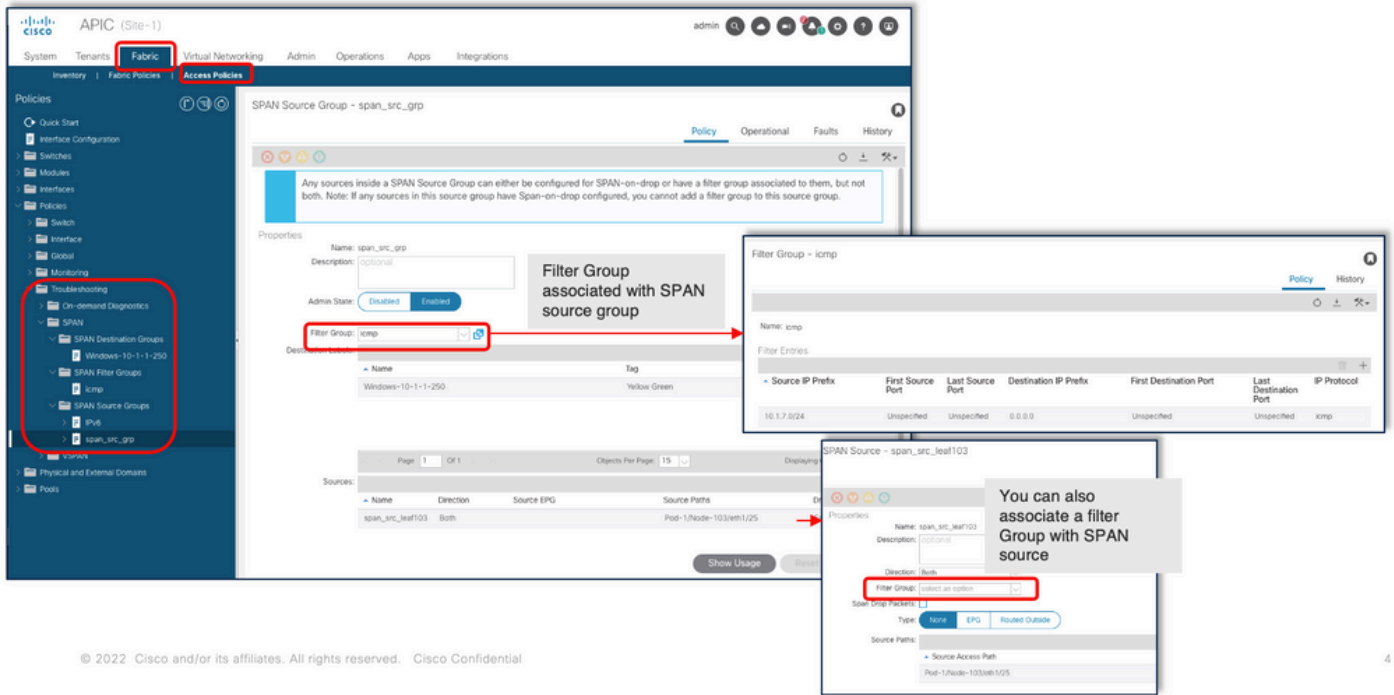
存取SPAN -使用ACL過濾器

您可以在存取SPAN來源上使用ACL過濾器。此功能提供跨SPAN來源之間的特定流量或流量流量的能力。當需要SPAN流量特定流量時，使用者可以將SPAN Acl套用到來源。交換矩陣SPAN和租戶SPAN源組/源不支援該功能。在過濾器組中增加過濾器條目時必須小心，因為它可以為當前使用過濾器組的每個源增加tcam條目。

「篩選群組」可以關聯至：

- Span源：過濾器組用於過濾在此Span源下定義的所有介面上的流量。
- Span源組：過濾器組(例如x)用於過濾在此Span源組的每個Span源下定義的所有介面上的流量。

在此配置快照中，過濾器組應用到Span源組。

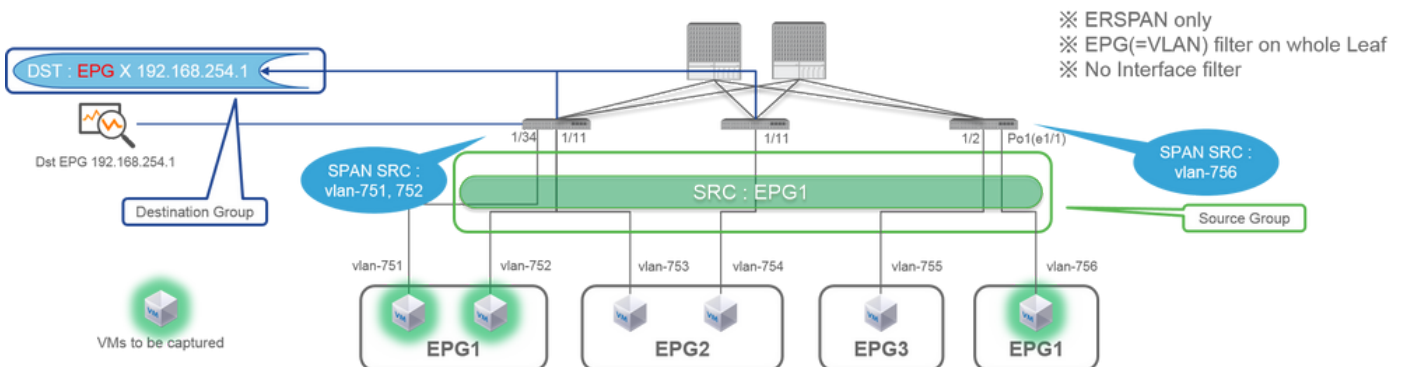


如果特定Span來源已經與篩選群組建立關聯（例如y），則會使用該篩選群組(y)來篩選此特定Span來源下所有介面上的群組

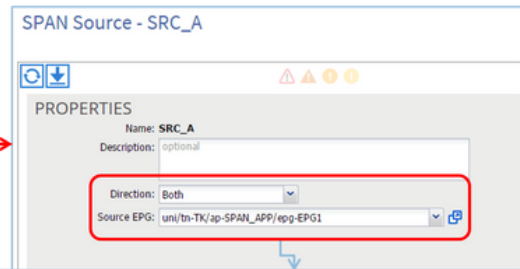
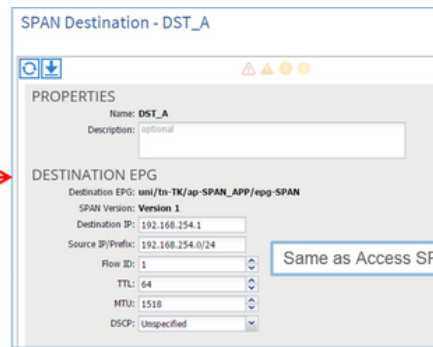
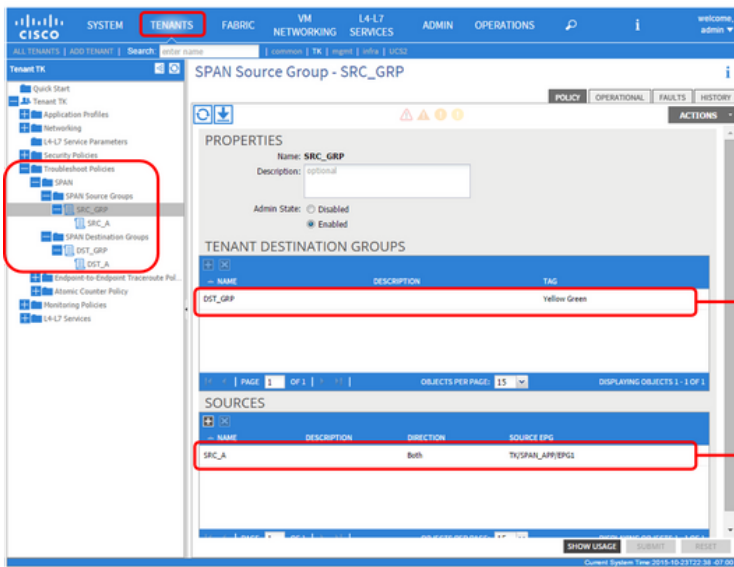
- 在來源群組套用的篩選群組會自動套用至該來源群組中的所有來源。
- 在源應用的過濾器組僅適用於該源。
- 過濾器組同時應用於源組以及該源組中的源，在源處應用的過濾器組優先。
- 刪除在來源套用的篩選群組，在父項來源群組套用的篩選群組會自動套用。
- 在來源群組套用的篩選群組會被刪除，它也會從目前繼承於該來源群組的所有來源中刪除。

租使用者SPAN (ERSPAN)

示例拓撲



組態範例



Direction :
Both / Incoming / Outgoing
Source EPG :
SPAN source EPG.
(appropriate VLAN sources are automatically configured on each Leaf)
(Source Paths cannot be configured)

• 其中：

Tenants > {tenant name} > Troubleshoot Policies > SPAN

- SPAN Source Groups

- SPAN Destination Groups

※ SPAN來源群組關聯Destination和Sources.

• 方式：

1. 建立SPAN Source Group(SRC_GRP)

- 在SPAN Source Group(SRC_GRP)下建立SPAN Source(SRC_A)

- 為SPAN Source(SRC_A)配置這些引數

- 方向
- 源EPG

※請參閱圖片瞭解每個引數的詳細資訊。

- 建立SPAN Destination Group(DST_GRP)

- 建立SPAN Destination (DST_A)

- 為SPAN Destination(DST_A)配置這些引數

- 目標EPG
- 目的地 IP
- 源IP/字首
- 其他引數可以保留為預設值

※請參閱圖片瞭解每個引數的詳細資訊。

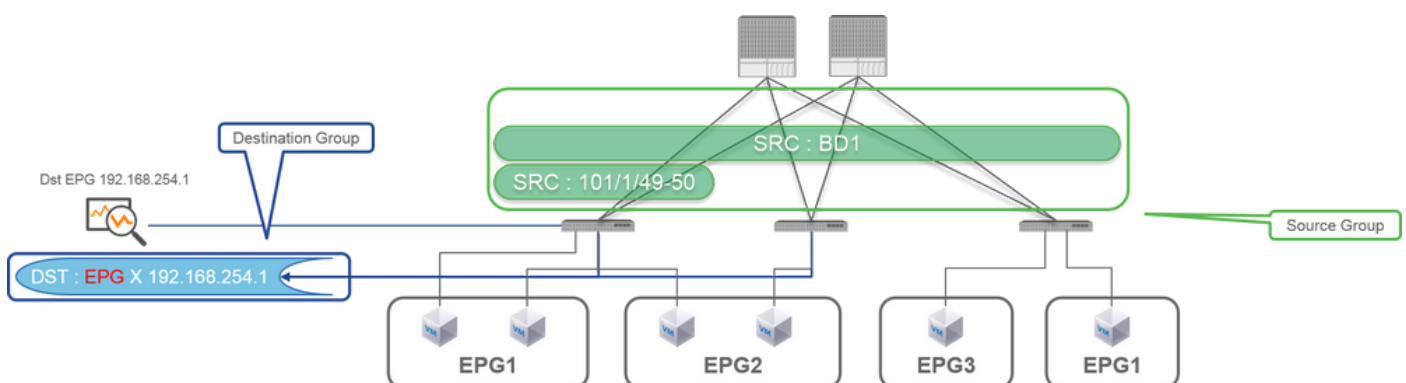
- 確保SPAN Destination Group繫結到適當的SPAN Source Group。

- 確保Admin State已啟用。

當您在此管理狀態上選取停用※，SPAN便會停止。如果以後重複使用這些策略，則不需要刪除所有策略。

光纖SPAN (ERSPAN)

示例拓撲



組態範例

The image shows a Cisco Fabric Manager interface with three main panels:

- Left Panel:** Navigation tree showing 'FABRIC POLICIES' > 'Troubleshoot Policies' > 'SPAN' > 'SPAN Source Groups' > 'SRC_GRP'.
- Center Panel:** 'SPAN Source Group - SRC_GRP' configuration page. It shows 'DESTINATION GROUPS' with a table:

NAME	DESCRIPTION	TAG
DST_GRP		Yellow Green

 Below this is a 'SOURCES' table:

NAME	DESCRIPTION	DIRECTION	SOURCE PATHS
SRC_A		Both	Node-101/eth1/49, Node-101/eth1/50
- Right Panel (Top):** 'SPAN Destination - DST_A' configuration page. It shows 'DESTINATION EPG' with 'SPAN Version: Version 2' highlighted. A callout box notes: 'SPAN Version (ERSPAN Type) : 2 Others are same as Access SPAN'.
- Right Panel (Bottom):** 'SPAN Source - SRC_A' configuration page. It shows 'Direction: Both' and 'Source Paths' including 'SOURCE FABRIC PATH' with sub-items 'Node-101/eth1/49' and 'Node-101/eth1/50'. A callout box notes: 'Direction : Both / Incoming / Outgoing Private Network / Bridge Domain : Either of them. Filter packets on Fabric ports with specific VRF/BD'.

