

# ACI SPANガイド

## 内容

---

[はじめに](#)

[背景説明](#)

[Cisco ACIのSPANタイプ](#)

[制限とガイドライン](#)

[コンフィギュレーション](#)

[アクセスSPAN\(ERSPAN\)](#)

[トポロジの例](#)

[設定例](#)

[アクセスSPAN \( ローカル \)](#)

[トポロジの例](#)

[設定例](#)

[アクセスSPAN:ACLフィルタを使用](#)

[テナントSPAN\(ERSPAN\)](#)

[トポロジの例](#)

[設定例](#)

[ファブリックSPAN\(ERSPAN\)](#)

[トポロジの例](#)

[設定例](#)

[GUIによる確認](#)

[ACI SPANタイプの選択](#)

[アクセスSPAN\(ERSPAN\)](#)

[Case 1.送信元「Leaf1 e1/11 e1/34およびLeaf2 e1/11」 | Dst「192.168.254.1」](#)

[Case 2.送信元「Leaf1 e1/11およびLeaf2 e1/11」 | Dst「192.168.254.1」](#)

[Case 3.送信元「Leaf1 e1/11 & Leaf2 e1/11 & EPG1 filter」 | Dst「192.168.254.1」](#)

[ケース 4.送信元「Leaf1-Leaf2 vPC」 | Dst「192.168.254.1」](#)

[アクセスSPAN \( ローカルSPAN \)](#)

[Case 1.送信元「Leaf1 e1/11 e1/34」 | Dst「Leaf1 e1/33」](#)

[Case 2.送信元「Leaf1 e1/11 e1/34 & EPG1 filter」 | Dst「リーフ1 e1/33」](#)

[Case 3.送信元「Leaf1 e1/11およびLeaf2 e/11」 | Dst「Leaf1 e1/33」 \( 悪いケース \)](#)

[ケース 4.送信元「Leaf1 e1/11 & EPG3 filter」 | Dst「Leaf1 e1/33」 \( 悪いケース \)](#)

[ケース5 : 送信元「EPG1フィルタ」 | Dst「Leaf1 e1/33」 \( 悪いケース \)](#)

[Case 6.送信元「Leaf1 - Leaf2 vPC」 | Dst「Leaf1 e1/33」 \( 悪いケース \)](#)

[Case 7.送信元「Leaf1 e1/11 | Dst「Leaf1 e1/33 & e1/33 belongs to EPG」 \( 障害あり \)](#)

[テナントSPAN\(ERSPAN\)](#)

[Case 1.送信元「EPG1」 | Dst「192.168.254.1」](#)

[ファブリックSPAN\(ERSPAN\)](#)

[Case 1.送信元「Leaf1 e1/49-50」 | Dst「192.168.254.1」](#)

[Case 2.送信元「Leaf1 e1/49-50 & VRF filter」 | Dst「192.168.254.1」](#)

[Case 3.送信元「Leaf1 e1/49-50 & BDフィルタ」 | Dst「192.168.254.1」](#)

---

[SPAN宛先デバイスに必要なものは何ですか。](#)

[ERSPANの場合](#)

[ローカルSPAN用](#)

[ERSPANデータの読み方](#)

[ERSPANバージョン \(タイプ\)](#)

[ERSPANタイプI \(Broadcom Trident 2で使用\)](#)

[ERSPANタイプIIまたはIII](#)

[ERSPANデータの例](#)

[テナントSPAN/アクセスSPAN\(ERSPAN\)](#)

[キャプチャパケットの詳細 \(ERSPANタイプI\)](#)

[ファブリックSPAN\(ERSPAN\)](#)

[キャプチャパケットの詳細 \(ERSPANタイプII\)](#)

[ERSPANタイプIのデコード方法](#)

[iVxLANヘッダーのデコード方法](#)

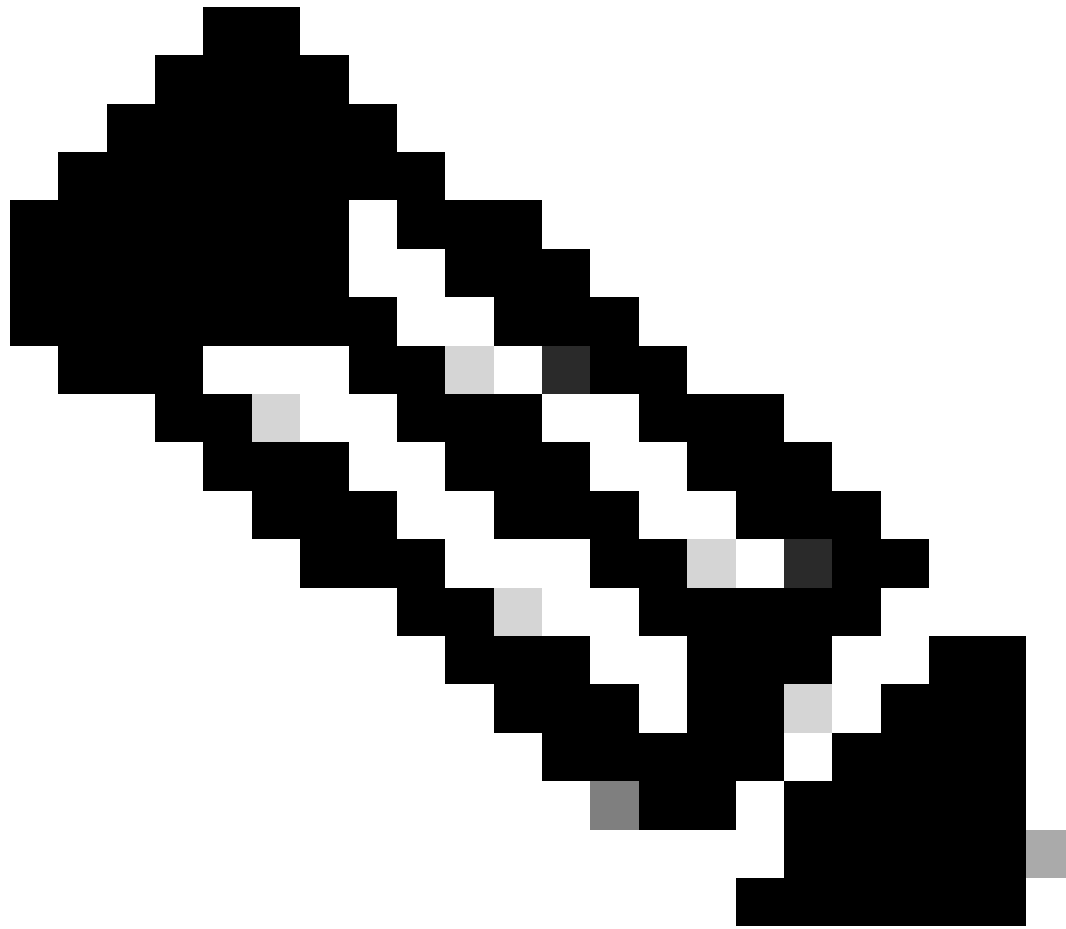
---

## はじめに

このドキュメントでは、シスコアプリケーションセントリックインフラストラクチャ(ACI)でスイッチドポートアナライザ(SPAN)を設定する方法について説明します。

## 背景説明

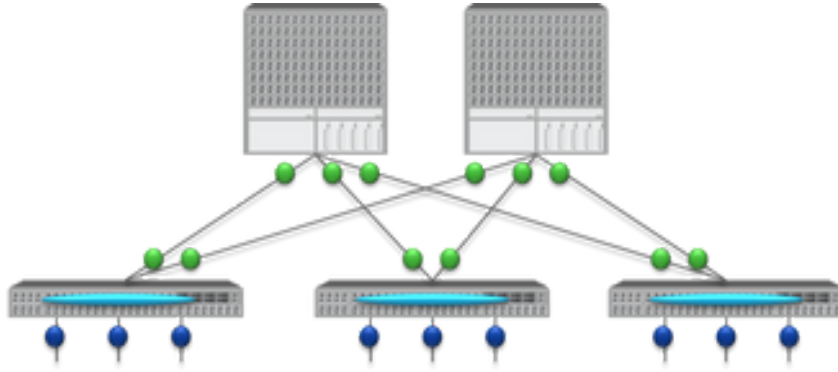
一般に、SPANには3つのタイプがあります。ローカルSPAN、リモートSPAN(RSPAN)、およびEncapsulated Remote SPAN(ERSPAN)これらのSPAN間の違いは、主にコピーパケットの宛先です。Cisco ACIはローカルSPANとERSPANをサポートします。



注：このドキュメントでは、読者がローカルSPANやERSPANの違いなど、一般的なSPANについて理解していることを前提としています。

---

## Cisco ACIのSPANタイプ



== 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

Cisco ACIには、Fabric SPAN、Tenant SPAN、およびAccess SPANの3種類のSPANがあります。各SPANの違いは、コピーパケットの送信元です。

すでに述べたように -

#### interfaces between Leaf and Spine switches

- Fabric SPAN で送受信されるパケットをキャプチャすることです。
- Access SPAN interfaces between Leaf switches and external devicesで送受信されるパケットをキャプチャすることです。
- Tenant SPAN EndPoint Group (EPG) on ACI Leaf switchesで送受信されるパケットをキャプチャすることです。

このSPAN名は、Cisco ACI GUIで設定する場所に対応します。

- ファブリックSPANは、Fabric > Fabric Policies

•

アクセスSPANは、 Fabric > Access Policies

- テナントSPANは、 Tenants > {each tenant}

各SPANの宛先に関しては、Access SPANだけがLocal SPANとERSPANの両方に対応しています。他の2つのSPAN(FabricおよびTenant)は、ERSPANのみをサポートしています。

## 制限とガイドライン

『[Cisco APICトラブルシューティングガイド](#)』の「制限事項とガイドライン」を参照してください。Troubleshooting Tools and Methodology > Using SPANで説明されています。

## コンフィギュレーション

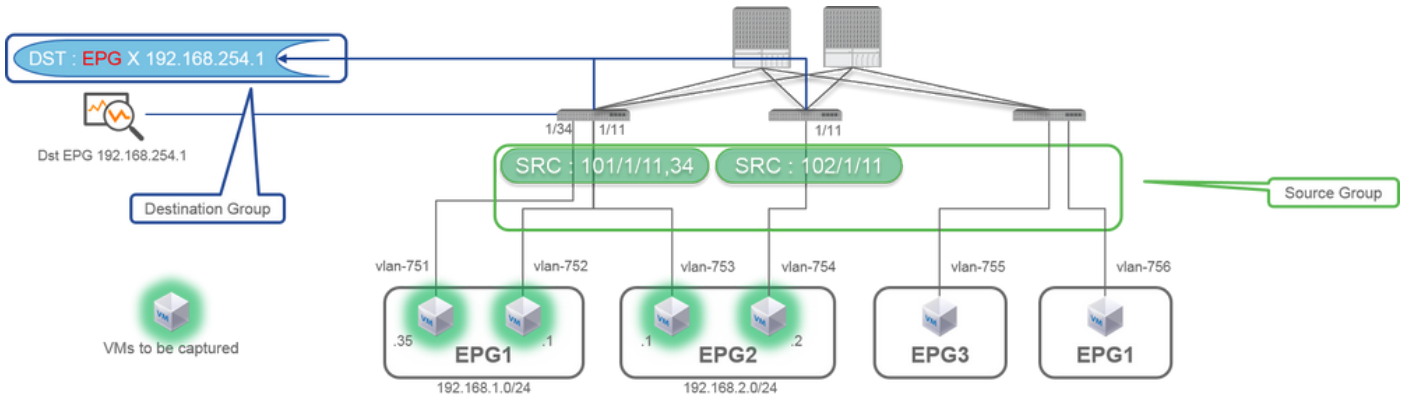
このセクションでは、各SPANタイプの設定に関連する簡単な例を紹介します。後のセクションで、スパンのタイプを選択する方法に関する特定のサンプルケースがあります。

SPANの設定については、『[Cisco APICトラブルシューティングガイド：トラブルシューティングツールと方法論> SPANの使用](#)』も参照してください。

UIが現在のバージョンと異なって表示されることがありますが、設定方法は同じです。

## アクセスSPAN(ERSPAN)

### トポロジの例



## 設定例

SPAN Destination - DST

PROPERTIES

Name: DST

Description: optional

DESTINATION EPG

Destination EPG: **src/tn:TK/ap-SPAN\_APP/epg-SPAN**

SPAN Version: **Version 3**

Destination IP: 192.168.254.1

Source IP/Prefix: 192.168.254.0/24

Flow ID: 1

TTL: 64

MTU: 1518

DSCP: Unspecified

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)

SPAN Source - SRC1

PROPERTIES

Name: SRC1

Description: optional

Direction: Both

Source EPG: select an option

Source Paths

SOURCE ACCESS PATH

Node-101/4/1/11

Node-102/4/1/34

Node-102/4/1/11

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

場所 :

FABRIC > ACCESS POLICIES > Troubleshoot Policies > SPAN

に移動します。

- SPAN Source Groups
- SPAN Destination Groups

SPAN Source Group tiesおよびDestinationSources。

方法：

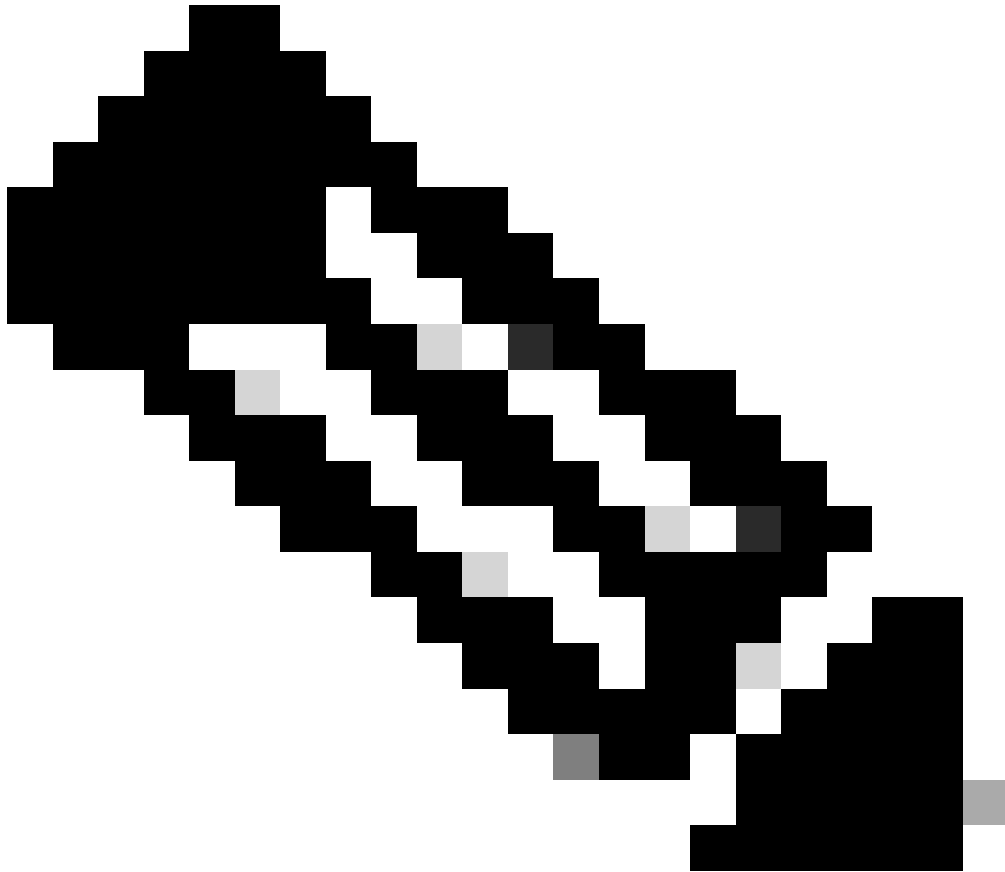
SPAN Source Group

1. (SRC\_GRP1)を作成します。
2. (SRC\_GRP1)の下にSPAN SourceSPAN Source Group (SRC1)を作成します。

