ACIでのスイッチドポートアナライザ(SPAN)の設定

内容

はじめに

このドキュメントでは、Cisco Application Centric Infrastructure(ACI)バージョン5.xおよび6.x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。

バックグラウンド情報

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およびERSPANをサポートします。

注：このドキュメントは、読者がSPANに精通しており、ローカルSPANとERSPANの相違点を理解していることを前提としています。

Cisco ACIのSPANタイプ

Cisco ACIには、ファブリックSPAN、テナントSPAN、およびアクセス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 –

- ファブリックSPANでは、リーフ/スパインスイッチ間のインターフェイスで送受信されるパケットをキャプチャします。
- アクセスSPANは、リーフスイッチと外部デバイス間のインターフェイスで送受信されるパケットをキャプチャします。
- テナントSPAN(TSPAN)では、ACIリーフスイッチのエンドポイントグループ(EPG)で発着信するパケットをキャプチャします。

- SPANから

CPU(SPAN)では、リーフスイッチと外部デバイス間のインターフェイスで送受信されるパケットをキャプチャします（6.2以降）。

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で設定します。
- アクセスSPANは、Fabric > Access Policiesで設定します。
- SPAN to CPUは、Fabric > Access Policies
- テナントSPANはTenants > {each tenant}で設定します。

各SPANの宛先では、アクセスSPANだけが、ローカルSPANとERSPANの両方に対応しています。他の2つのSPAN(ファブリックとテナント)は、ERSPANだけが可能です。

制限事項とガイドライン

『Cisco APIC Troubleshooting Guide』の「Limitations & Guidelines」を参照してください。これは、「トラブルシューティングツールと手法> SPANの使用」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ついて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 Troubleshooting Guide: Troubleshooting Tools and Methodology > Using SPAN』でも説明しています。

アクセスSPAN(ERSPAN)

トポロジの例

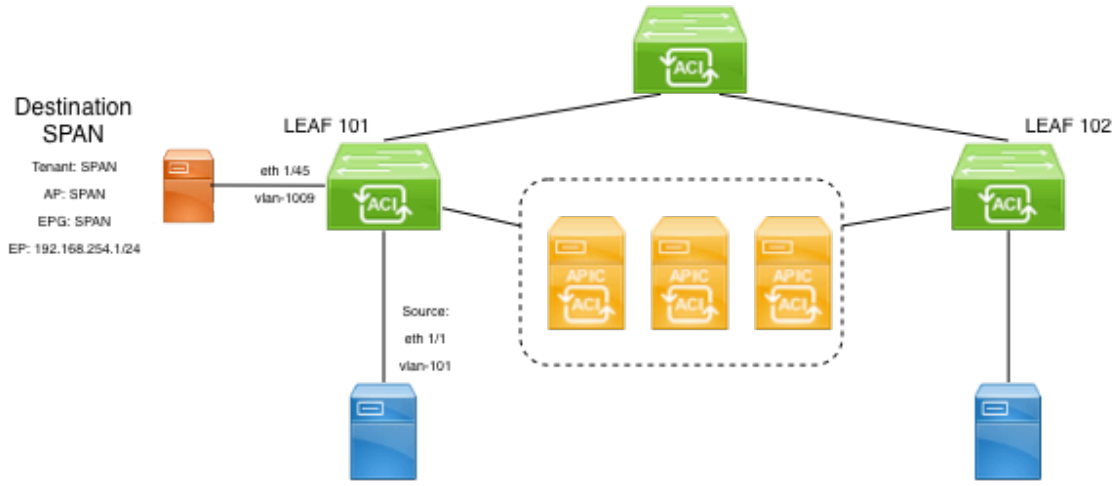

図1：アクセスERSPANのサンプルトポロジ

設定例

Fabric > Access Policies > Policies > Troubleshooting > SPANの順に選択します。

- 「SPAN Destination Groups」を右クリックし、SPAN Destination Group(DST_EPG)を作成するオプションを選択します。

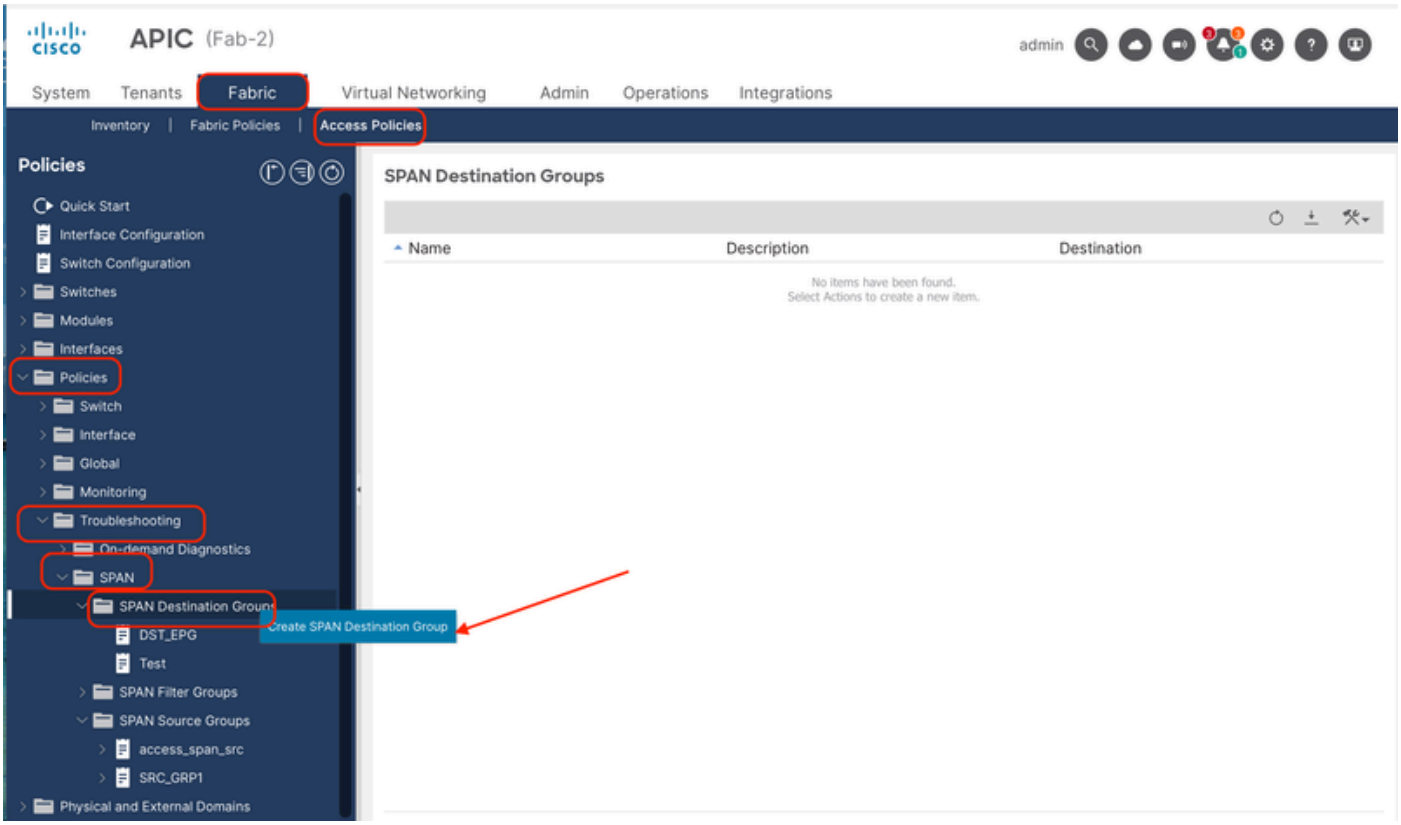

図2：アクセスERSPAN宛先グループを作成するパス

次の情報を入力します。

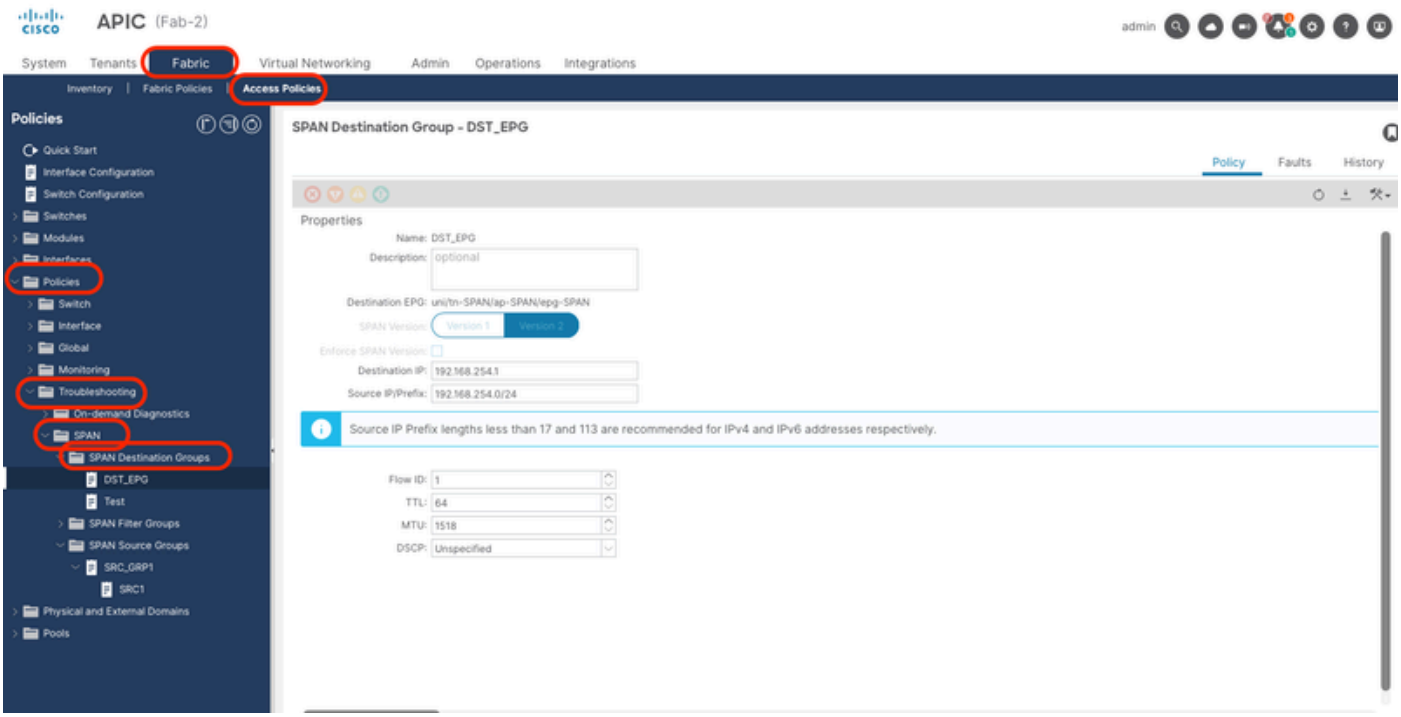

図3：アクセスERSPAN宛先グループの設定

ここで、

宛先タイプ：EPG（アクセスERSPANであることが必須）

宛先EPG:宛先エンドポイントが学習されるテナント/AP/EPG

宛先IP：宛先エンドポイントのIP

送信元IP:任意のIPを指定できます。プレフィックスが使用される場合、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のprefix: 192.168.254.0/24 => src IP 192.168.254.101のようになります。

フローID:デフォルトでは1に設定され、ERSPANヘッダーでフローによってパケットを識別するのに役立ちます。

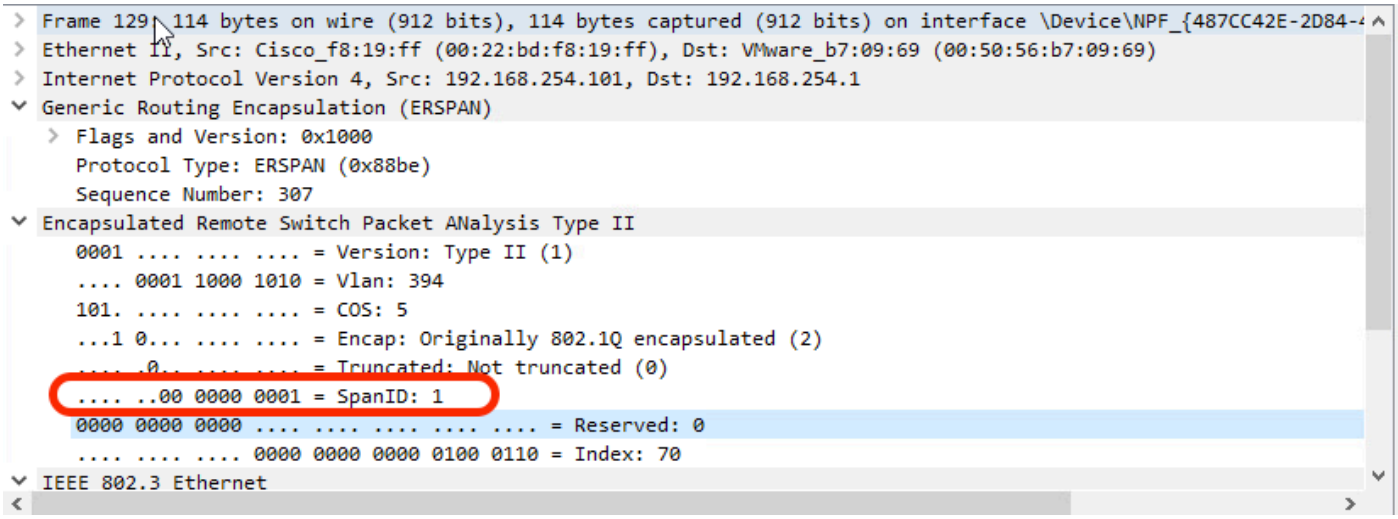

図4：フローIDを表示するWiresharkのパケット

ヒント：フローIDをフィルタリングするには、次のWiresharkフィルタを使用できます。erspan.spanid == <Flow ID>

- SPAN Source Group(SRC_GRP1)を作成し、「SPAN Source Groups」を右クリックして「Create SPAN Source groups」を選択します。