• 其中：

Fabric > FABRIC POLICIES > Troubleshoot Policies > SPAN

- Fabric

- SPAN Destination Groups

※SPAN Source Group 領帶 Destination 和 Sources

• 方式：

1. 建立SPAN Source Group(SRC_GRP)

- 在SPAN Source Group(SRC_GRP)下建立SPAN Source(SRC_A)

- 為SPAN Source(SRC_A)配置這些引數

- 方向
- 私人網路 (選項)
- 橋接域 (選項)
- 源路徑 (可以是多個介面)

※請參閱圖片以瞭解每個引數的詳細資訊。

- 建立SPAN Destination Group(DST_GRP)

- 建立SPAN Destination (DST_A)

- 為SPAN Destination(DST_A)配置這些引數

- 目標EPG
- 目的地 IP
- 源IP/字首
- 其他引數可以保留為預設值

※請參閱圖片以瞭解每個引數的詳細資訊。

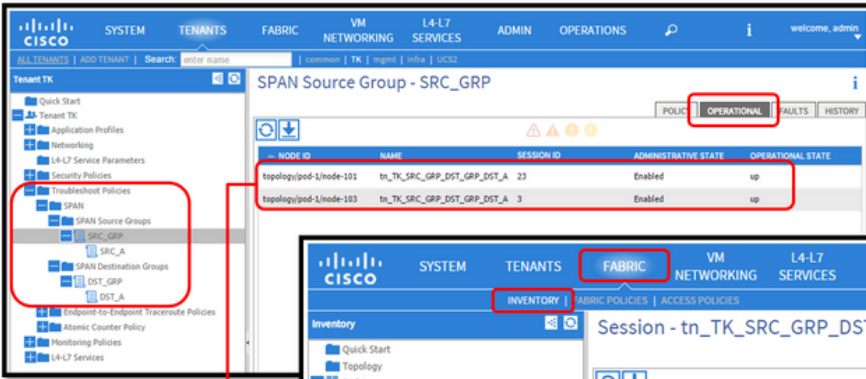
- 確保SPAN Destination Group繫結到適當的SPAN Source Group。

- 確定Admin State 已啟用。

※此Admin State上選取停用時，SPAN會停止。如果以後重複使用這些策略，則不需要刪除所有策略。

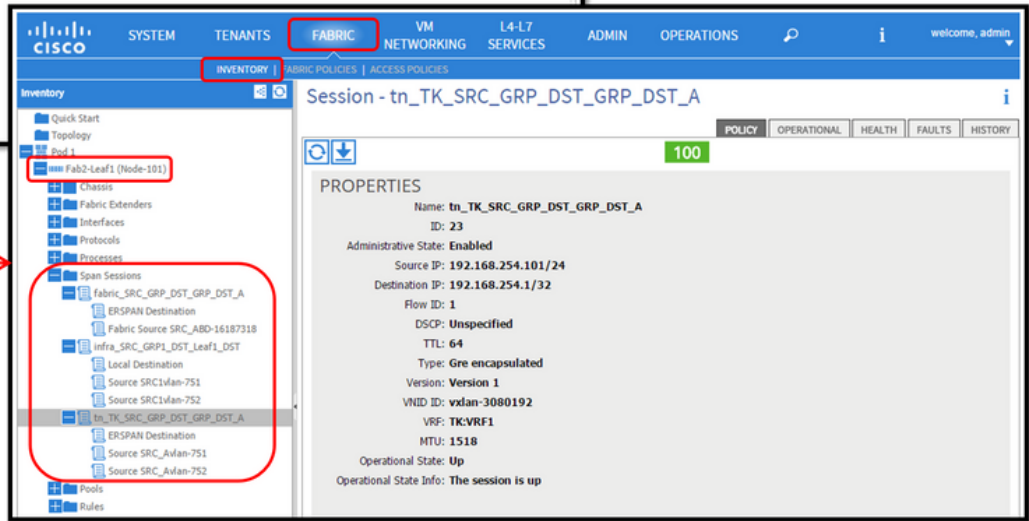
雖然稍後的「ERSPAN版本 (型別)」一節會對此進行說明，但您可以判斷ERSPAN版本II用於網狀架構SPAN，而版本I用於租戶和存取SPAN。

GUI驗證



✳ See Use Case for CLI verification

Double Click



• 驗證SPAN設定原則

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

請確保運行狀態為up。

- 在節點本身驗證SPAN作業階段

1. 連按兩下來自SPAN Configuration Policy或的每個階段作業 Fabric > INVENTORY > Node > Span Sessions > { SPAN session name }

請確保運行狀態為up。

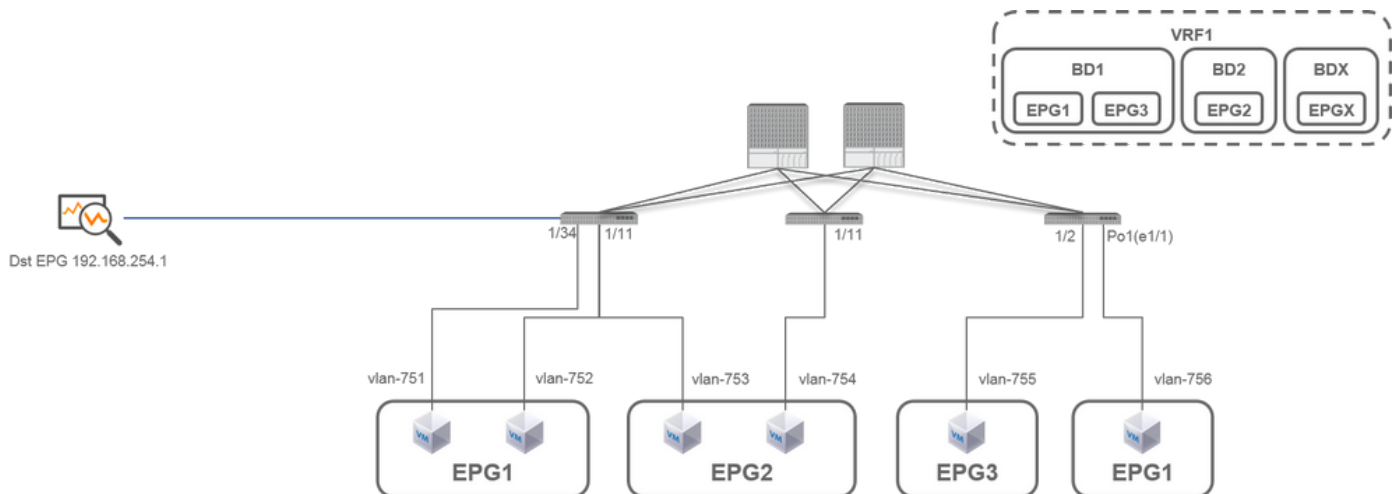
SPAN作業階段命名慣例：

- 交換矩陣SPAN：fabric_xxxx

- 存取SPAN：infra_xxxx

- 租戶SPAN：tn_xxxx

選擇ACI SPAN型別

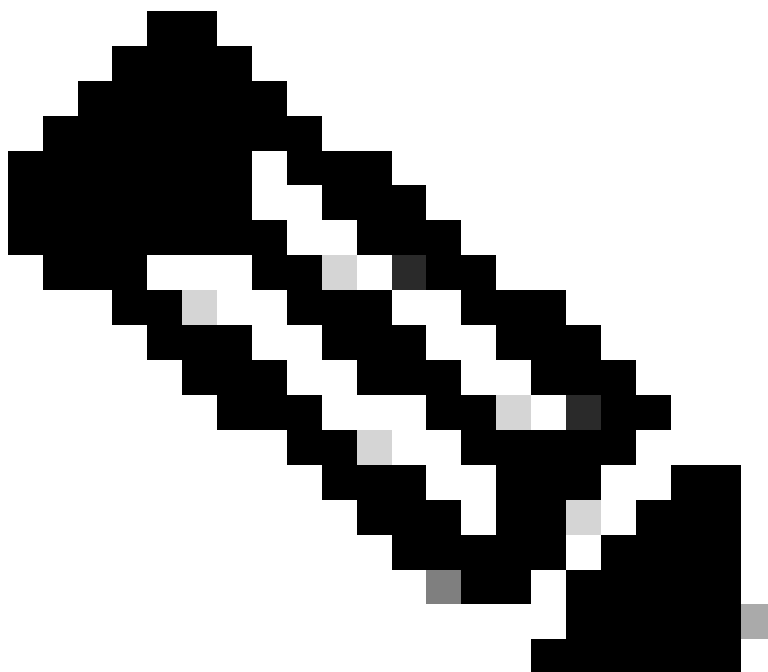


本節介紹每個ACI SPAN型別的詳細方案(Access, Tenant, Fabric)。上一個部分介紹了每個方案的基礎拓撲。

如果您瞭解這些場景，則可以根據需要選擇適當的ACI SPAN型別，例如必須僅捕獲特定介面上的資料包或捕獲特定EPG上的所有資料包（無論介面如何），等等。

在Cisco ACI中，SPAN是使用source group和destination group配置的。源組包含多個源因素，例如介面或EPG。目的地群組包含目的地資訊，例如本地SPAN的目的地介面或ESPAN的目標IP。

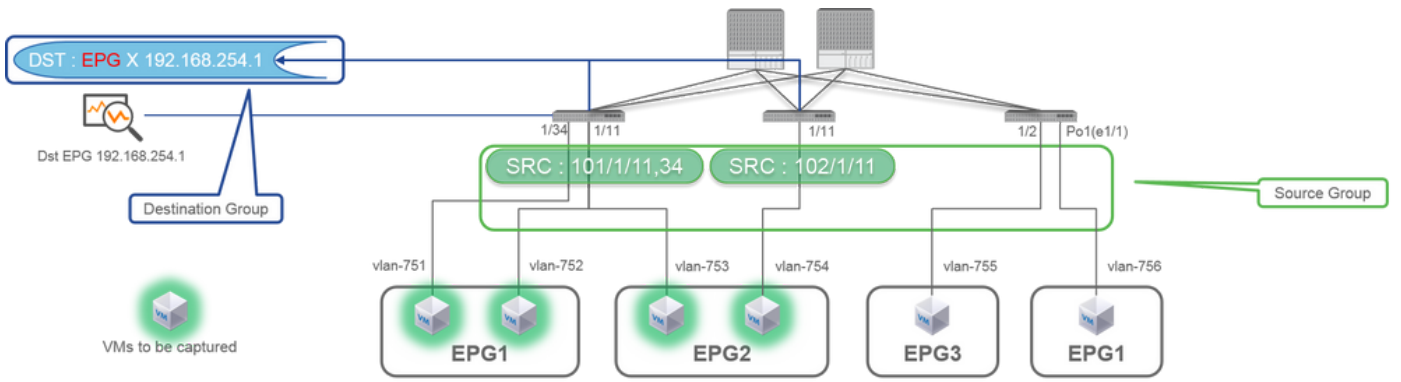
擷取封包後，請參閱「如何讀取SPAN資料」一節以解碼擷取封包。



注意：請重點關注每個拓撲中以綠色指示燈突出顯示的虛擬機器。每種場景都是從這些突出顯示的虛擬機器捕獲資料包。

存取SPAN (ERSPAN)

案例 1.源「Leaf1 e1/11 e1/34和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       :
granularity     : 1
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       :
granularity     : 1
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
 - 枝葉1 e1/11
 - 枝葉1 e1/34
 - 枝葉2 e1/11

