Configurazione di Switched Port Analyzer su ACI

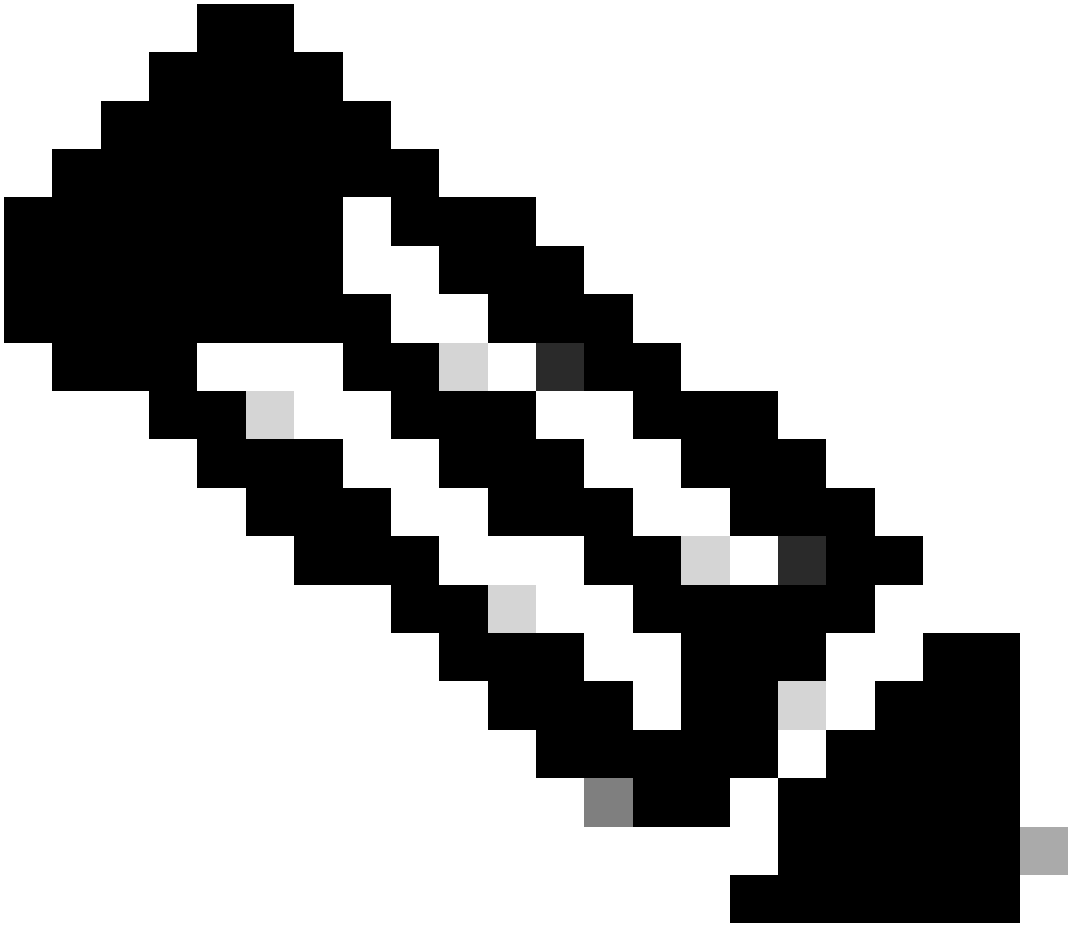
Sommario

Introduzione

Questo documento descrive come configurare Switched Port Analyzer (SPAN) su Cisco Application Centric Infrastructure (ACI).

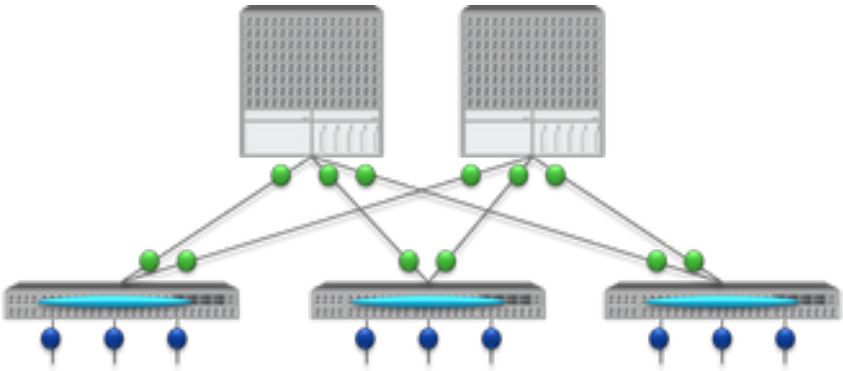
Premesse

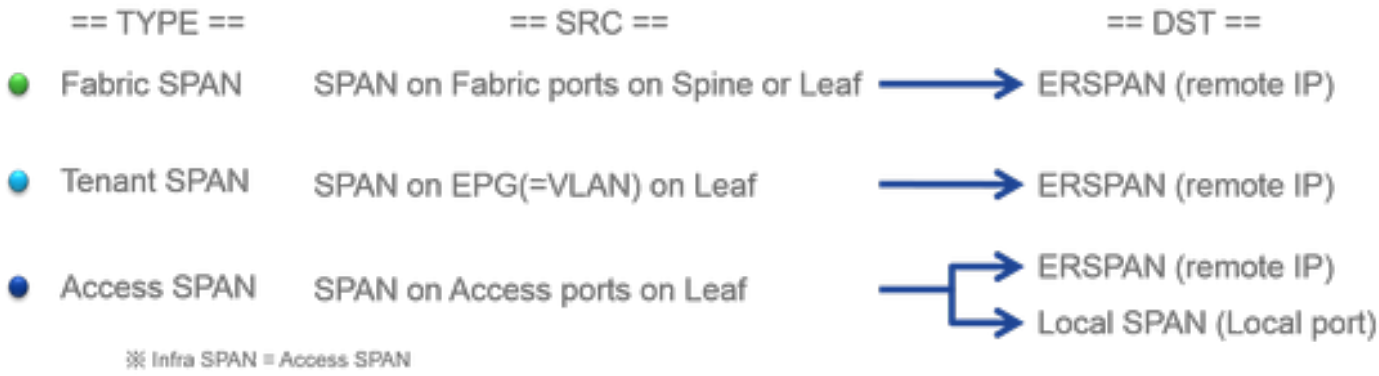
In generale, esistono tre tipi di SPAN. SPAN locale, RSPAN (Remote SPAN) ed ERSPAN (Encapsulated Remote SPAN). Le differenze tra questi SPAN sono principalmente la destinazione dei pacchetti di copia. Cisco ACI supporta Local SPAN ed ERSPAN.



Nota: in questo documento si presume che i lettori abbiano già familiarità con SPAN in generale, come ad esempio le differenze Local SPAN ed ERSPAN.

Tipo SPAN in Cisco ACI





Cisco ACI dispone di tre tipi di SPAN: Fabric SPAN, Tenant SPAN e Access SPAN. La differenza tra ciascuna SPAN è l'origine dei pacchetti di copia.

Come indicato in precedenza,

- **Fabric SPAN** cattura i pacchetti che entrano ed escono da **interfaces between Leaf and Spine switches**.
- Access SPAN cattura i pacchetti che entrano ed escono da interfaces between Leaf switches and external devices.
- Tenant SPAN cattura i pacchetti che entrano ed escono da EndPoint Group (EPG) on ACI Leaf switches.

Questo nome SPAN corrisponde alla posizione in cui deve essere configurato sull'interfaccia utente di Cisco ACI.

- SPAN fabric configurato in Fabric > Fabric Policies
- L'SPAN di accesso è configurato in Fabric > Access Policies
- L'SPAN del tenant è configurato in Tenants > {each tenant}

Per quanto riguarda la destinazione di ogni SPAN, solo Access SPAN è in grado di supportare sia Local SPAN che ERSPAN. Gli altri due SPAN (Fabric e Tenant) sono solo in grado di ERSPAN.

Limitazioni e linee guida

Consultare la sezione Limitazioni e linee guida della guida per la risoluzione dei problemi di Cisco APIC. È menzionato in Troubleshooting Tools and Methodology > Using SPAN.

Configurazione

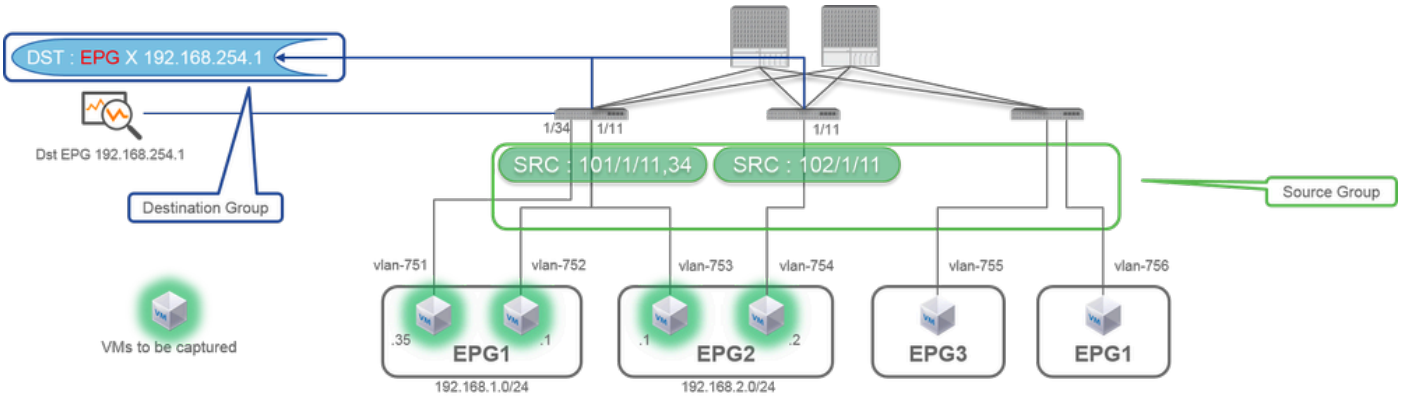
In questa sezione vengono presentati brevi esempi relativi alla configurazione di ciascun tipo SPAN. In alcuni casi specifici viene illustrato come selezionare il tipo di estensione nella sezione successiva.