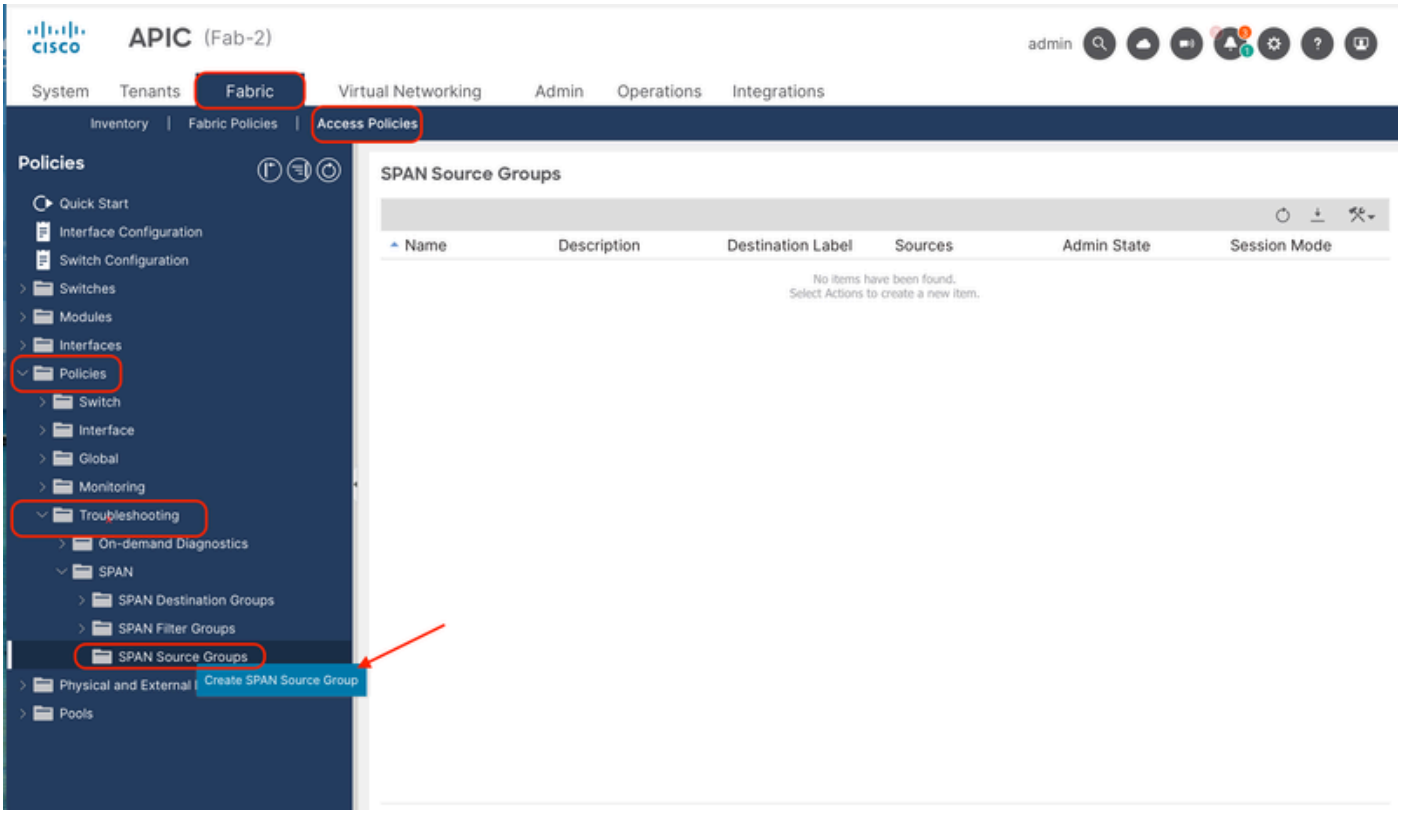

図5：アクセスERSPANソースグループを作成するパス

次の情報を入力します。

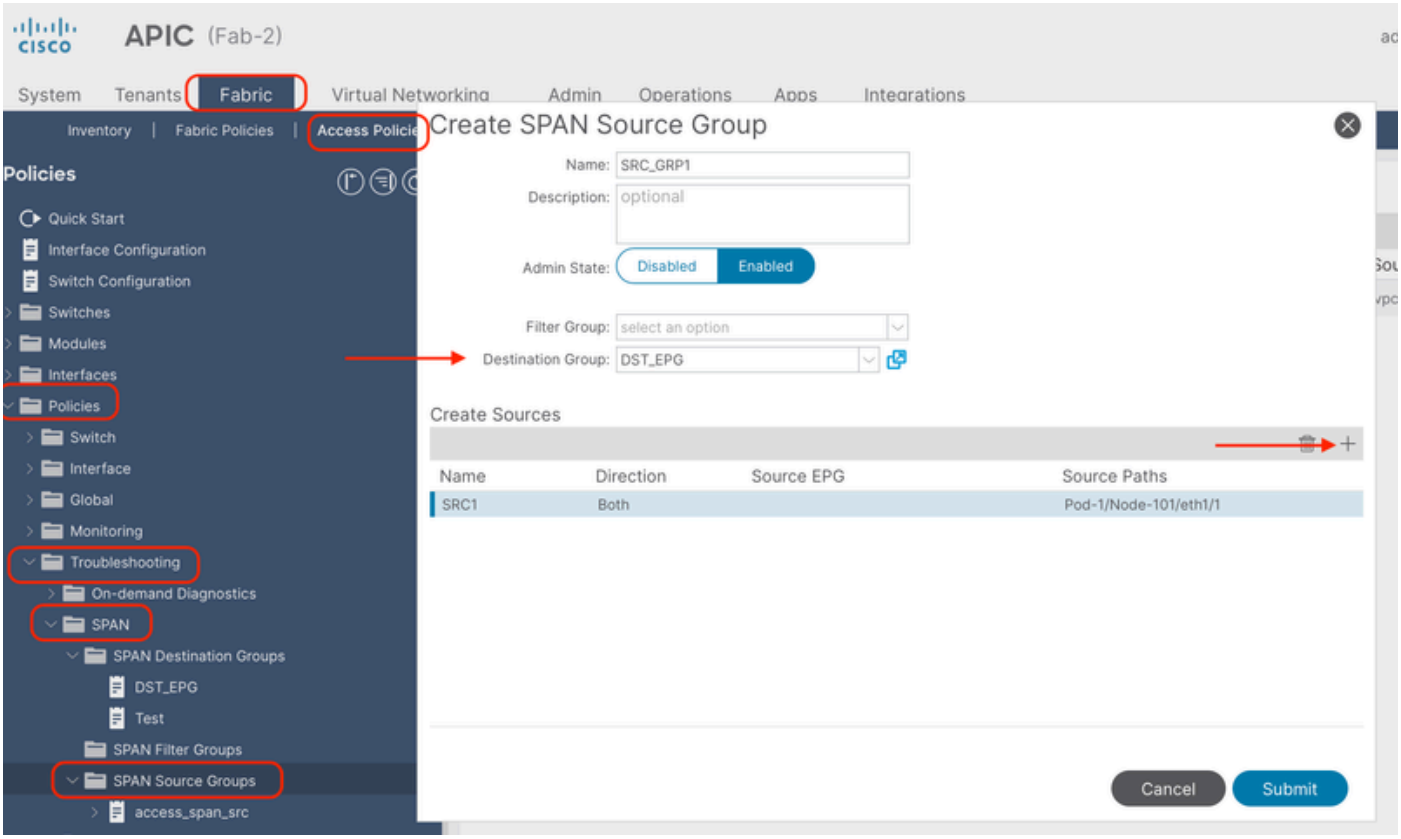

図6：アクセスERSPANソースグループの設定

ここで、

Admin State（管理状態）:Enabled（有効）

通知先グループ：以前作成した通知先グループ(DST_EPG)を選択します。

- この同じボックスで、プラスボタン(+)をクリックして、少なくとも1つのSPANソースを追加します。
- SPAN Source(SRC1)を作成するには、次のパラメータを設定します。

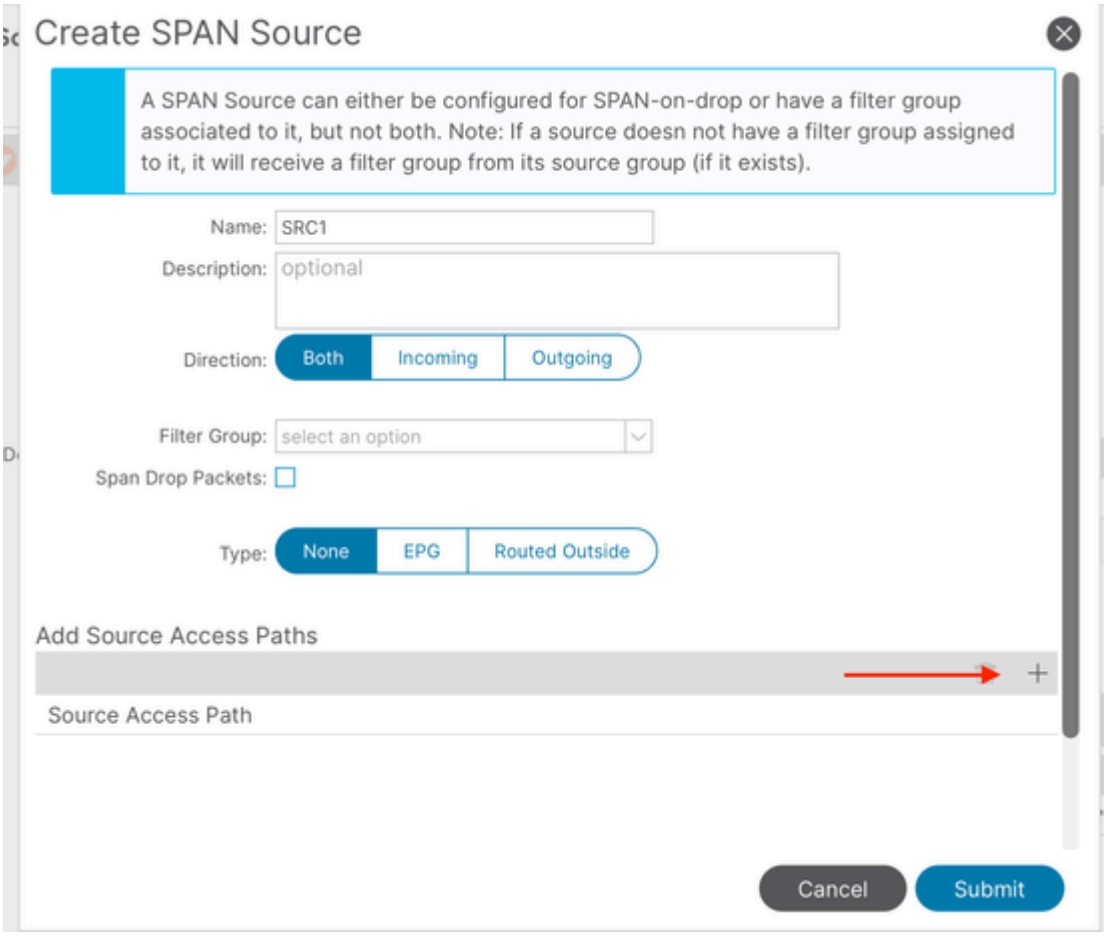

図7：アクセスERSPAN送信元の設定

ここで、

方向：着信、発信、または両方向のいずれかを選択できます。

タイプ：なし（通常の前面ポート）、EPG（EPGでスタティックバインディングとして導入されたインターフェイス、EPGトラフィックのみがミラーリングされる）、またはRouted Outside（L3outで使用されるインターフェイス）のいずれかを選択できます。

この例では、通常の前面ポートが使用されます。

- プラスボタン(+)をクリックして、ソースアクセスパスを追加します。次の情報を入力します。

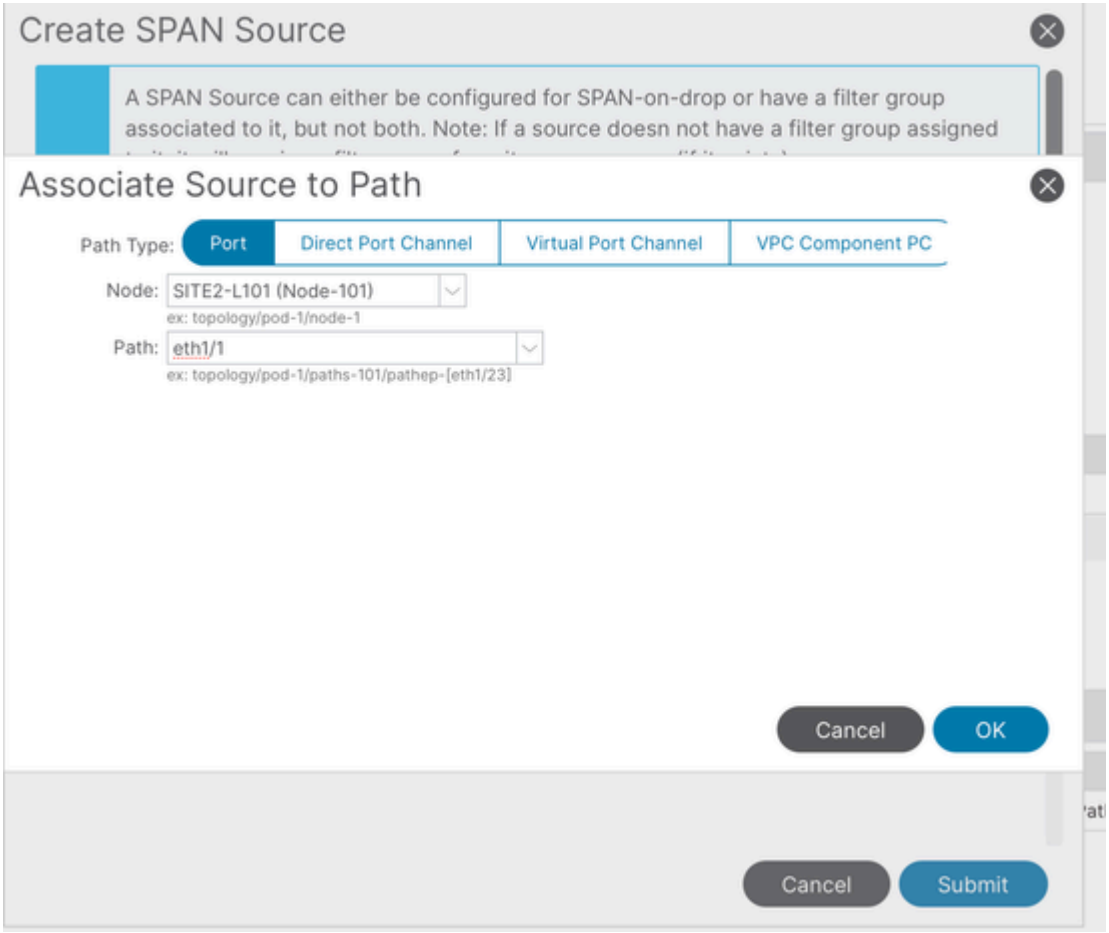

図8：アクセスERSPANソースパスの作成

ここで、

パスタイプ：ポート（個別）、ダイレクトポートチャネル、仮想ポートチャネル（このオプションを選択すると、パスにはVPCがすでに形成されていることが示されます）、およびVPCコンポーネントPC（VPCの一方のレッグだけ、特定のノードを選択します）のいずれかを選択します。

ノード：ソースノードを選択します（トポロジの例ではノード101）。

パス：送信元インターフェイス（トポロジ例によるeth1/1）

アクセスローカルSPAN

トポロジの例

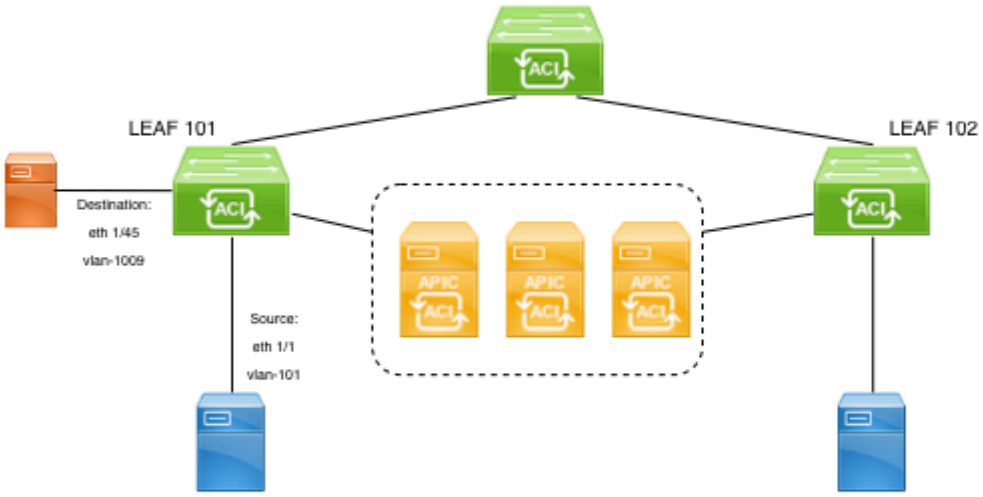

図9：ローカルアクセスSPANのトポロジ例

設定例

Fabric > Access Policies > Policies > Troubleshooting > SPANの順に選択します。

- 「SPAN Destination Groups」を右クリックし、SPAN Destination Group(DST_EPG)を作成するオプションを選択します。