SPAN Source

- (SRC1)にこれらのパラメータを設定します。
  - 方向 – ソースEPG ( オプション )
  - 送信元パス ( 複数のインターフェイスが可能 )



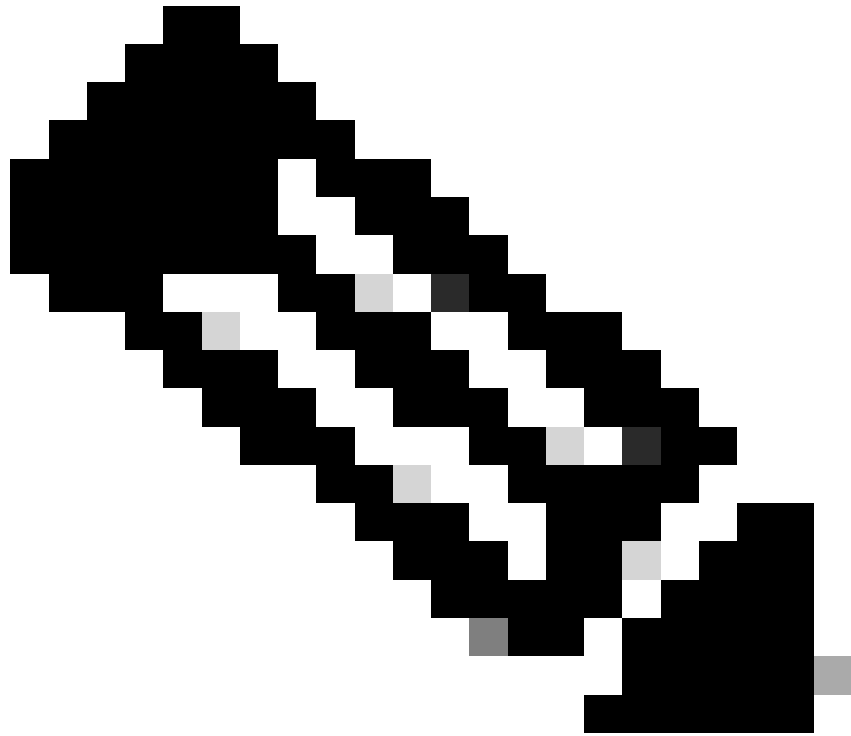


注：各パラメータの詳細については、図を参照してください。

#### SPAN Destination Group

- 
- (DST\_EPG)を作成します。  
SPAN Destination
  - (DST)を作成します。  
SPAN Destination
  - (DST)の次のパラメータを設定します
    - 宛先EPG
    - 宛先 IP
    - 送信元IP/プレフィクス(任意のIPを指定できます。プレフィックスが使用されている場合、未定義ビットにはソースノードのノードIDが使用されます。たとえば、node-101 => src IP 1.0.0.101のprefix: 1.0.0.0/8)
    - その他のパラメータはデフォルトのままにしておくことができます

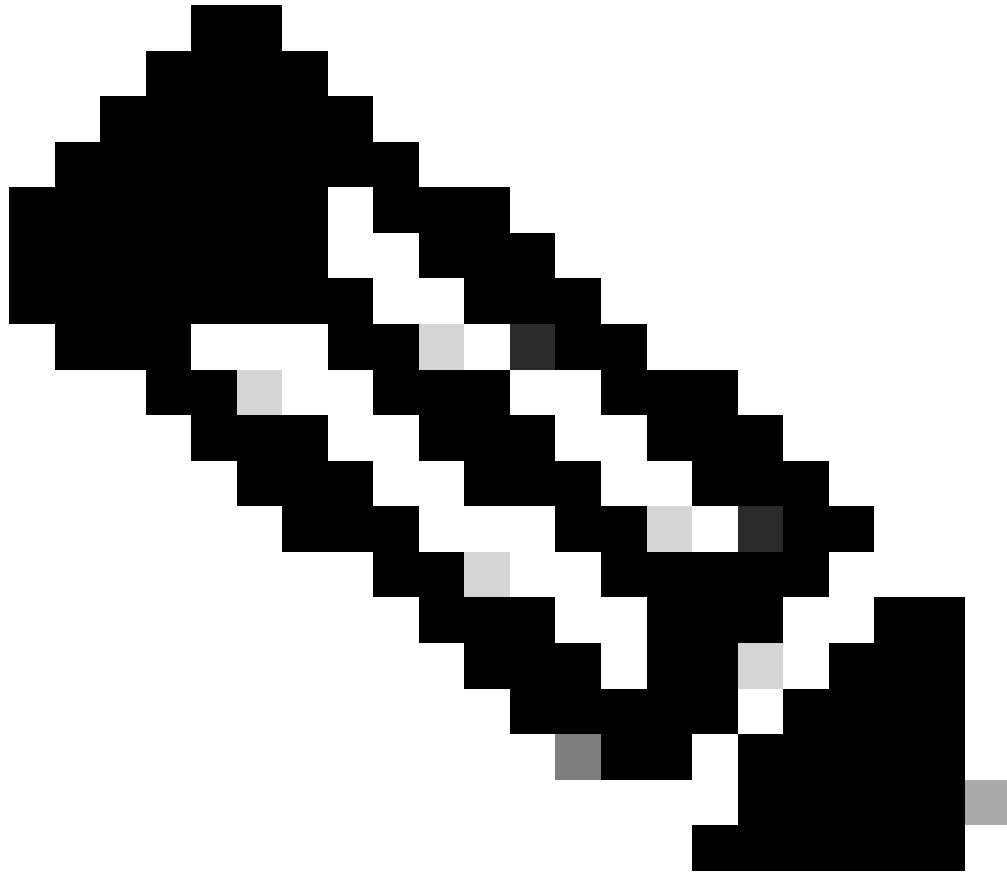




注：各パラメータの詳細については、図を参照してください。

#### SPAN Destination Group

- 
- が適切なSPAN Source Groupに関連付けられていることを確認します。  
Admin State
  - が有効になっていることを確認します。
- 
-



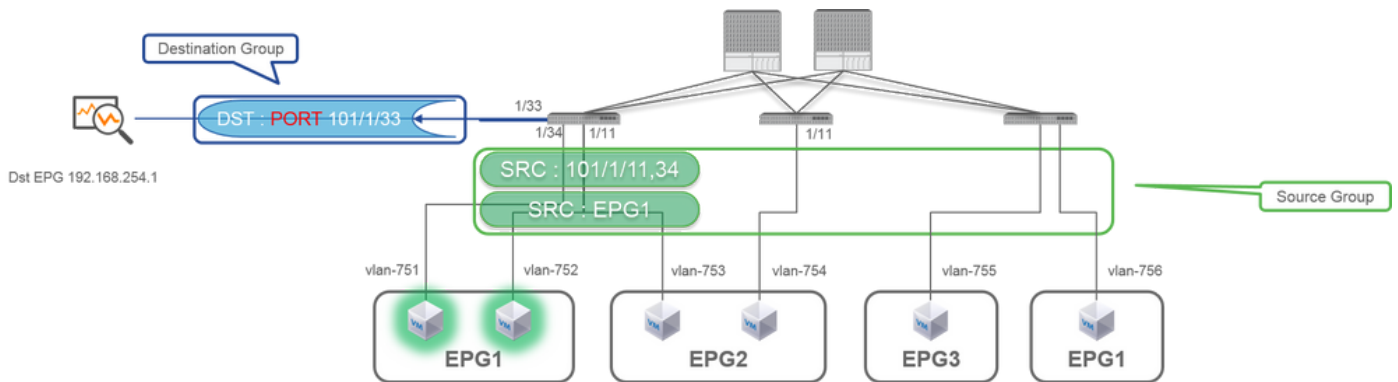
注：この管理状態でDisabledを選択すると、SPANは停止します。後で再利用する場合は、すべてのポリシーを削除する必要はありません。

---

また、ERSPANの宛先IPが、指定された宛先EPGの下のエンドポイントとして学習されていることを確認してください。前述の例では、192.168.254.1はTenant TK > Application profile SPAN\_APP > EPG SPANで学習する必要があります。または、宛先デバイスがサイレントホストの場合、宛先IPをこのEPGの下で静的エンドポイントとして設定できます。

アクセスSPAN ( ローカル )

## トポロジの例



## 設定例

**SPAN Source Group - SRC\_GRP1**

PROPERTIES: Name: SRC\_GRP1, Admin State: Enabled

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 ACCESS PATH: Node-101/eth1/11, Node-101/eth1/24

- 場所 :

Fabric > ACCESS POLICIES > Troubleshoot Policies > SPAN

- SPAN Source Groups

## - SPAN Destination Groups

SPAN Source Group タイ Destination と Sources.

- 方法 :

### 1. 作成SPAN Source Group(SRC\_GRP1)

- (SRC\_GRP1)の下にSPAN Source SPAN Source Group (SRC1)を作成します  
SPAN Source

- (SRC1)の次のパラメータを設定します

-方向

- ソースEPG ( オプション )

- 送信元パス ( 複数のインターフェイスが可能 )

※各パラメータの詳細は画像を参照してください。

- 作成SPAN Destination Group(DST\_Leaf1)

- 作成SPAN Destination(DST)

SPAN Destination

- (DST)の次のパラメータを設定します

-宛先インターフェイスおよびノード。

SPAN Destination Group

- が適切なSPAN Source Groupに関連付けられていることを確認します。

Admin State

- 

が有効になっていることを確認します。

こ※管理状態でDisabledを選択すると、SPANが停止します。後で再利用する場合は、すべてのポリシーを削除する必要はありません。

宛先インターフェイスでは、インターフェイスポリシーグループによる設定は必要ありません。ACIリーフのインターフェイスにケーブルを接続すると機能します。

制限 :

- ローカルSPANでは、宛先インターフェイスと送信元インターフェイスを同じリーフ上に設定する必要があります。
- 宛先インターフェイスは、UPである限り、EPG上にある必要はありません。
- 仮想ポートチャネル(vPC)インターフェイスが送信元ポートとして指定されている場合、ローカルSPANは使用できません。ただし、回避策があります。第1世代のリーフでは、vPCまたはPCのメンバである個々の物理ポートをSPANソースとして設定できます。このローカルSPANを使用して、vPCポート上のトラフィックに使用できます。ただし、このオプションは第2世代リーフ([CSCvc11053](#))では使用できません。代わりに、「VPCコンポーネントPC」でのSPANのサポートは、2.1(2e)、2.2(2e)以降で[CSCvc44643](#)を介して追加されました。これにより、どの世代のリーフでも、vPCのメンバであるポートチャネルをSPANソースとして設定できます。これにより、どの世代のリーフでも、vPCポート上のトラフィックにローカルSPANを使用できます。
- 第2世代のリーフでポートチャネルの個々のポートを指定すると、パケットのサブセットのみがスパンニングされます([CSCvc11053](#)も原因)。
- PCとvPCは、ローカルSPANの宛先ポートとしては使用できません。4.1(1)から、PCはローカルSPANの宛先ポートとして使用できます。

## アクセスSPAN:ACLフィルタを使用

アクセスSPANソースでACLフィルタを使用できます。この機能により、特定のフローまたはSPANソースに出入りするトラフィックのフローにSPANを適用できます。

ユーザは、フロー固有のトラフィックにSPANを適用する必要がある場合に、SPAN Aclを送信元に適用できます。

ファブリックSPANおよびテナントSPANのソースグループ/ソースではサポートされません。

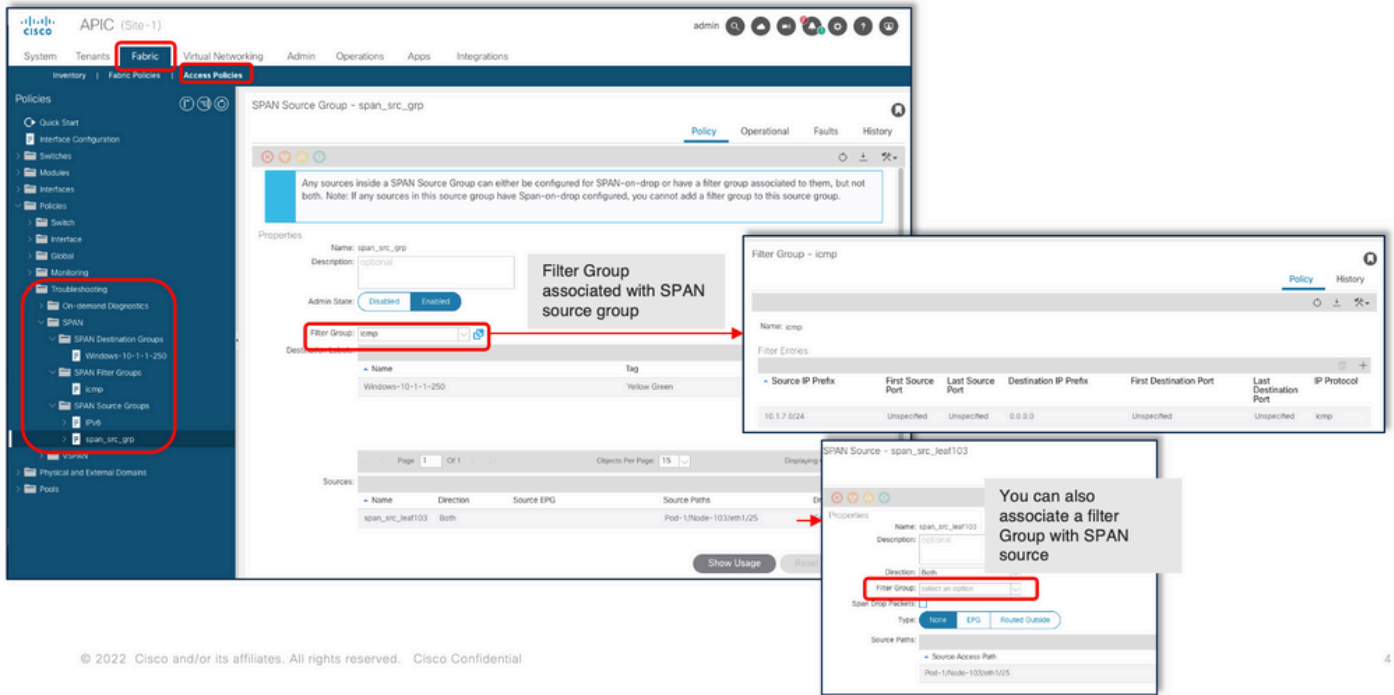
フィルタグループにフィルタエントリを追加する場合は注意が必要です。その理由は、現在フィルタグループを使用しているすべてのソースに対してtcamエントリが追加される可能性があるためです。

フィルタグループは次のものに関連付けることができます。

-Span Source : フィルタグループは、このSpan Sourceの下で定義されているすべてのインターフェイスのトラフィックをフィルタリングするために使用されます。

-Span Source Group : フィルタグループ ( xなど ) は、このSpan Source Groupの各Span Sourceで定義されたすべてのインターフェイスのトラフィックをフィルタリングするために使用されます。