La configurazione SPAN è descritta anche in Cisco APIC Troubleshooting Guide: Troubleshooting Tools and method > Using SPAN (Strumenti per la risoluzione dei problemi e metodologia Cisco APIC > Utilizzo di SPAN).

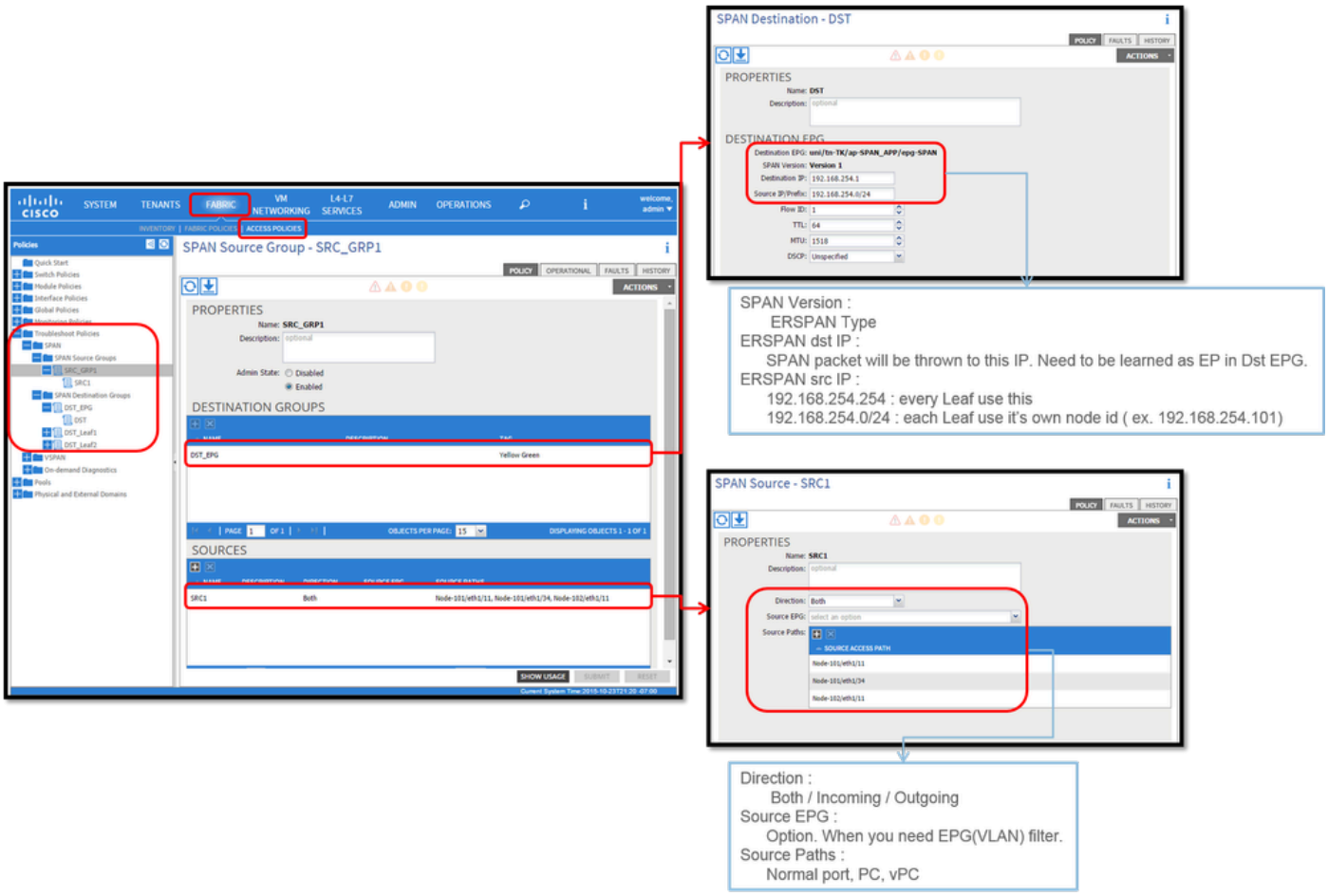
L'interfaccia utente può apparire diversa dalle versioni correnti, ma l'approccio di configurazione è lo stesso.

ERSPAN (Access SPAN)

Topologia di esempio



Esempio di configurazione



Dove:

Passare a FABRIC > ACCESS POLICIES > Troubleshoot Policies > SPAN.

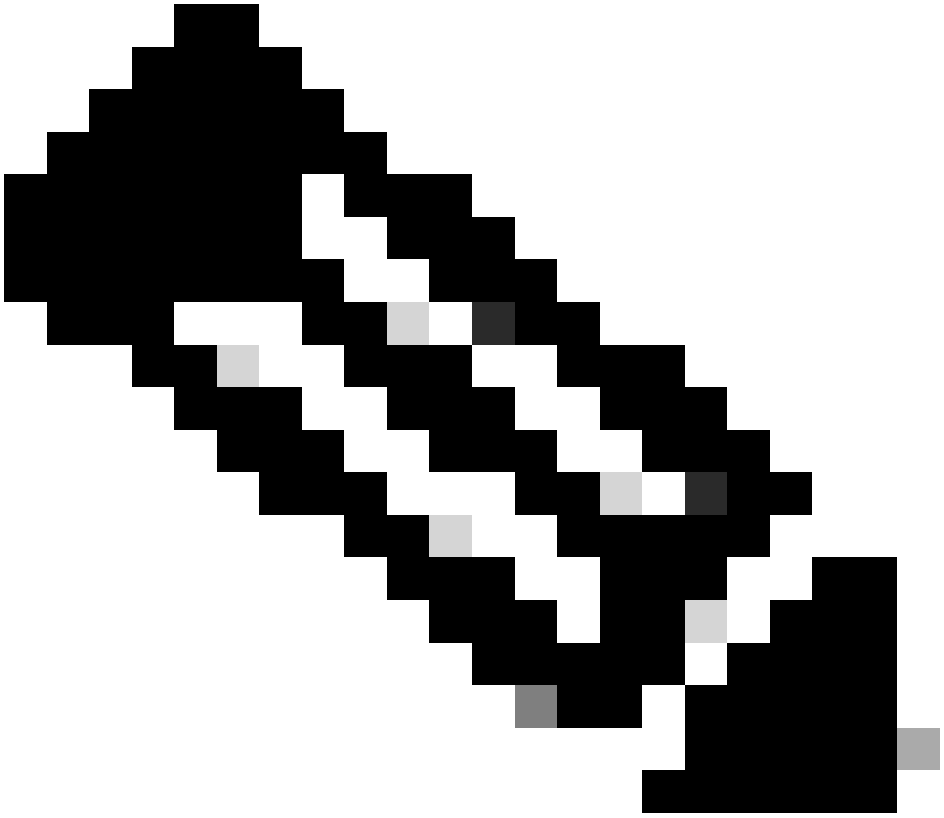
- SPAN Source Groups
- SPAN Destination Groups

SPAN Source Group cravatte Destination e Sources.

Procedura:

- Creare SPAN Source Group (SRC_GRP1).
- Creare SPAN Source (SRC1) sotto SPAN Source Group (SRC_GRP1).
- Configurare questi parametri per SPAN Source (SRC1).

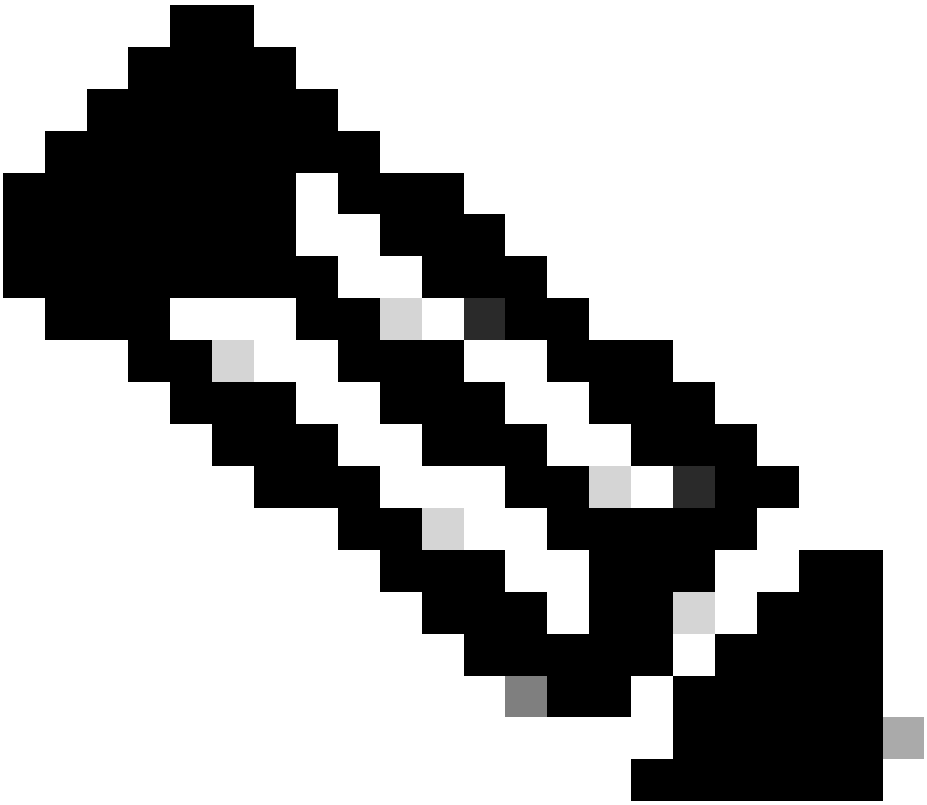
- Direzione - Origine EPG (opzione)
- Percorsi di origine (possono essere più interfacce)



Nota: fare riferimento all'immagine per i dettagli di ciascun parametro.