- Destination Group
 - EPG X上的192.168.254.1

存取SPAN可以為一個SPAN作業階段指定多個介面。它可捕獲從指定介面傳入或傳出的所有資料包，而不管它們的EPG如何。

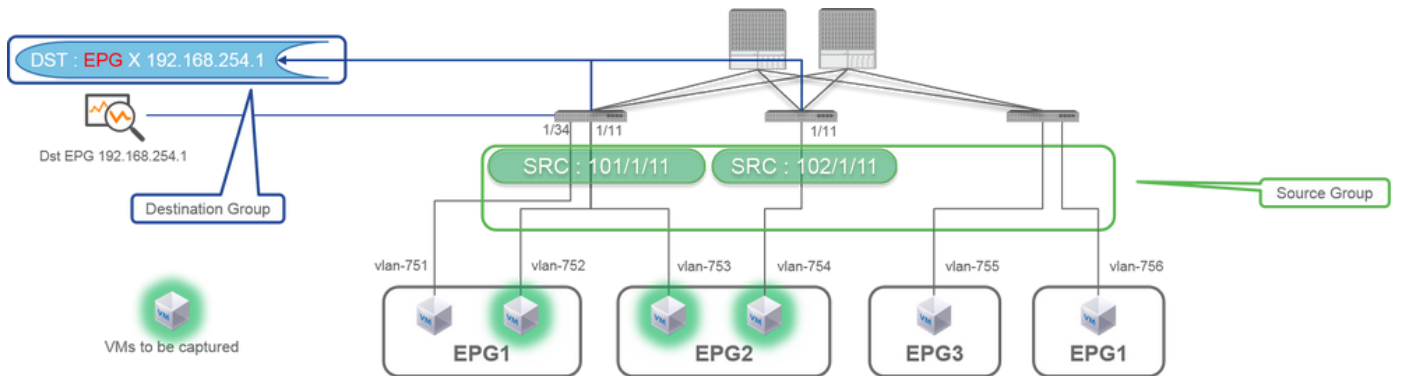
將多個介面指定為來自多個枝葉交換機的源組時，目標組必須是ERSPAN而不是本地SPAN。