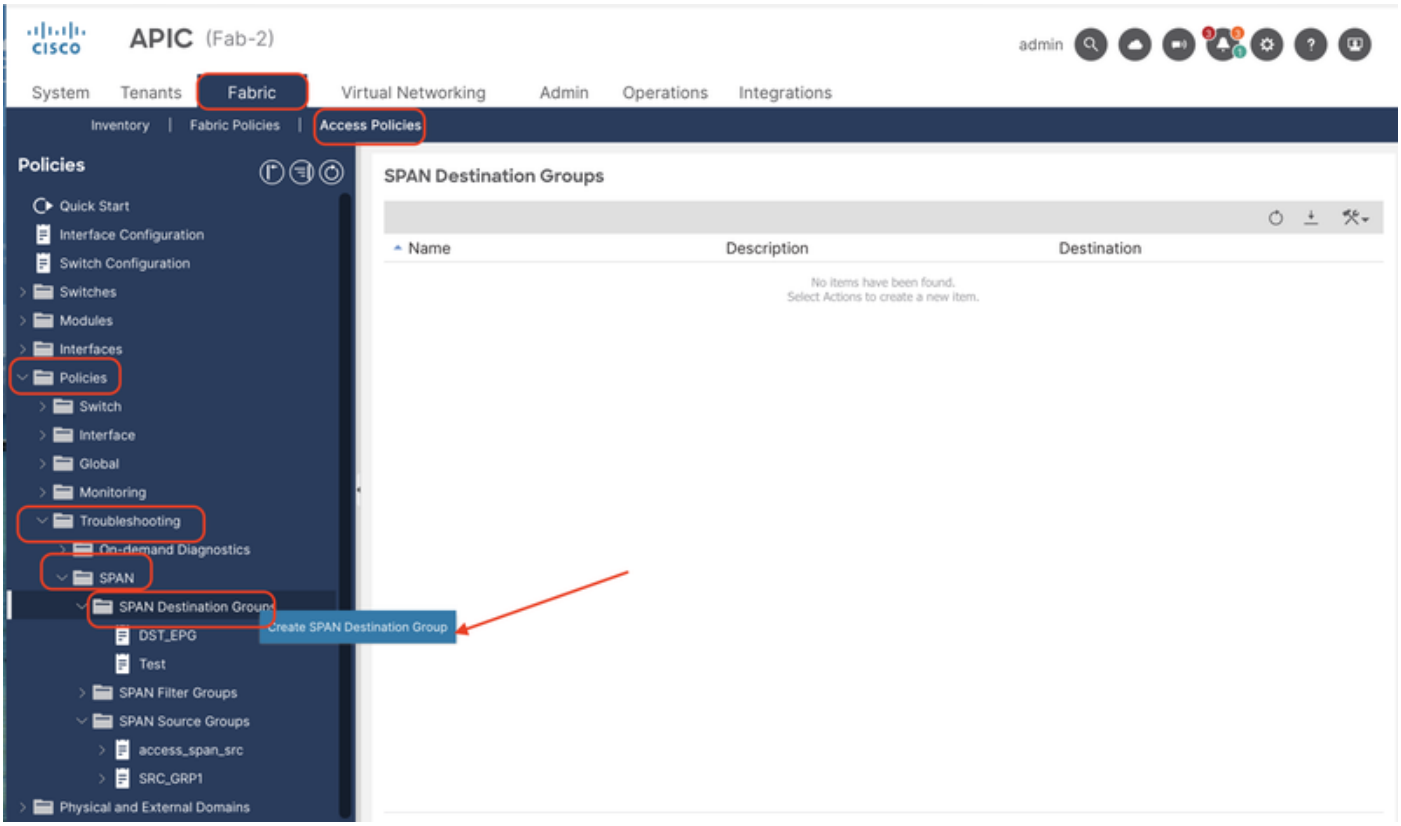

図10：ローカルアクセスSPAN宛先グループを作成するパス

次の情報を入力します。

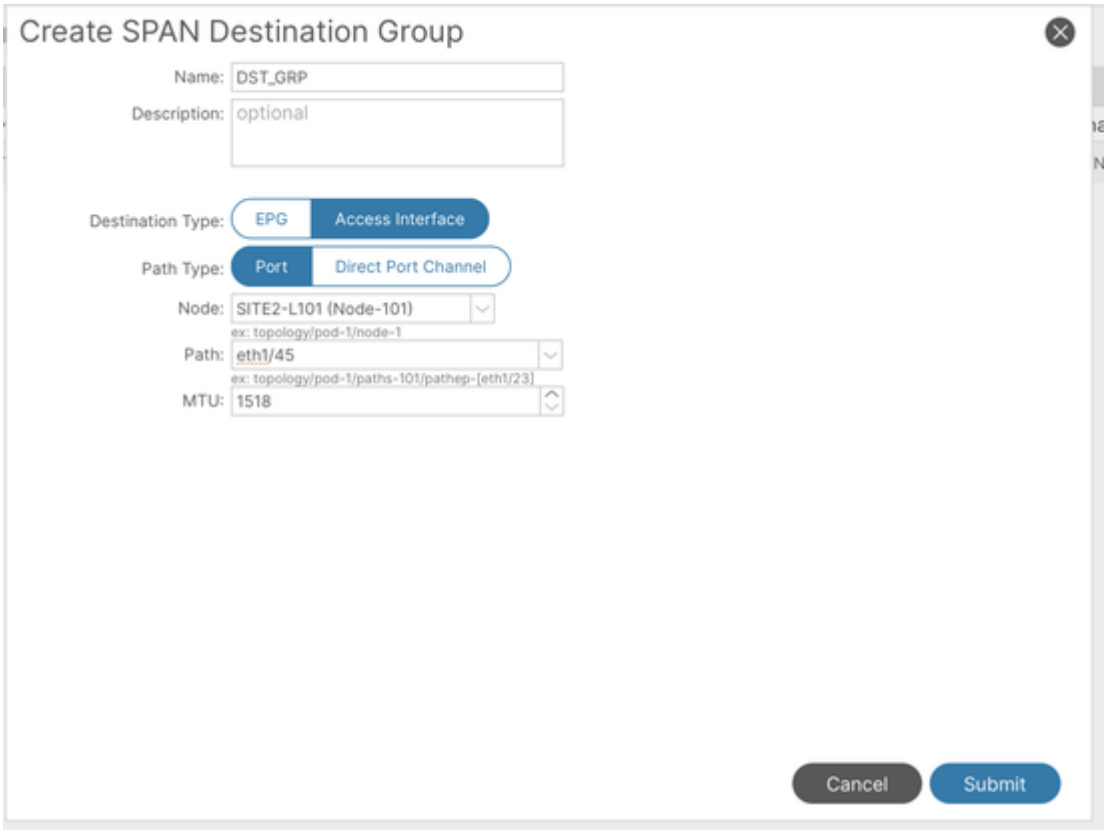

図11：ローカルアクセスSPAN宛先グループの設定

ここで、

宛先タイプ：アクセスインターフェイス（ローカルSPANであることが必須）

パスタイプ：ポート

ノード：ノード101（トポロジによる）

パス：eth1/45（トポロジによる）

注：宛先ポートにはテナントポリシー（EPG、L3out、infra展開など）を適用する必要はありません。適用しない場合、このエラーが発生します。

障害： F1559

説明：フォールトデリゲート：SPANの安全でない宛先ポートが原因で、宛先グループDST_GRPの宛先DST_GRPを使用してSPANを設定できませんでした。ポートにはすでにアプリケーションEPG、L3Out、またはインフラストラクチャVLANが導入されている

宛先ポートがEPGの一部である場合、代替はアクセスERSPANへの切り替えです。

- SPAN Source Group(SRC_GRP1)を作成し、「SPAN Source Groups」を右クリックして「Create SPAN Source groups」を選択します。

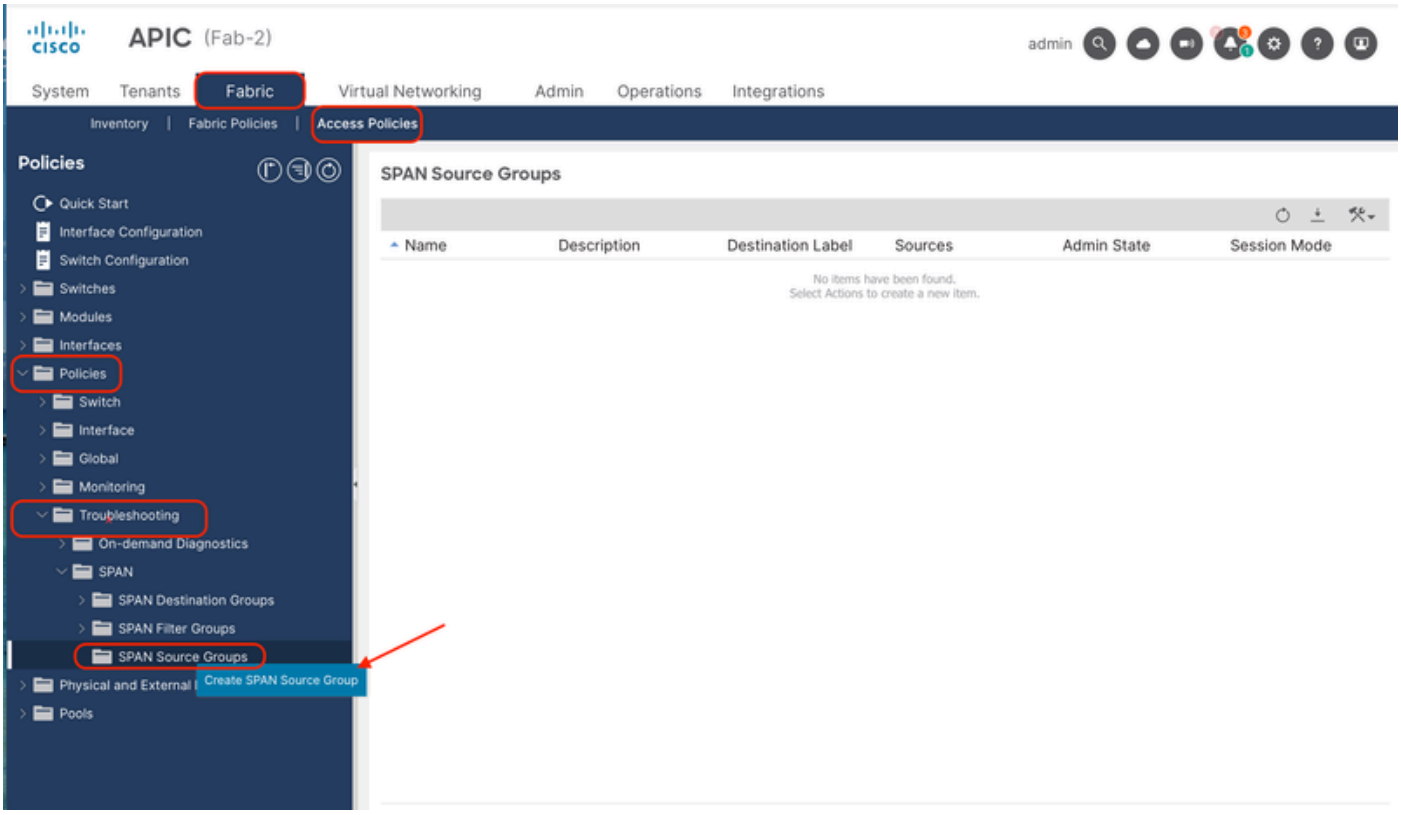

図12：ローカルアクセスSPANソースグループを作成するパス

次の情報を入力します。

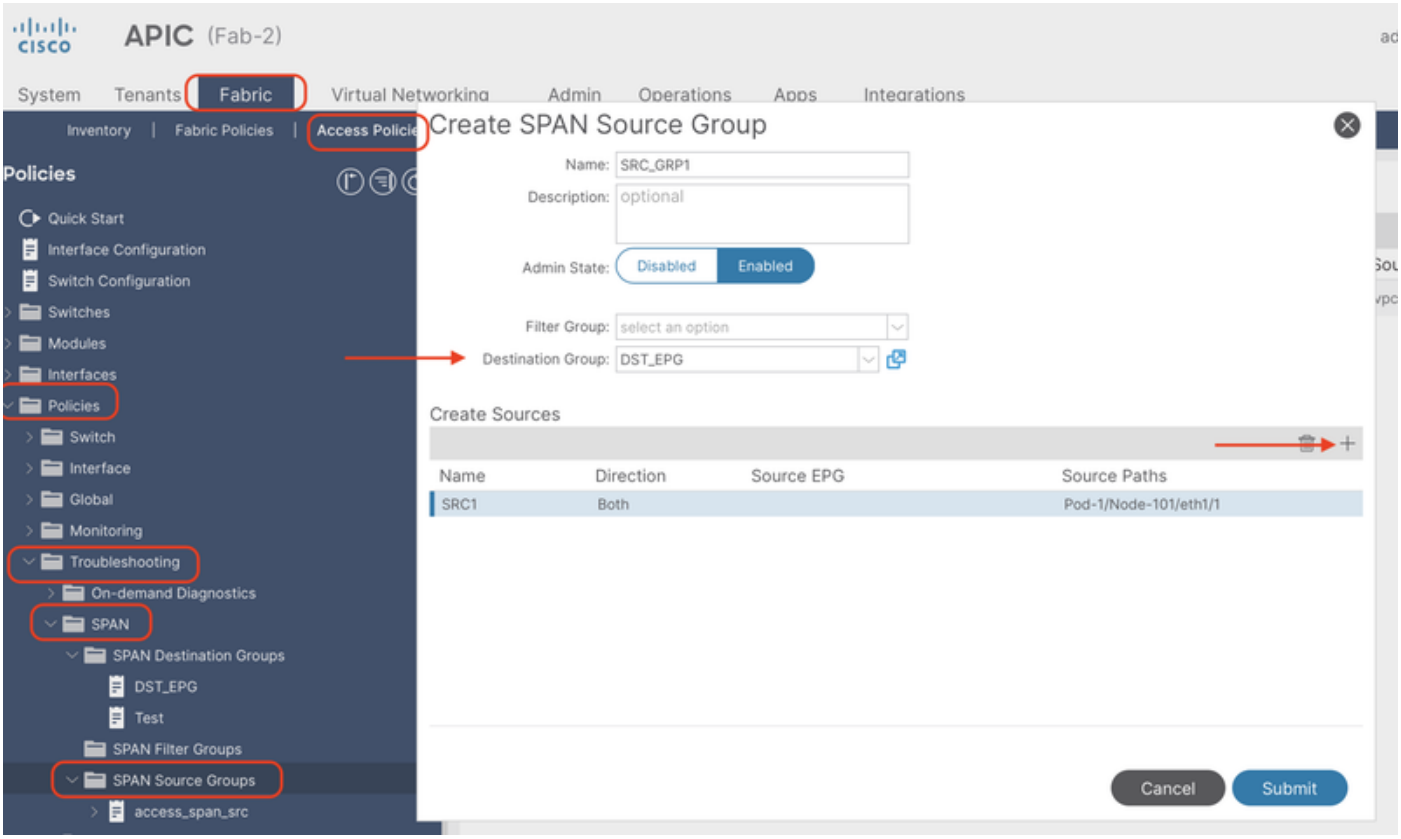

図13：ローカルアクセスSPANソースグループの作成

ここで、

Admin State（管理状態）:Enabled（有効）

通知先グループ：以前作成した通知先グループ(DST_EPG)を選択します。

- この同じボックスで、プラスボタン(+)をクリックして、少なくとも1つのSPANソースを追加します。
- SPAN Source(SRC1)を作成するには、次のパラメータを設定します。