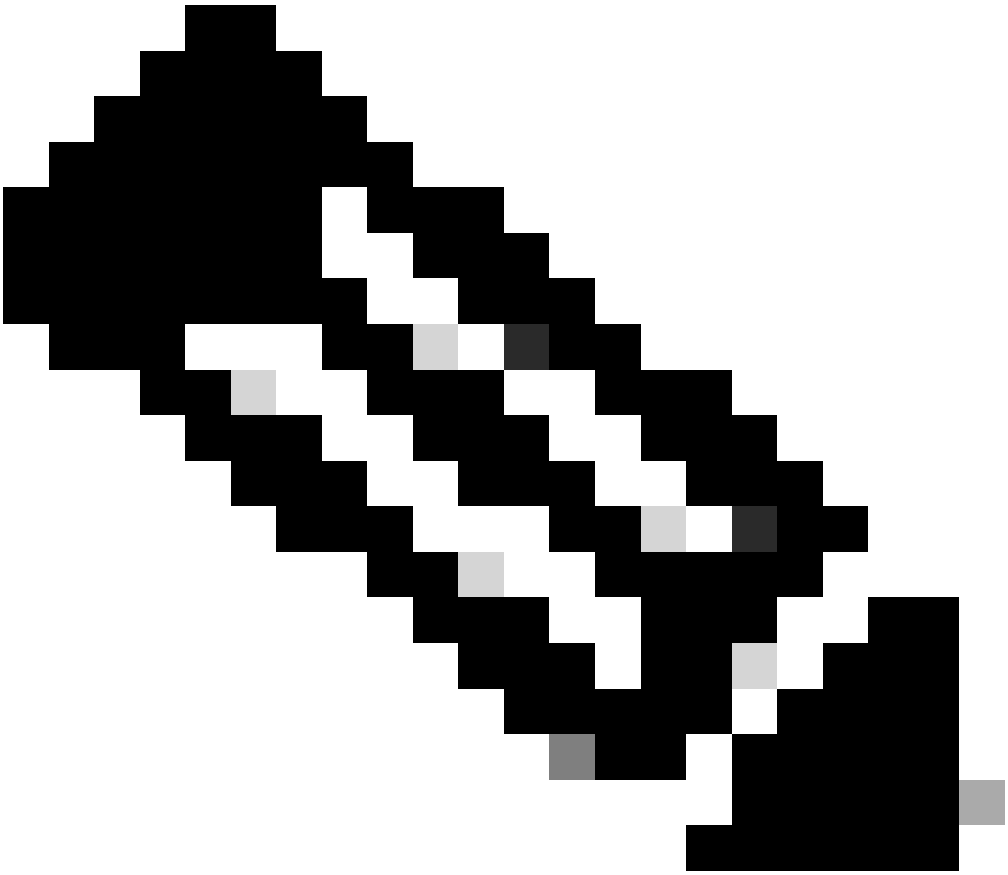
- Create SPAN Destination Group (DST_EPG).
- Crea SPAN Destination (DST).
- Configura questi parametri per SPAN Destination (DST)

- EPG di destinazione
-IP di destinazione
- IP/Prefisso di origine (può essere qualsiasi IP. Se viene utilizzato il prefisso, per i bit non definiti viene utilizzato l'ID nodo del nodo di origine. Ad esempio, prefisso: 1.0.0.0/8 su node-101 => src IP 1.0.0.101)
- Altri parametri possono essere lasciati come predefiniti



Nota: fare riferimento all'immagine per i dettagli di ciascun parametro.

- Assicurarsi che siaSPAN Destination Group collegato a un SPAN Source Grouprouter appropriato.
- Accertarsi che Admin Statesia abilitato.

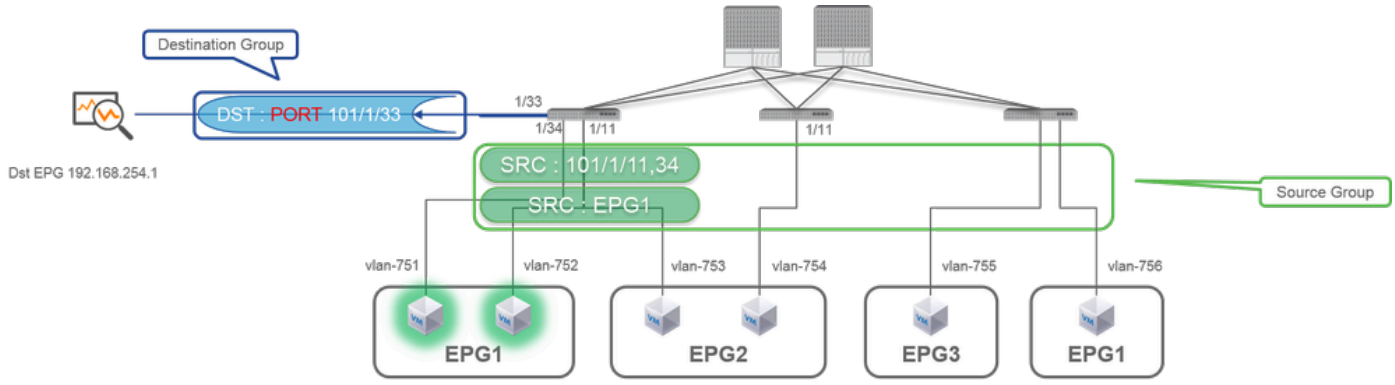


Nota: l'SPAN si arresta quando si seleziona Disabilitato su questo stato di amministrazione. Non è necessario eliminare tutti i criteri se vengono riutilizzati in un secondo momento.

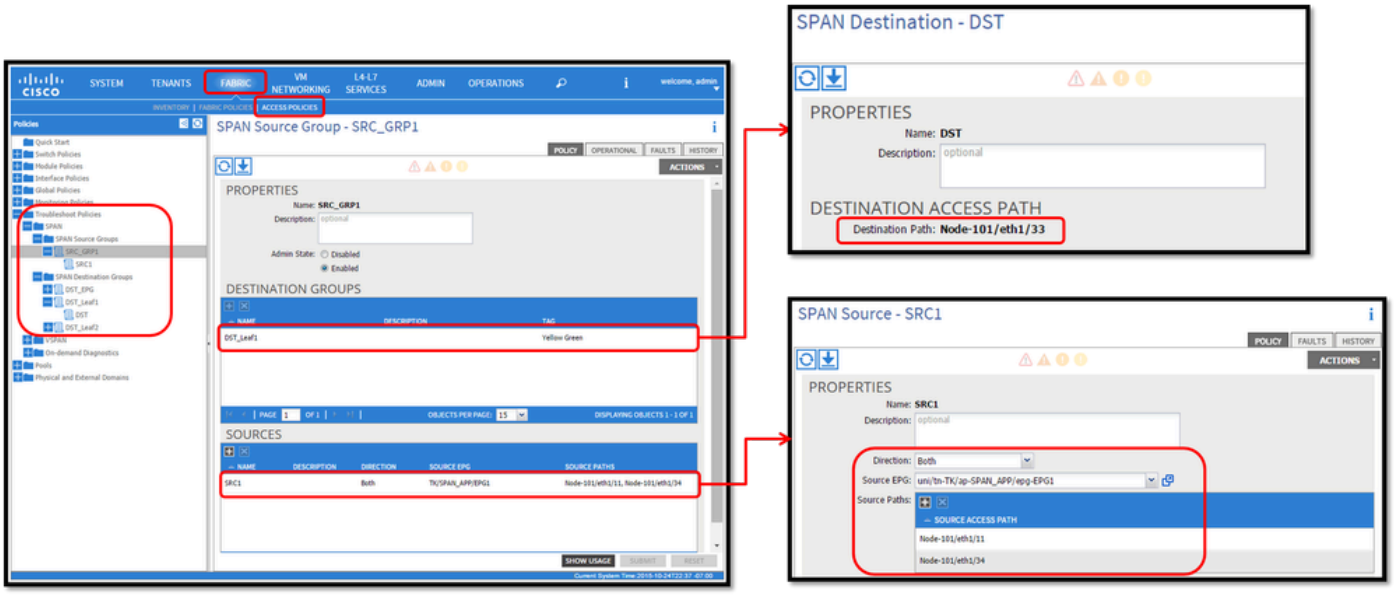
Verificare inoltre che l'IP di destinazione per ERSPAN venga appreso come endpoint nella destinazione EPG specificata. Nell'esempio sopra menzionato, si deve imparare 192.168.254.1 sotto Tenant TK > Application profile SPAN_APP > EPG SPAN. In alternativa, l'IP di destinazione può essere configurato come endpoint statico in questo EPG se il dispositivo di destinazione è un host invisibile all'utente.