在本示例中，它從EPG1和EPG2上的所有VM複製資料包。

CLI檢查點

- 請確保狀態為「up (active)」
- 「destination-ip」是ERSPAN的目標IP
- 「origin-ip」是ERSPAN的來源IP

案例 2.源「Leaf1 e1/11和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
```

- 來源群組

- 枝葉1 e1/11
- 枝葉2 e1/11

- 目標組

- EPG X上的192.168.254.1

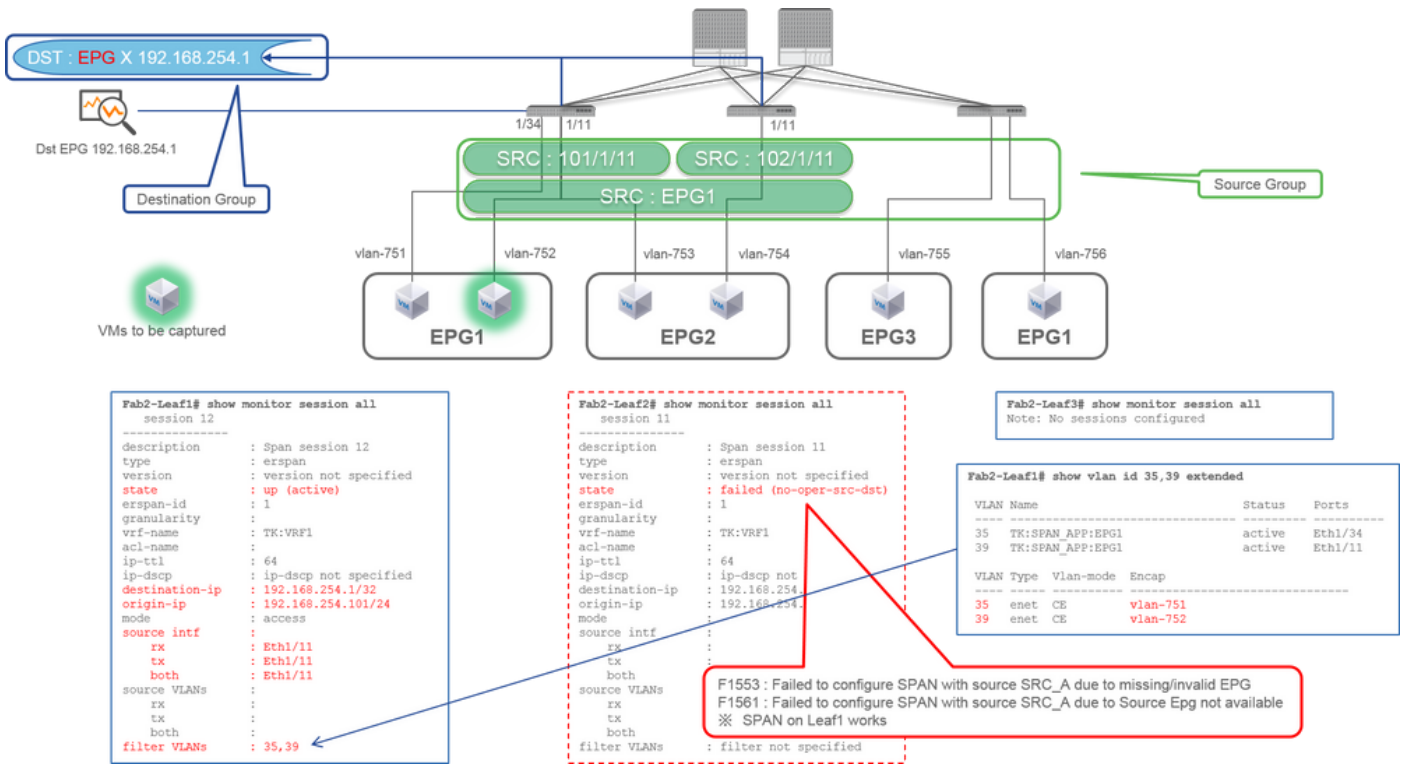
在本範例中，Leaf1 e1/34從之前案例1設定的SPAN來源群組移除。

此範例中的關鍵點在於，Access SPAN可以指定來源介面，而無論EPG如何。

CLI檢查點

- leaf1上的源介面已從「Eth1/11 Eth1/34」更改為「Eth1/11」

案例 3.Src「Leaf1 e1/11和Leaf2 e1/11和EPG1過濾器」 | Dst「192.168.254.1」



- 來源群組

- 枝葉1 e1/11
- 枝葉2 e1/11
- 過濾器EPG1

- 目標組

- EPG X上的192.168.254.1

此範例顯示，存取SPAN也可以在來源連線埠上指定特定的EPG。當多個EPG在單個介面上流動時，此功能非常有用，並且僅需要捕獲該介面上EPG1的流量。

由於EPG1未部署在Leaf2上，Leaf2的SPAN發生故障，故障為F1553和F1561。但是，Leaf1上的SPAN仍然有效。

此外，由於EPG1在Leaf1上使用兩個VLAN (VLAN-751,752)，因此會自動為Leaf1上的SPAN作業階段新增兩個VLAN過濾器。

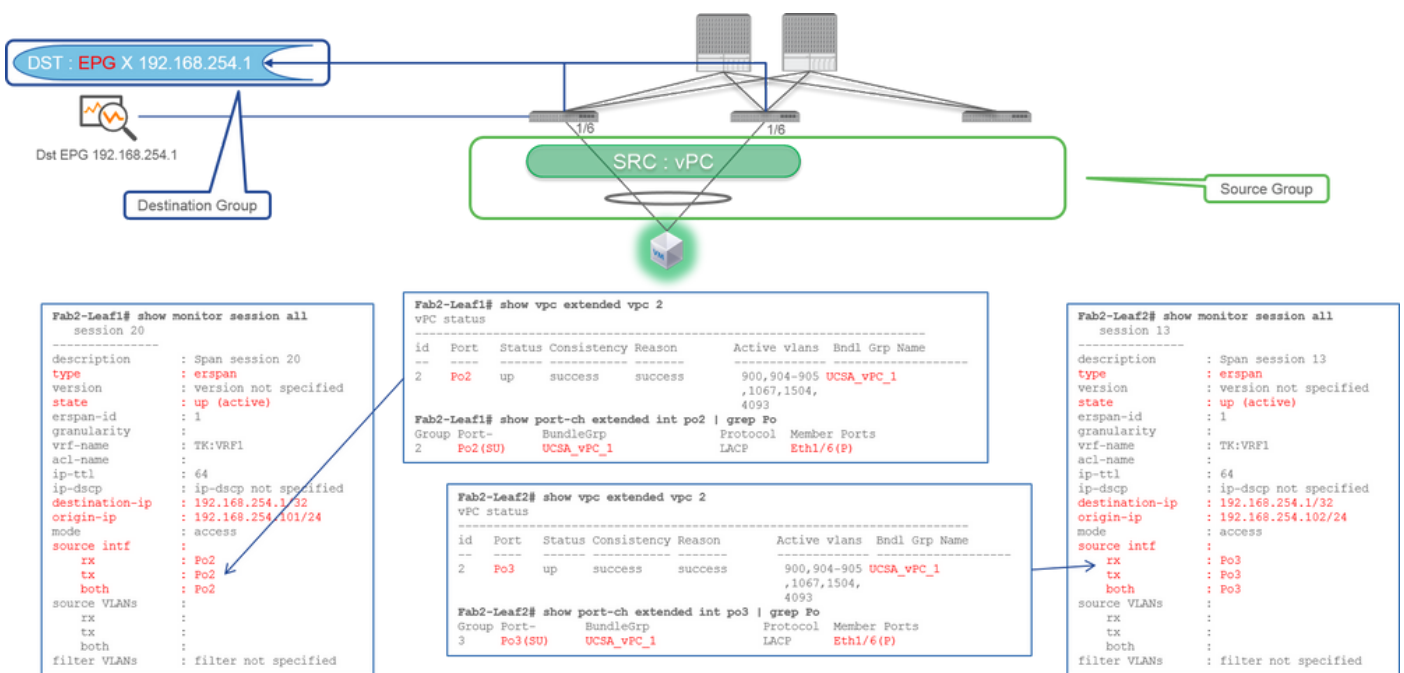
請注意，CLI(35、39)上的VLAN ID是內部VLAN，即所謂的PI-VLAN (平台獨立VLAN)，它不是線路上的實際ID。如圖所示，show vlan extended 命令顯示了實際封裝VLAN ID和PI-VLAN的對映。

即使EPG2 (VLAN-753)在相同介面上流動，此SPAN作業階段仍允許我們僅擷取Leaf1 e1/11上EPG1(VLAN-752)的封包。

CLI檢查點

- 過濾器VLAN是根據用於過濾器的EPG增加的。
- 如果枝葉上沒有對應的EPG，則該枝葉上的SPAN會話將失敗。

案例 4.源「Leaf1-Leaf2 vPC」 | Dst 「192.168.254.1」



- 來源群組

- 枝葉1 – 2e1/11

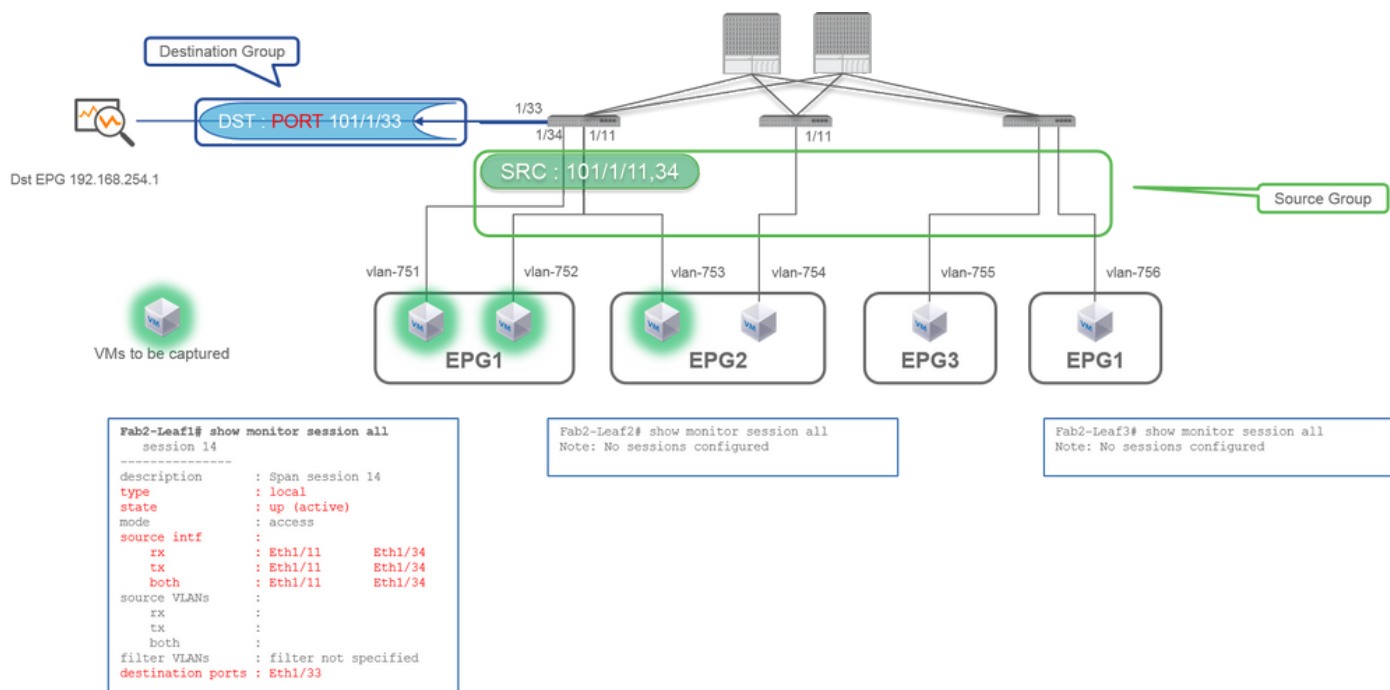
- 目標組

- EPG X上的192.168.254.1

將vPC介面設定為來源時，目的地必須為遠端IP (ERSPAN)而不是介面 (本地SPAN)

存取SPAN (本地SPAN)

案例 1.源「Leaf1 e1/11 e1/34」 | Dst 「Leaf1 e1/33」



- 來源群組

- 枝葉1 e1/11
- 枝葉1 e1/34