この設定スナップショットでは、フィルタグループがSpanソースグループに適用されます。

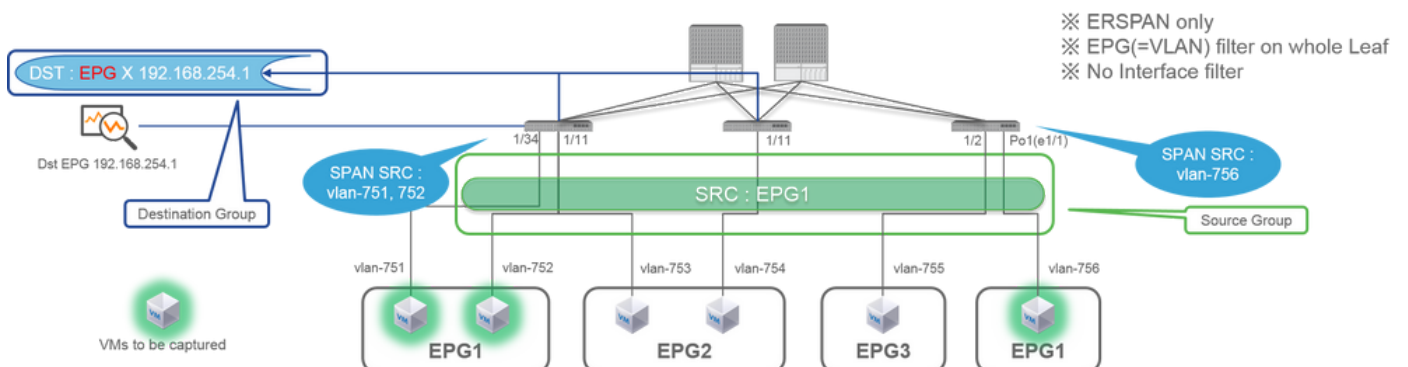


特定のSPANソースがすでにフィルタグループ ( y など ) に関連付けられている場合、そのフィルタグループ ( y ) が、この特定のSPANソースの下すべてのインターフェイスでグループをフィルタリングするために使用されます

- ソースグループに適用されたフィルタグループは、そのソースグループ内のすべてのソースに自動的に適用されます。
- ソースに適用されるフィルタグループは、そのソースにのみ適用されます。
- フィルタグループは、ソースグループとそのソースグループ内のソースの両方に適用され、ソースに適用されたフィルタグループが優先されます。
- ソースに適用されたフィルタグループが削除され、親ソースグループに適用されたフィルタグループが自動的に適用されます。
- ソースグループに適用されたフィルタグループが削除され、現在そのソースグループを継承しているすべてのソースから削除されます。

## テナントSPAN(ERSPAN)

### トポロジの例



# 設定例

The screenshot shows the Cisco tenant configuration interface. The left sidebar has 'Troubleshoot Policies' highlighted. The main area shows 'SPAN Source Group - SRC\_GRP' with a table of 'TENANT DESTINATION GROUPS' and a table of 'SOURCES'. Red boxes highlight 'DST\_GRP' in the destination groups table and 'SRC\_A' in the sources table. Callouts provide details for 'SPAN Destination - DST\_A' and 'SPAN Source - SRC\_A'.

**SPAN Destination - DST\_A**

PROPERTIES

Name: DST\_A

Description: optional

DESTINATION EPG

Destination EPG: uni/tn-TK/ap-SPAN\_APP/epg-SPAN

SPAN Version: Version 1

Destination IP: 192.168.254.1

Source IP/Prefix: 192.168.254.0/24

Flow ID: 1

TTL: 64

MTU: 1518

DSCP: Unspecified

Same as Access SPAN

**SPAN Source - SRC\_A**

PROPERTIES

Name: SRC\_A

Description: optional

Direction: Both

Source EPG: uni/tn-TK/ap-SPAN\_APP/epg-EPG1

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

• 場所 :

Tenants > {tenant name} > Troubleshoot Policies > SPAN

- SPAN Source Groups

- SPAN Destination Groups

※ SPAN送信元グループDestinationの関係と Sources.

• 方法 :

## 1. 作成SPAN Source Group(SRC\_GRP)

- (SRC\_GRP)の下にSPAN SourceSPAN Source Group(SRC\_A)を作成します  
SPAN Source
  - (SRC\_A)用に次のパラメータを設定します
    - 方向
    - 送信元EPG
- ※各パラメータの詳細は画像を参照してください。

## 作成SPAN Destination Group(DST\_GRP)

- 作成SPAN Destination(DST\_A)  
SPAN Destination
  - (DST\_A)の次のパラメータを設定します
    - 宛先EPG
    - 宛先 IP
    - 送信元IP/プレフィックス
    - その他のパラメータはデフォルトのままにしておくことができます
- ※各パラメータの詳細は画像を参照してください。

## SPAN Destination Group

- が適切なSPAN Source Groupに関連付けられていることを確認します。

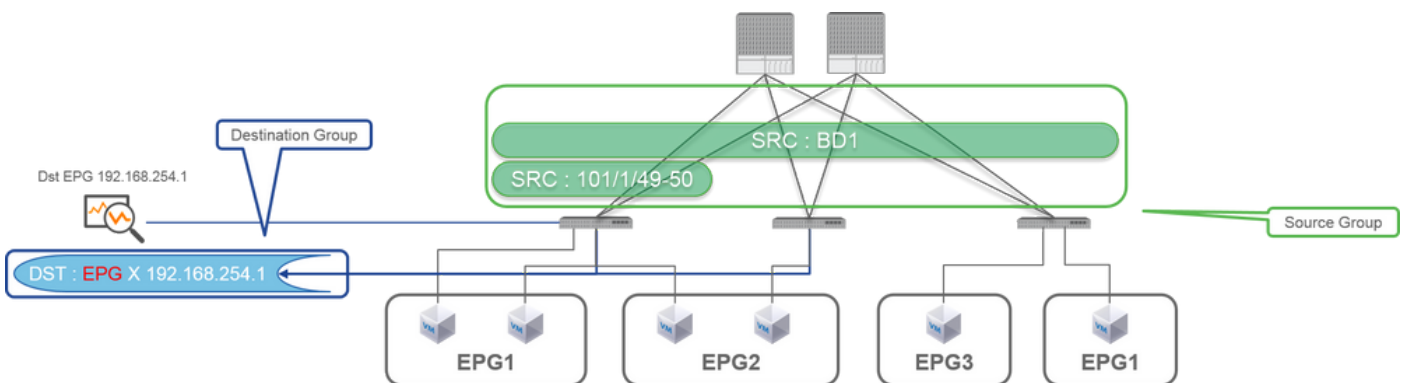
## Admin State

- が有効になっていることを確認します。

こ※管理状態でDisabledを選択すると、SPANが停止します。後で再利用する場合は、すべてのポリシーを削除する必要はありません。

## ファブリックSPAN(ERSPAN)

### トポロジーの例



### 設定例



Direction :  
Both / Incoming / Outgoing  
Private Network / Bridge Domain :  
Either of them. Filter packets on Fabric ports with specific VRF/BD

• 場所 :

Fabric > FABRIC POLICIES > Troubleshoot Policies > SPAN

- Fabric

- SPAN Destination Groups

※SPAN Source GroupDestination Sources

• 方法 :

## 1. 作成SPAN Source Group(SRC\_GRP)

- (SRC\_GRP)の下にSPAN Source SPAN Source Group(SRC\_A)を作成します  
SPAN Source

- (SRC\_A)用に次のパラメータを設定します
  - 方向
    - プライベートネットワーク ( オプション )
    - ブリッジドメイン ( オプション )
    - 送信元パス ( 複数のインターフェイスが可能 )※各パラメータの詳細は画像を参照してください。

- 作成SPAN Destination Group(DST\_GRP)

- 作成SPAN Destination(DST\_A)

SPAN Destination

- (DST\_A)用に次のパラメータを設定します
  - 宛先EPG
  - 宛先 IP
  - 送信元IP/プレフィックス
  - その他のパラメータはデフォルトのままにしておくことができます

※各パラメータの詳細は画像を参照してください。

SPAN Destination Group

- が適切なSPAN Source Groupに関連付けられていることを確認します。

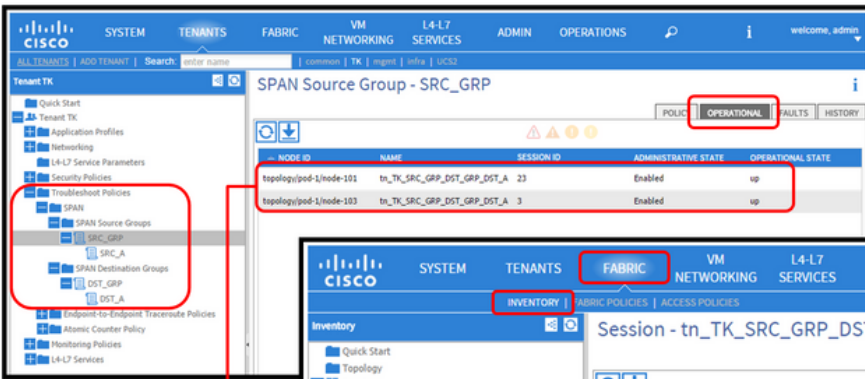
Admin State

- が有効になっていることを確認します。

こ※Admin StateでDisabledを選択すると、SPANが停止します。後で再利用する場合は、すべてのポリシーを削除する必要はありません。

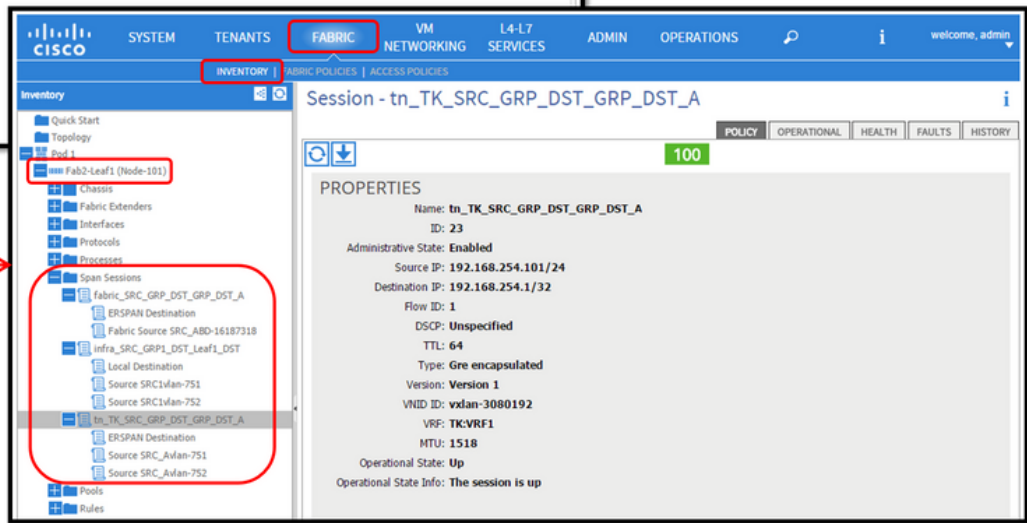
ERSPANバージョン ( タイプ ) については後のセクションで説明しますが、ERSPANバージョンIIがファブリックSPANに使用され、バージョンIがテナントSPANとアクセスSPANに使用されていることを確認できます。

## GUI による確認



※ See Use Case for CLI verification

Double Click



• SPAN設定ポリシーの検証

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

動作状態が稼働していることを確認してください。

• ノード自体のSPANセッションの検証

1. またはSPAN Configuration Policyから各セッションをダブルクリックします。 Fabric > INVENTORY > Node > Span Sessions > { SPAN session name }

動作状態が稼働していることを確認してください。

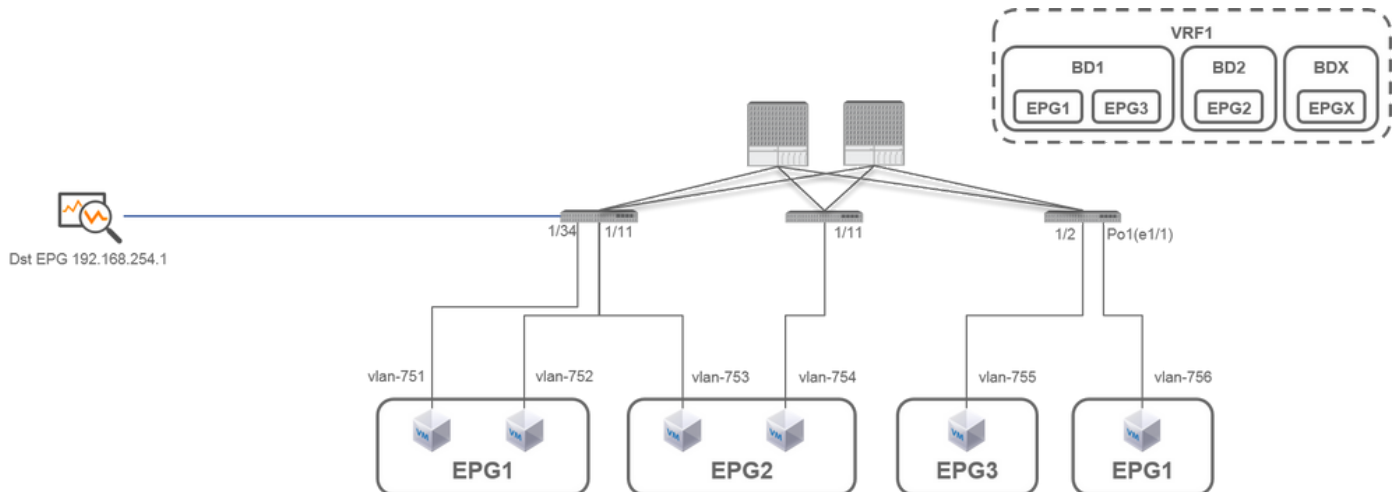
SPANセッション命名規則：

- ファブリックSPAN:fabric\_xxxx

- アクセスSPAN:infra\_xxxx

- テナントSPAN:tn\_xxxx

## ACI SPANタイプの選択

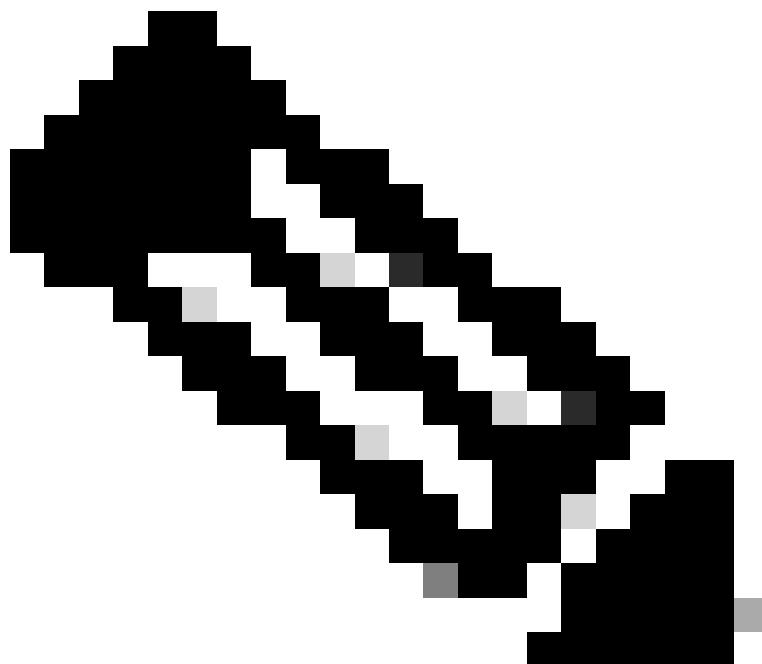


このセクションでは、各ACI SPANタイプ(Access, Tenant, Fabric)の詳細なシナリオについて説明します。各シナリオの基本トポロジは、前のセクションで説明しています。

これらのシナリオを理解していれば、要件に適したACI SPANタイプを選択できます。たとえば、特定のインターフェイス上のパケットだけをキャプチャする必要がある、またはインターフェイスに関係なく特定のEPG上のすべてのパケットをキャプチャする必要があるなどです。

Cisco ACIでは、source groupおよびdestination groupを使用してSPANを設定します。送信元グループには、インターフェイスやEPGなどの複数の送信元ファクタが含まれています。宛先グループには、ローカルSPANの宛先インターフェイスやESpanの宛先IPなどの宛先情報が含まれます。