Access SPAN (locale)

Topologia di esempio



Esempio di configurazione



- Dove:

Fabric > ACCESS POLICIES > Troubleshoot Policies > SPAN

- SPAN Source Groups

- SPAN Destination Groups

SPAN Source Group cravatte Destination e Sources.

- Procedura:

- Crea SPAN Source Group (SRC_GRP1)
- Crea SPAN Source(SRC1) sotto SPAN Source Group (SRC_GRP1)

- Configurare questi parametri per SPAN Source (SRC1)

-Direzione
- EPG di origine (opzionale)
- Percorsi di origine (possono essere più interfacce)
→ fare riferimento all'immagine per i dettagli di ciascun parametro.

- Crea SPAN Destination Group(DST_Leaf1)

- Crea SPAN Destination(DST)

- Configura questi parametri per SPAN Destination (DST)

- Interfaccia e nodo di destinazione.

- Assicurarsi che siaSPAN Destination Group collegato a un SPAN Source Grouprouter appropriato.

-

Accertarsi che siaAdmin State abilitato.
※ SPAN si arresta quando si seleziona Disattivato su questo stato di amministrazione. Non è necessario eliminare tutti i criteri se vengono riutilizzati in un secondo momento.

L'interfaccia di destinazione non richiede alcuna configurazione da parte dei gruppi di criteri di interfaccia. Funziona quando si collega un cavo all'interfaccia su ACI Leaf.

Limitazioni:

- Per Local SPAN, un'interfaccia di destinazione e le interfacce di origine devono essere configurate sulla stessa foglia.

- L'interfaccia di destinazione non richiede che si trovi su un EPG finché è attivo.

- Quando si specifica l'interfaccia del canale della porta virtuale (vPC) come porta di origine, non è possibile utilizzare Local SPAN Tuttavia, è disponibile una soluzione. Su un'interfaccia di prima generazione, una singola porta fisica che è membro di vPC o PC può essere configurata come origine SPAN. Con questo Local SPAN può essere usato per il traffico sulle porte vPC.
Questa opzione, tuttavia, non è disponibile per le foglie di seconda generazione (CSCvc11053). È stato invece aggiunto il supporto per SPAN su "VPC component PC" tramite CSCvc44643in 2.1(2e), 2.2(2e) e versioni successive. In questo modo, qualsiasi foglia di generazione può configurare un canale della porta, che è membro di vPC, come origine SPAN. Ciò consente a qualsiasi foglia di generazione di utilizzare Local SPAN per il traffico sulle porte vPC.

- Se si specificano le singole porte di un canale di porta sulle porte di seconda generazione, viene eseguito lo spanning di solo un sottoinsieme dei pacchetti (anche a causa di CSCvc11053).

- PC e vPC non possono essere utilizzati come porta di destinazione per Local SPAN. Dalla versione 4.1(1), il PC può essere usato come porta di destinazione per Local SPAN.

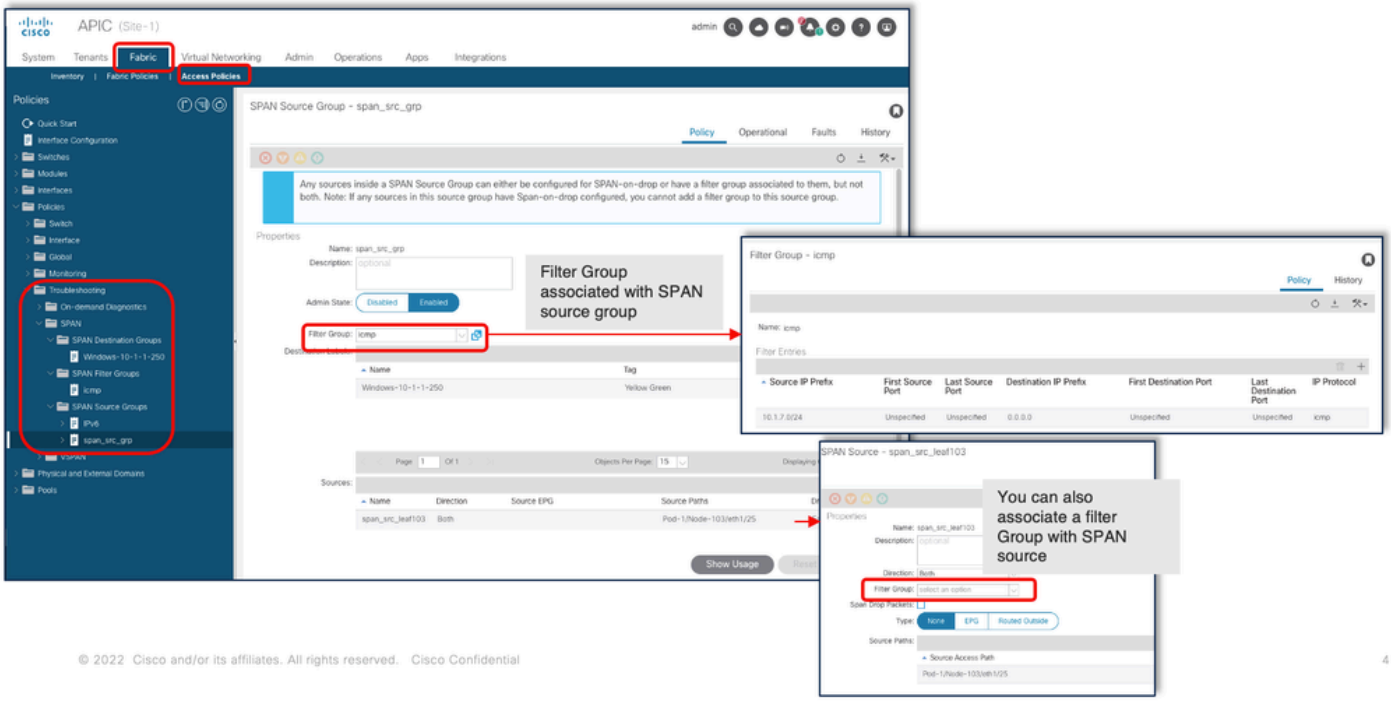
Access SPAN - Con filtri ACL

È possibile utilizzare i filtri ACL sulle origini di estensione dell'accesso. Questa funzione consente di eseguire lo SPAN di un particolare flusso o flusso di traffico in entrata e in uscita da un'origine SPAN.
Gli utenti possono applicare gli ACL SPAN a un'origine quando è necessario eseguire lo SPAN sul traffico specifico del flusso.
Non è supportato nei gruppi di origine/origini SPAN Fabric e Tenant Span.

È necessario prestare attenzione quando si aggiungono voci di filtro in un gruppo di filtri, poiché potrebbe aggiungere voci tcam per ogni sorgente che attualmente utilizza il gruppo di filtri.

Un gruppo di filtri può essere associato a:
-Span Origine: il gruppo di filtri viene utilizzato per filtrare il traffico su TUTTE le interfacce definite in questa origine Span.
-Span Source Group: il gruppo di filtri (ad esempio, x) viene utilizzato per filtrare il traffico su TUTTE le interfacce definite in ognuna delle origini di span di questo gruppo di origini di span.

In questo snapshot di configurazione, il gruppo di filtri viene applicato al gruppo di origine Span.

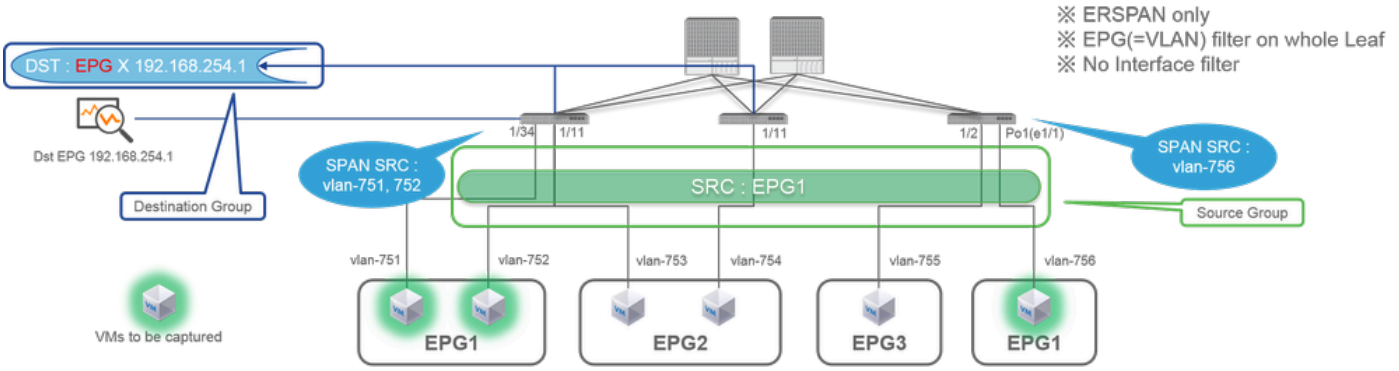


Se una determinata origine Span è già associata a un gruppo di filtri (ad esempio y), tale gruppo di filtri (ad) viene utilizzato per filtrare il gruppo su tutte le interfacce in questa specifica origine Span