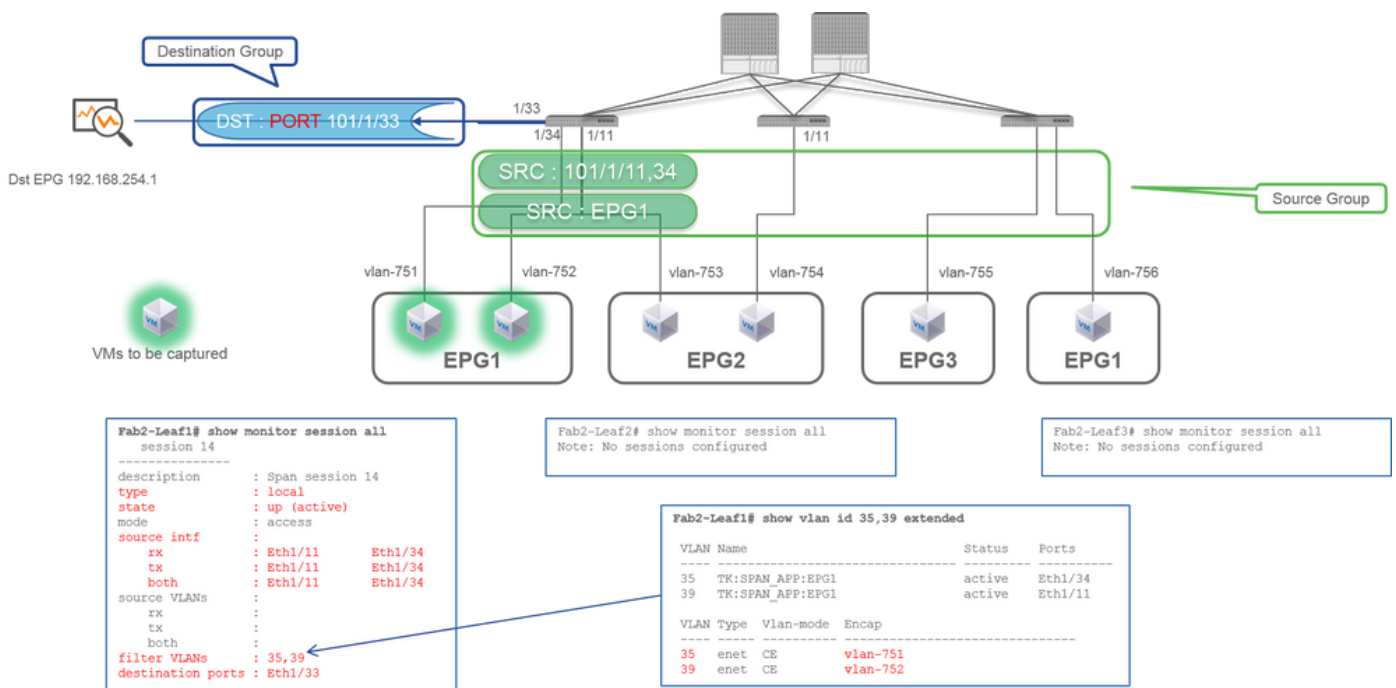
- 目標組

- 枝葉1 e1/33

存取SPAN也可以使用本地SPAN (即特定介面作為目的地)

但是，在這種情況下，源介面必須與目標介面位於同一枝葉上。

案例 2. Src "Leaf1 e1/11 e1/34和EPG1過濾器 | Dst "Leaf1 e1/33"

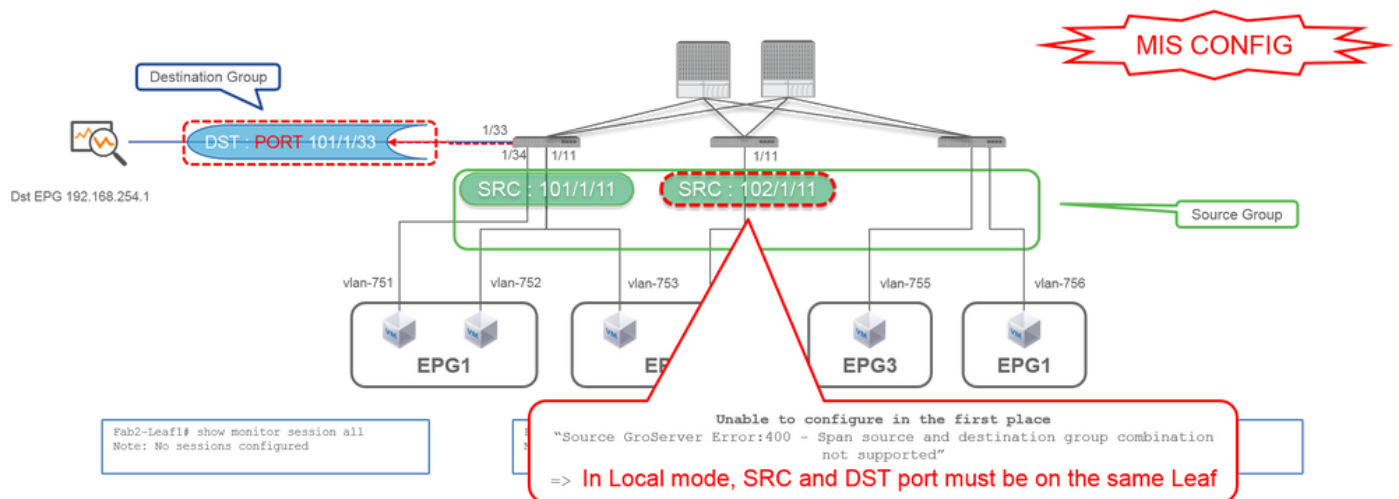


- 來源群組
 - 枝葉1 e1/11
 - 枝葉1 e1/34
 - EPG1過濾器

- 目標組
 - 枝葉1 e1/33

使用本地SPAN存取SPAN也可以使用EPG篩選和ERSPAN。

案例 3.源「Leaf1 e1/11和Leaf2 e/11」 | Dst「Leaf1 e1/33」(錯誤案例)



- 來源群組

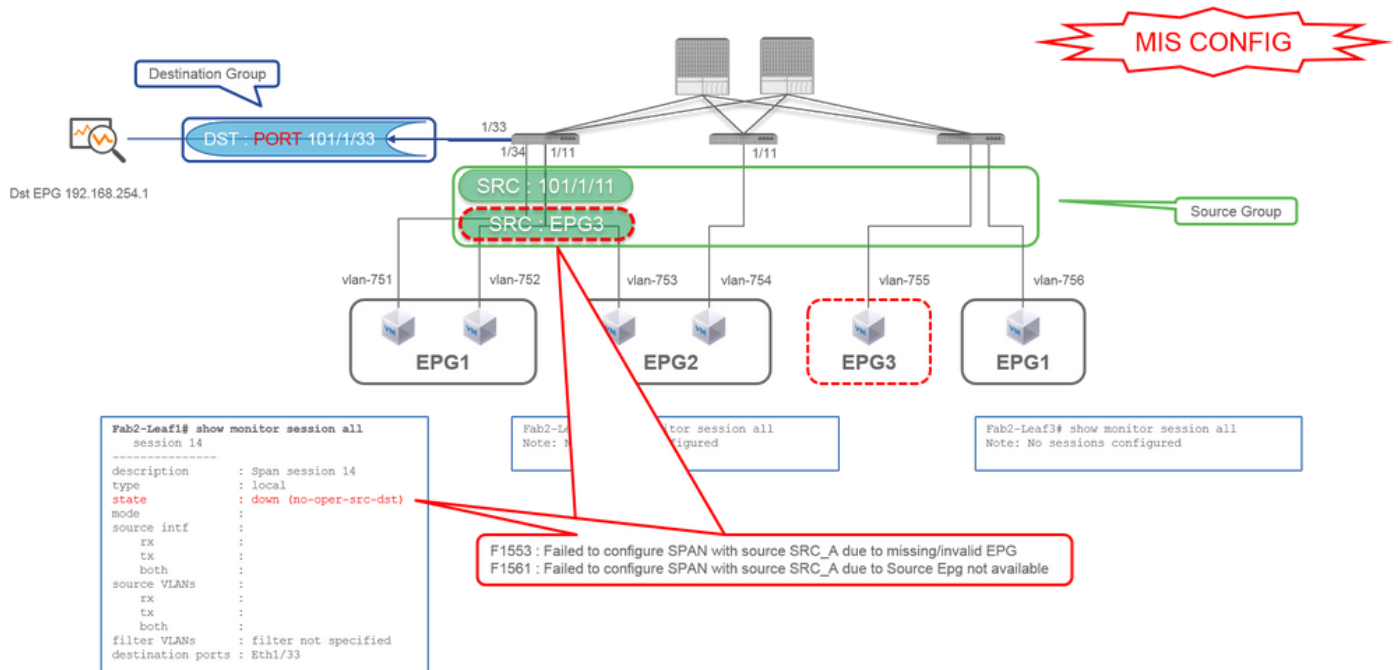
 - 枝葉1 e1/11

 - 枝葉2 e1/11

- 目標組

 - 枝葉1 e1/33

案例 4. Src「Leaf1 e1/11和EPG3過濾器」 | Dst「Leaf1 e1/33」 (錯誤案例)



- 來源群組

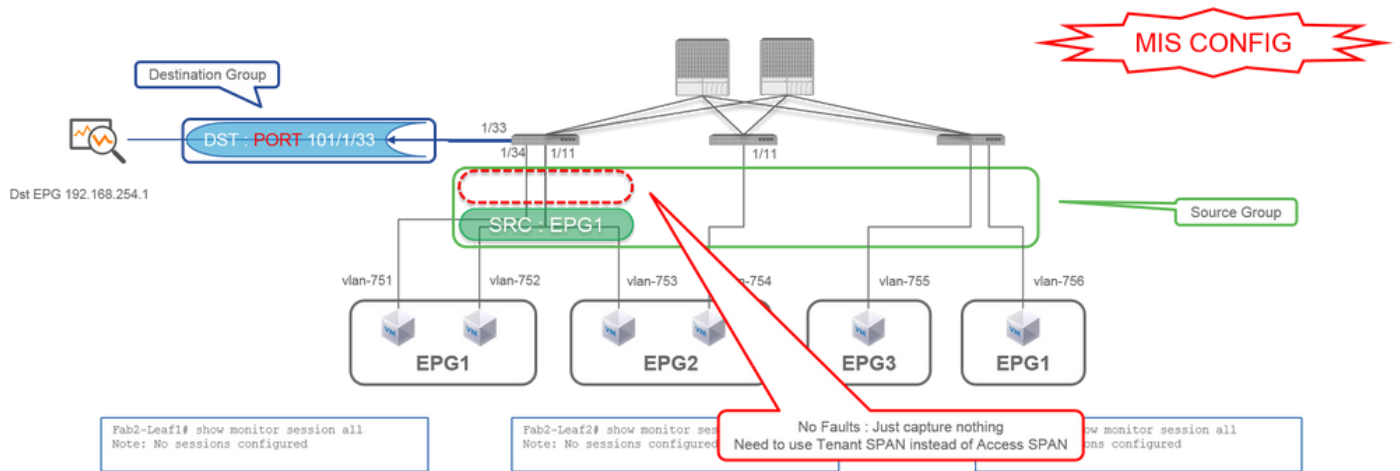
- 枝葉1 e1/11
- EPG3過濾器

- 目標組

- 枝葉1 e1/33

這與存取SPAN (ERSPAN)上的案例3類似，但在本範例中，由於EPG3不存在於Leaf1上，因此Leaf1上唯一的一個SPAN作業階段失敗。因此，SPAN完全無法運作。

案例5：源「EPG1過濾器」 | Dst「Leaf1 e1/33」(錯誤案例)



- 來源群組

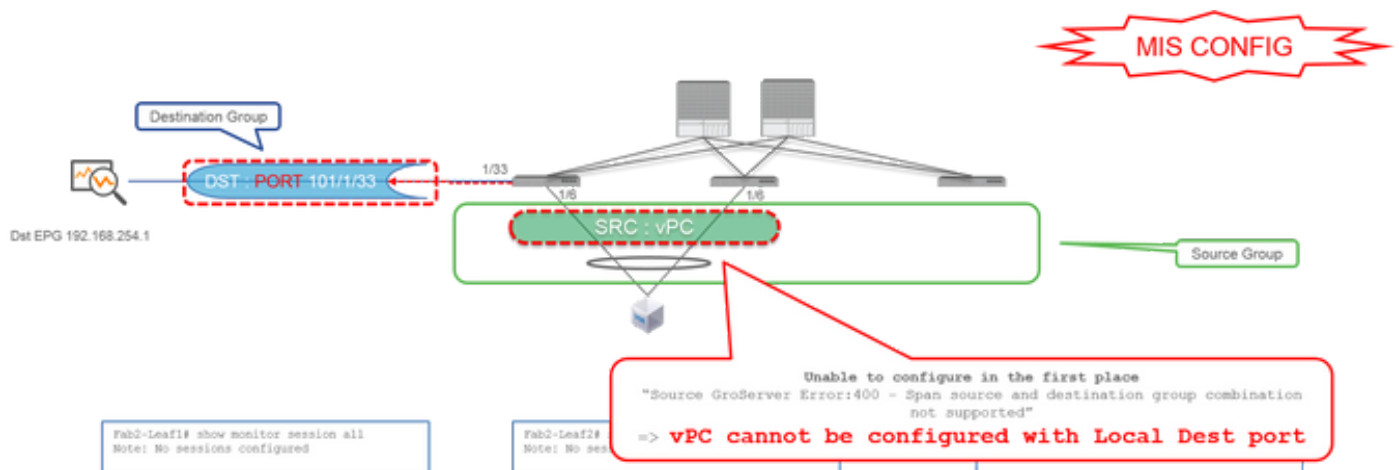
- EPG1過濾器

- 目標組

- 枝葉1 e1/33

存取SPAN上的EPG篩選只有在設定來源連線埠時才能使用。如果EPG是唯一要指定的源，則必須使用租戶SPAN而不是訪問SPAN。

案例 6.源「Leaf1 - Leaf2 vPC」 | Dst「Leaf1 e1/33」(錯誤案例)



- 來源群組

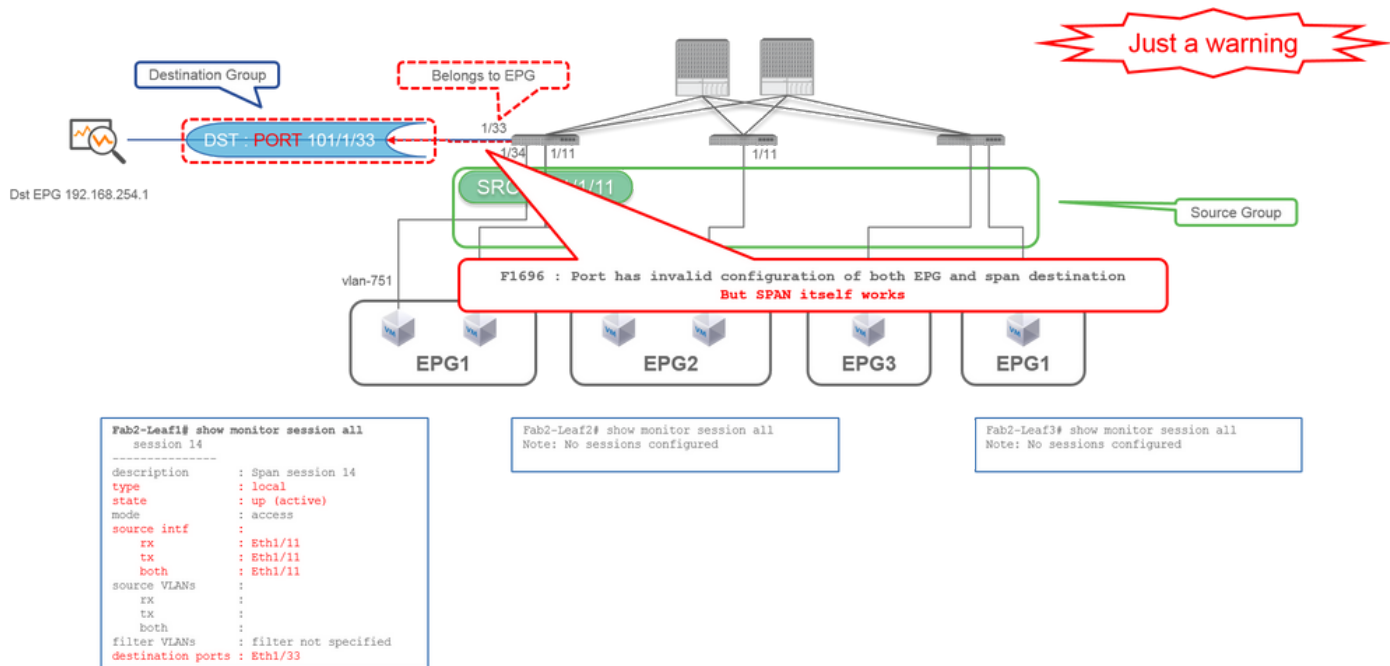
- 枝葉1-2 vPC

- 目標組

- 枝葉1 e1/33

不能將vPC介面配置為具有本地SPAN的源。請使用ERSPAN。請參閱案例4以瞭解存取SPAN (ERSPAN)。

案例 7.源「Leaf1 e1/11 | Dst 「Leaf1 e1/33和e1/33屬於EPG」 (工作有故障)

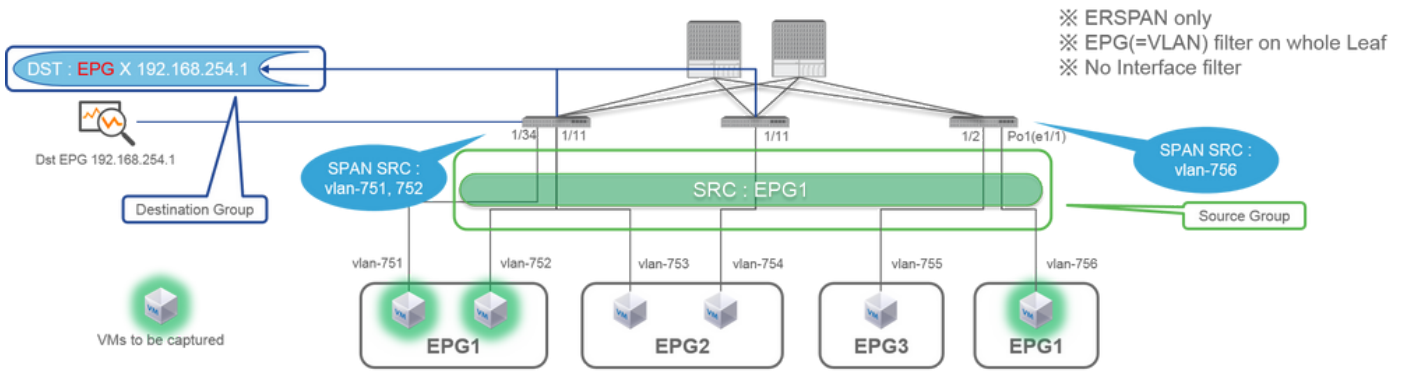


如果SPAN的目標I/F已屬於EPG，在物理I/F下會引發故障「F1696：埠的EPG和span目標配置無效」。

但即使發生此故障，SPAN仍可順利運作。此故障只是SPAN造成額外流量的警告，因為它可能會影響同一I/F上客戶的正常EPG流量。

租使用者SPAN (ERSPAN)

案例 1.源「EPG1」 | Dst 「192.168.254.1」