パケットがキャプチャされた後、キャプチャされたパケットをデコードするには、「SPANデータの読み方」の項を参照してください。

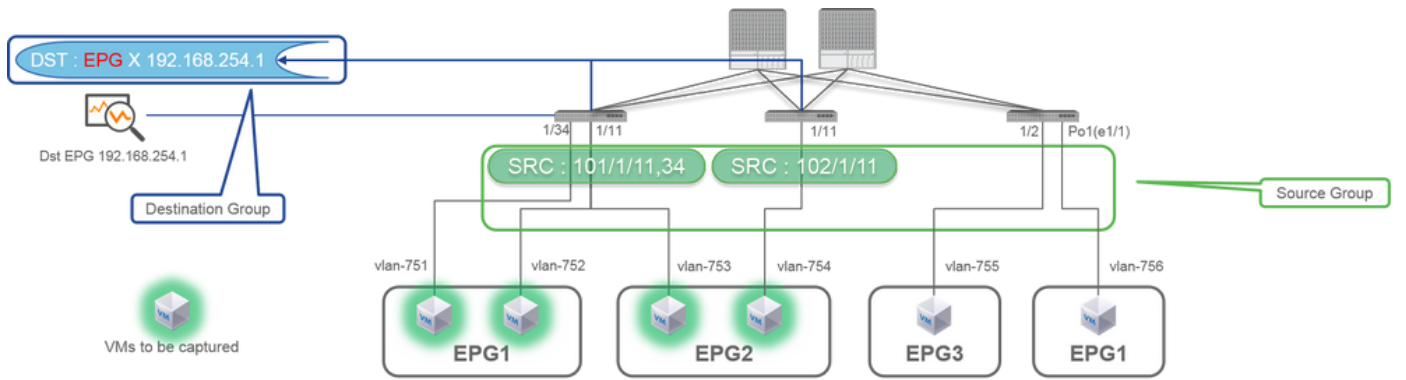


注：各トポロジ内で緑色のライトで強調表示されているVMに注目してください。各シナリオでは、これらの強調表示されたVMからパケットをキャプチャします。

---

## アクセスSPAN(ERSPAN)

Case 1.送信元「Leaf1 e1/11 e1/34および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
  - リーフ1 e1/11
  - リーフ1 e1/34
  - リーフ2 e1/11

- Destination Group
  - EPG Xの192.168.254.1

アクセスSPANでは、1つのSPANセッションに対して複数のインターフェイスを指定できます。EPGに関係なく、指定したインタ

一フェイスで送受信されるすべてのパケットをキャプチャできます。

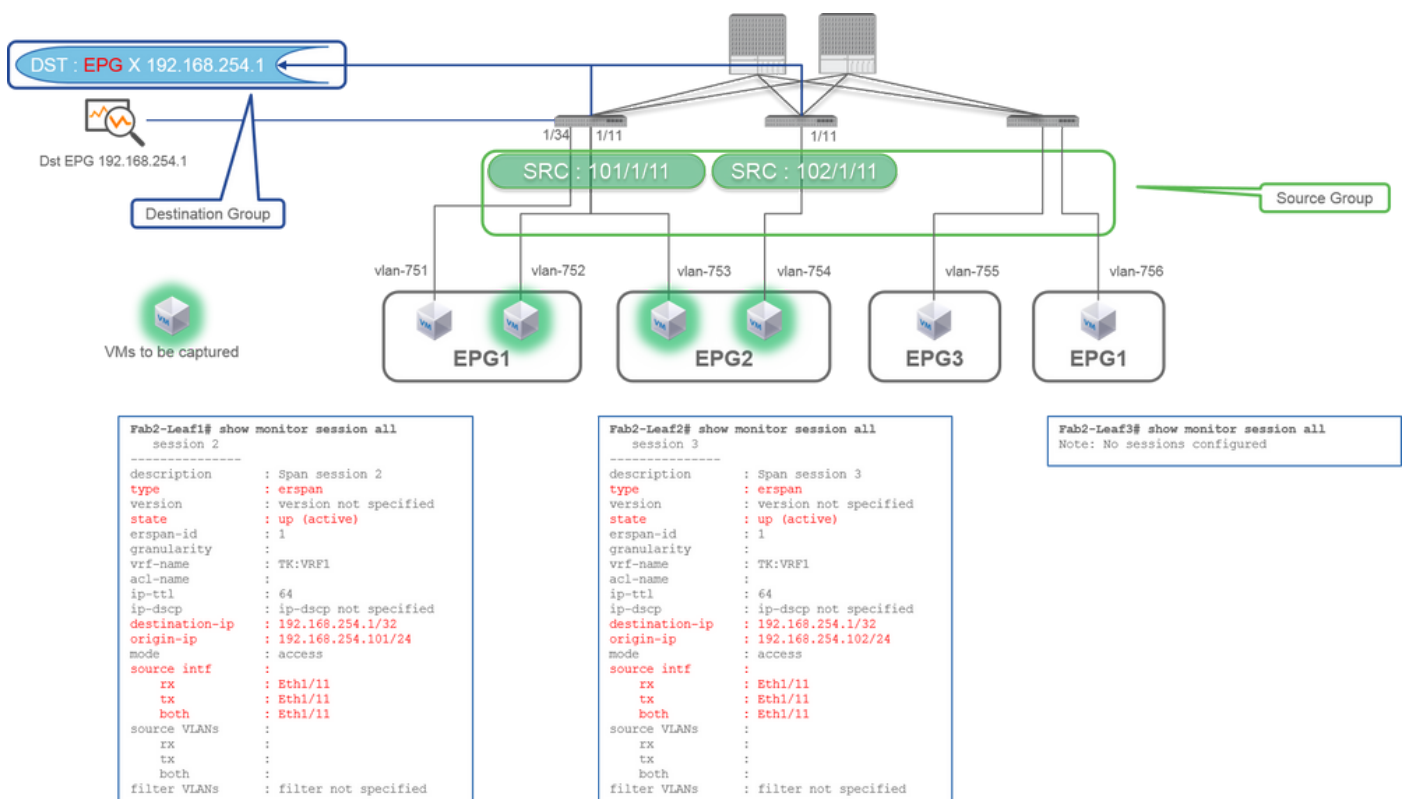
複数のリーフスイッチから複数のインターフェイスを送信元グループとして指定する場合、宛先グループはローカルSPANではなくERSPANである必要があります。

この例では、EPG1とEPG2のすべてのVMからパケットをコピーします。

### CLIのチェックポイント

- ステータスが「up (active)」であることを確認してください。
- 「destination-ip」はERSPANの宛先IPです。
- 「origin-ip」はERSPANの送信元IPです。

### Case 2.送信元「Leaf1 e1/11およびLeaf2 e1/11」 | Dst「192.168.254.1」



- ソースグループ
  - リーフ1 e1/11
  - リーフ2 e1/11

- 通知先グループ
  - EPG Xの192.168.254.1

この例では、Leaf1 e1/34が、前のCase1で設定されたSPANソースグループから削除されています。

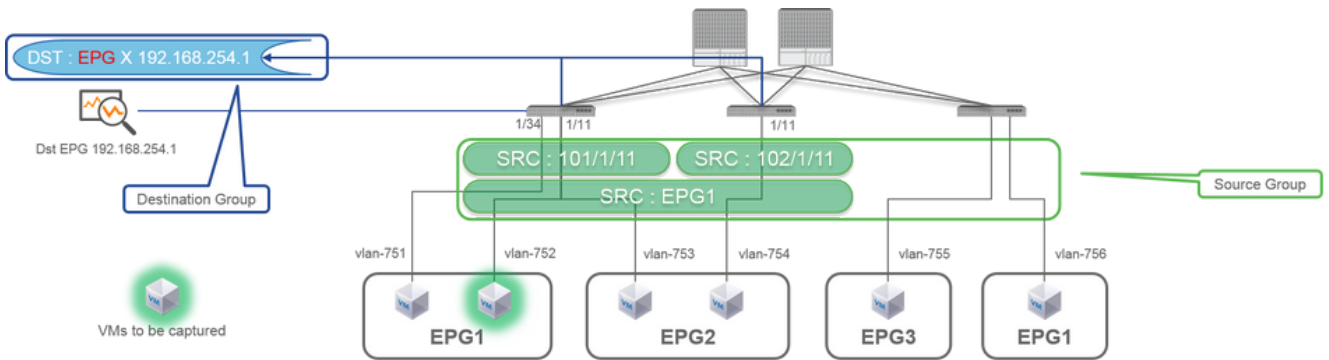
この例で重要な点は、アクセスSPANがEPGに関係なく送信元インターフェイスを指定できることです。

#### CLIのチェックポイント

- leaf1の送信元インターフェイスが「Eth1/11 Eth1/34」から「Eth1/11」に変更されます。

**Case 3.送信元「Leaf1 e1/11 & Leaf2 e1/11 & EPG1 filter」 | Dst「192.168.254.1」**





```

Fab2-Leaf1# 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         :
acl-number       :
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    : 35,39
  
```

```

Fab2-Leaf2# show monitor session all
-----
session 11
-----
description      : Span session 11
type             : erspan
version          : version not specified
state            : failed (no-oper-src-dst)
erspan-id        : 1
granularity      :
vrf-name         : TK:VRF1
acl-name         :
acl-number       :
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               :
tx               :
both            :
filter VLANs    : filter not specified
  
```

```

Fab2-Leaf3# 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
  
```

F1553 : Failed to configure SPAN with source SRC\_A due to missing/invalid EPG  
 F1561 : Failed to configure SPAN with source SRC\_A due to Source Epg not available  
 ※ SPAN on Leaf1 works

• ソースグループ

- リーフ1 e1/11
- リーフ2 e1/11
- フィルタEPG1

• 通知先グループ

- EPG Xの192.168.254.1

この例は、アクセスSPANが送信元ポートで特定のEPGを指定できることを示しています。これは、複数のEPGが1つのインターフェイス上を流れる場合に便利で、このインターフェイス上のEPG1のトラフィックのみをキャプチャする必要があります。

EPG1はリーフ2に展開されていないため、リーフ2のSPANは障害F1553およびF1561で失敗します。ただし、Leaf1上のSPANは引き続き動作します。

また、EPG1はLeaf1で2つのVLAN(VLAN-751、752)を使用するため、2つのVLANフィルタがLeaf1のSPANセッションに自動的に追加されます。

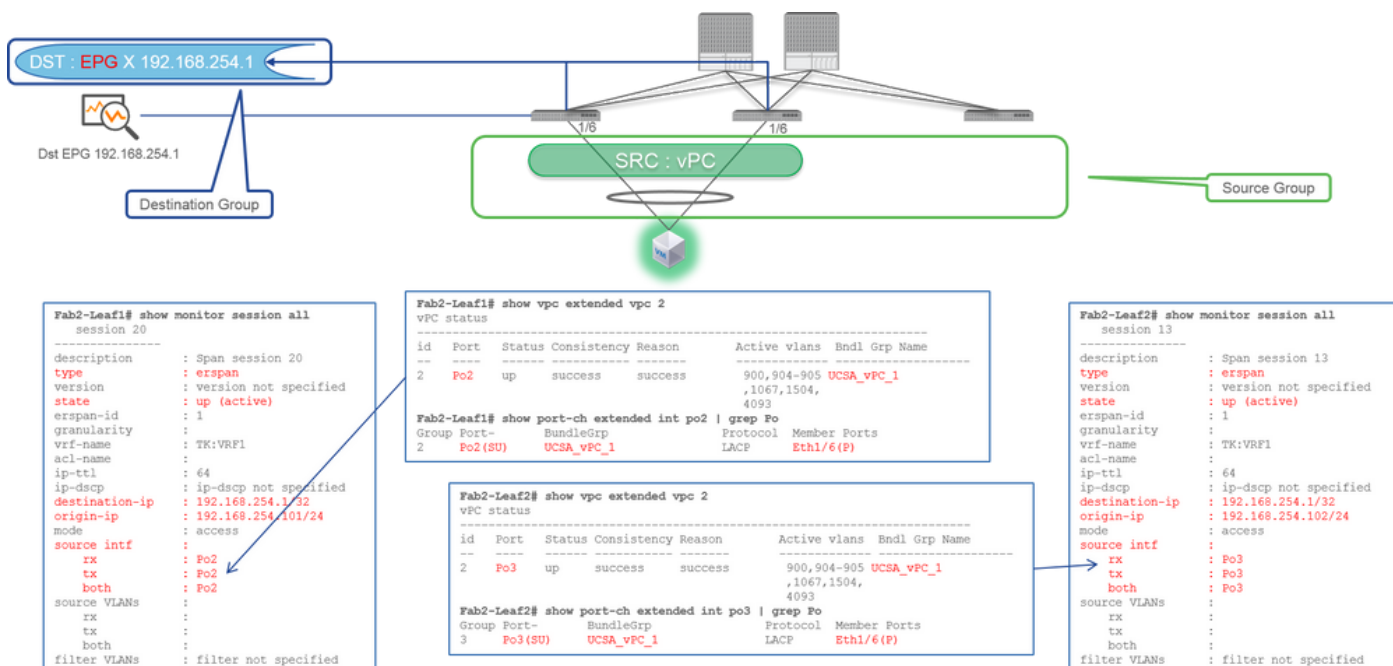
CLI(35、39)のVLAN IDは、いわゆるPI-VLAN(Platform Independent VLAN)と呼ばれる内部VLANであり、実際の回線上のIDではないことに注意してください。図に示すように、`show vlan extended`コマンドは、実際のカプセル化VLAN IDとPI-VLANのマッピングを示します。

このSPANセッションでは、EPG2(VLAN-753)が同じインターフェイス上を流れる場合でも、Leaf1 e1/11上のEPG1(VLAN-752)のパケットだけをキャプチャできます。

### CLIのチェックポイント

- フィルタVLANは、フィルタに使用されるEPGに従って追加されます。
- リーフに対応するEPGがない場合、そのリーフでのSPANセッションは失敗します。

### ケース 4.送信元「Leaf1-Leaf2 vPC」 | Dst「192.168.254.1」



- ソースグループ

- リーフ1 - 2e1/11

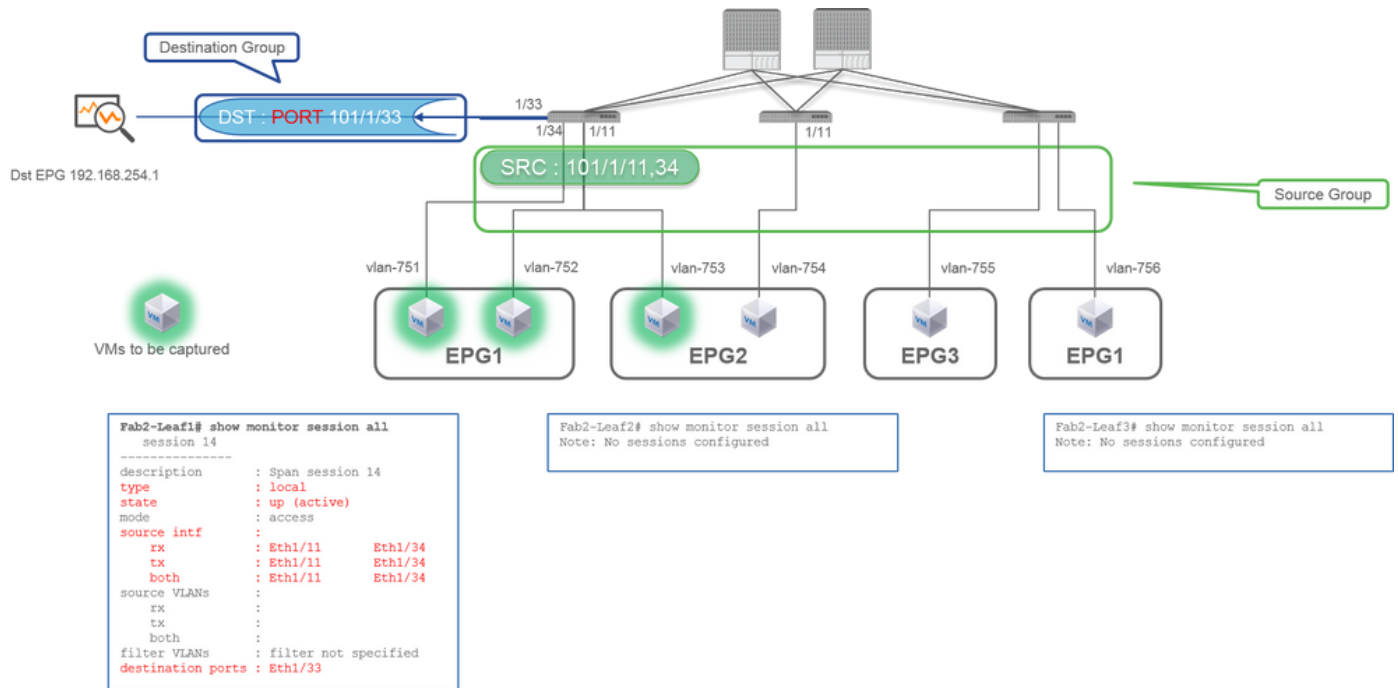
- 通知先グループ

- EPG Xの192.168.254.1

vPCインターフェイスが送信元として設定されている場合、宛先はインターフェイス ( ローカルSPAN ) ではなくリモートIP(ERSPAN)である必要があります