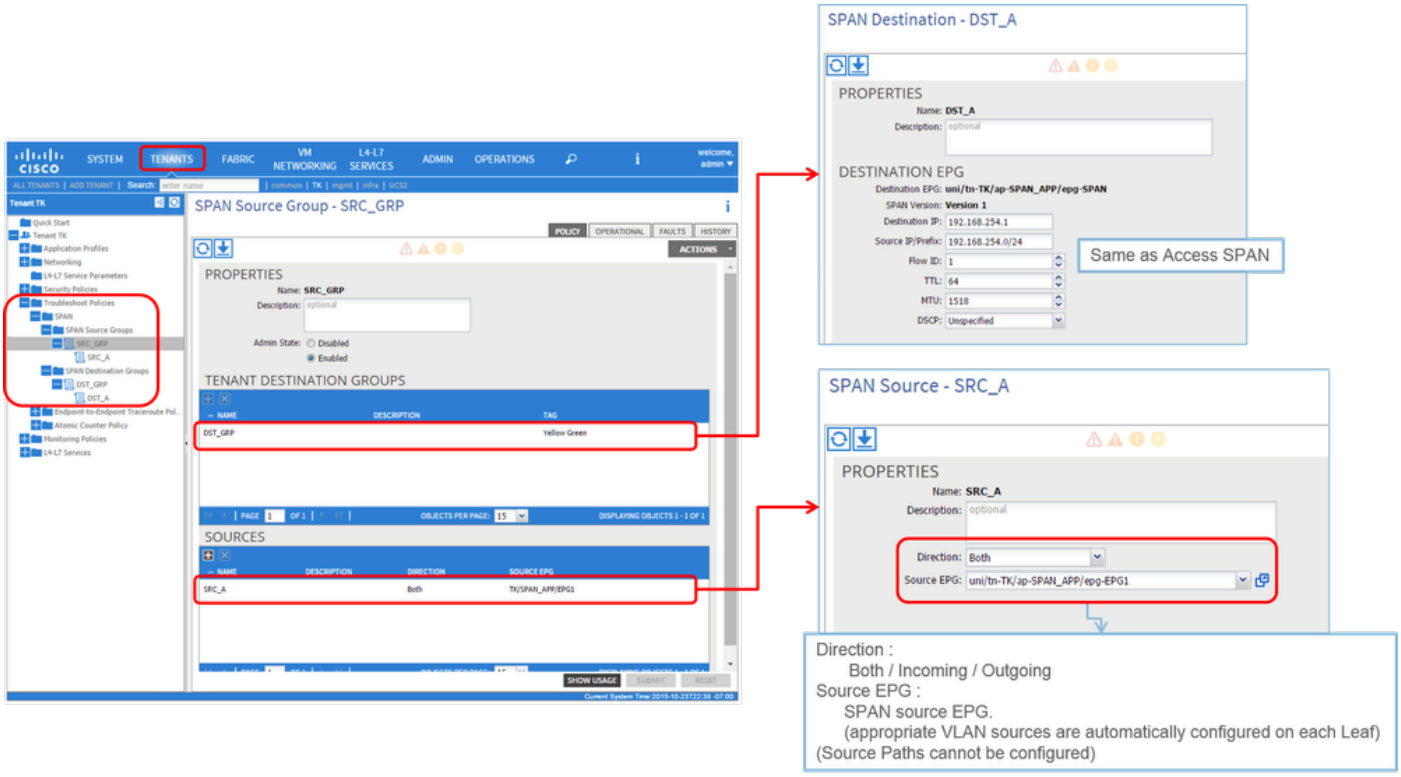
- Un gruppo di filtri applicato a un gruppo di origini viene applicato automaticamente a tutte le origini in tale gruppo.
- Un gruppo di filtri applicato a un'origine è applicabile solo a tale origine.
- Un gruppo di filtri viene applicato sia al gruppo di origine che a un'origine in tale gruppo di origine. Il gruppo di filtri applicato all'origine ha la precedenza.
- Un gruppo di filtri applicato a un'origine viene eliminato, il gruppo di filtri applicato al gruppo di origine padre viene applicato automaticamente.
- Un gruppo di filtri applicato a un gruppo di origine viene eliminato da tutte le origini attualmente ereditate da tale gruppo di origine.

ERSPAN (Tenant SPAN)

Topologia di esempio



Esempio di configurazione



- Dove:

Tenants > {tenant name} > Troubleshoot Policies > SPAN

- SPAN Source Groups

- SPAN Destination Groups

※ Rapporti Destinatione gruppi di origini SPAN Sources.

- Procedura:

- Crea SPAN Source Group (SRC_GRP)

- Crea SPAN Source (SRC_A) sotto SPAN Source Group (SRC_GRP)

- Configurare questi parametri per SPAN Source (SRC_A)
  -Direzione
  - EPG di origine

→ Fare riferimento all'immagine per i dettagli di ciascun parametro.

- Crea SPAN Destination Group (DST_GRP)

- Crea SPAN Destination (DST_A)

- Configurare questi parametri per SPAN Destination(DST_A)
  - EPG di destinazione
  -IP di destinazione
  - IP/Prefisso origine
  - Altri parametri possono essere lasciati come predefiniti

→ Fare riferimento all'immagine per i dettagli di ciascun parametro.

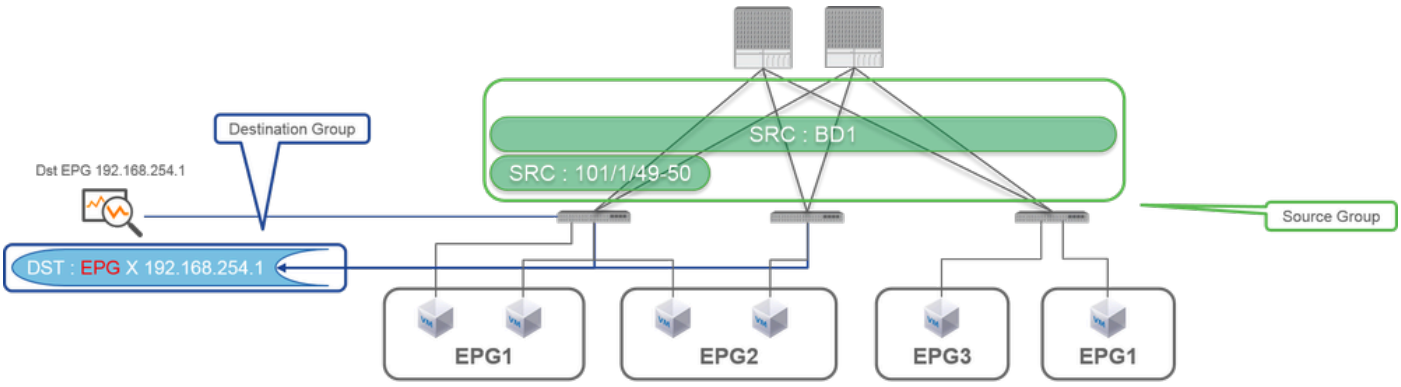
- Accertarsi cheSPAN Destination Group sia collegato a un SPAN Source Groupsistema appropriato.

- Accertarsi che siaAdmin State abilitato.

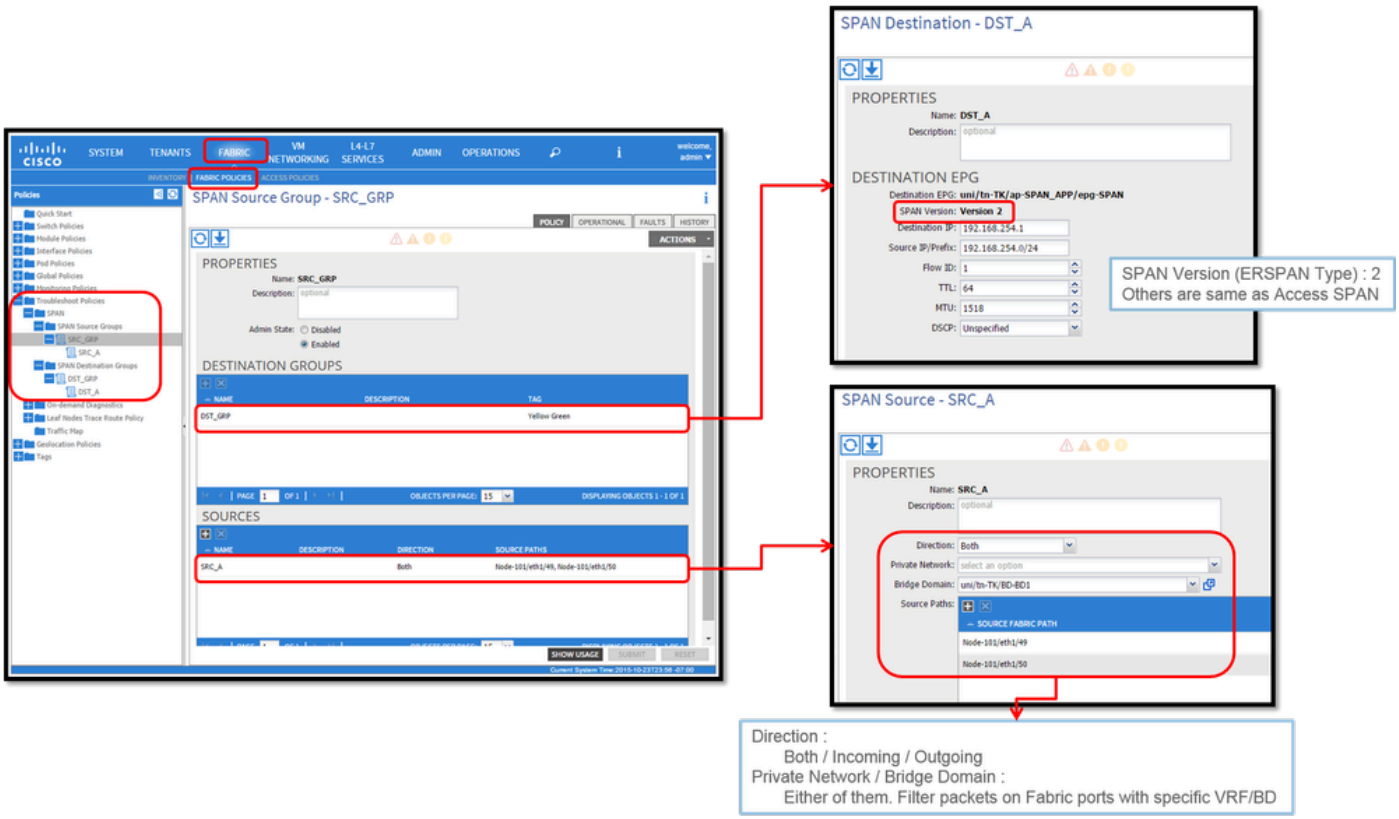
※ SPAN si arresta quando si seleziona Disattivato su questo stato di amministrazione. Non è necessario eliminare tutti i criteri se vengono riutilizzati in un secondo momento.