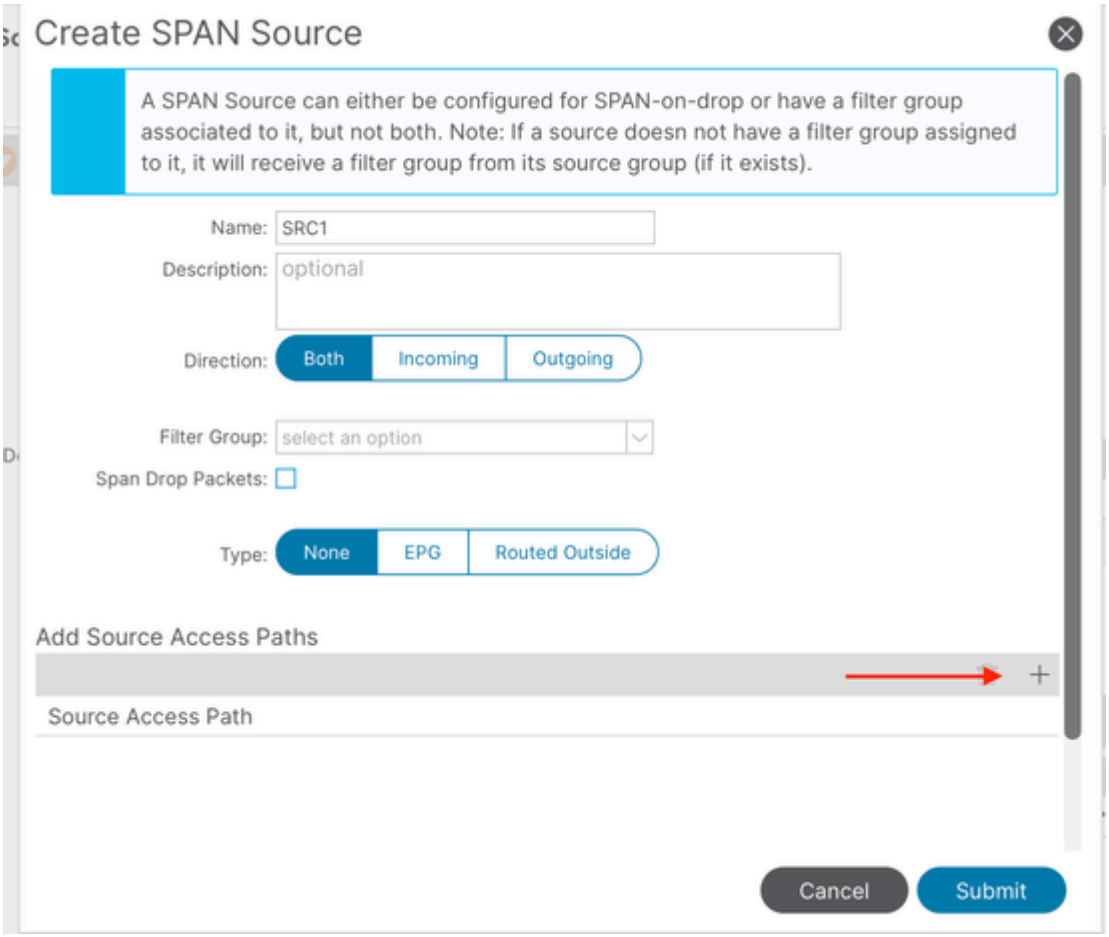

図14：ローカルアクセスSPANソースの作成手順

ここで、

方向：着信、発信、または両方向を選択します。

タイプ：なし（通常の前面ポート）、EPG（EPGでスタティックバインディングとして導入されたインターフェイス、EPGトラフィックのみがミラーリングされる）、またはRouted Outside（L3outで使用されるインターフェイス）のいずれかを選択できます。

この例では、通常の前面ポートが使用されます。後で追加するソースアクセスパスが同じノードに展開される限り、設定はサポートされます。

- プラスボタン(+)をクリックして、ソースアクセスパスを追加します。次の情報を入力します。

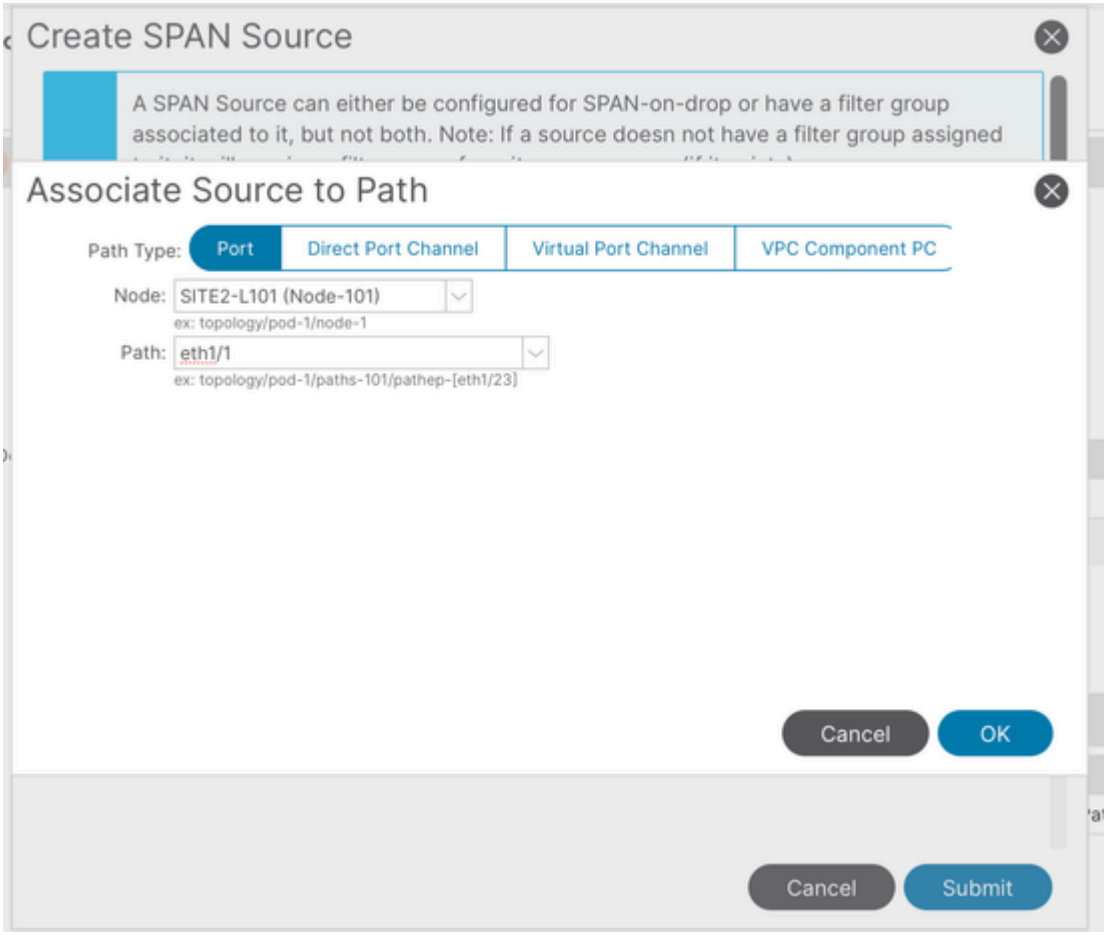

図15：ローカルアクセスSPANソースパスの作成

ここで、

パスタイプ：ポート（個別）、ダイレクトポートチャネル、仮想ポートチャネル（このオプションを選択すると、パスにはVPCがすでに形成されていることが示されます）、およびVPCコンポーネントPC（VPCの一方のレッグだけ、特定のノードを選択します）のいずれかを選択します。

注：仮想ポートチャネルは、ローカルアクセスSPANではサポートされていません

ノード：ソースノードを選択します（トポロジの例ではノード101）。

パス：送信元インターフェイス（トポロジ例によるeth1/1）

制限：

注：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世代リーフでは使用できません(Cisco Bug ID CSCvc11053)。 代わりに、2.1(2e)、2.2(2e)以降で、Cisco Bug ID CSCvc44643により「VPCコンポーネントPC」でのSPANのサポートが追加されました。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leaves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ニングされます(Cisco Bug ID CSCvc11053によるも同様です)。
- 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)からは、PCをローカルSPANの宛先ポートとして使用できます。

テナントSPAN(ERSPAN)

トポロジの例

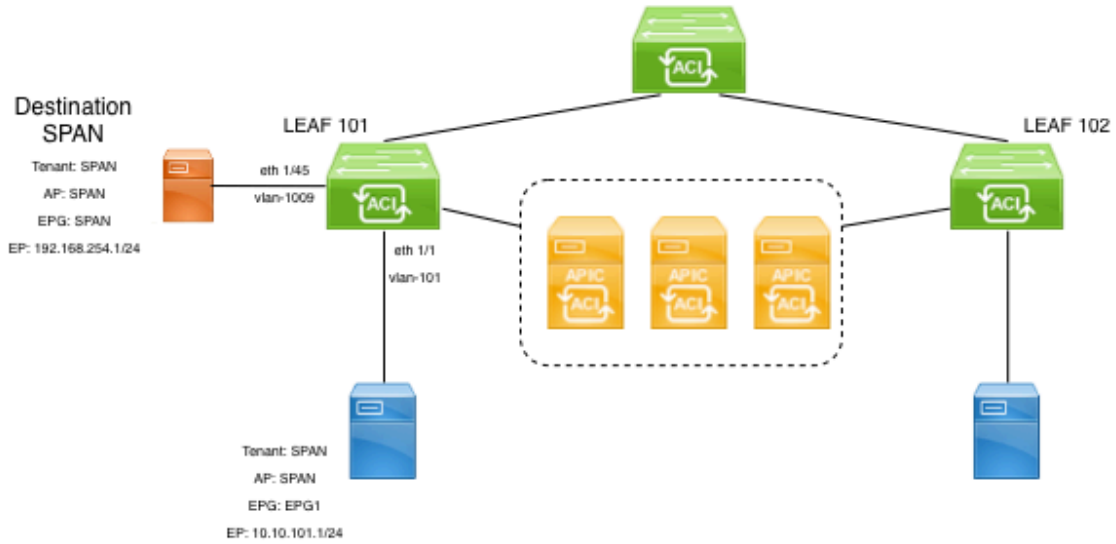

図16：テナントERSPANのサンプルトポロジ

設定例

Tenant > <TENANT> > Policies > Troubleshooting > SPANの順に移動します。

- 「SPAN Destination Groups」を右クリックし、SPAN Destination Group(DST_EPG)を作成するオプションを選択します。

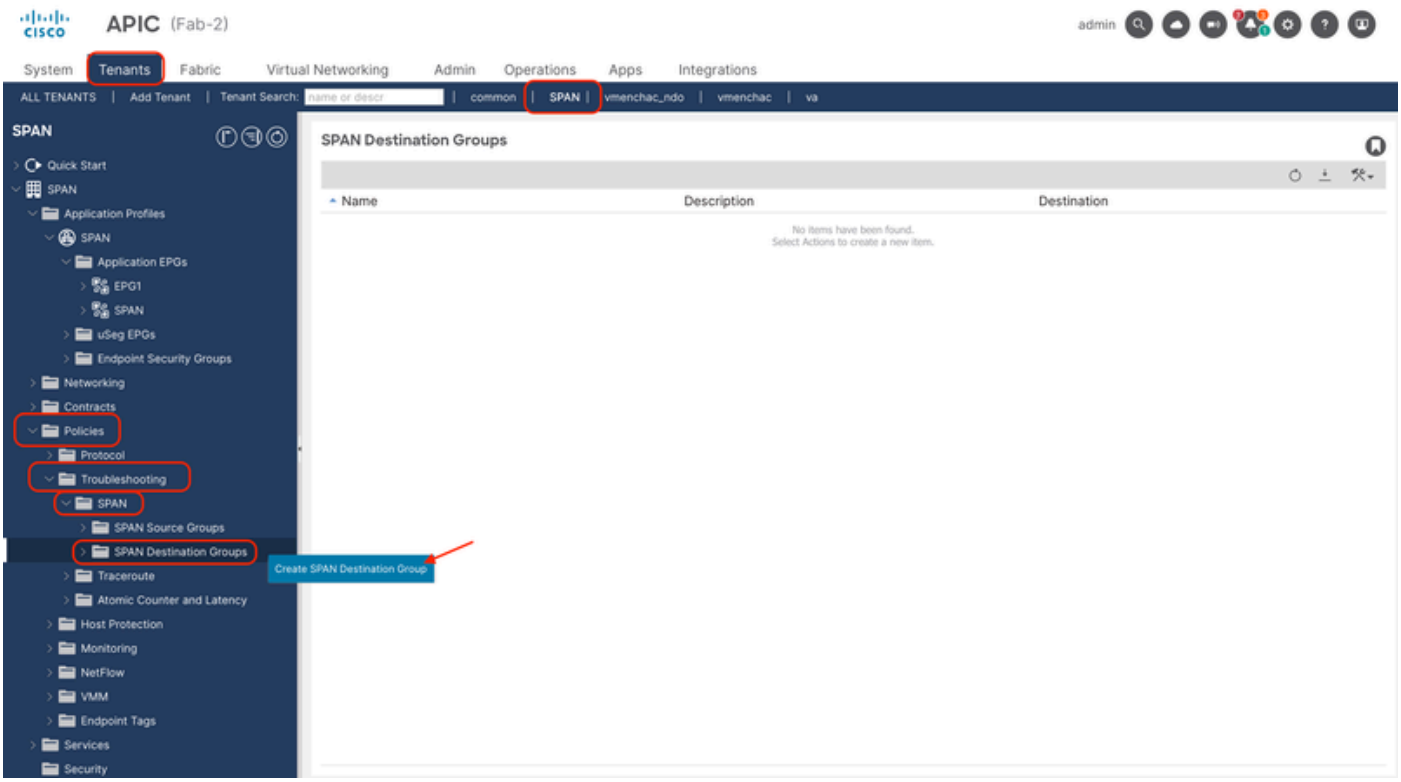

図17：テナントERSPAN宛先グループを作成するパス

次の情報を入力します。

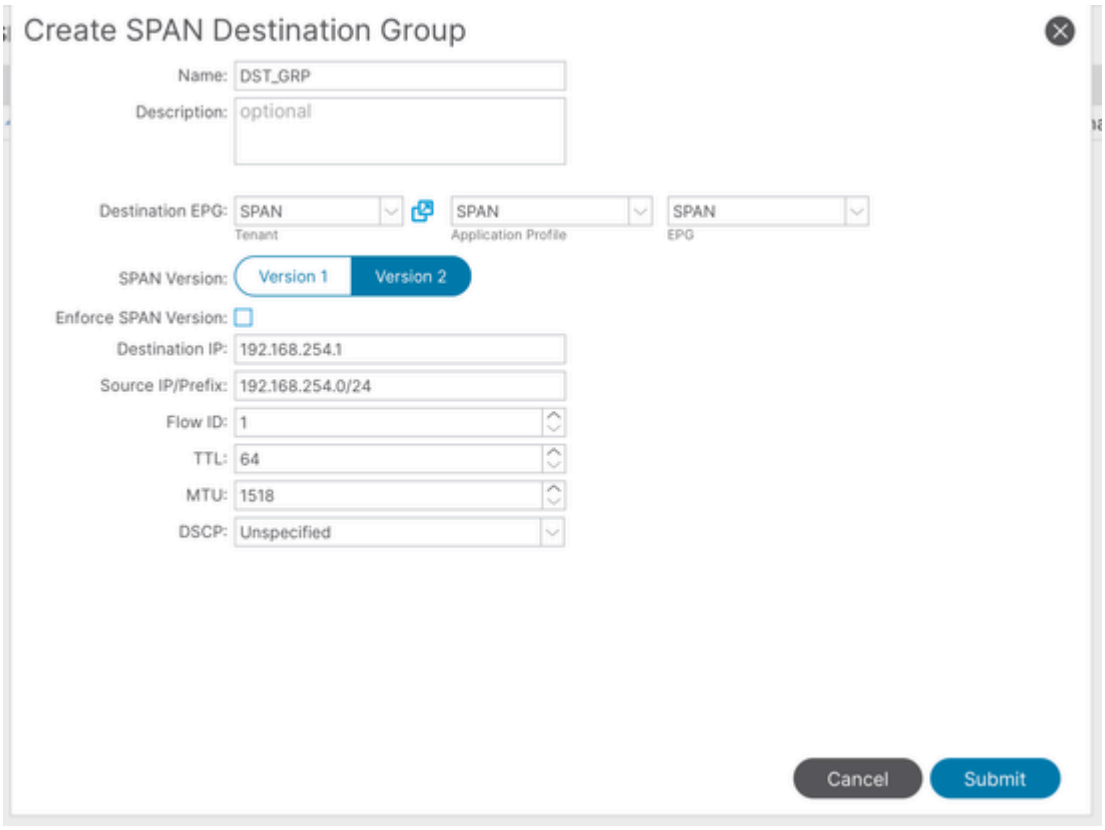

図18：テナントERSPAN宛先グループの作成

ここで、

宛先EPG:テナントをセットアップします（デフォルトでは、ERSPANが設定されている場所と同じテナントを使用します）。また、宛先エンドポイントを学習するAPおよびEPGもセットアップします。

宛先IP：宛先エンドポイントのIP

送信元IP:任意のIPを指定できます。プレフィックスが使用される場合、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のprefix: 192.168.254.0/24 => src IP 192.168.254.101のようになります。

フローID:デフォルトでは1に設定され、ERSPANヘッダーでフローによってパケットを識別するのに役立ちます。このフローIDがカスタマイズされている場合は、Access ERSPANに示されているヒントを使用してキャプチャをフィルタリングします。

- SPAN Source Group(SRC_GRP1)を作成し、「SPAN Source Groups」を右クリックして「Create SPAN Source groups」を選択します。