```

Fab2-Leaf1# show monitor session all
session 15
-----
description      : Span session 15
type             : erspan
version          : version not specified
state            : up (active)
erspan-id        : 1
granularity      : 1
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               :
tx               :
both            :
source VLANs     :
rx               : 35,39
tx               : 35,39
both            : 35,39
filter VLANs     : filter not specified
  
```

```

Fab2-Leaf1# show monitor session all
Note: No sessions configured

Fab2-Leaf1# show vlan id 35,39 extended
VLAN Name                Status Ports
-----
35 TK:SPAN_APP:EPG1      active Eth1/34
39 TK:SPAN_APP:EPG1      active Eth1/11

VLAN Type  Vlan-mode  Encap
-----
35 enet    CE       vlan-751
39 enet    CE       vlan-752
  
```

```

Fab2-Leaf3# show vlan id 9 extended
VLAN Name                Status Ports
-----
9 TK:SPAN_APP:EPG1      active Eth1/1, Pol

VLAN Type  Vlan-mode  Encap
-----
9 enet    CE       vlan-756
  
```

```

Fab2-Leaf3# show monitor session all
session 1
-----
description      : Span session 1
type             : erspan
version          : version not specified
state            : up (active)
erspan-id        : 1
granularity      : 1
vrf-name         : TK:VRF1
acl-name         :
ip-ttl           : 64
ip-dscp          : ip-dscp not specified
destination-ip   : 192.168.254.1/32
origin-ip        : 192.168.254.103/24
mode             : access
source intf      :
rx               :
tx               :
both            :
source VLANs     :
rx               : 9
tx               : 9
both            : 9
filter VLANs     : filter not specified
  
```

- 來源群組

- EPG1 (無過濾器)

- 目標組

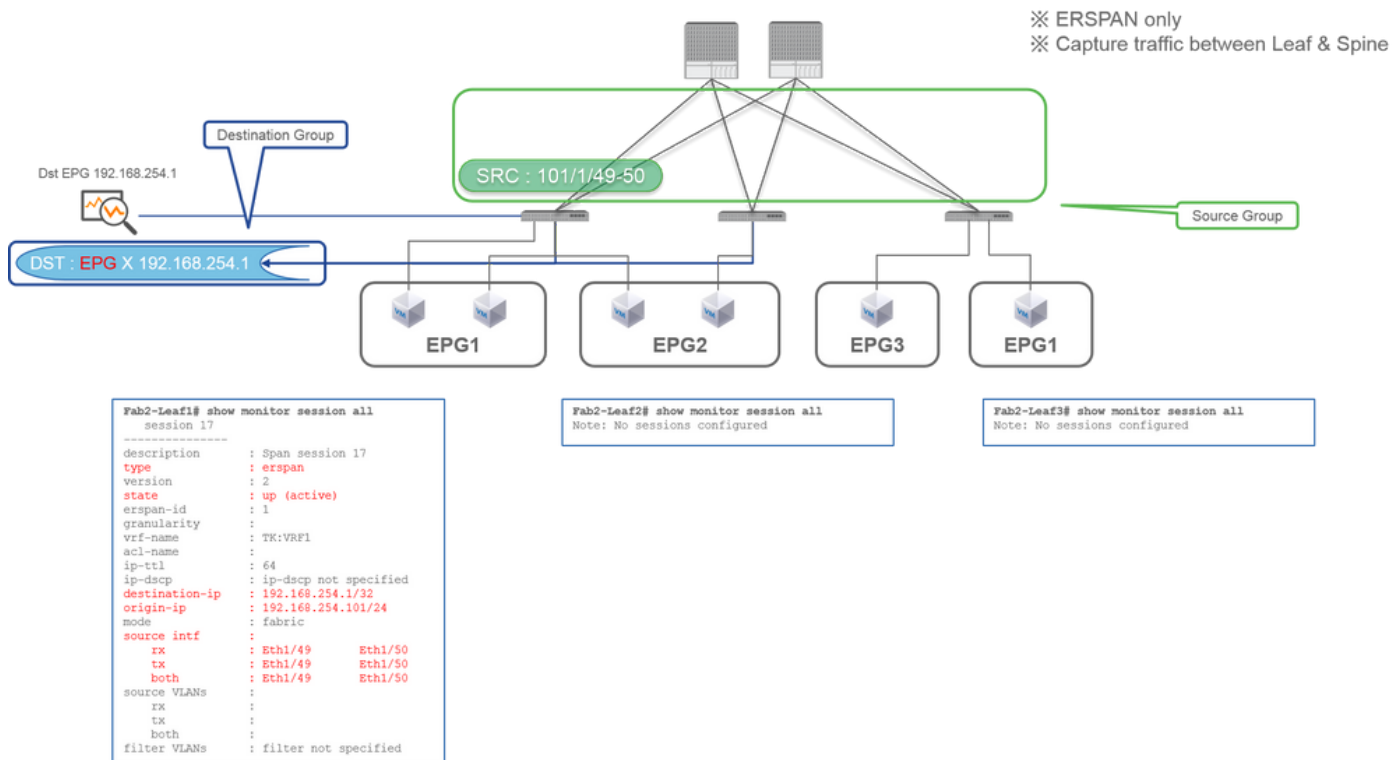
- EPG X上的192.168.254.1

租戶SPAN使用EPG本身作為源，而訪問SPAN僅使用EPG作為過濾器。

租戶SPAN的關鍵點是，您無需指定每個單獨的埠，ACI會自動檢測每台枝葉交換機上的相應VLAN。因此，當必須監控特定EPG的所有資料包，並且該EPG的終端屬於枝葉交換機上的多個介面時，這將很有用。

光纖SPAN (ERSPAN)

案例 1. Src "Leaf1 e1/49-50" | Dst 「192.168.254.1」



- 來源群組

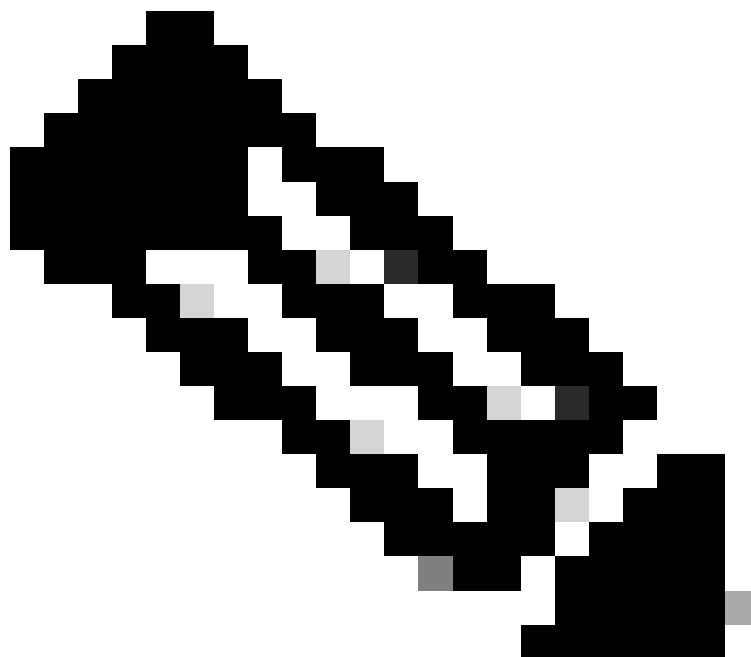
- 枝葉1 e1/49-50

- 目標組

- EPG X上的192.168.254.1

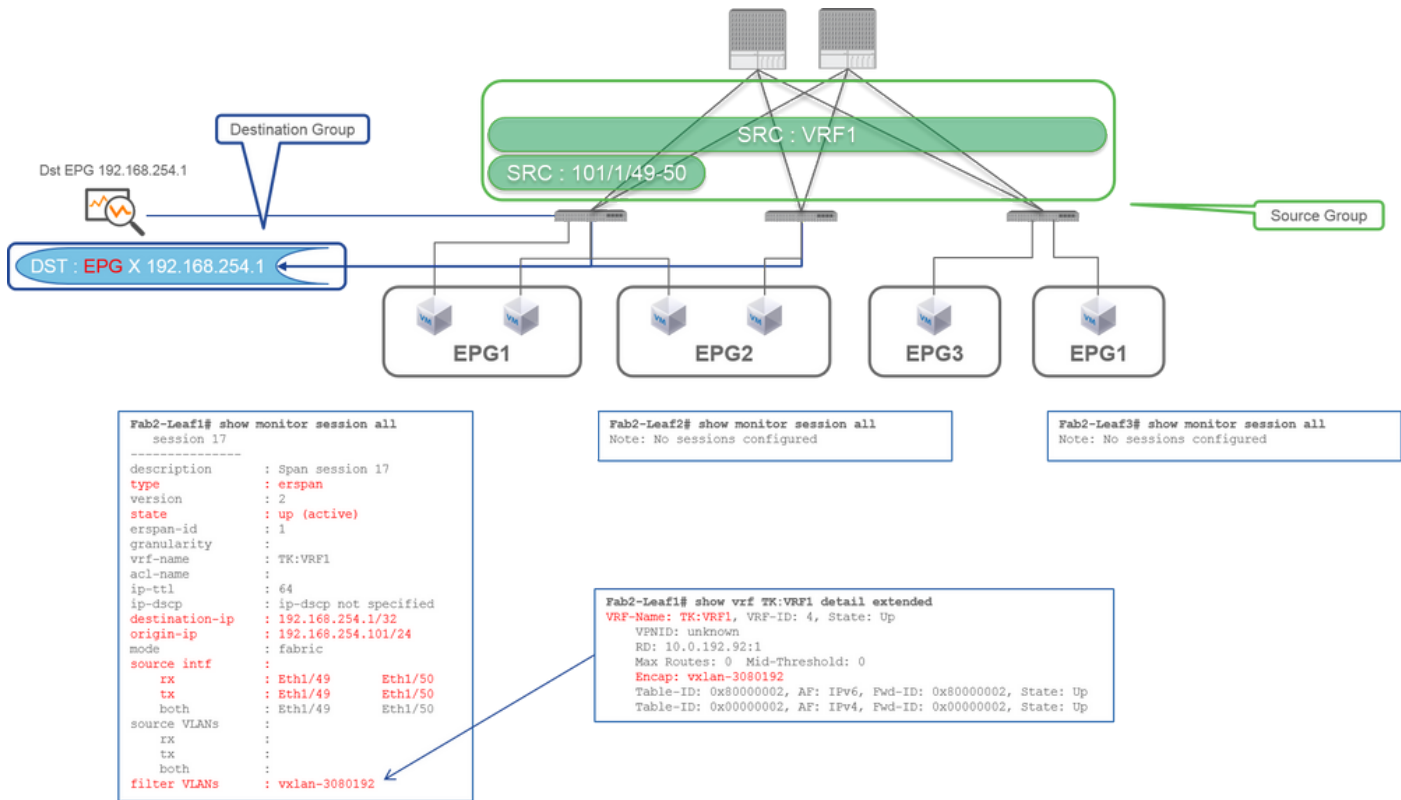
交換矩陣SPAN將交換矩陣埠指定為源，其中交換矩陣埠是枝葉和主幹交換機之間的介面。

當需要在枝葉和主幹交換機之間複製資料包時，此SPAN非常有用。但是，枝葉和主幹交換機之間的資料包使用iVxLAN報頭進行封裝。所以需要一點小竅門才能讀出來。請參閱如何讀取SPAN資料。



註：iVxLAN報頭是增強型VxLAN報頭，僅供ACI交換矩陣內部使用。

案例 2. Src「Leaf1 e1/49-50和VRF過濾器」 | Dst「192.168.254.1」



- 來源群組

- 枝葉1 e1/49-50
- VRF過濾器

- 目標組

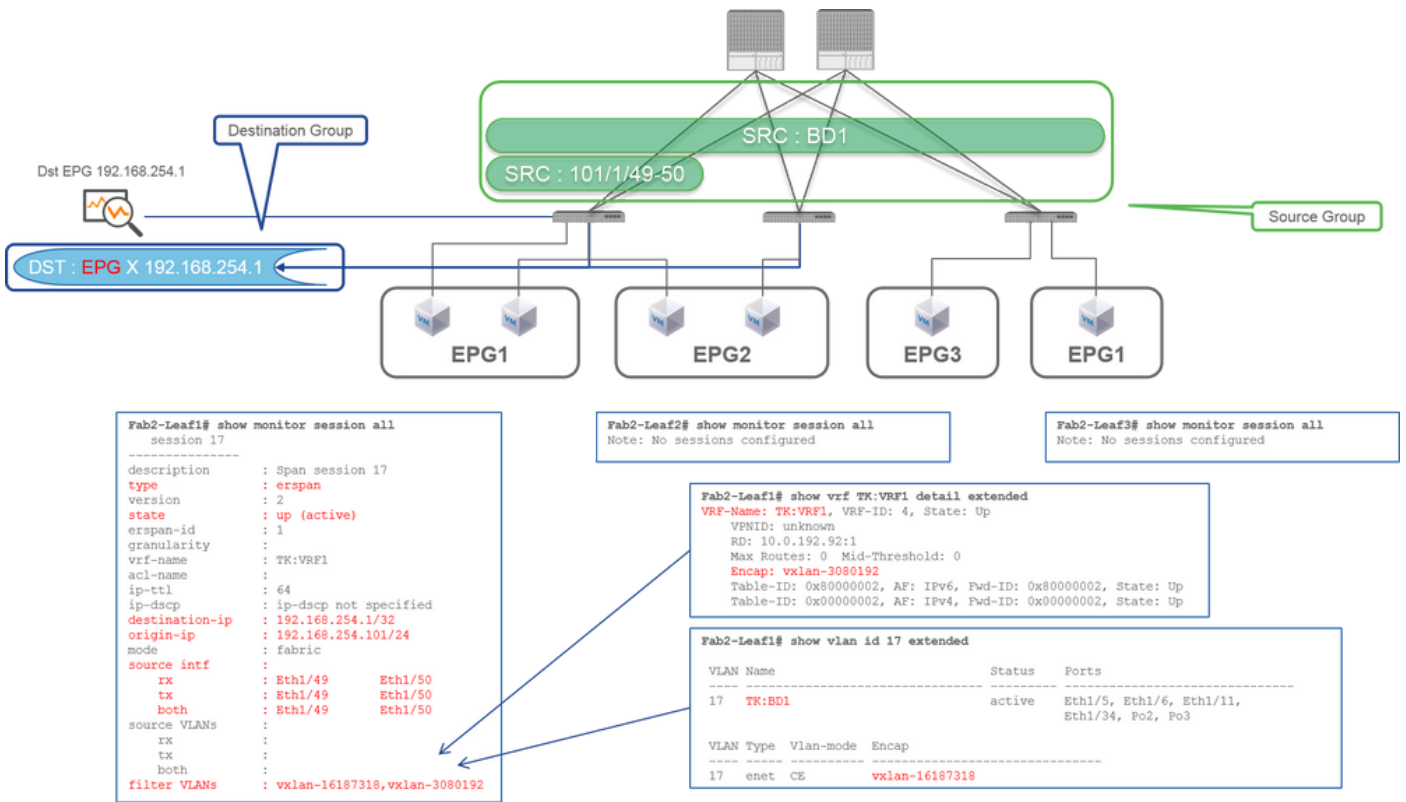
- EPG X上的192.168.254.1

交換矩陣SPAN可以使用篩選器和存取SPAN。但過濾器型別不同。交換矩陣SPAN使用虛擬路由和轉發(VRF)或BD作為過濾器。

在思科ACI中，如前所述，透過交換矩陣埠的資料包使用iVxLAN報頭進行封裝。此iVxLAN報頭將VRF或BD資訊作為虛擬網路識別符號(VNID)。當資料包作為第2層(L2)轉發時，iVxLAN VNID代表BD。當資料包作為第3層(L3)轉發時，iVxLAN VNID代表VRF。

因此，當需要捕獲交換矩陣埠上的路由流量時，使用VRF作為過濾器。

案例 3. Src「Leaf1 e1/49-50 & BD filter」 | Dst「192.168.254.1」



- 來源群組