ERSPAN (Fabric SPAN)

Topologia di esempio



Esempio di configurazione



- Dove:

Fabric > FABRIC POLICIES > Troubleshoot Policies > SPAN

- Fabric

- SPAN Destination Groups

※ SPAN Source Group cravatte Destination e Sources

- Procedura:

- Crea SPAN Source Group (SRC_GRP)

- Crea SPAN Source (SRC_A) sotto SPAN Source Group (SRC_GRP)

- Configurare questi parametri per SPAN Source (SRC_A)
  -Direzione
  - Rete privata (opzionale)
  - Dominio bridge (opzione)
  - Percorsi di origine (possono essere più interfacce)

→ fare riferimento all'immagine per i dettagli di ciascun parametro.

- Crea SPAN Destination Group (DST_GRP)

- Crea SPAN Destination (DST_A)

- Configurare questi parametri per SPAN Destination (DST_A)
  - EPG di destinazione
  -IP di destinazione
  - IP/Prefisso origine
  - Altri parametri possono essere lasciati come predefiniti

→ fare riferimento all'immagine per i dettagli di ciascun parametro.

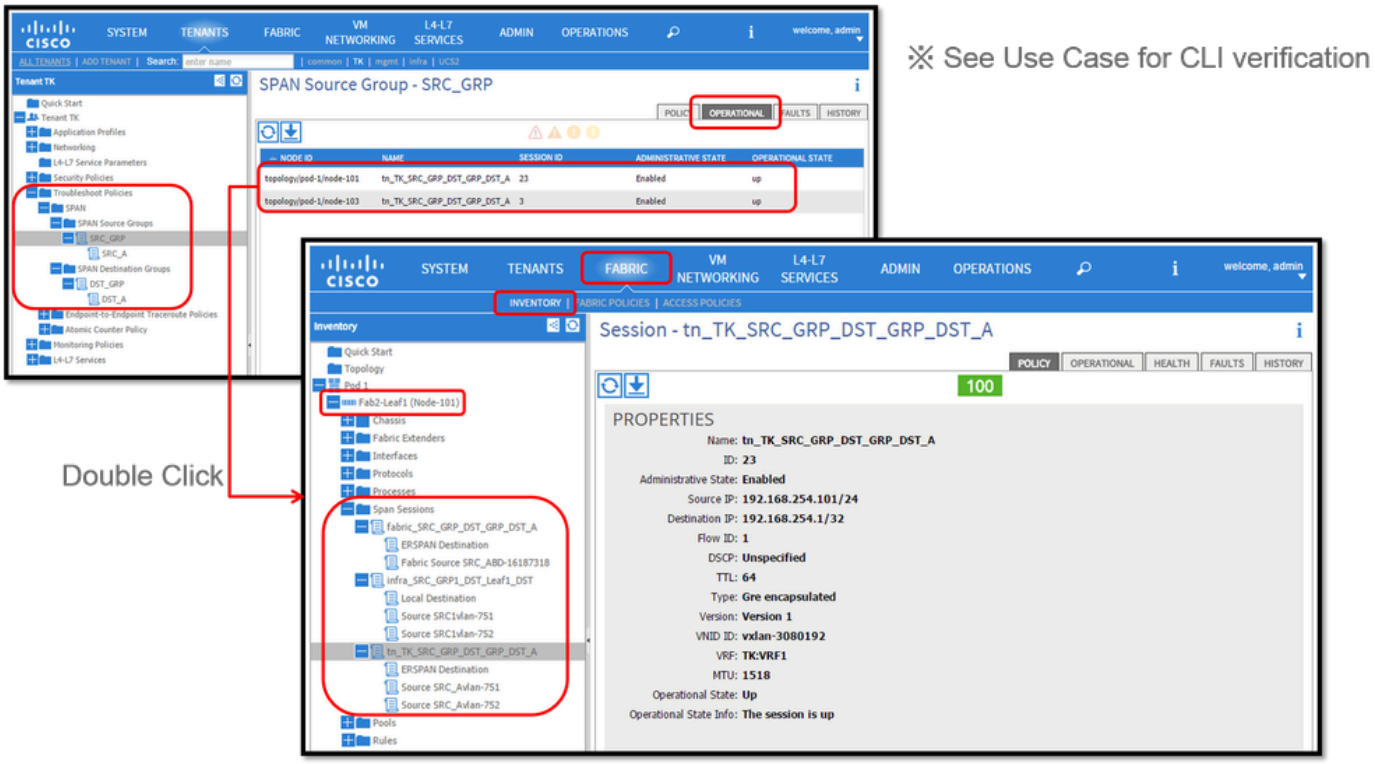
- Accertarsi cheSPAN Destination Group sia collegato a un SPAN Source Groupsistema appropriato.

- Accertarsi che Admin State sia abilitato.

※ L'SPAN si arresta quando si seleziona Disabilitato su questo Admin State. Non è necessario eliminare tutti i criteri se vengono riutilizzati in un secondo momento.

Sebbene sia descritta in una sezione successiva "ERSPAN Version (type)", è possibile stabilire che la versione II di ERSPAN è utilizzata per Fabric SPAN e la versione I per Tenant e Access SPAN.

Verifica GUI



- Verifica dei criteri di configurazione SPAN

- 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

Verificare che lo stato operativo sia attivo.

- Verifica nella sessione SPAN sul nodo stesso

- Fare doppio clic su ciascuna sessione da SPAN Configuration Policyo Fabric > INVENTORY > Node > Span Sessions > { SPAN session name }

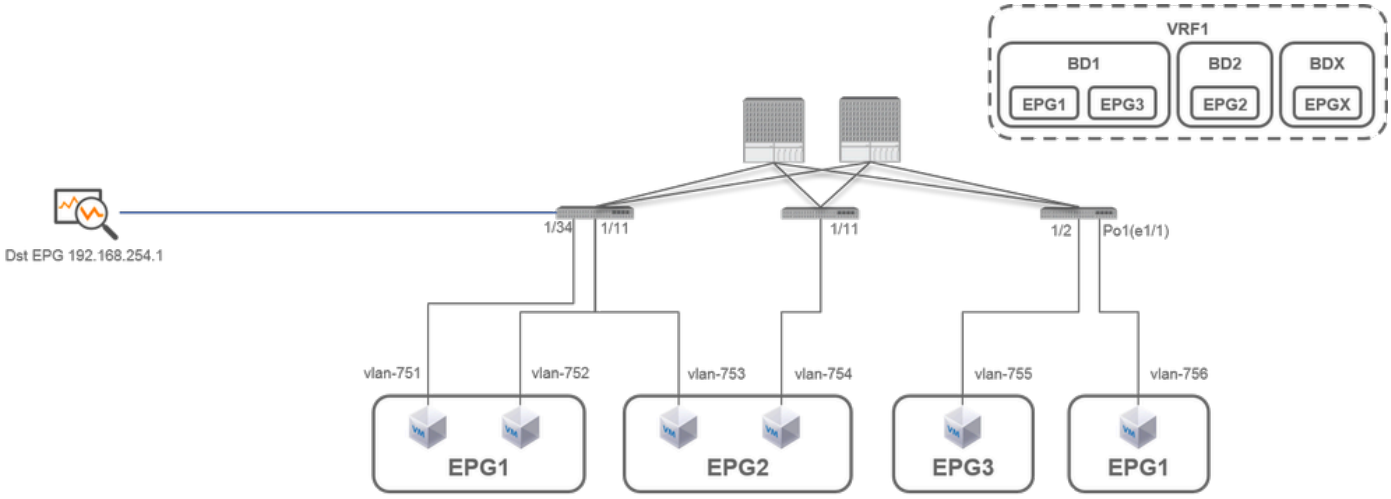
Verificare che lo stato operativo sia attivo.