## アクセスSPAN ( ローカルSPAN )

Case 1.送信元「Leaf1 e1/11 e1/34」 | Dst「Leaf1 e1/33」



- ソースグループ

- リーフ1 e1/11
- リーフ1 e1/34

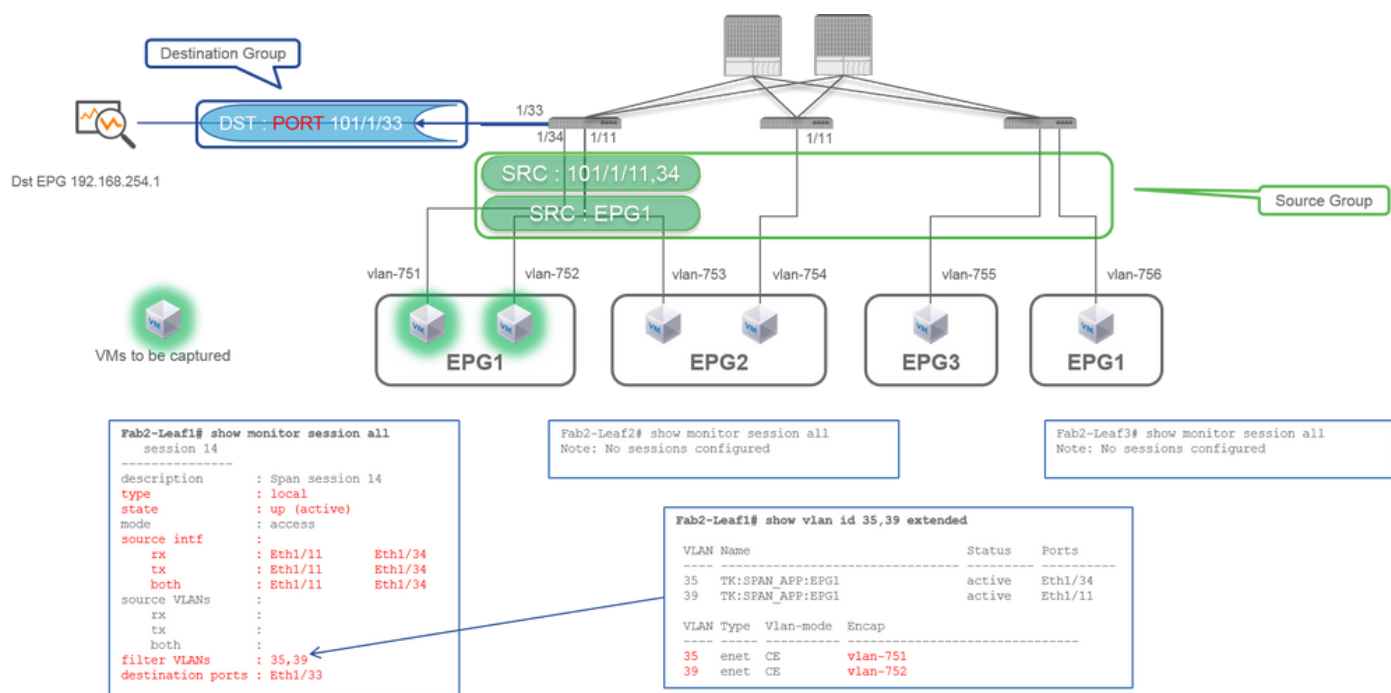
- 通知先グループ

- リーフ1 e1/33

アクセスSPANは、ローカルSPAN (宛先として特定のインターフェイス) を使用することもできます

ただし、この場合、送信元インターフェイスは宛先インターフェイスと同じリーフ上に存在する必要があります。

## Case 2.送信元「Leaf1 e1/11 e1/34 & EPG1 filter | Dst「リーフ1 e1/33」



- ソースグループ

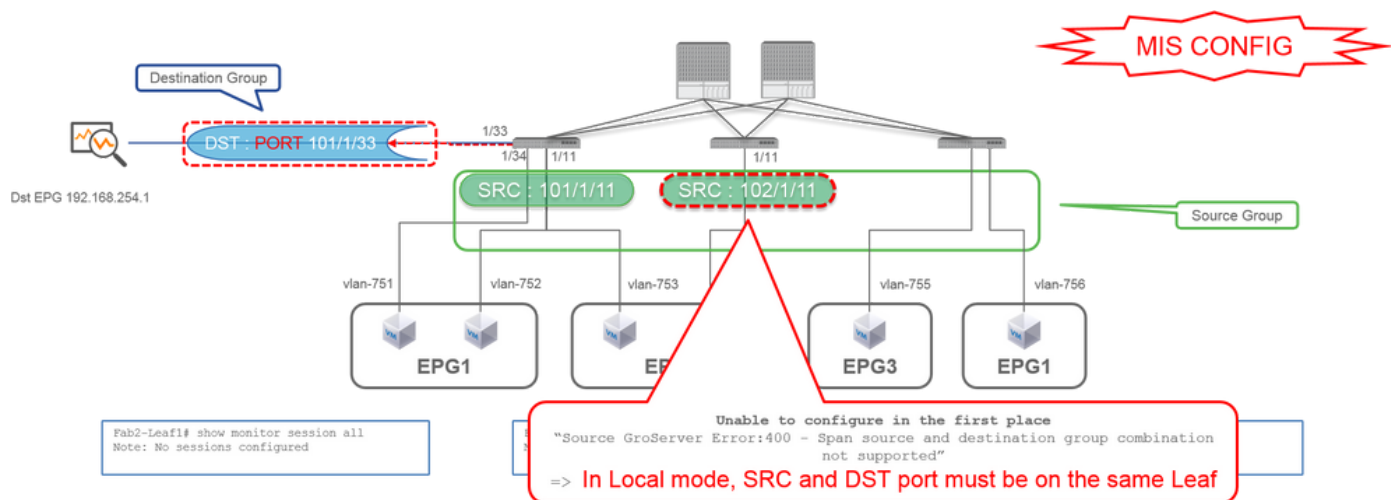
- 。リーフ1 e1/11
- 。リーフ1 e1/34
- 。EPG1フィルタ

- 通知先グループ

- 。リーフ1 e1/33

ローカルSPANを使用するアクセスSPANは、ERSPANと同様にEPGフィルタも使用できます。

### Case 3.送信元「Leaf1 e1/11およびLeaf2 e1/11」 | Dst "Leaf1 e1/33" (悪いケース)



- ソースグループ

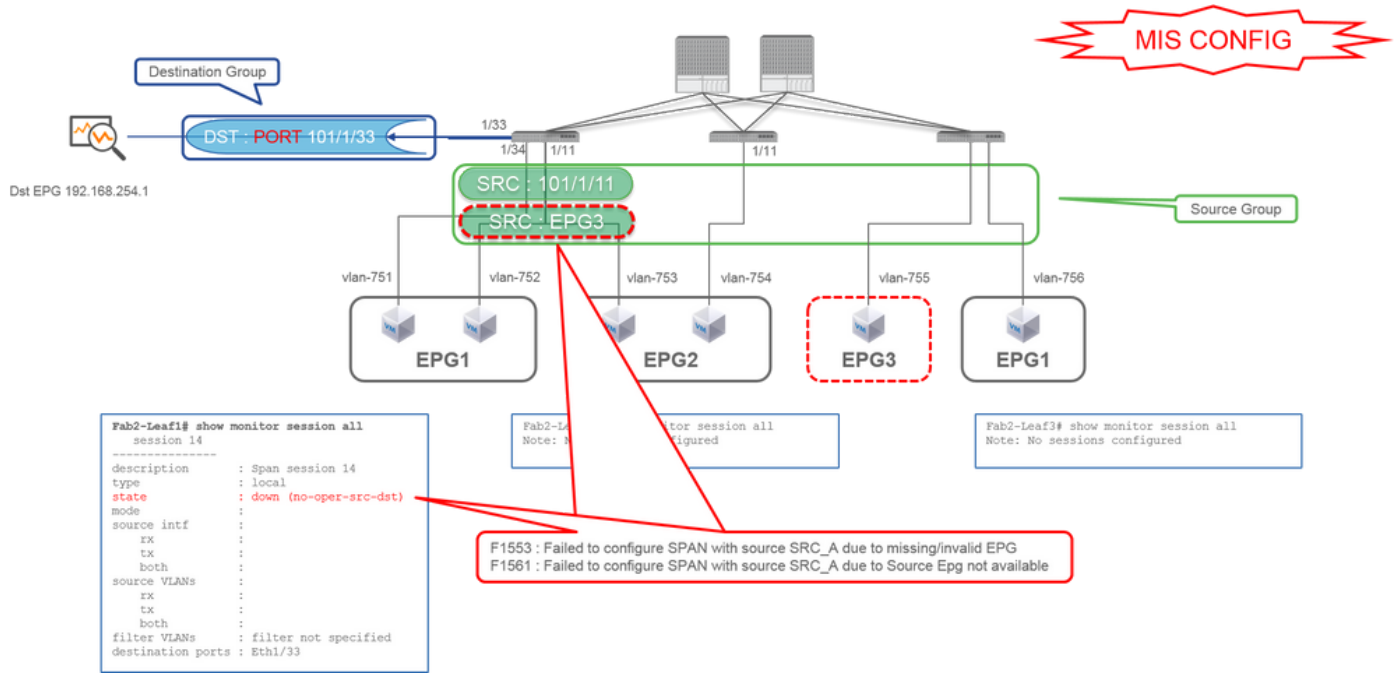
- リーフ1 e1/11

- リーフ2 e1/11

- 通知先グループ

- リーフ1 e1/33

### ケース 4.送信元「Leaf1 e1/11 & EPG3 filter」 | Dst "Leaf1 e1/33" (悪いケース)



- ソースグループ

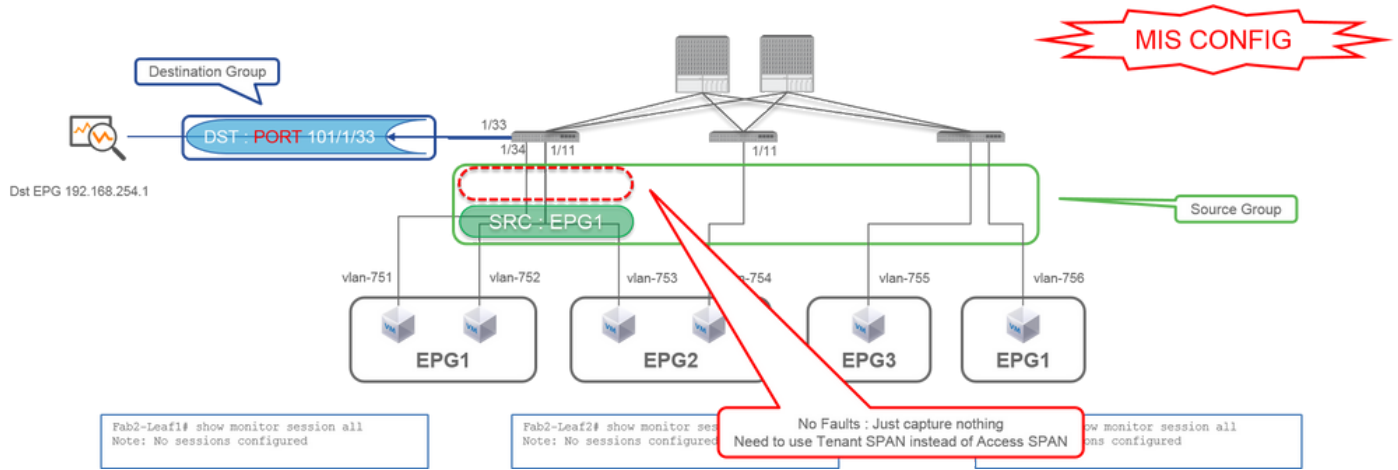
- リーフ1 e1/11
- EPG3フィルタ

- 通知先グループ

- リーフ1 e1/33

これは、アクセスSPAN(ERSPAN)のケース3に似ていますが、この例では、EPG3がLeaf1に存在しないため、Leaf1上の1つだけのSPANセッションが失敗します。そのため、SPANはまったく機能しません。

ケース5：送信元「EPG1フィルタ」 | Dst "Leaf1 e1/33" (悪いケース)



- ソースグループ

- EPG1フィルタ

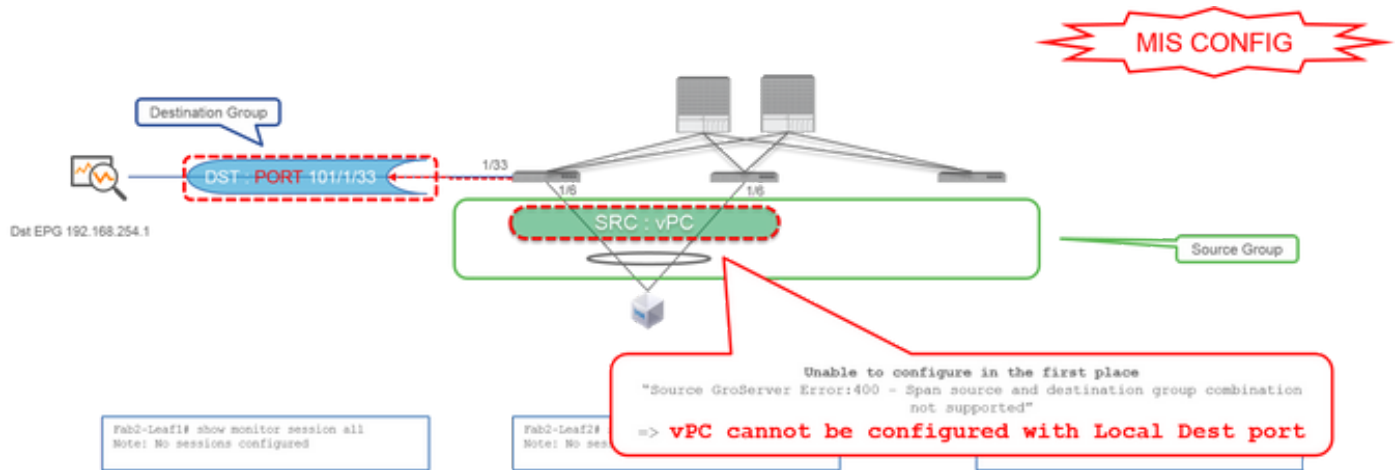
- 通知先グループ

- リーフ1 e1/33

アクセスSPANのEPGフィルタは、送信元ポートが設定されている場合のみ機能します。指定するソースがEPGのみである場合は、アクセスSPANの代わりにテナントSPANを使用する必要があります。