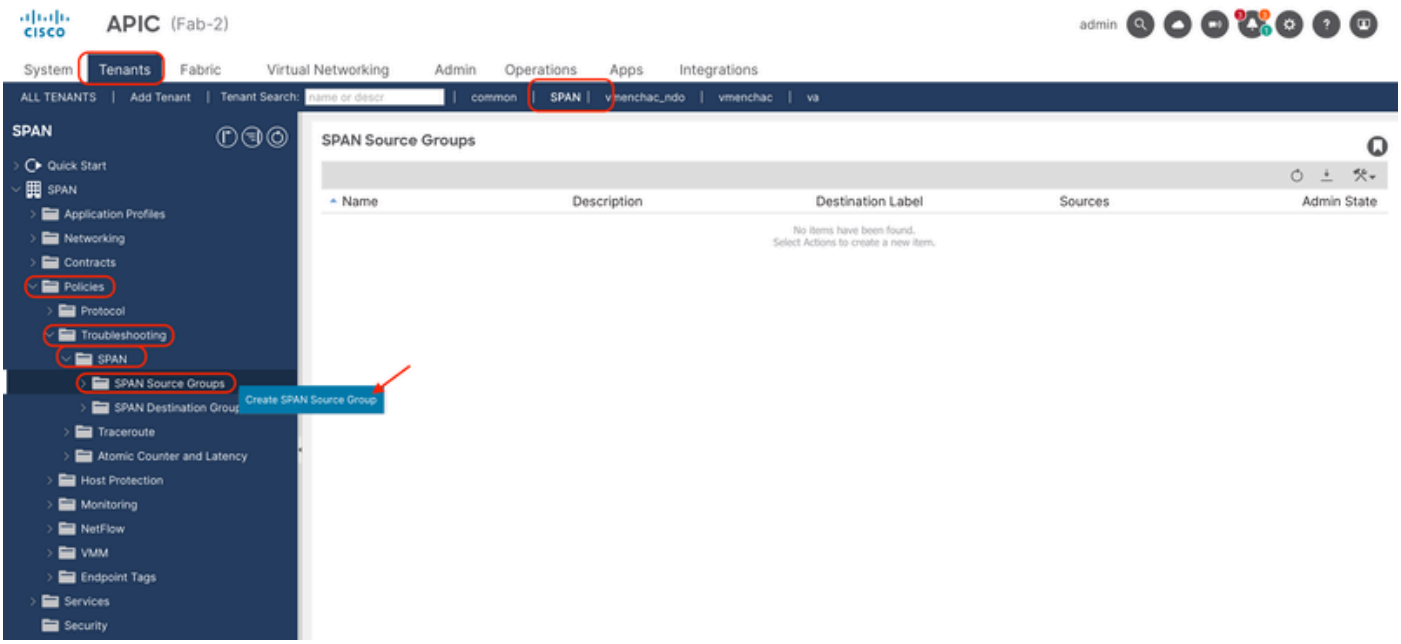

図19：テナントERSPANソースグループを作成するパス

次の情報を入力します。

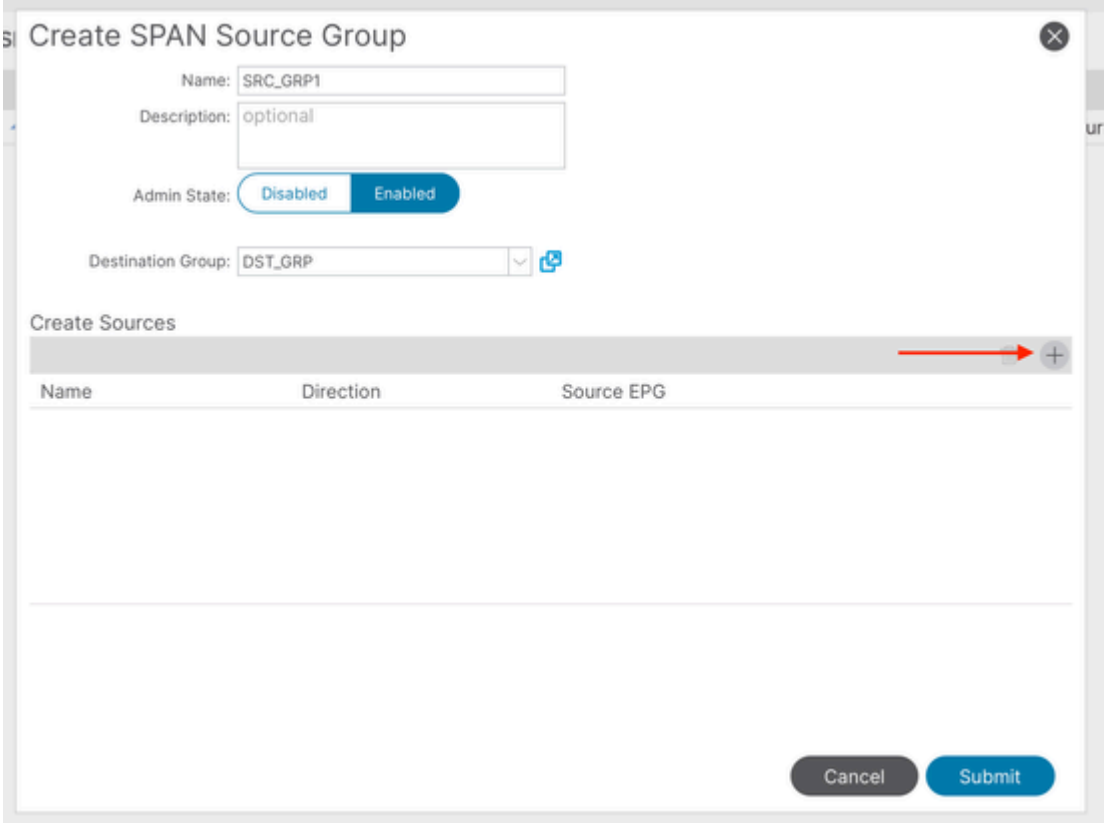

図20：テナントERSPANソースグループの作成

ここで、

Admin State（管理状態）:Enabled（有効）

通知先グループ：以前作成した通知先グループ(DST_EPG)を選択します。

- この同じボックスで、プラスボタン(+)をクリックして、少なくとも1つのSPANソースを追加します。
- SPAN Source(SRC1)を作成するには、次のパラメータを設定します。

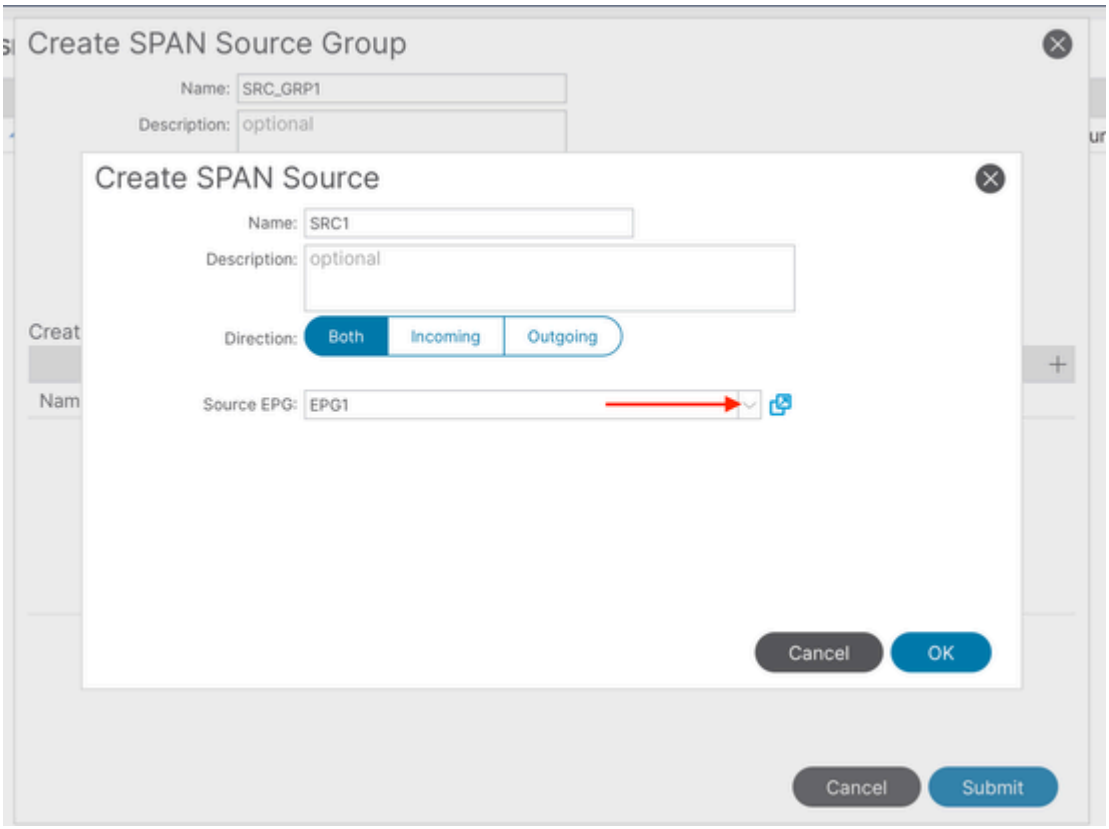

図21：テナントERSPANソースEPGの作成

ここで、

方向：着信、発信、または両方向を選択します。

ソースEPG:同じテナント内のすべてのEPGから選択できます。（トポロジの例によるEPG1）

ファブリックSPAN(ERSPAN)

トポロジの例

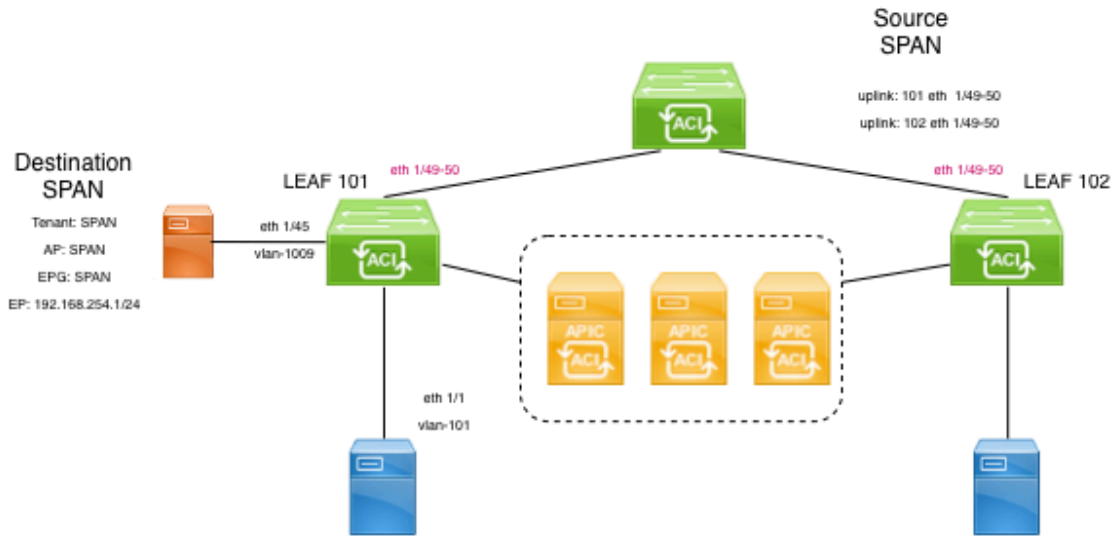

図22：ファブリックERSPANのサンプルトポロジ

設定例

Fabric > Fabric Policies > Policies > Troubleshooting > SPANの順に選択します。

- 「SPAN Destination Groups」を右クリックし、SPAN Destination Group(DST_EPG)を作成するオプションを選択します。

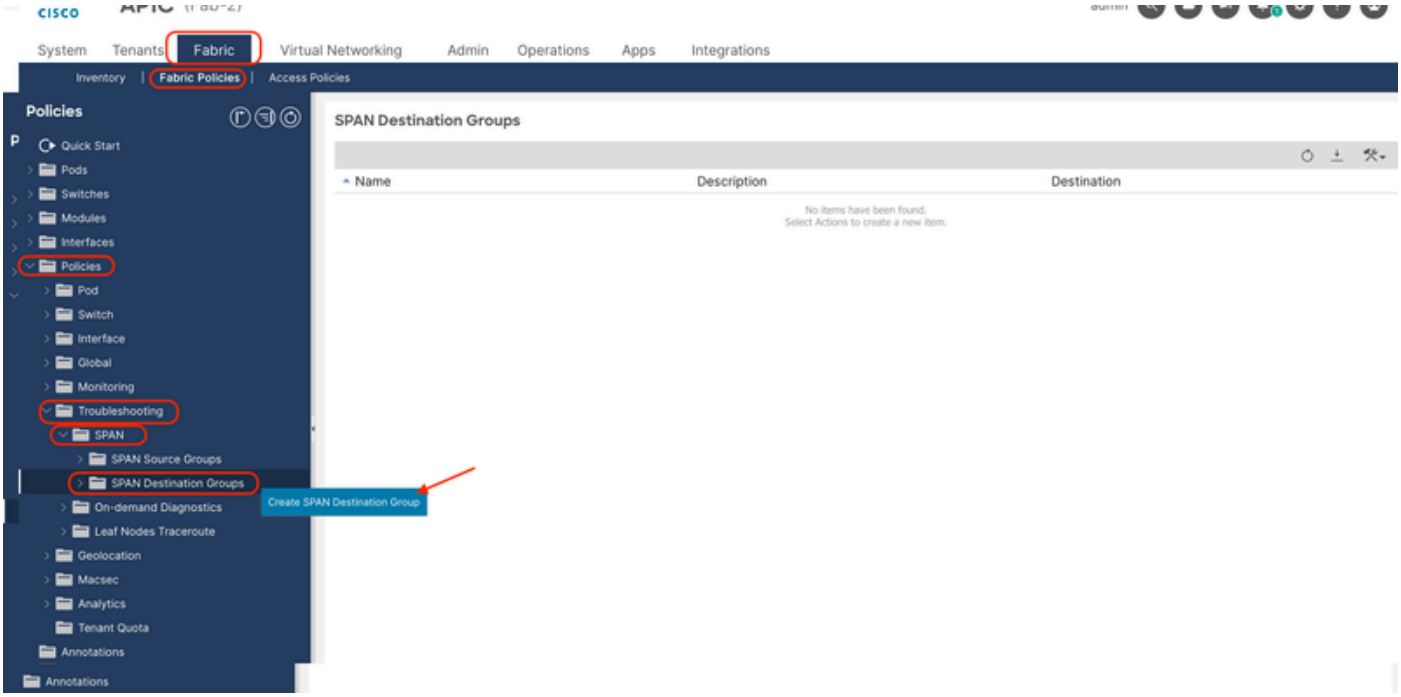

図23：ファブリックERSPAN宛先グループを作成するパス

次の情報を入力します。

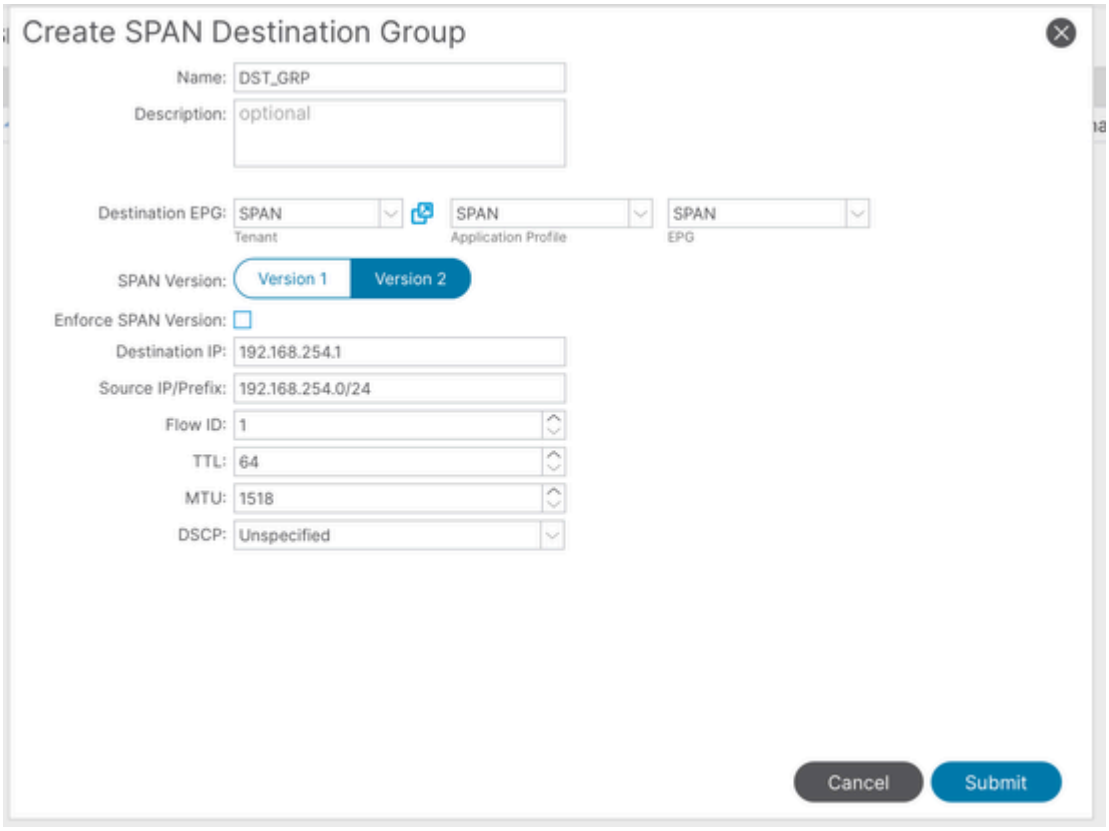

図24：ファブリックERSPAN宛先グループの作成

ここで、

宛先EPG:宛先エンドポイントを学習するテナント、AP、およびEPGをセットアップします。

宛先IP：宛先エンドポイントのIP

送信元IP:任意のIPを指定できます。プレフィックスが使用される場合、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のprefix: 192.168.254.0/24 => src IP 192.168.254.101のようになります。