Convenzione di denominazione delle sessioni SPAN:

- SPAN fabric: fabric_xxxx

- Accesso SPAN: infra_xxxx
- SPAN tenant: tn_xxxx

Selezionare il tipo ACI SPAN

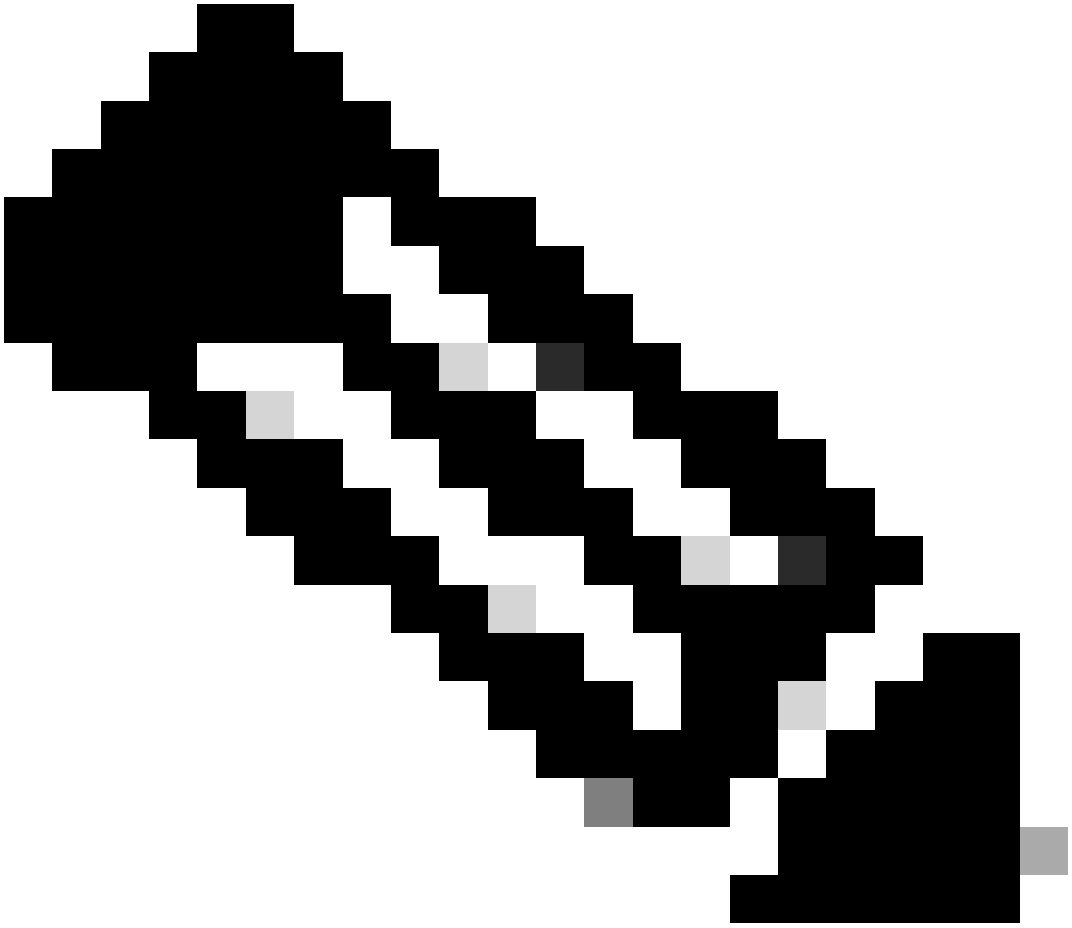


In questa sezione vengono descritti gli scenari dettagliati per ciascun tipo ACI SPAN (Access, Tenant, Fabric). La topologia di base per ciascuno scenario è descritta nella sezione precedente.

Se si conoscono questi scenari, è possibile selezionare il tipo ACI SPAN appropriato per le proprie esigenze, ad esempio è necessario acquisire i pacchetti solo su interfacce specifiche o tutti i pacchetti su un EPG specifico, a prescindere dalle interfacce, e altro ancora.

In Cisco ACI, lo SPAN è configurato con source group e destination group. Il gruppo Origine contiene più fattori di origine, ad esempio interfacce o EPG. Il gruppo di destinazione contiene informazioni sulla destinazione, ad esempio l'interfaccia di destinazione per SPAN locale o l'indirizzo IP di destinazione per ESPAN.

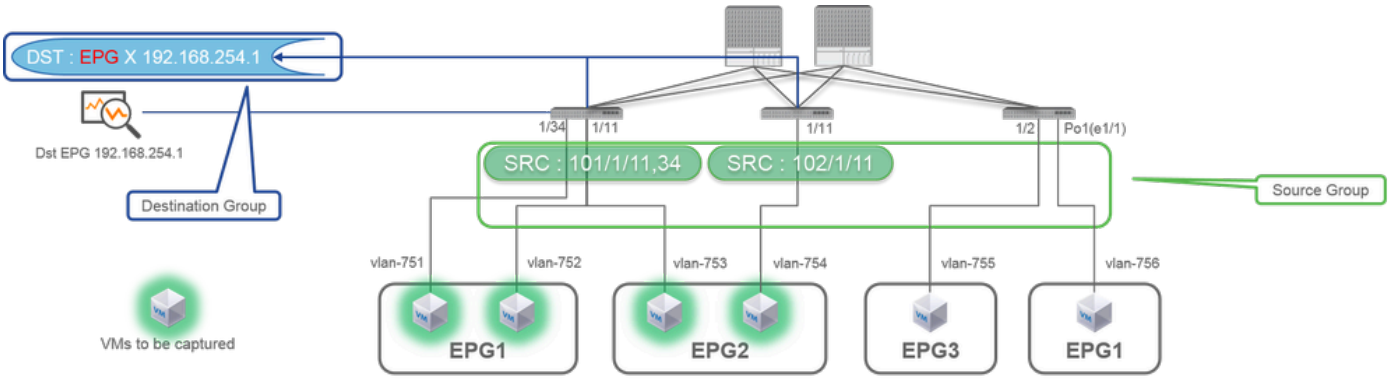
Dopo aver acquisito i pacchetti, consultare la sezione "Come leggere i dati SPAN" per decodificare i pacchetti acquisiti.



Nota: concentrarsi sulle VM evidenziate con una luce verde in ciascuna topologia. Ogni scenario prevede l'acquisizione di pacchetti da queste VM evidenziate.

ERSPAN (Access SPAN)

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




```
Fab2-Leaf1# show monitor session all
   session 13
---------------
description         : Span session 13
type                : erspan
version             : version not specified
state               : up (active)
erspan-id           : 1
granularity         :
vrf-name            : TK:VRF1
acl-name            :
ip-ttl              : 64
ip-dscp             : ip-dscp not specified
destination-ip      : 192.168.254.1/32
origin-ip           : 192.168.254.101/24
mode                : access
source intf         :
    rx              : Eth1/11       Eth1/34
    tx              : Eth1/11       Eth1/34
    both            : Eth1/11       Eth1/34
source VLANs        :
    rx              :
    tx              :
    both            :
filter VLANs        : filter not specified
```

```
Fab2-Leaf2# show monitor session all
   session 12
---------------
description         : Span session 12
type                : erspan
version             : version not specified
state               : up (active)
erspan-id           : 1
granularity         :
vrf-name            : TK:VRF1
acl-name            :
ip-ttl              : 64
ip-dscp             : ip-dscp not specified
destination-ip      : 192.168.254.1/32
origin-ip           : 192.168.254.102/24
mode                : access
source intf         :
    rx              : Eth1/11
    tx              : Eth1/11
    both            : Eth1/11
source VLANs        :
    rx              :
    tx              :
    both            :
filter VLANs        : filter not specified
```

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

- Source Group
  - Foglia 1 e1/11
  - Foglia 1 e1/34
  - Foglia2 e1/11
- Destination Group
  - 192.168.254.1 su EPG X

Access SPAN può specificare più interfacce per una singola sessione SPAN. Può acquisire tutti i pacchetti che entrano o escono da interfacce specifiche, indipendentemente dal loro EPG.

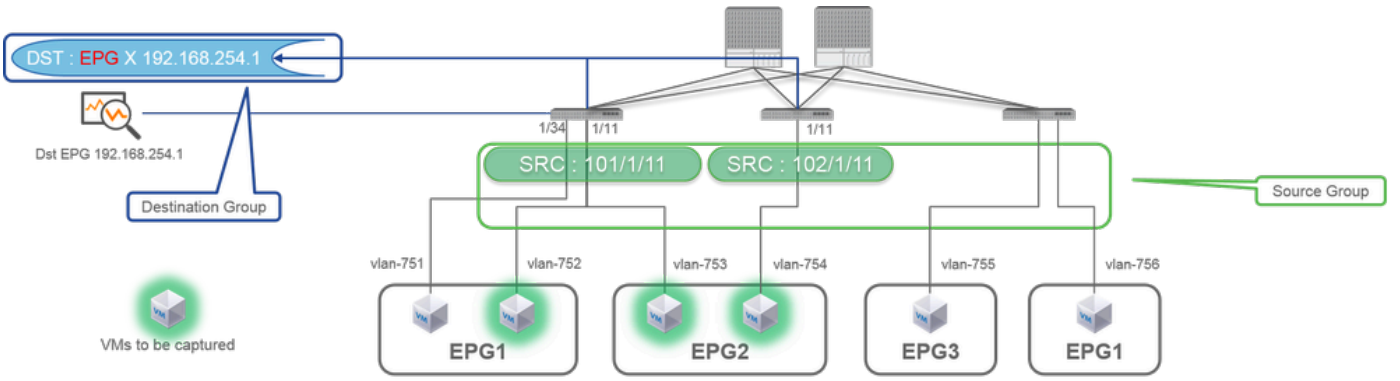
Quando si specificano più interfacce come gruppo di origine da più switch foglia, il gruppo di destinazione deve essere ERSPAN, non Local SPAN.