### Case 6.送信元「Leaf1 - Leaf2 vPC」 | Dst "Leaf1 e1/33" (悪いケース)





- ソースグループ

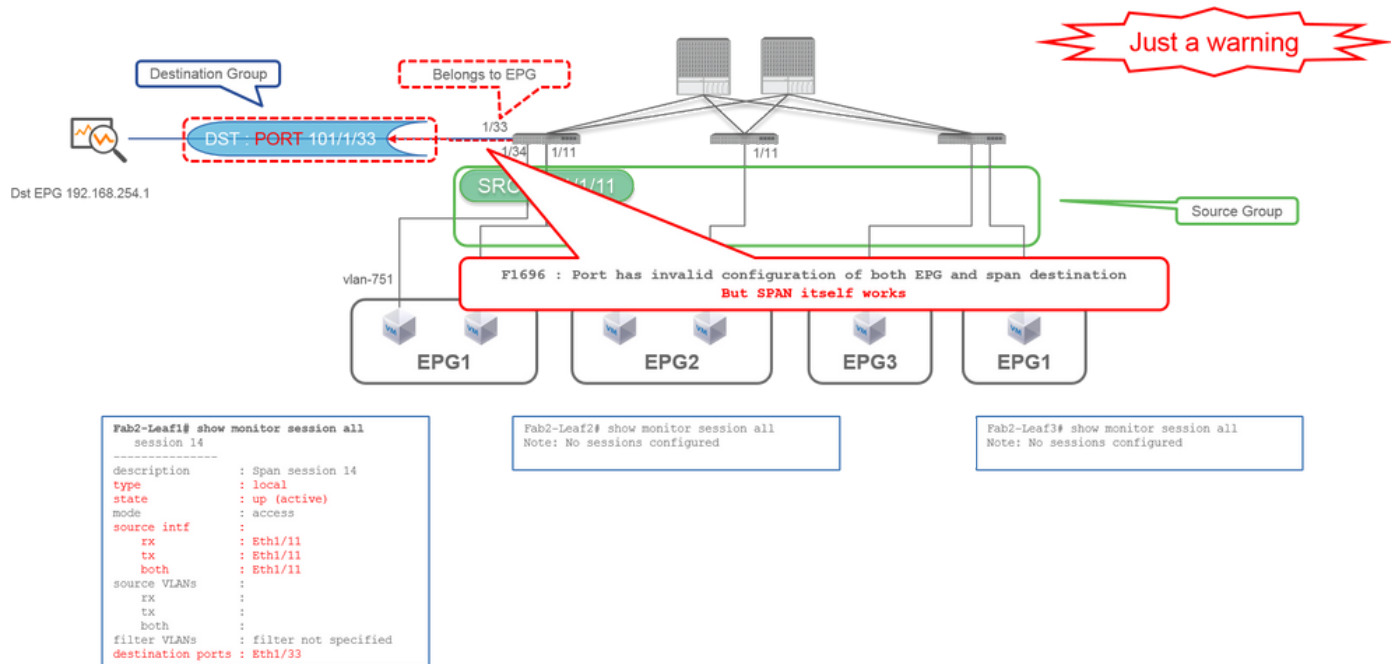
- リーフ1-2 vPC

- 通知先グループ

- リーフ1 e1/33

vPCインターフェイスは、ローカルSPANを使用して送信元として設定できません。ERSPANを使用してください。アクセスSPAN(ERSPAN)については、ケース4を参照してください。

### Case 7.送信元「Leaf1 e1/11 | Dst “Leaf1 e1/33 & e1/33 belongs to EPG” (障害あり)

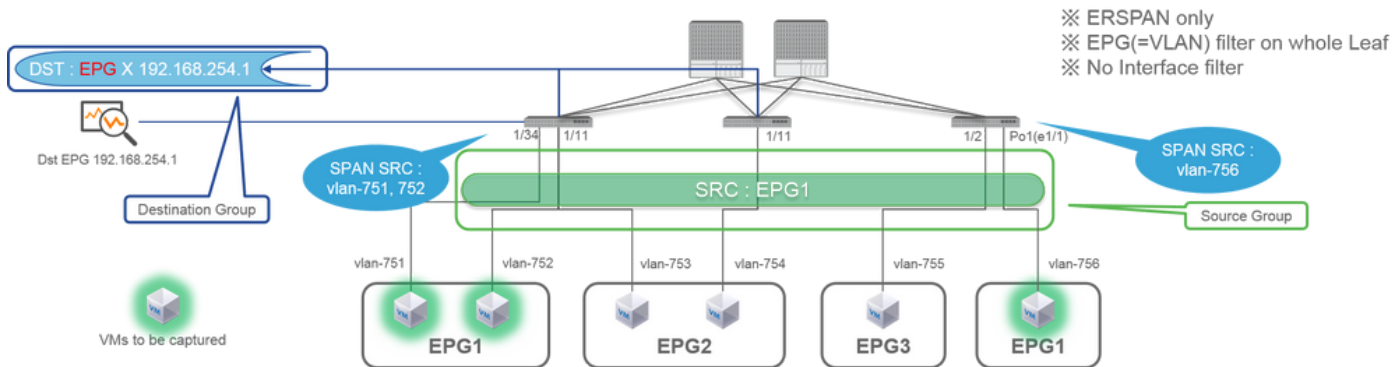


SPANの宛先I/FがすでにEPGに属している場合、物理I/Fの下で障害「F1696 : Port has an invalid configuration of EPG and span destination」が発生します。

しかし、この障害が発生しても、SPANは問題なく動作します。このエラーは、同じI/F上の顧客の通常のEPGトラフィックに影響を与える可能性があるため、SPANによって引き起こされる追加のトラフィックに関する警告にすぎません。