フローID:デフォルトでは1に設定され、ERSPANヘッダーでフローによってパケットを識別するのに役立ちます。このフローIDがカスタマイズされている場合は、Access ERSPANに示されているヒントを使用してキャプチャをフィルタリングします。

- SPAN Source Group(SRC_GRP1)を作成し、「SPAN Source Groups」を右クリックして「Create SPAN Source groups」を選択します。

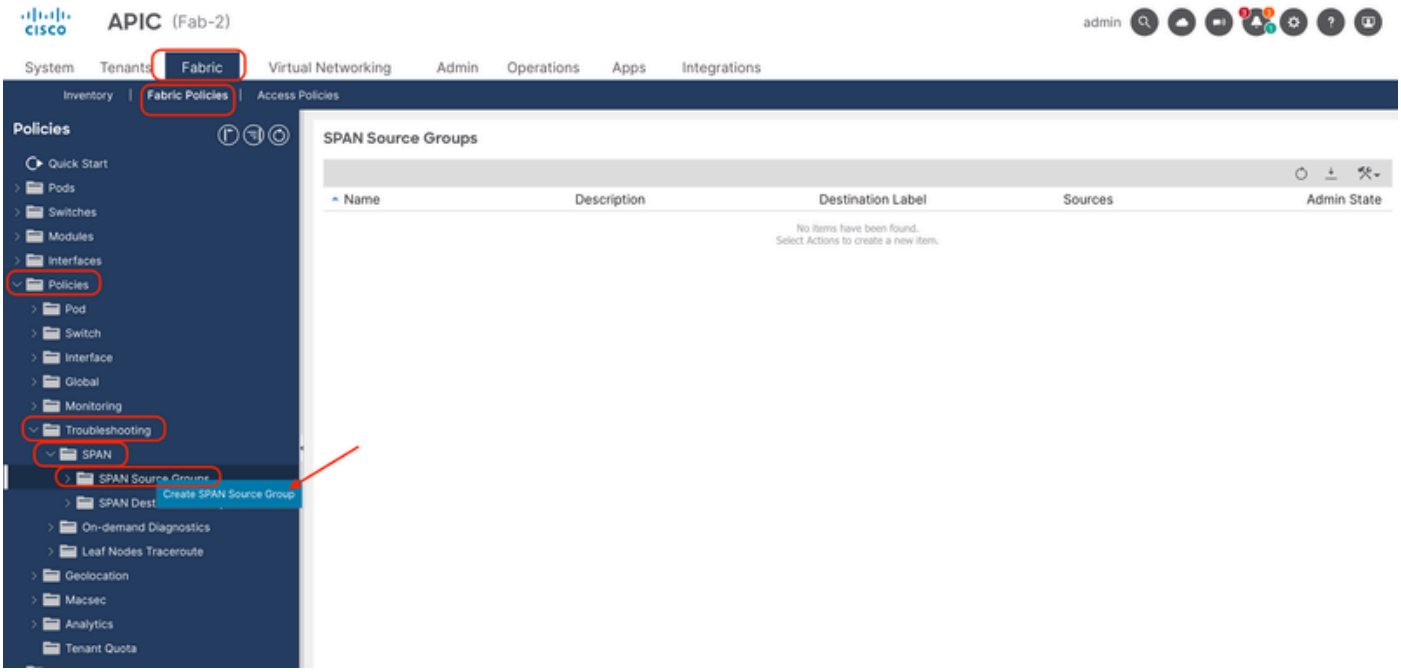

図25：ファブリックERSPANソースグループを作成するパス

次の情報を入力します。

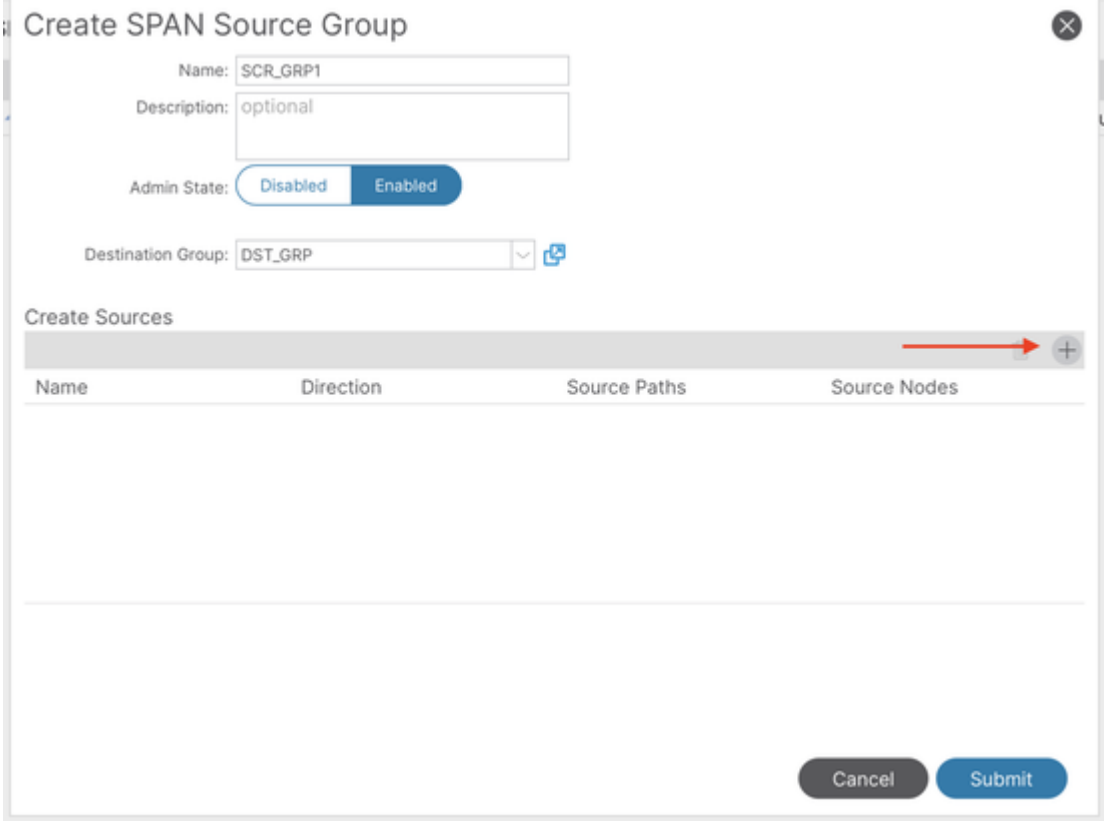

図26：ファブリックERSPANソースグループの作成

ここで、

Admin State（管理状態）:Enabled（有効）

通知先グループ：以前作成した通知先グループ(DST_EPG)を選択します。

- この同じボックスで、少なくとも[ソース]に追加するには、プラス(+)ボタンをクリックします。
- ソース(SRC1)を作成するには、次のパラメータを設定します。

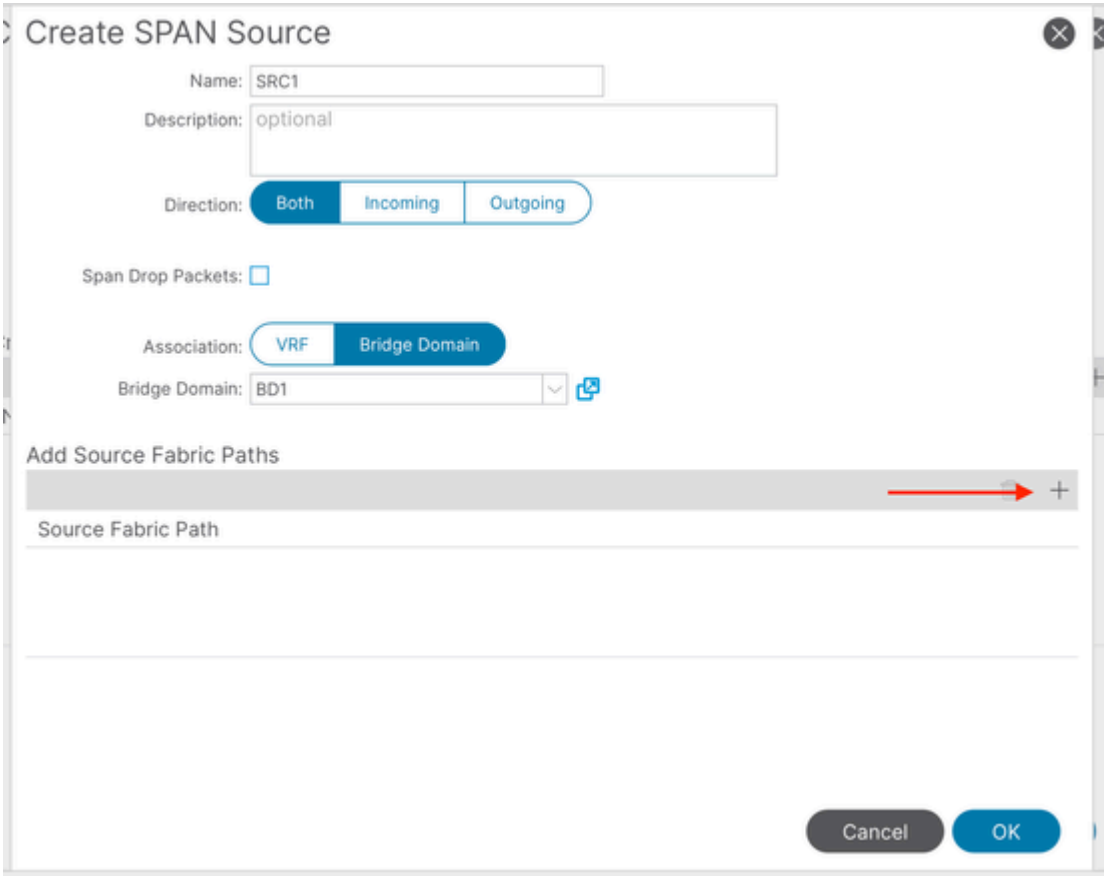

図27：テナントERSPANファブリックパスの作成

ここで、

方向：着信、発信、または両方向を選択します。

Association:VRFまたはブリッジドメインを選択します（この例では、キャプチャする特定のBDが選択されています）。

- +ボタン(+)をクリックして、ソースファブリックパスを追加します。次の情報を入力します。

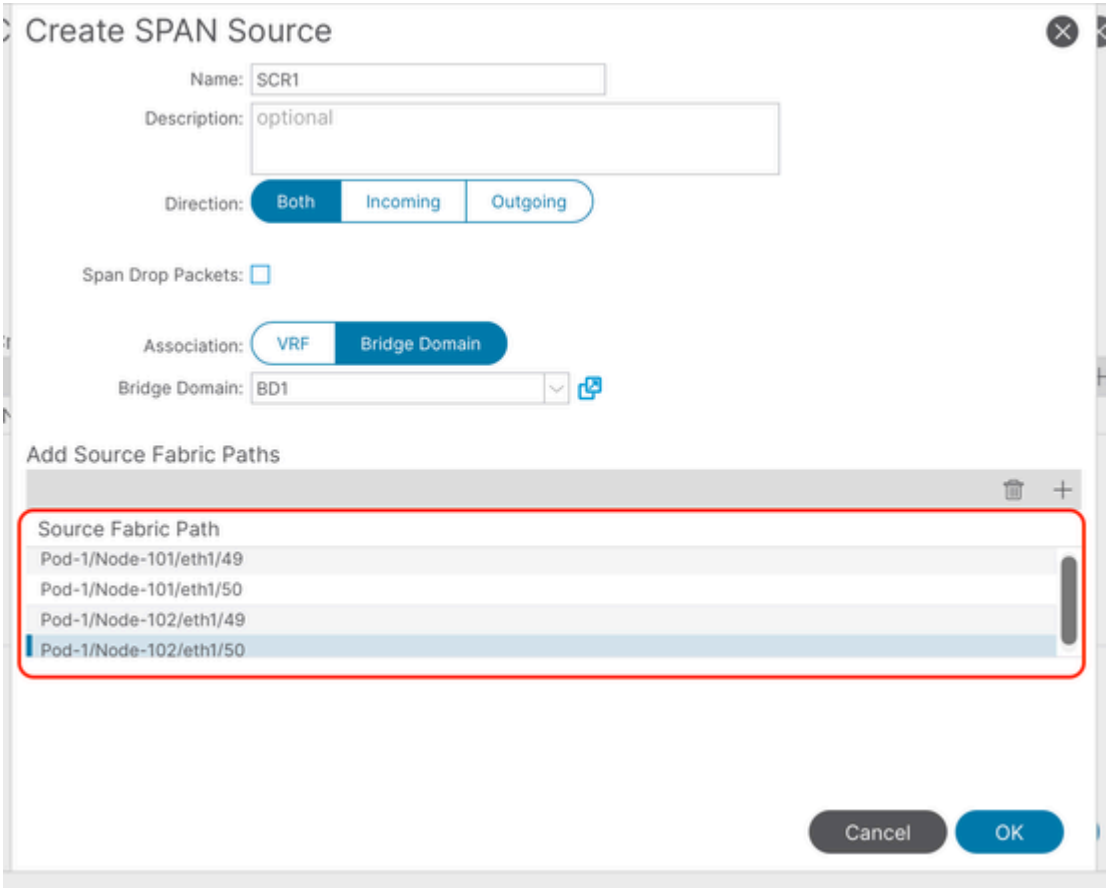

図28：ファブリックERSPANの送信元パスの作成

ここで、

ノード：ソースノード

Interface:ドロップダウンメニューには、選択したノードからのアップリンクのみが表示されます（この例では、すでに追加されたトポロジからの4つのアップリンクが表示されています）。

CPUへのスパン

ACI 6.2.1よりも前のバージョンでは、ACIリーフスイッチはローカルSPAN(Switched Port Analyzer)セッションをスイッチのCPUポート(`sup-eth0`)に直接送信する操作をサポートしていなかったため、オンボックスのキャプチャと分析が非常に困難になっていました。