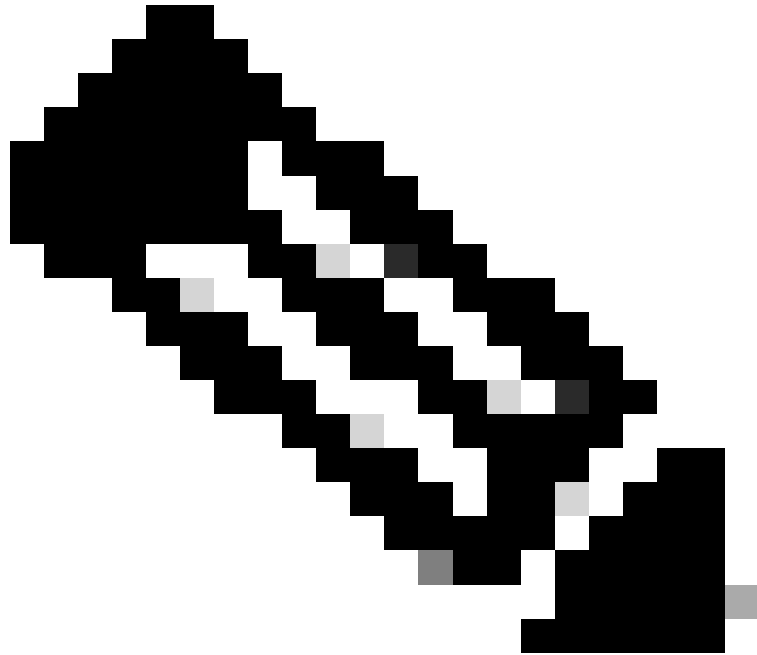
- 枝葉1 e1/49-50
- BD過濾器

- 目標組

- EPG X上的192.168.254.1

如前例2中所述，交換矩陣SPAN可以使用BD作為過濾器。

當需要捕獲交換矩陣埠上的橋接流量時，使用BD作為過濾器。



註：一次只能配置一個BD或VRF過濾器。

您在SPAN目的地裝置上需要什麼？

只需運行資料包捕獲應用程式(如運行tcpdump, wireshark)。設定ERSPAN目的地作業階段或其他任何專案都不是必要的。

對於ERSPAN

請務必使用ERSPAN的目的IP在介面上運行捕獲工具，因為SPAN資料包被轉發到目標IP。

收到的資料包使用GRE報頭進行封裝。請參閱有關如何解碼ERSPAN GRE標頭的「如何讀取ERSPAN資料」一節。

本地SPAN

請確保在連線到ACI枝葉上的SPAN目標介面的介面上運行捕獲工具。

在此介面中接收原始封包。不需要處理ERSPAN標頭。

如何讀取ERSPAN資料

ERSPAN版本 (型別)

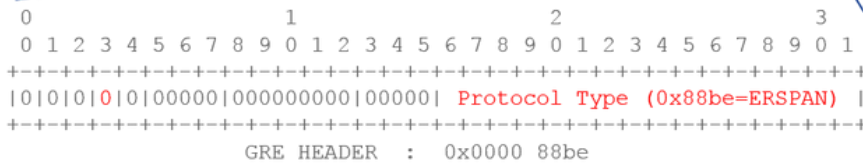
ERSPAN會封裝複製封包，將其轉送到遠端目的地。GRE用於此封裝。GRE標頭上ERSPAN的通訊協定型別為0x88be。

在Internet工程任務組(IETF)文檔中，ERSPAN版本被描述為型別而不是版本。

ERSPAN有三種型別。I、II和III。此[RFC草稿](#)中提及了ERSPAN型別。此外，此GRE [RFC1701](#)也有助於瞭解每種ERSPAN型別。

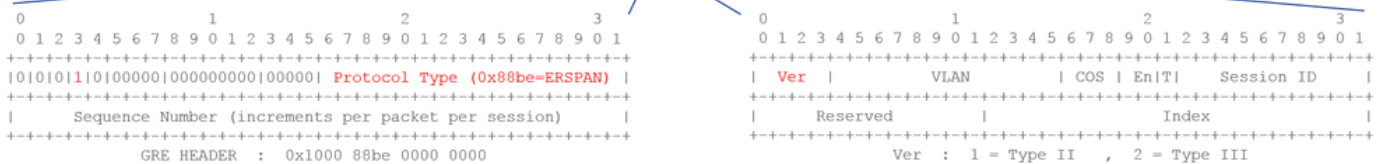
以下是每種型別的資料包格式：

ERSPAN型別I (由Broadcom Trident 2使用)



型別I不使用GRE報頭上的序列欄位。如果是ERSPAN型別II和III，它甚至不會使用GRE標頭後必須跟的ERSPAN標頭。Broadcom Trident 2僅支援此ERSPAN型別I。

ERSPAN型別II或III



如果序列欄位是由S位啟動，則此欄位必須是ERSPAN型別II或III。ERSPAN標頭上的version欄位會辨識ERSPAN型別。在ACI中，自2016年3月20日起不支援第III類。

如果存取或租戶SPAN的SPAN來源群組在第1代和第2代節點上都有來源，ERSPAN目的地會收到來自每一代節點的ERSPAN型別I和II封包。但是，Wireshark一次只能解碼其中一個ERSPAN型別。預設情況下，它只會解碼ERSPAN型別II。如果您啟用ERSPAN型別I的解碼，Wireshark不會解碼ERSPAN型別II。請參閱後面有關如何在Wireshark上解碼ERSPAN型別I的部分。

若要避免此類問題，您可以在SPAN目的地群組上設定ERSPAN型別。

Policies

- Quick Start
- Switches
- Modules
- Interfaces
- Policies**
 - Switch
 - Interface
 - Global
 - Monitoring
 - Troubleshooting
 - SPAN
 - SPAN Source Groups
 - SRC1
 - SPAN Filter Groups
 - SPAN Destination Groups
 - SPAN_DST**

SPAN Destination Group - SPAN_DST

Properties

Name: SPAN_DST

Description: optional

Destination EPG: uni/tn-SPAN/ap-AP/epg-SPAN

SPAN Version: Version 1 Version 2

Enforce SPAN Version:

Destination IP: 80.80.80.80

Source IP/Prefix: 1.0.0.0/8

Flow ID: 1

TTL: 64

MTU: 1518

DSCP: Unspecified

- SPAN版本（版本1或版本2）：這是指ERSPAN型別I或II
- 強制SPAN版本（核取或取消核取）：這決定SPAN作業階段是否必須失敗，以防來源節點硬體不支援設定的ERSPAN型別。

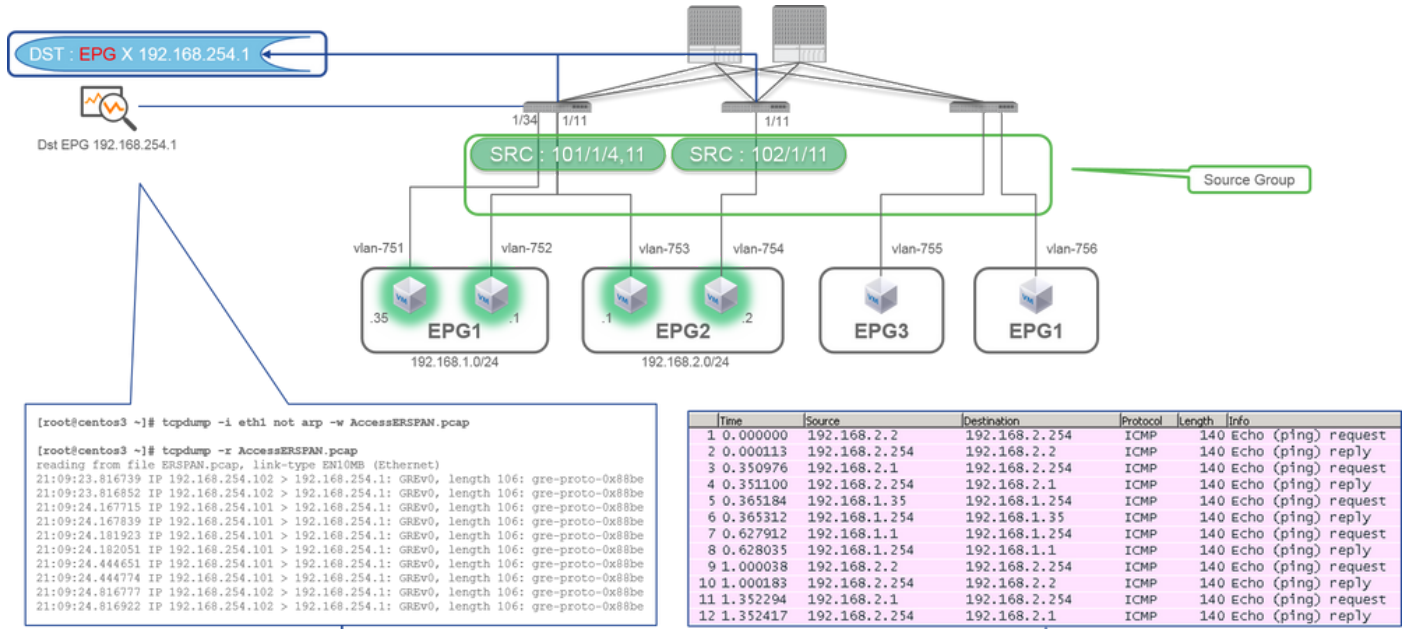
預設情況下，SPAN版本為版本2，而強制SPAN版本未選中。這表示如果來源節點是支援ERSPAN型別II的第2代或更新版本，它就會產生型別II的ERSPAN。如果來源節點是不支援ERSPAN型別II（交換矩陣SPAN除外）的第一代，它會回覆為型別I，因為未核取強制SPAN版本。因此，ERSPAN目的地收到混合型別的ERSPAN。

下表說明了接入和租戶SPAN的每個組合。

SPAN版本	強制SPAN版本	第1代來源節點	第2代來源節點
版本2	未核取	使用型別I	使用型別II
版本2	已核取	失敗	使用型別II
版本1	未核取	使用型別I	使用型別I
版本1	已核取	使用型別I	使用型別I

ERSPAN資料範例

租戶SPAN/存取SPAN (ERSPAN)



※ ERSpan = GRE encap'd packet = Src/Dst are GRE IP
 ※ 192.168.254.101 = from node-101
 ※ "not arp" : suppress arp for ERSpan src from capture machine (may not need)

※ After decode it on Wireshark = real IPs are shown
 ※ See How to Decode ERSpan Type 1 on Wireshark

封包是由ERSpan型別I封裝，因此必須對其進行解碼。這可以透過Wireshark來實現。請參閱「如何解碼ERSpan型別1」一節。

擷取封包的詳細資訊 (ERSpan型別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.bdf8.19ff
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
  