## テナントSPAN(ERSPAN)

Case 1.送信元「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

```

- ソースグループ

- EPG1 (フィルタなし)

- 通知先グループ

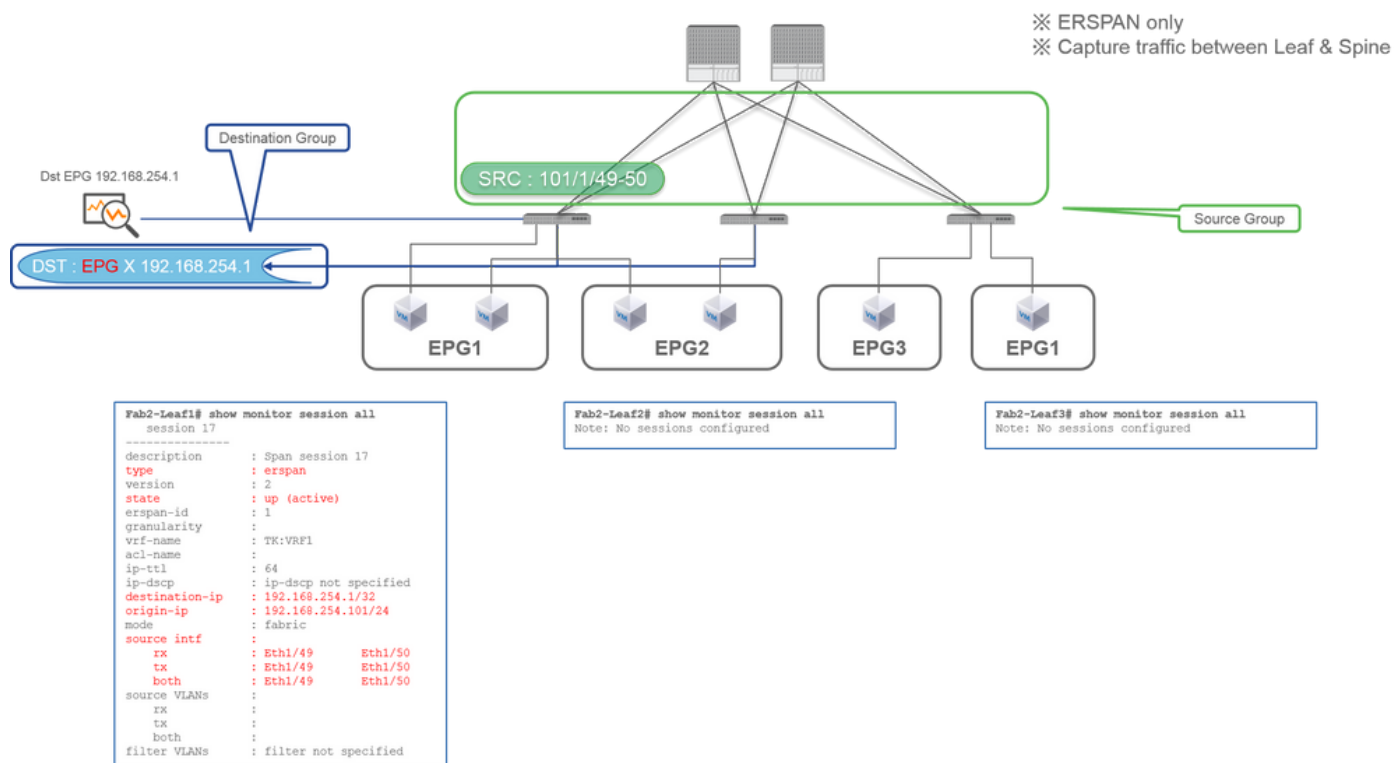
- EPG Xの192.168.254.1

テナントSPANはEPG自体を送信元として使用し、アクセスSPANはフィルタのためだけにEPGを使用します。

テナントSPANの重要な点は、個々のポートを指定する必要がなく、ACIが各リーフスイッチで適切なVLANを自動的に検出することです。したがって、これは特定のEPGのすべてのパケットをモニタする必要があるため、そのEPGのエンドポイントがリーフスイッチ経由の複数のインターフェイスに属している場合に役立ちます。

# ファブリックSPAN(ERSPAN)

## Case 1.送信元「Leaf1 e1/49-50」 | Dst「192.168.254.1」



- ソースグループ

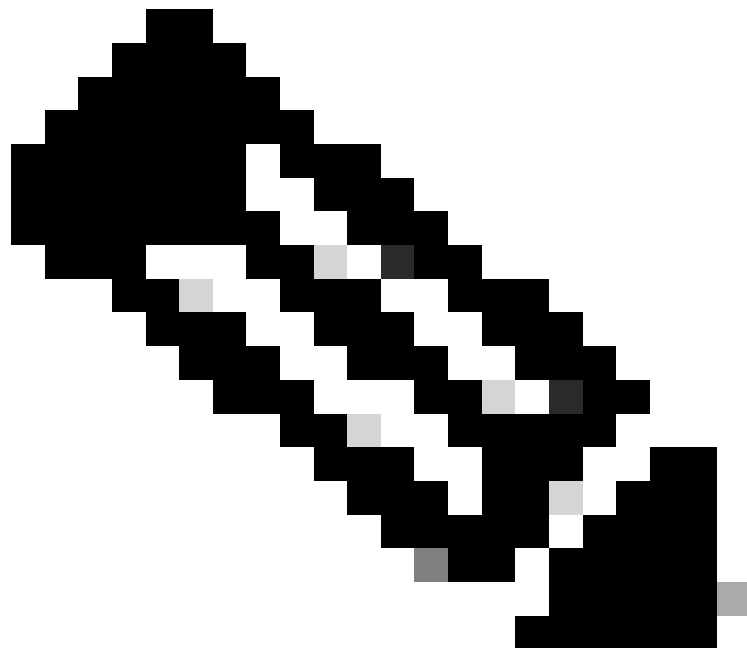
- リーフ1 e1/49-50

- 通知先グループ

- EPG Xの192.168.254.1

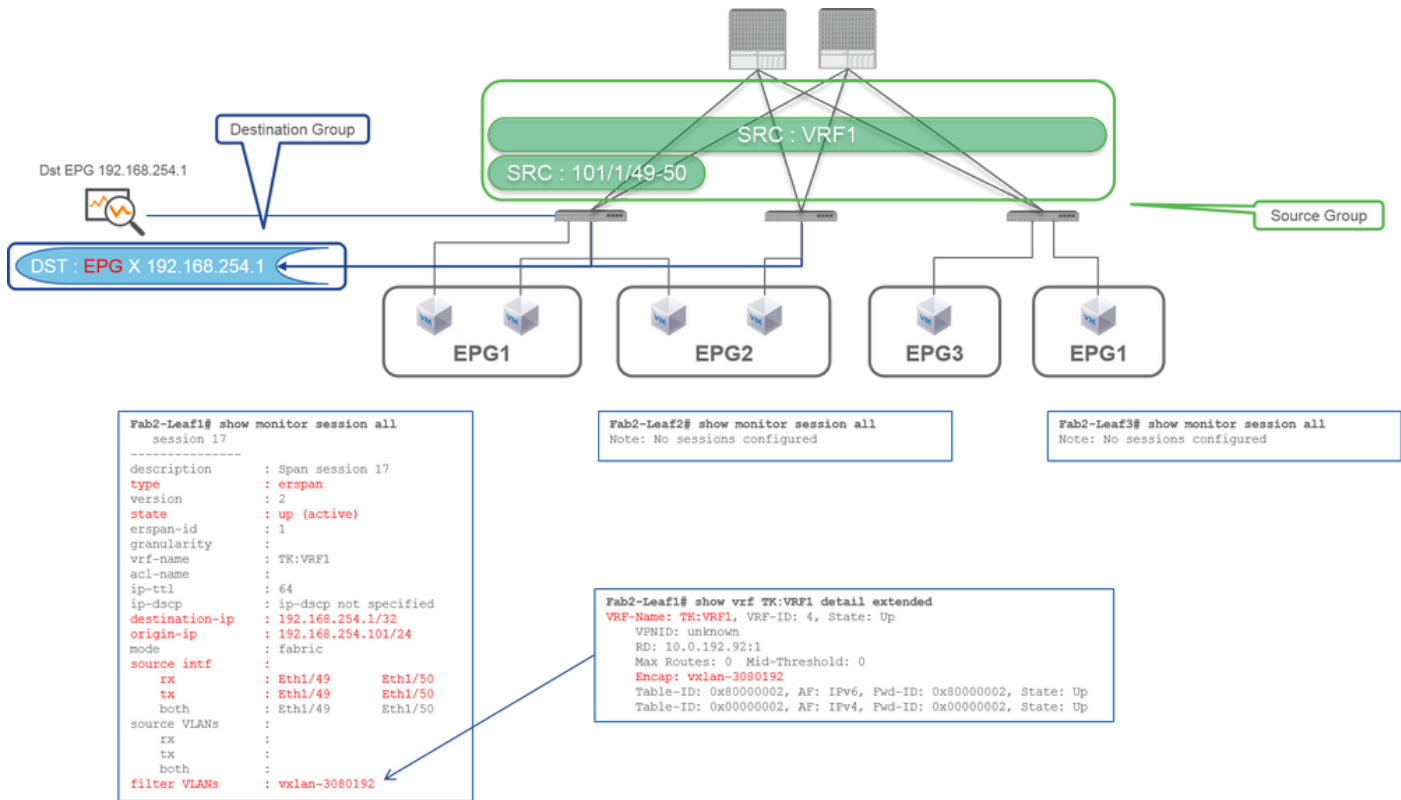
ファブリックSPANは、送信元としてファブリックポートを指定します。ファブリックポートは、リーフスイッチとスパインスイッチ間のインターフェイスです。

このSPANは、リーフスイッチとスパインスイッチ間でパケットをコピーする必要がある場合に便利です。ただし、リーフスイッチとスパインスイッチ間のパケットは、iVxLANヘッダーでカプセル化されます。だから、それを読むにはちょっとしたトリックが必要です。「SPANデータの読み方」を参照してください。



注:iVxLANヘッダーは、ACIファブリック内部使用のみの拡張VxLANヘッダーです。

Case 2.送信元「Leaf1 e1/49-50 & VRF filter」 | Dst「192.168.254.1」



- ソースグループ

- リーフ1 e1/49-50
- VRFフィルタ

- 通知先グループ

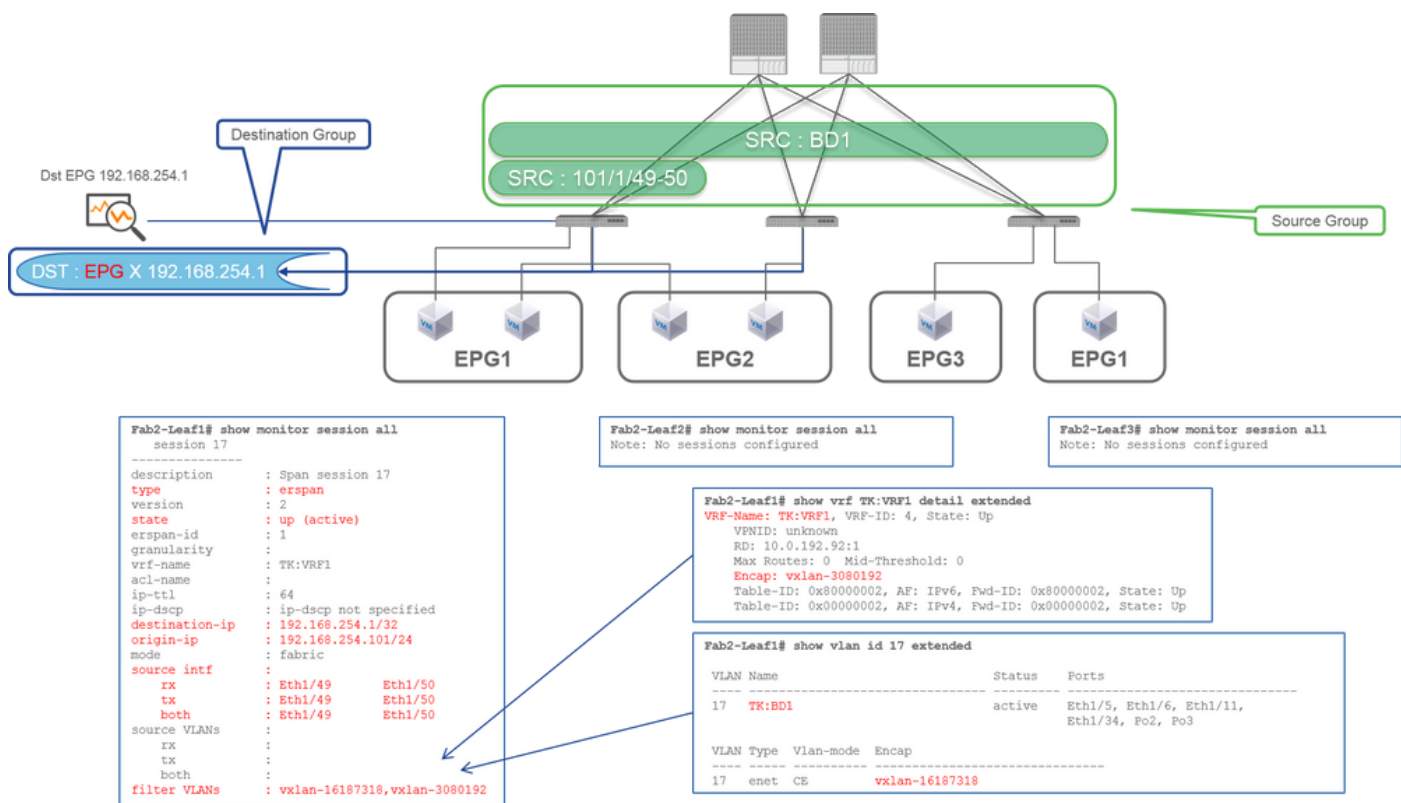
- EPG Xの192.168.254.1

ファブリックSPANでは、アクセスSPANだけでなくフィルタも使用できます。ただし、フィルタタイプは異なります。ファブリックSPANは、フィルタとして仮想ルーティングおよび転送(VRF)またはBDを使用します。

Cisco ACIでは、前述のように、ファブリックポートを通過するパケットはiVxLANヘッダーでカプセル化されます。このiVxLANヘッダーには、仮想ネットワーク識別子(VNID)としてVRFまたはBD情報が含まれています。パケットがレイヤ2(L2)として転送されると、iVxLAN VNIDはBDを表します。パケットがレイヤ3(L3)として転送される場合、iVxLAN VNIDはVRFを表します。

そのため、ファブリックポート上のルーテッドトラフィックをキャプチャする必要がある場合は、フィルタとしてVRFを使用します。

### Case 3.送信元「Leaf1 e1/49-50 & BDフィルタ」 | Dst「192.168.254.1」



- ソースグループ

- リーフ1 e1/49-50

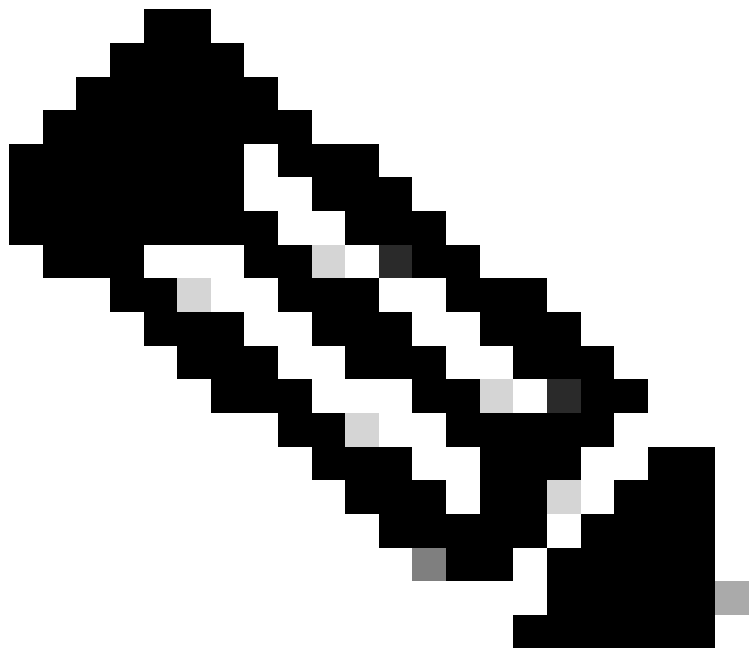
- BDフィルタ

- 通知先グループ

- EPG Xの192.168.254.1

前のケース2で説明したように、ファブリックSPANはフィルタとしてBDを使用できます。

ファブリックポートでブリッジされたトラフィックをキャプチャする必要がある場合は、フィルタとしてBDを使用します。



注：一度に設定できるフィルタは、BDまたはVRFの1つだけです。

---



## SPAN宛先デバイスに必要なものは何ですか。

tcpdump, wireshark

などのパケットキャプチャアプリケーションを実行します。ERSPAN宛先セッションなどを設定する必要はありません。

## ERSPANの場合

SPANパケットは宛先IPに転送されるため、必ずERSPANの宛先IPを持つインターフェイスでキャプチャツールを実行してください。

受信されたパケットはGREヘッダーでカプセル化されます。ERSPAN GREヘッダーをデコードする方法については、このセクションの「ERSPANデータの読み方」を参照してください。

## ローカルSPAN用

必ず、ACIリーフのSPAN宛先インターフェイスに接続するインターフェイスでキャプチャツールを実行してください。

このインターフェイスではrawパケットが受信されます。ERSPANヘッダーを処理する必要はありません。

## ERSPANデータの読み方

### ERSPANバージョン (タイプ)

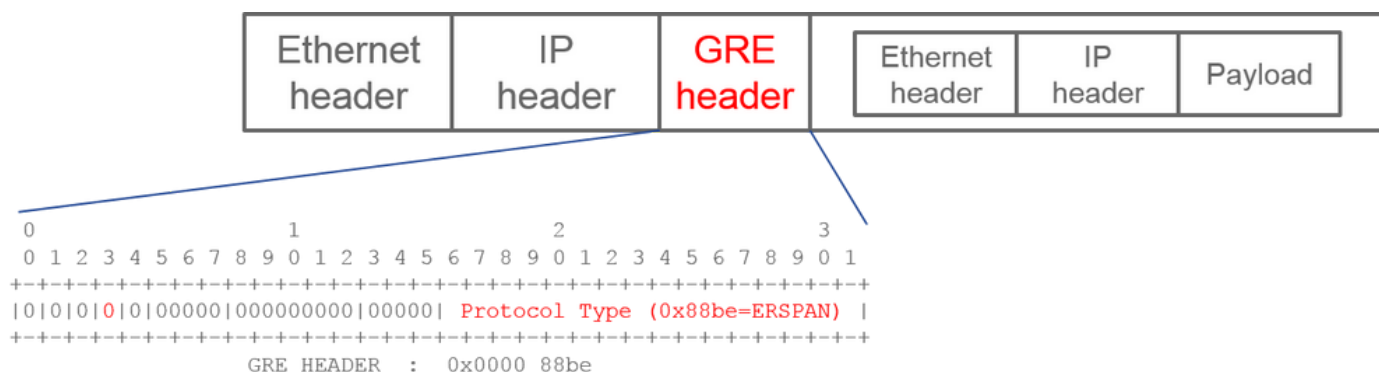
ERSPANは、コピーされたパケットをカプセル化して、リモートの宛先に転送します。このカプセル化にはGREが使用されます。GREヘッダーでのERSPANのプロトコルタイプは0x88beです。

Internet Engineering Task Force ( IETF ; インターネット技術特別調査委員会 ) のドキュメントでは、ERSPANのバージョンは version ではなく type と記述されています。

ERSPANには3つのタイプがあります。I、II、およびIII。ERSPANタイプについては、この[RFCドラフト](#)で説明されています。また、このGRE [RFC1701](#)は各ERSPANタイプを理解するためにも役立つ可能性があります。

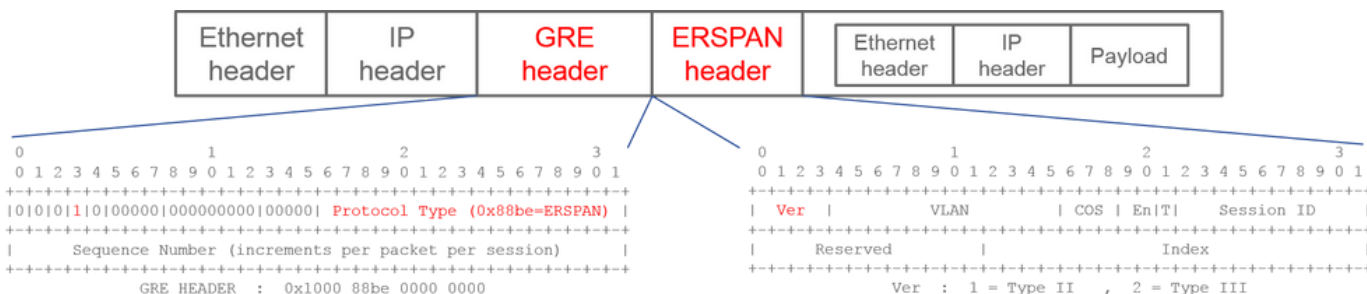
各タイプのパケット形式を次に示します。

## ERSPANタイプI (Broadcom Trident 2で使用)



タイプIは、GREヘッダーのシーケンスフィールドを使用しません。ERSPANタイプIIおよびIIIの場合、GREヘッダーの後に続く必要があるERSPANヘッダーも使用しません。Broadcom Trident 2はこのERSPANタイプIのみをサポートします。

## ERSPANタイプIIまたはIII



シーケンスフィールドがSビットによってアクティブ化される場合、これはERSPANタイプIIまたはIIIである必要があります。ERSPANヘッダーのバージョンフィールドで、ERSPANタイプが識別されます。ACIでは、タイプIIIは2016年3月20日の時点ではサポートされていません。

アクセスまたはテナントSPANのSPAN送信元グループに、第1世代と第2世代の両方のノードの送信元がある場合、ERSPAN宛先は、ノードの各世代からERSPANタイプIとIIの両方のパケットを受信します。ただし、Wiresharkで一度にデコードできるERSPANタイプは1つだけです。デフォルトでは、ERSPAN Type IIだけがデコードされます。ERSPANタイプIのデコードを有効にすると、WiresharkはERSPANタイプIIをデコードしません。WiresharkでERSPANタイプIを復号化する方法については、後述のセクションを参照してください。

この種の問題を回避するには、SPAN宛先グループでERSPANタイプを設定します。

**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バージョン (バージョン1またはバージョン2) :ERSPANタイプIまたはIIを指します
- Enforce SPAN Version (オンまたはオフ) : ソースノードハードウェアで設定されたERSPANタイプがサポートされていない場合に、SPANセッションを失敗させるかどうかを決定します。

デフォルトでは、SPANバージョンはバージョン2で、Enforce SPAN Versionはチェックされていません。つまり、送信元ノードがERSPANタイプIIをサポートする第2世代以降の場合、送信元ノードはタイプIIでERSPANを生成します。ソースノードが、ERSPANタイプII (ファブリックSPANを除く) をサポートしない第1世代の場合、「Enforce SPAN Version」がチェックされていないため、タイプIにフォールバックします。その結果、ERSPANの宛先は、混合タイプのERSPANを受信します。

次の表に、アクセスSPANとテナントSPANの各組み合わせについて説明します。

SPANバージョン	SPANバージョンの適用	第1世代ソースノード	第2世代ソースノード
バージョン2	非選択	タイプIを使用	タイプIIを使用
バージョン2	オン	失敗	タイプIIを使用
バージョン1	非選択	タイプIを使用	タイプIを使用



## ファブリック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は自動的にERSPAN Type IIをデコードします。ただし、iVxLANヘッダーによってカプセル化されたままです。

デフォルトでは、WiresharkはACI内部ヘッダーであるため、iVxLANヘッダーを認識しません。「iVxLANヘッダーのデコード方法」を参照してください。

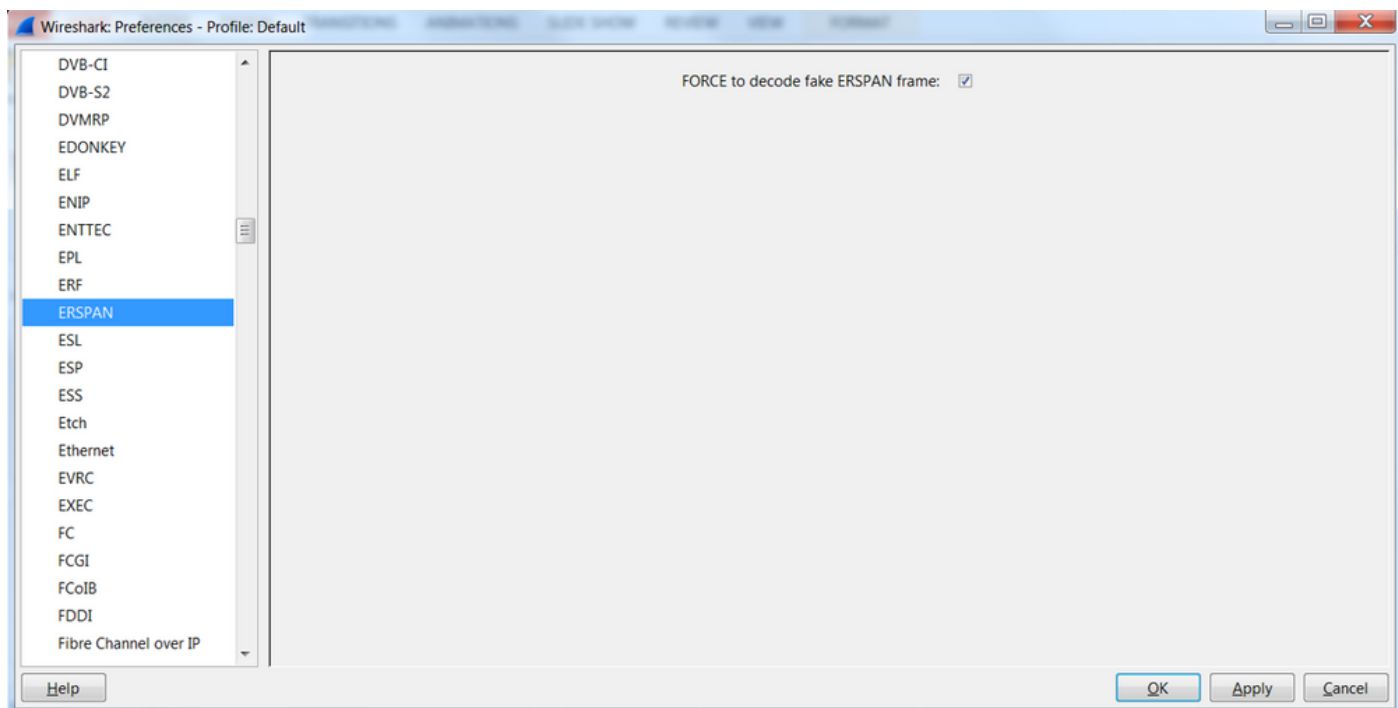
### キャプチャパケットの詳細 (ERSPANタイプII)