トポロジの例

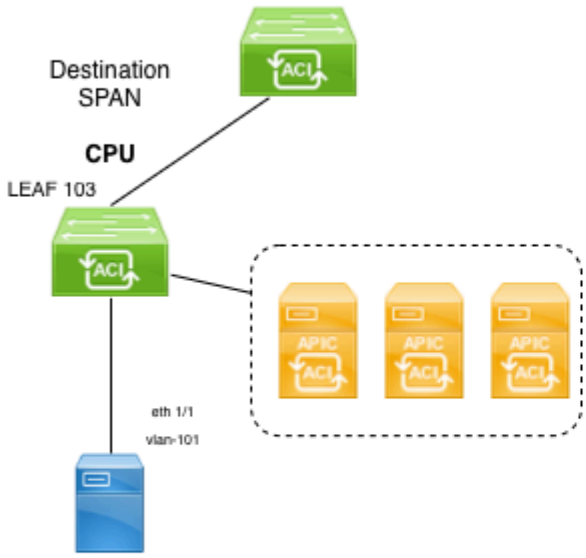

図29:SPANからCPUへのトポロジ例

設定例

Fabric > Access Policies > Policies > Troubleshooting > SPANの順に選択します。

- 「SPAN Destination Groups」を右クリックし、SPAN Destination Groupを作成するオプションを選択します。

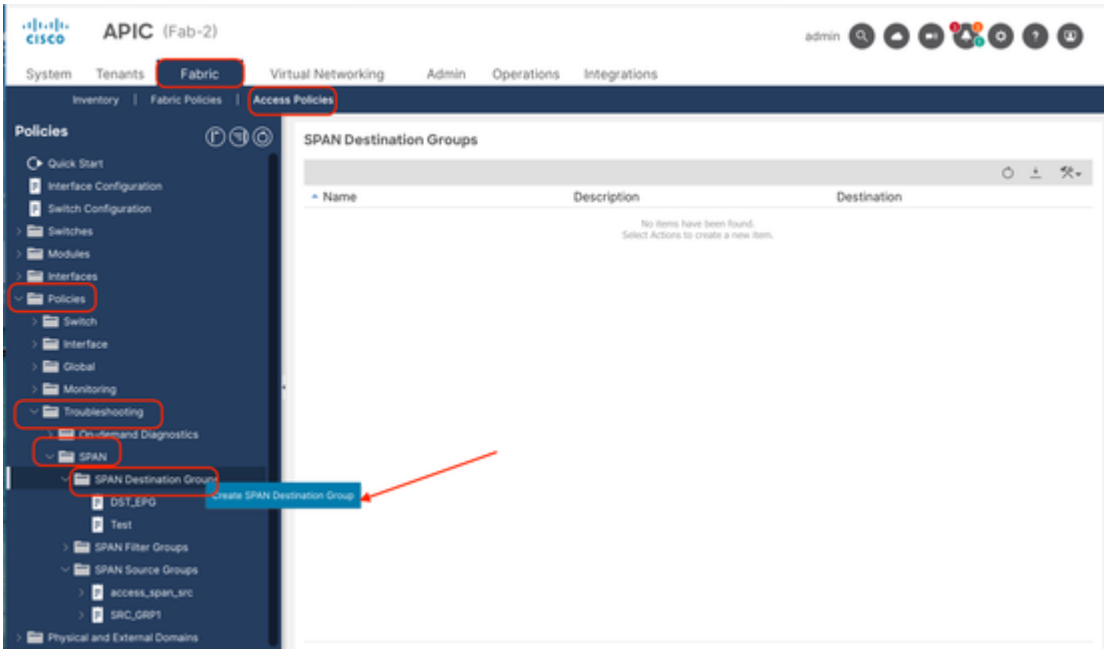

図30:SPANからCPUへの宛先グループを作成するパス

次の情報を入力します。

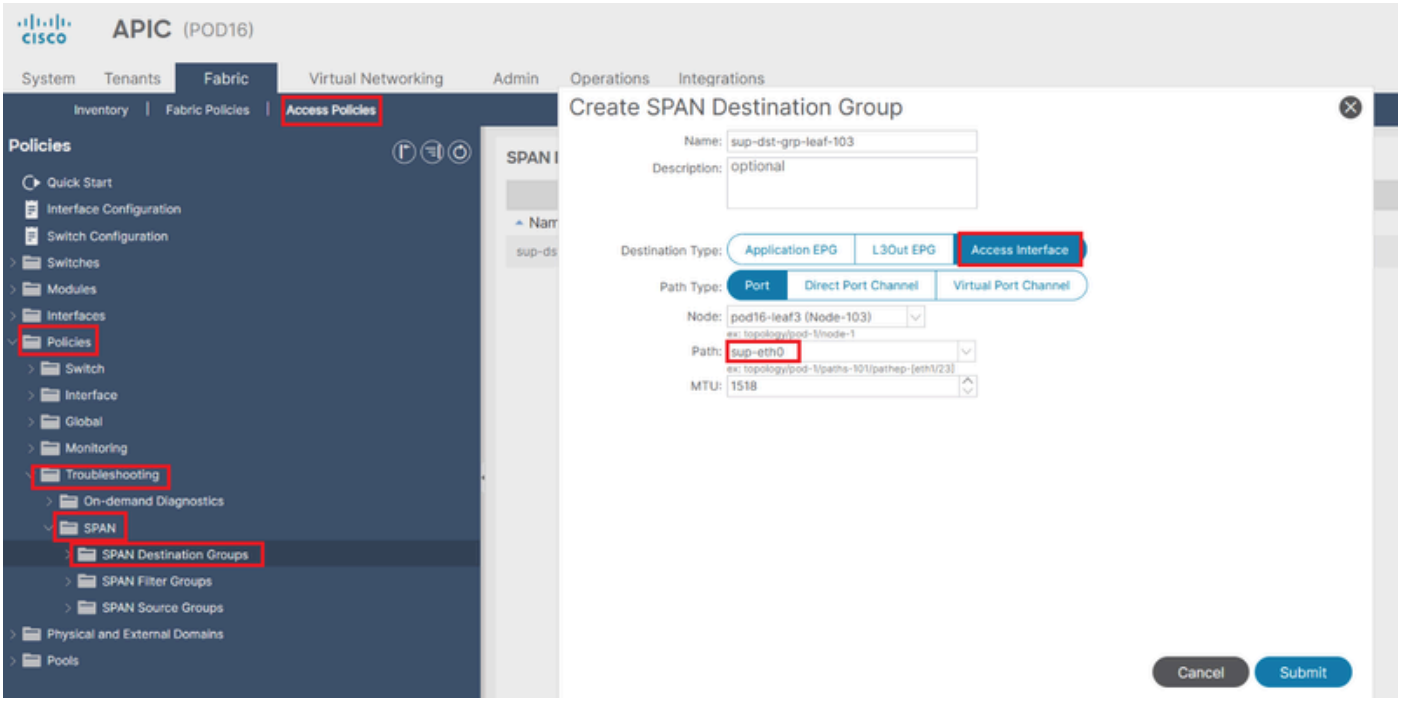

図31:SPANからCPUへの宛先グループの作成

ここで、

宛先タイプ：アクセスインターフェイス

部品タイプ：ポート

パス：sup-eth0を選択

- セクション「ローカルSPANへのアクセス」に示されているように、設定を続行します。

設定手順は、このビデオでも示されています。

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

制限：

SPANからCPUがサポートされているのは、次のプラットフォームだけです。

- FX2（天国）
- FX3（サンダウン）
- GX（ウォルフリッジ）
- GX2（クワッドピーク）
- HX（アララット）

フィルタ/ACL

アクセスSPANには、アクセスSPANソースでACLフィルタを使用する機能があります。

この機能により、特定のフローまたはSPAN送信元に入出力されるトラフィックのフローにSPANを適用できます。
SPANフロー固有のトラフィックが必要な場合は、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で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。

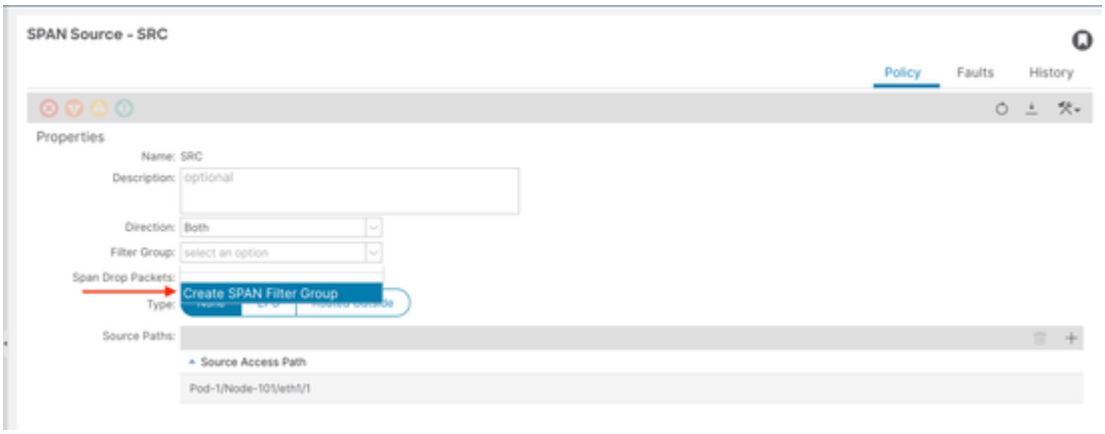

図32：アクセスソースにフィルタを追加するオプション

-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で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。

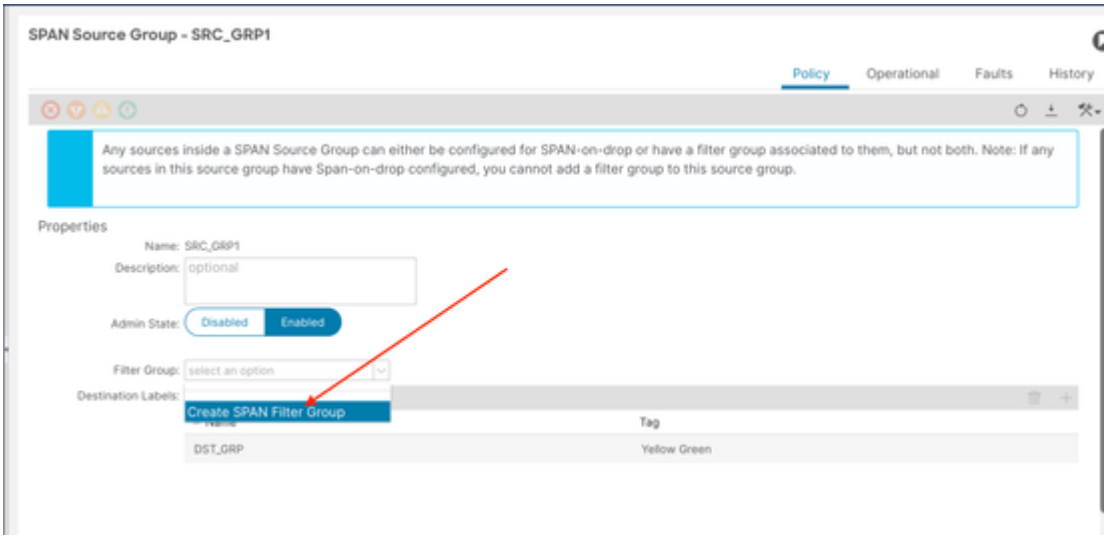

図33：アクセスソースグループにフィルタを追加するオプション

特定のSpan Source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 Sourceの下にあるすべてのインターフェイスのフィルタグループに代わって使用されます

– 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。
– 送信元で適用されるフィルタグループは、その送信元にのみ適用されます。
– フィルタグループが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は削除され、親ソースグループに適用されたフィルタグループは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に継承されているすべてのソースから削除されます。

フィルタを作成するには、次のオプションを使用できます。

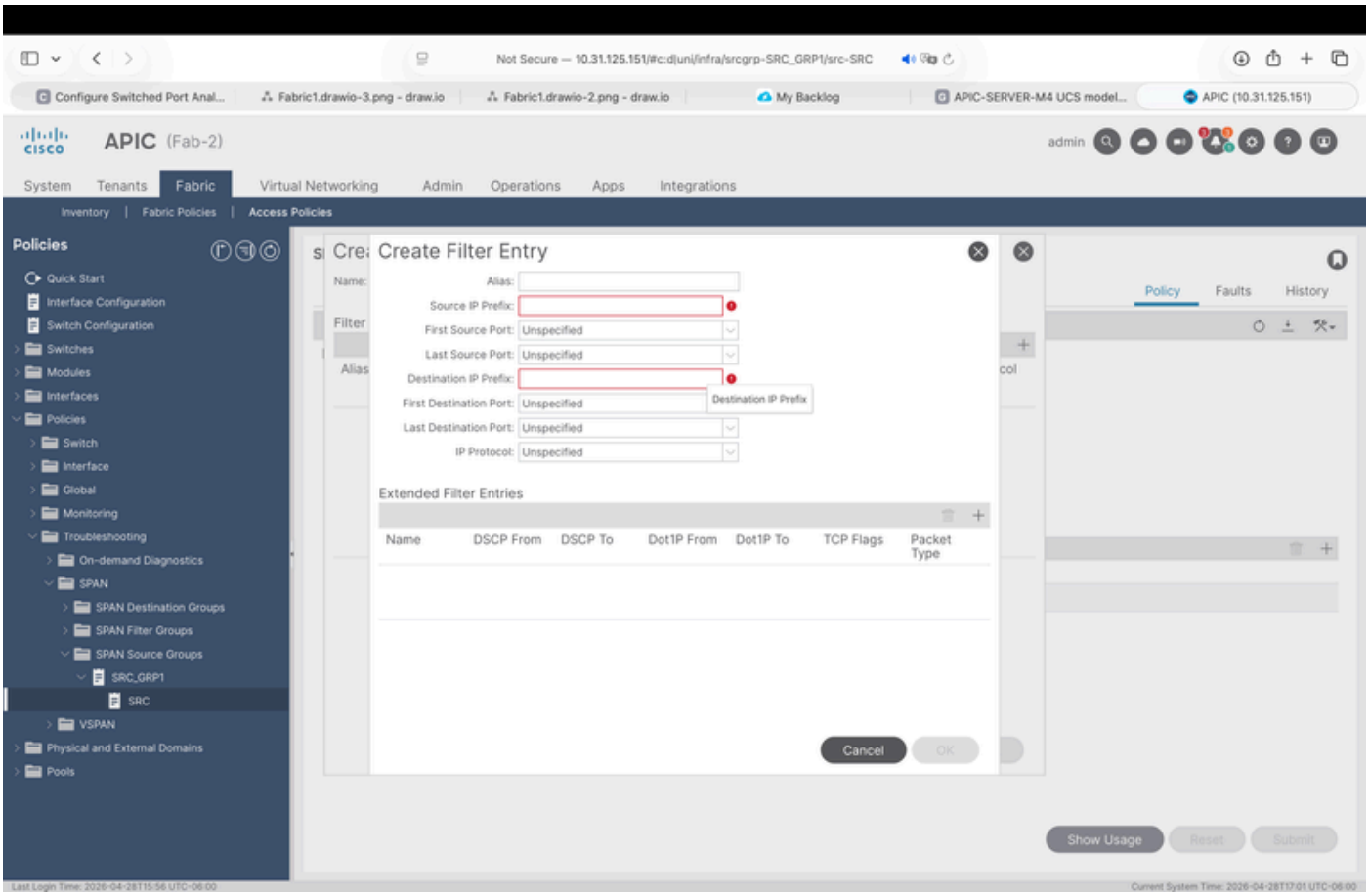

図34：フィルタエントリオプション

– 送信元プレフィクスと宛先プレフィクス

– 送信元/宛先ポート範囲

- IPプロトコル。

- DCSP、Dot1P、TCPフラグなどの拡張フィルタ

検証

- GUIで、対象のソースグループに移動し、そのグループをクリックして、Operationalタブに移動します。

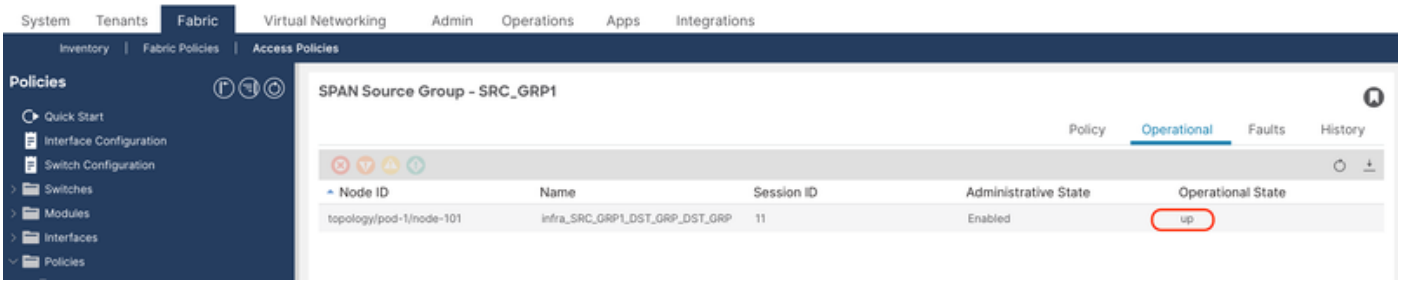

図35:GUIでのセッションの検証

- CLI APICで次の手順を実行します。

ファブリック内で構成されているすべてのSPAN/セッションを表示

```
 show monitor summary
```

タイプ別にセッションをフィルタするには、次の手順に従います。

```
show monitor access session all

show monitor tenant session all

show monitor fabric session all
```