```

光纖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

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	10.0.192.92	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->12151
234	1.185477	10.0.192.92	10.0.32.66	UDP	198	source port: 7248 Destination port: 48879
235	1.185606	10.0.192.92	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會自動解碼ERSPAN型別II。但是，它仍然由iVxLAN報頭封裝。

預設情況下，Wireshark無法理解iVxLAN報頭，因為它是ACI內部報頭。請參閱「如何解碼iVxLAN報頭」。

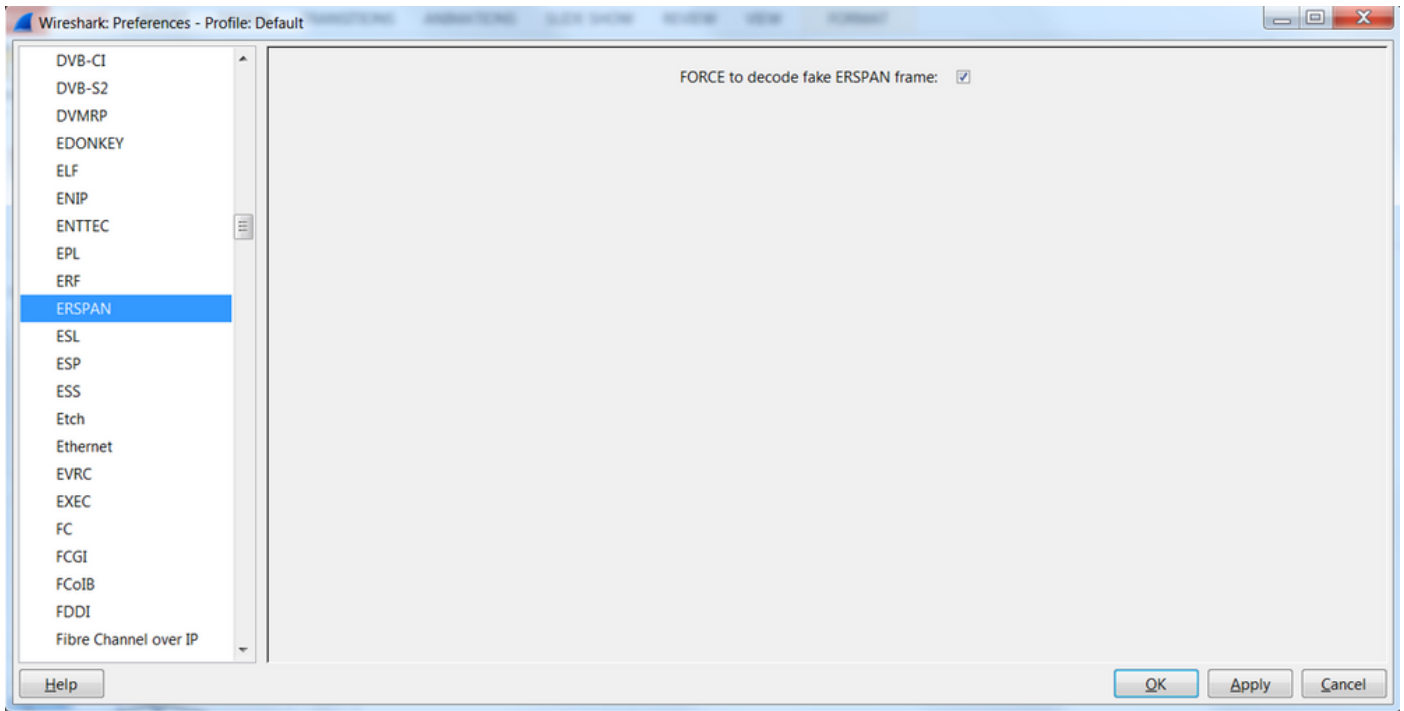
擷取封包的詳細資訊 (ERSPAN型別II)

```
[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 beaf 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.bdf8.19ff
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 10.0.192.92 , 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
```

如何解碼ERSPAN型別II

選項 1. 導航到 Edit > Preference > Protocols > ERSPAN，然後選中「FORCE」以對假ERSPAN幀進行解碼。

- Wireshark (GUI)



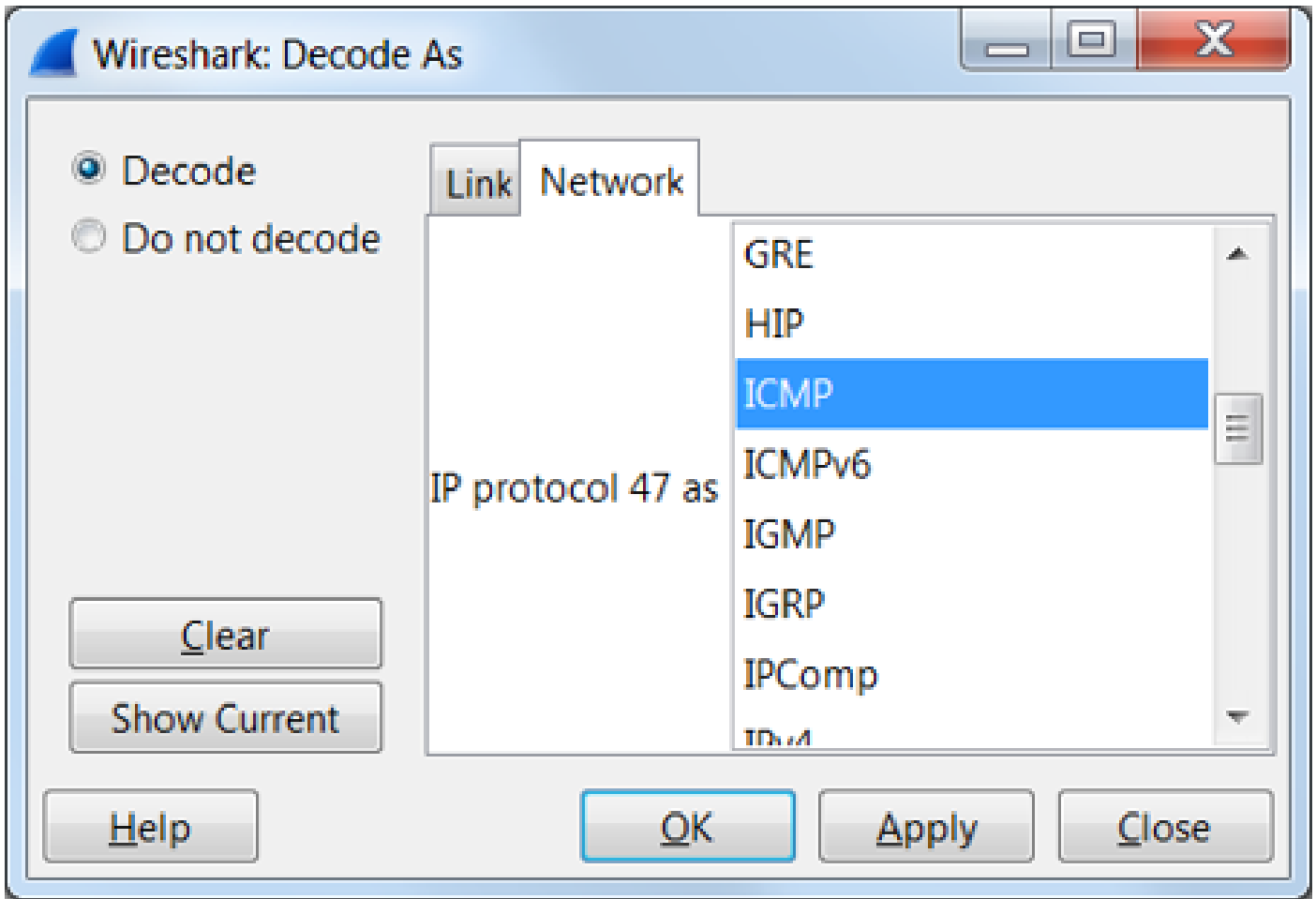
- Tshark (Wireshark的CLI版本) :

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

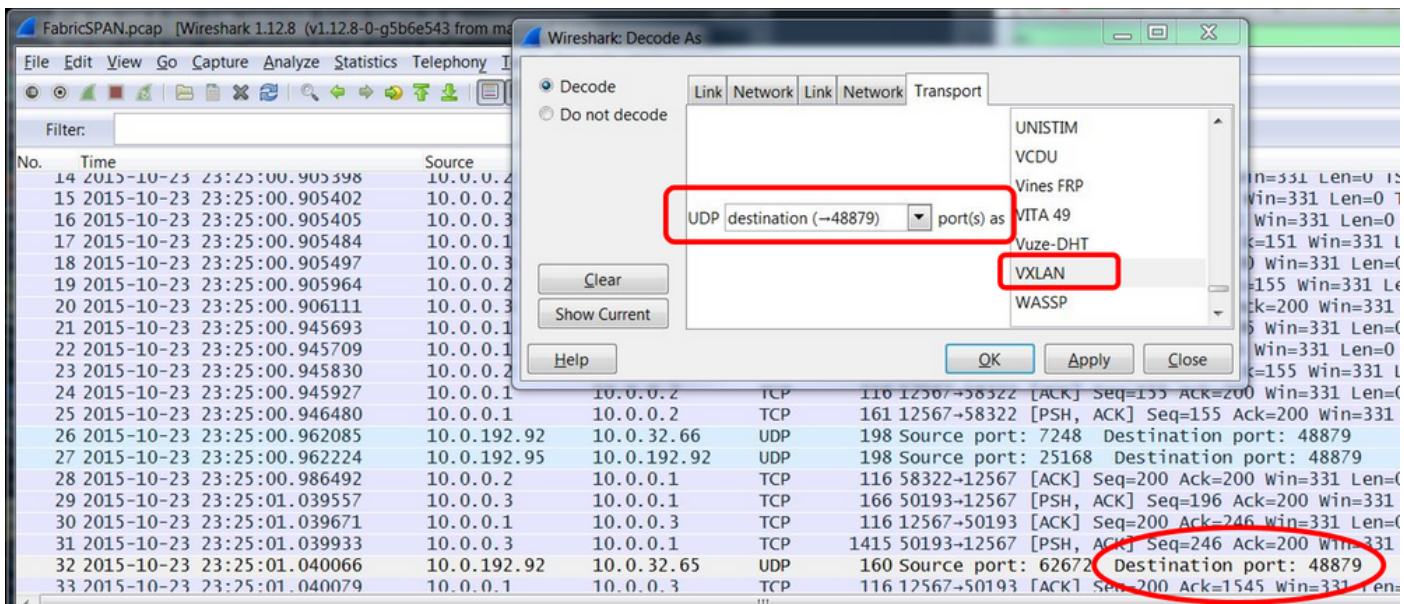


注意：請確定在閱讀ERSPAN型別II或III時停用此選項。

選項 2.導覽至 Decode As > Network > ICMP (if it's ICMP).

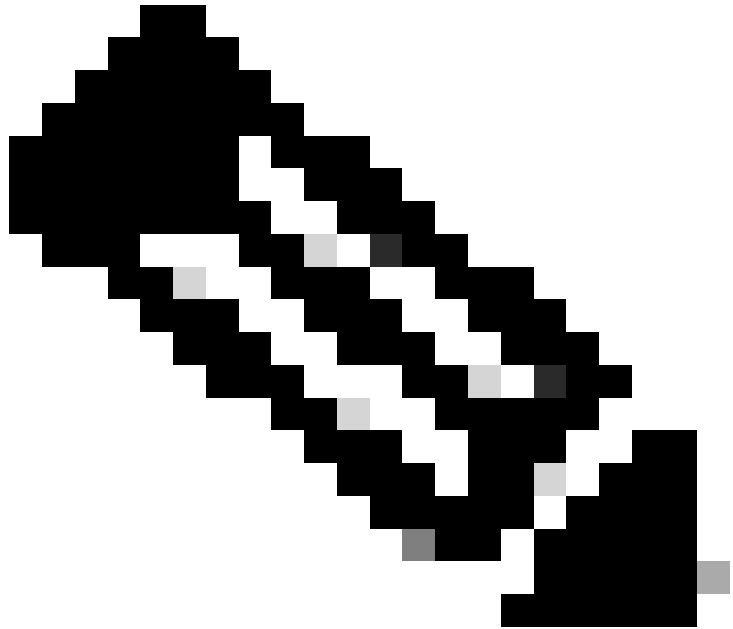


如何解碼iVxLAN報頭



iVxLAN標頭使用目的地連線埠48879。因此，如果您在Wireshark上將UDP目標埠48879配置為VxLAN，則可以解碼iVxLAN報頭和VxLAN。

1. 請確保首先選擇iVxLAN封裝的資料包。
2. 導航到Analyze > Decode As > Transport > UDP destination (48879) > VxLAN。
 - 然後Apply。



注意：交換矩陣埠上的APIC之間具有通訊資料包。這些封包不會以iVxLAN標頭封裝。

在運行Precision時間協定(PTP)的使用者網路上執行erspan捕獲時，有時會看到Wireshark由於GRE封裝(0x8988)中的未知ethertype而無法解釋資料。0x8988是啟用PTP時插入到資料平面資料包的時間標籤的ethertype。將ethertype 0x8988解碼為「Cisco ttag」以公開資料包的詳細資訊。


```
▶ 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: fea691a6d34908004500003cbaa0000f7019983a1874141...
  [Length: 68]
```

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。