```
[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          ESPAN Ethernet header           : Dst 0050.56bb.3096 , Src 0022.bdf8.19ff
0x0010: 00b8 0580 0000 3a2f f8de c0a8 fe65 c0a8          ERSPAN IP header                : Dst 192.168.254.1 , Src 192.168.254.101
0x0020: fe01 1000 88be 0000 d05d 1002 1001 0001          GRE header (= ERSPAN Type II)  : 0x88be = ERSPAN (S bit on 0x1000)
0x0030: abc0 000c 0c0c 0c0c 0000 0000 0000 0800          ERSPAN Type II header          : VLAN 2, ERSPAN ID 1
0x0040: 4500 0086 55aa 0000 1f11 b101 0a00 c05f          Ethernet header                 : Dst 0022.bdf8.19ff , Src 0050.56bb.d6c2
0x0050: 0a00 c05c 6250 beef 0072 0000 c8a0 c007          IP header                       : Dst 10.0.192.95 , Src 10.0.192.92
0x0060: fd7f 8200 0050 56bb d95f 0050 56bb d6c2          UDP header                      : Dst 0xbeef(48879) , Src 0x6250(25168)
0x0070: 0800 4500 0054 799b 0000 4001 7bba c0a8          iVxLAN header                   : sclass 0xc007 , VNID 0xfd7f82
0x0080: 0202 c0a8 0201 0000 4f21 b749 0027 3d24          Ethernet header                 : Dst 0050.56bb.d95f , Src 0050.56bb.d6c2
0x0090: 2b56 0000 0000 c720 0b00 0000 0000 1011          IP header                       : Dst 192.168.2.254 , Src 192.168.2.2
0x00a0: 1213 1415 1617 1819 1a1b 1c1d 1e1f 2021
0x00b0: 2223 2425 2627 2829 2a2b 2c2d 2e2f 3031
0x00c0: 3233 3435 3637
```

### ERSPANタイプIのデコード方法

オプション 1Edit > Preference > Protocols > ERSPANに移動し、FORCEにチェックマークを入れて疑似ERSPANフレームをデコードします。

- Wireshark(GUI)

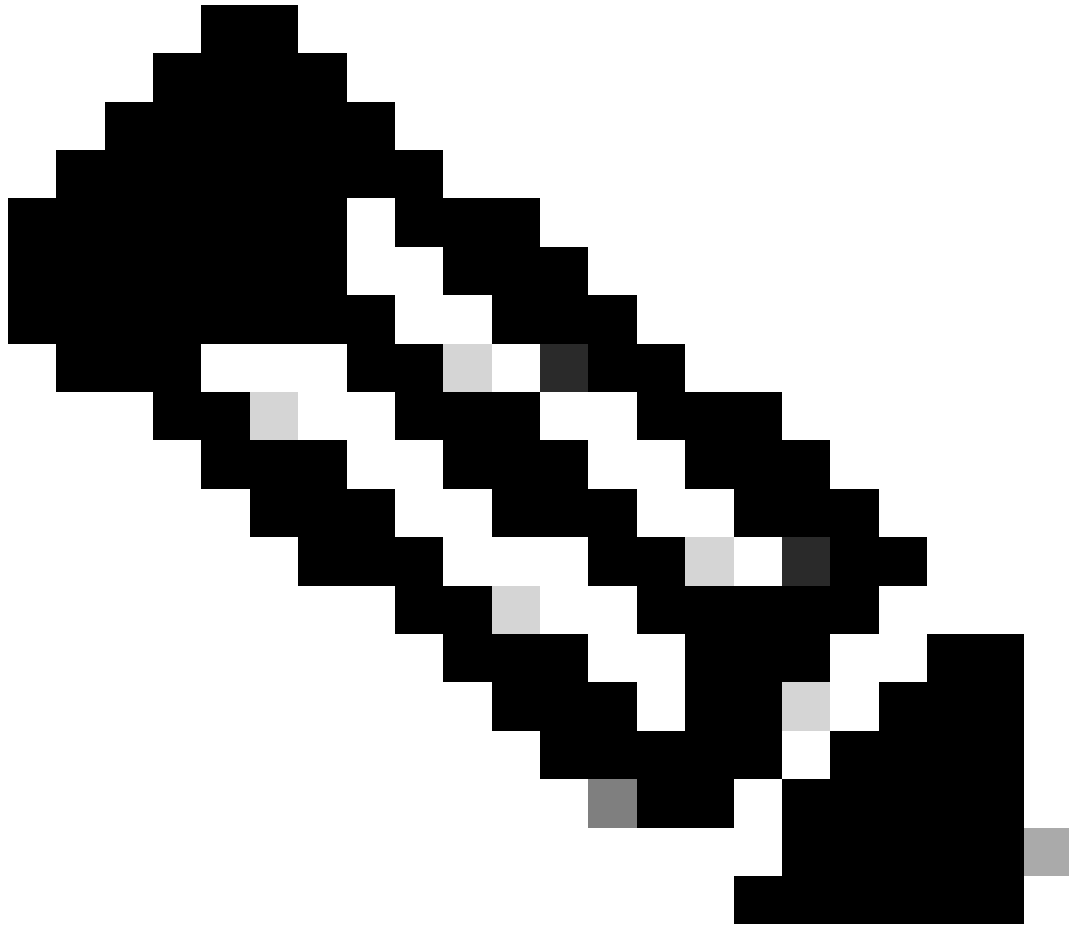


- Tshark ( WiresharkのCLIバージョン ) :

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

---

---

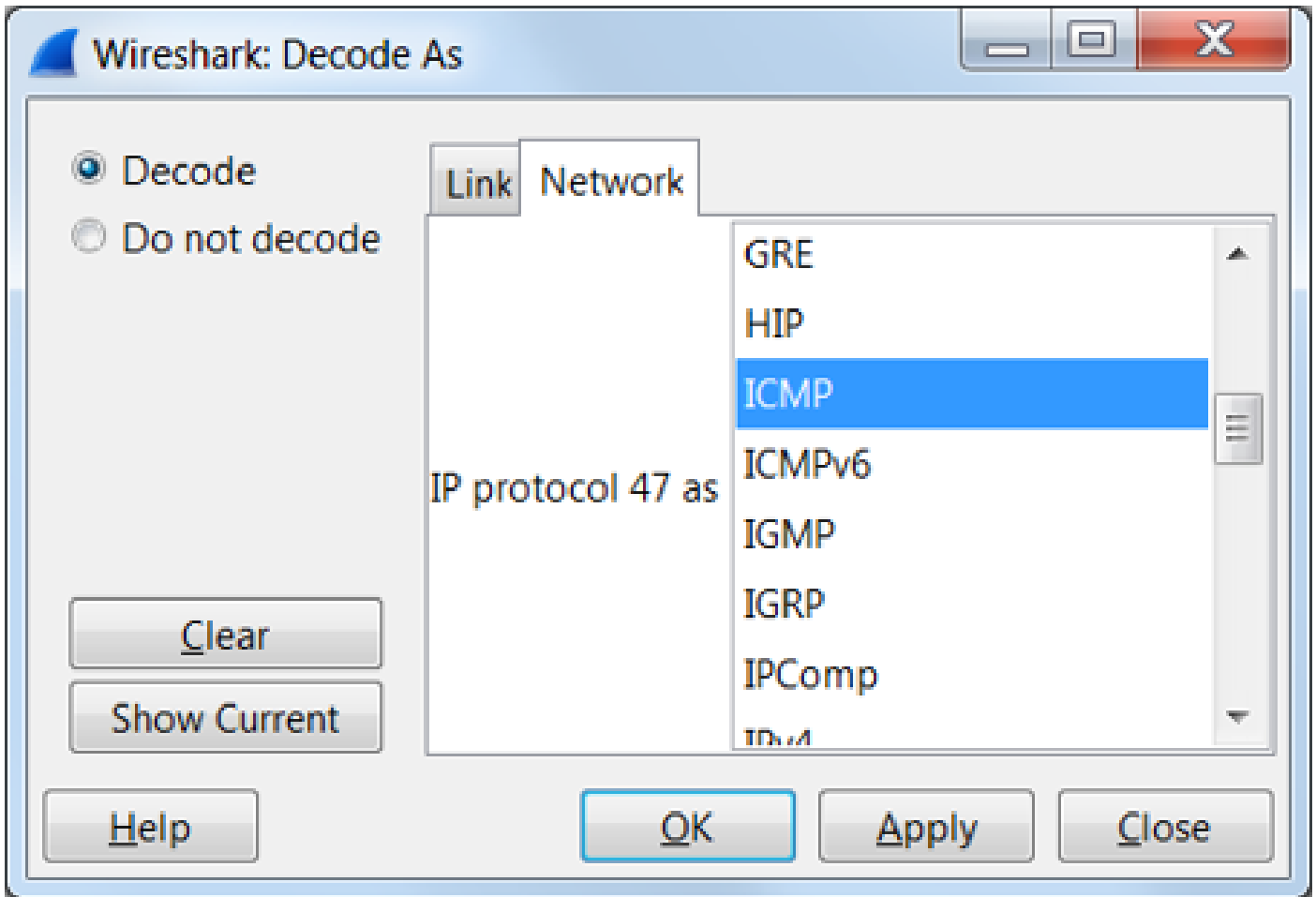


注:ERSPANタイプIIまたはIIIを読み取る場合は、必ずこのオプションを無効にしてください。

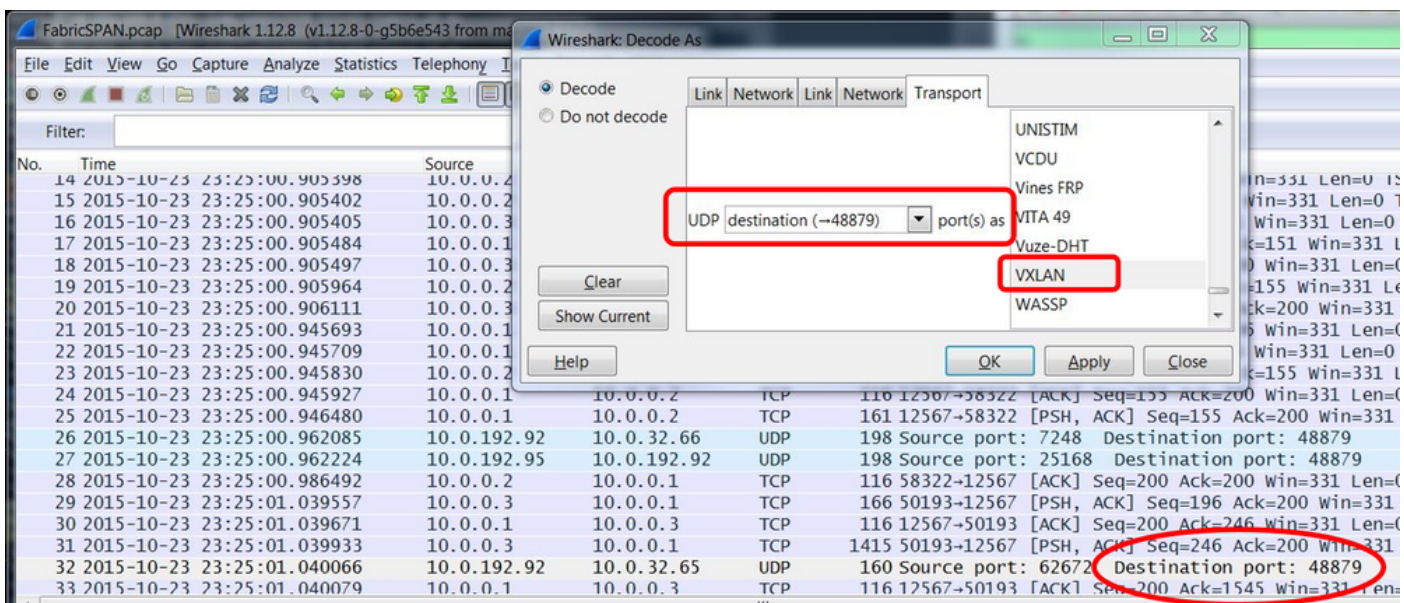
---

オプション 2移動先 Decode As > Network > ICMP (if it's ICMP).





### iVxLANヘッダーのデコード方法

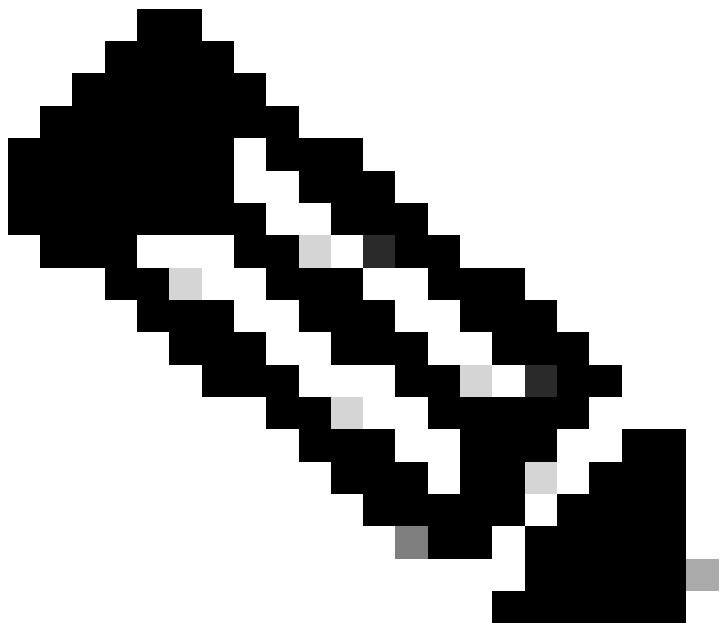


iVxLANヘッダーは宛先ポート48879を使用します。そのため、UDP宛先ポート48879をWireshark上のVxLANとして設定する場合は、VxLANだけでなくiVxLANヘッダーもデコードできます。

1. 最初にiVxLANカプセル化パケットを選択してください。

Analyze > Decode As > Transport > UDP destination (48879) > VxLAN

- に移動します。
- 次にApplyを発行します。



注：ファブリックポート上のAPIC間には通信パケットがあります。これらのパケットは、iVxLANヘッダーによってカプセル化されません。

---

Precision Time Protocol(PTP)を実行しているユーザネットワークでerspanキャプチャを取得すると、GREカプセル化(0x8988)内の未知のethertypeが原因で、Wiresharkがデータを解釈しない場合があります。0x8988は、PTPが有効なときにデータプレーンパケットに挿入される時間タグのethertypeです。Ethertype 0x8988を「Cisco ttag」としてデコードし、パケットの詳細を明らかにします。

```
▶ 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]
```

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。