- CLIソーススイッチ：

```
show monitor session all
```

例：

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

```
vrf-name : SPAN:SPAN
acl-name :
ip-ttl : 64
ip-dscp : ip-dscp not specified
destination-ip : 192.168.254.1/32
origin-ip : 192.168.254.101/24.  >>>> node ID 101
mode : access
Filter Group : None
source intf :
rx : [Eth1/1]
tx : [Eth1/1]
both : [Eth1/1]
source VLANs :
rx :
tx :
both :
filter VLANs : filter not specified
filter L3Outs : filter not specified
```

この出力は、セッションが有効であるかどうか、および送信元、宛先ヘッダー、送信元インターフェイス (rxおよびtxにリストされている場合、directionはbothに設定されています) を確認するのに役立ちます
これが正しく設定されていることを本当に確認するには、説明からspanセッションIDを取得し、次のコマンドを実行します。

例：

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

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

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

ERSPANデータの読み方

ERSPAN Version（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）

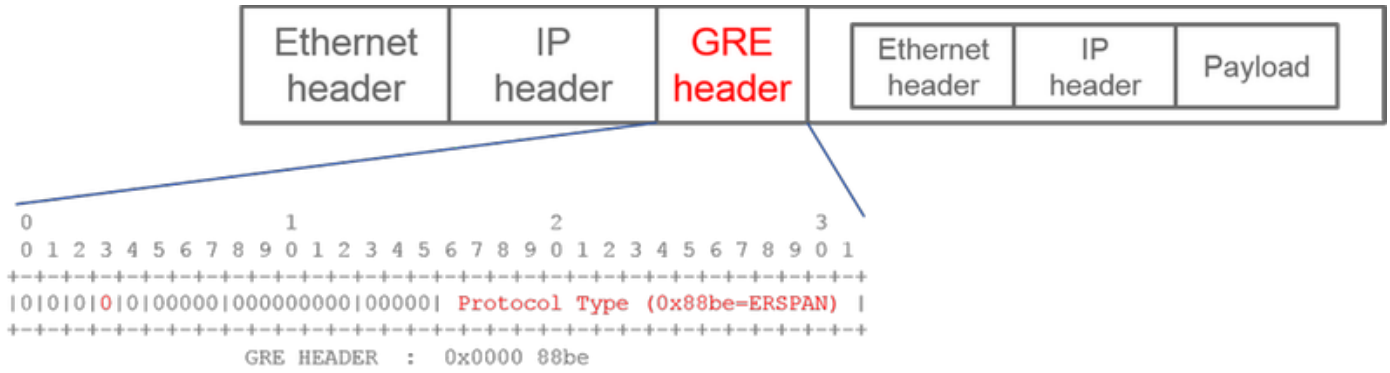

図36:ERSPANバージョンIのGREヘッダー

例を示すために、wiresharkは次のプロトコルタイプを示しています。

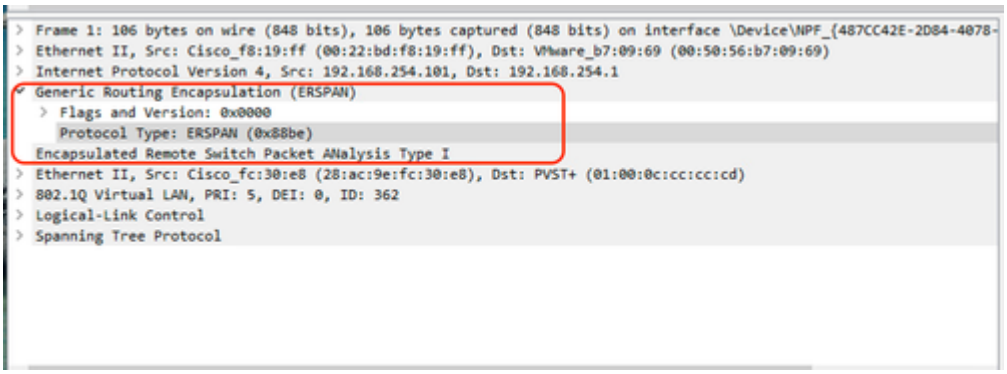

図37:Wiresharkでのバージョン検証

タイプIでは、GREヘッダーのシーケンスフィールドは使用されません。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 Type IIまたはIII

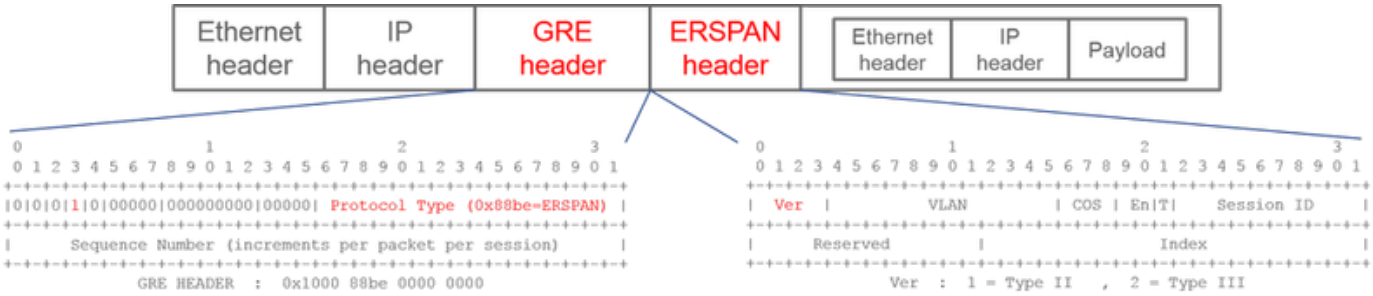

図38:ERSPAN/バージョンIIのGREヘッダー

Wiresharkの例：

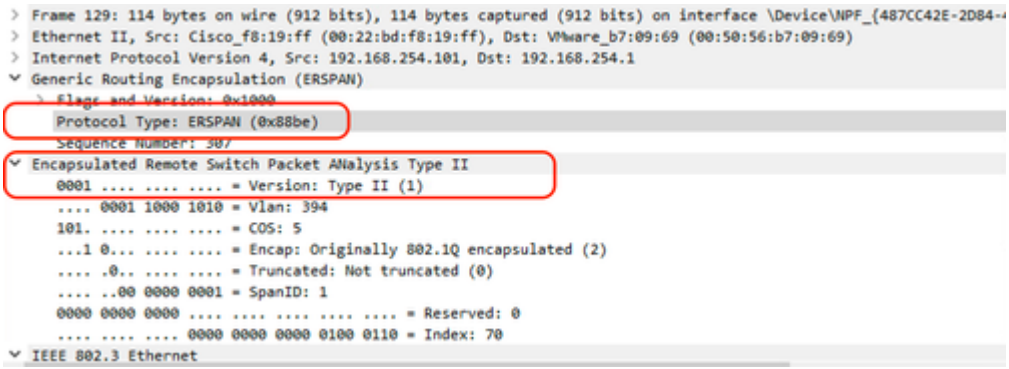

図39:Wiresharkでのバージョン検証

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は、ERSPANタイプを識別します。ACIでは、タイプIIIは2026年4月30日の時点ではサポートされていません。

ERSPANタイプとACI SPANタイプ

第1世代のリーフ/スパインノードでは、各ACI SPAN（ファブリック、アクセス、テナント）が各ノードの異なるチップで動作します。

- アクセスSPANおよびテナントSPANは、リーフ上のBroadcomチップ(T2:Trident2)で動作します。
- ファブリックSPANは、リーフ上のNS(NorthStar)チップまたはスパイン上のALPINE(Alpine)チップのいずれかで動作します。

したがって、Broadcomチップの制限により、

- アクセスSPANとテナントSPANはERSPANタイプIを使用

一方、NSチップとALPチップはタイプIIをサポートしています。そう

- ファブリックSPANはERSPANタイプIIを使用

第2世代以降のノードでは、すべてのACI SPANはデフォルトでERSPANタイプIIを使用します。

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で一度に復号化できる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。

このタイプの問題を回避するには、SPAN宛先グループでERSPANタイプを設定できます。

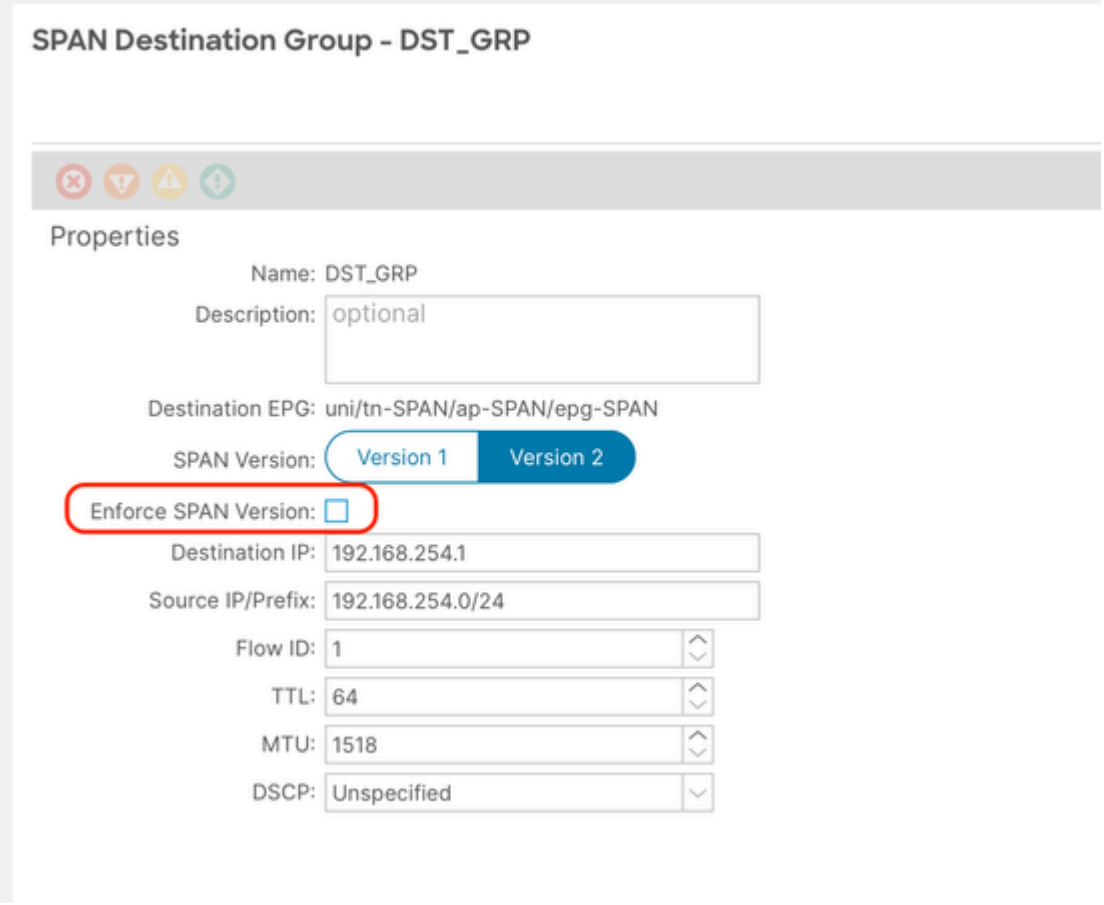

図40:SPANバージョンを適用するオプション

- 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）：ソースノードのハードウェアで、設定されたERSPAN Type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必要があるかどうかを決定します。

デフォルトでは、SPAN VersionはVersion 2で、Enforce SPAN Versionはオフになっています。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、タイプIIのERSPANを生成します。送信元ノードが、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
バージョン 1	オン	タイプIを使用	タイプIを使用

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、WiresharkでUDP宛先ポート48879をVxLANとして設定すると、iVxLANヘッダーとVxLANヘッダーを復号化できます。

1. 最初にiVxLANカプセル化パケットが選択されていることを確認してください。
2. Edit > Preferences > Protocols > VxLANの順に移動します。
3. ポートの最後にポート48879を追加します。
4. 次にApplyを実行します。

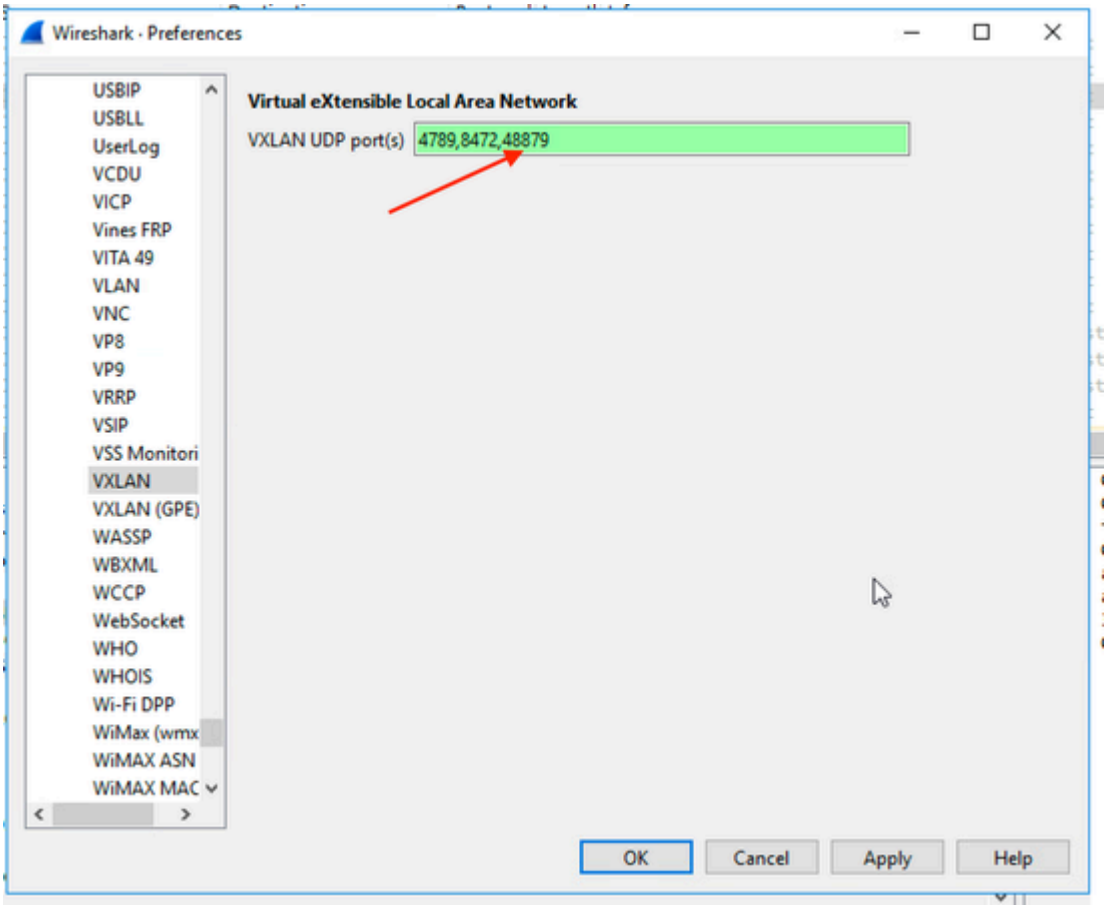

図41:iVXLANヘッダーをデコードするためのカスタムポートの追加方法

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ヘッダーでカプセル化されません。

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。