In questo esempio, vengono copiati i pacchetti da tutte le VM su EPG1 ed EPG2.

Check Point CLI

- Verificare che lo stato sia "attivo"
- "destination-ip" è l'IP di destinazione per ERSPAN
- "origin-ip" è l'IP di origine di ERSPAN

Caso 2. Src "Leaf1 e1/11 & 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
```

- **Gruppo di origine**
  - Foglia 1 e1/11
  - Foglia2 e1/11
- **Gruppo di destinazione**
  - 192.168.254.1 su EPG X

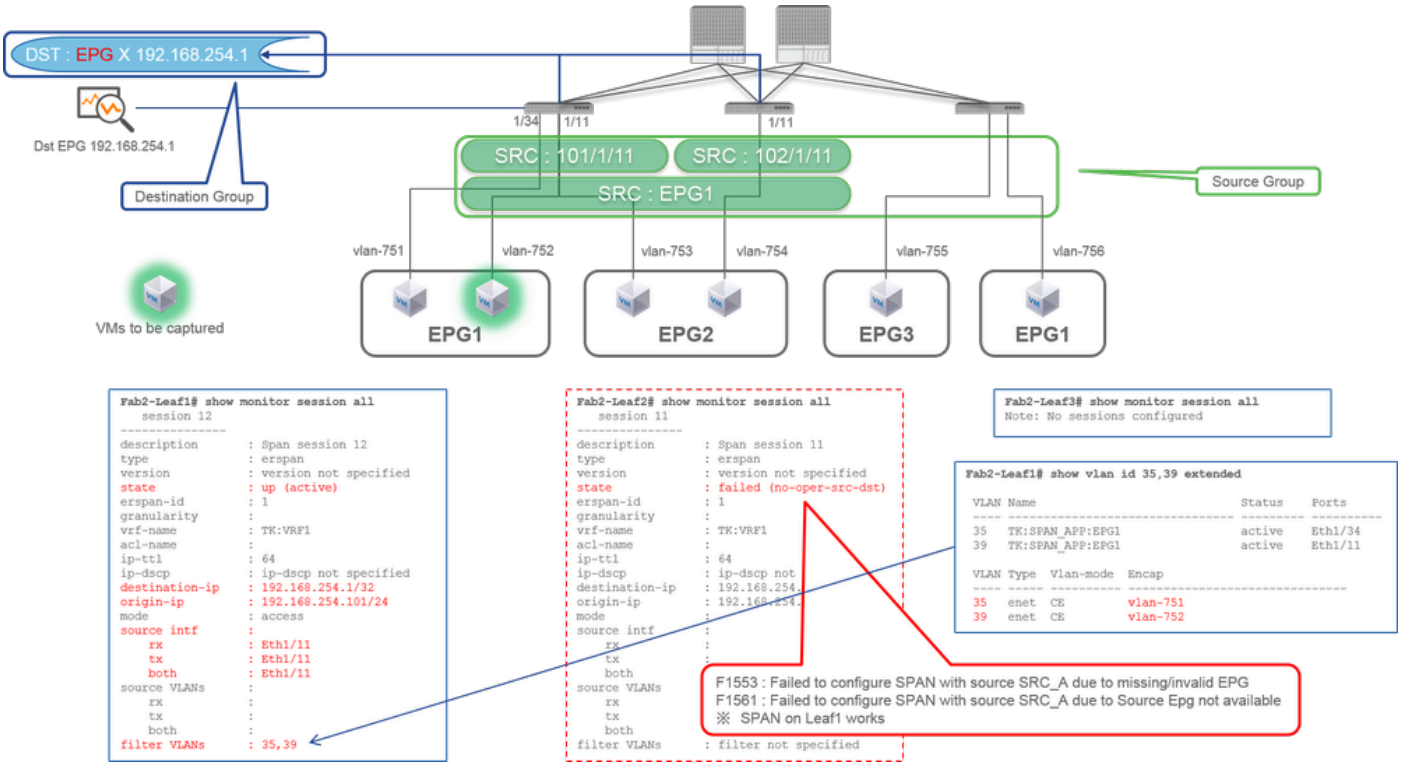
Nell'esempio, Leaf1 e1/34 viene rimosso dal gruppo di origini SPAN configurato nella precedente richiesta Case1.

Il punto chiave di questo esempio è che Access SPAN può specificare le interfacce di origine indipendentemente da EPG.

Check Point CLI

- L'interfaccia di origine su Leaf1 viene modificata in "Eth1/11" da "Eth1/11 Eth1/34"

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



- **Gruppo di origine**
  - Foglia 1 e1/11
  - Foglia2 e1/11
  - Filtro EPG1

- **Gruppo di destinazione**

- 192.168.254.1 su EPG X

Nell'esempio viene mostrato che Access SPAN può specificare anche un EPG specifico sulle porte di origine. Ciò è utile quando più EPG fluiscono su una singola interfaccia ed è necessario per acquisire il traffico solo per EPG1 su questa interfaccia.

Poiché EPG1 non è distribuito su Leaf2, SPAN per Leaf2 fallisce con i guasti F1553 e F1561. Tuttavia, SPAN su Leaf1 funziona ancora.

Inoltre, due filtri VLAN vengono aggiunti automaticamente per la sessione SPAN su Leaf1 perché EPG1 utilizza due VLAN (VLAN-751,752) su Leaf1.

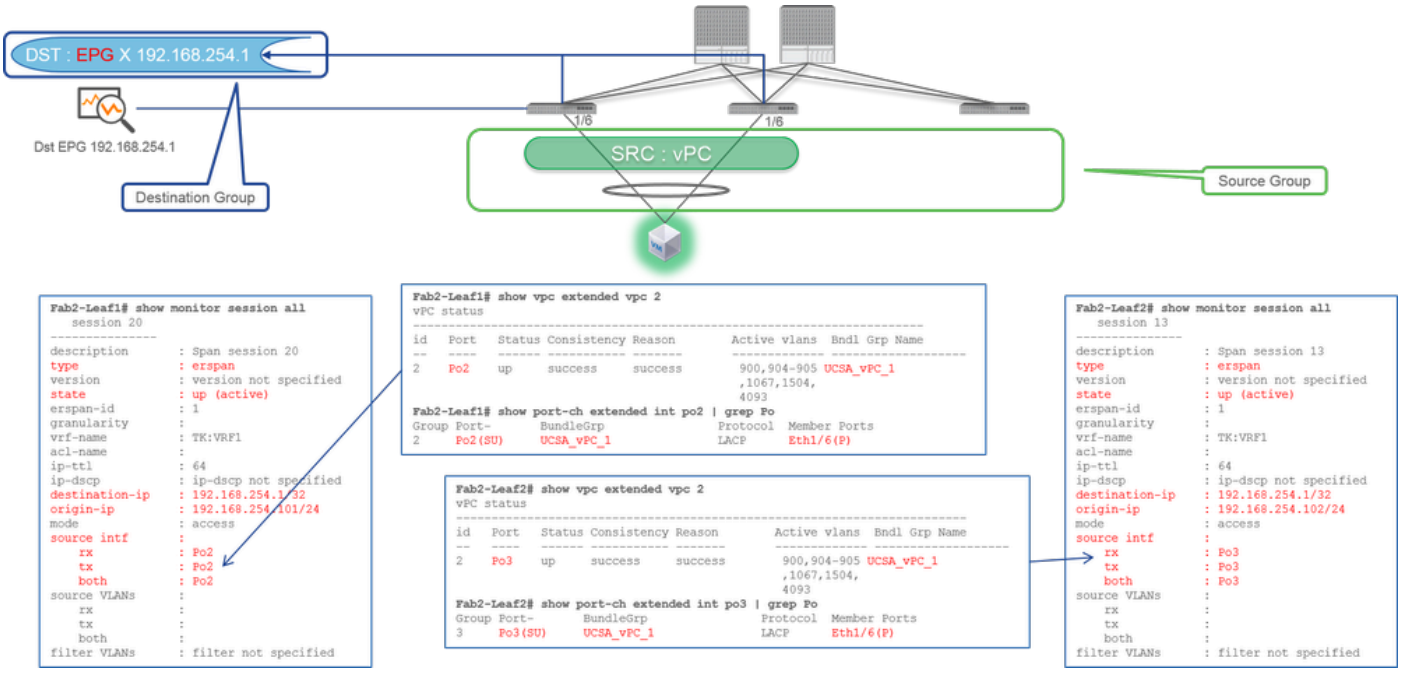
Notare che l'ID VLAN sulla CLI (35, 39) è la VLAN interna detta PI-VLAN (Platform Independent VLAN) e non è l'ID effettivo sul cavo. Come mostrato nella figura, il comando **show vlan extended** mostra la mappatura dell'ID VLAN di accesso e della VLAN IP effettivi.

Questa sessione SPAN ci permette di acquisire pacchetti solo per EPG1 (VLAN-752) su Leaf1 e1/11 anche se EPG2 (VLAN-753) scorre sulla stessa interfaccia.

Check Point CLI

- Le VLAN filtro vengono aggiunte in base agli EPG utilizzati per il filtro.
- Se non esistono EPG corrispondenti su Leaf, la sessione SPAN su tale Leaf ha esito negativo.

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



- **Gruppo di origine**

- Foglia1 - 2e1/11

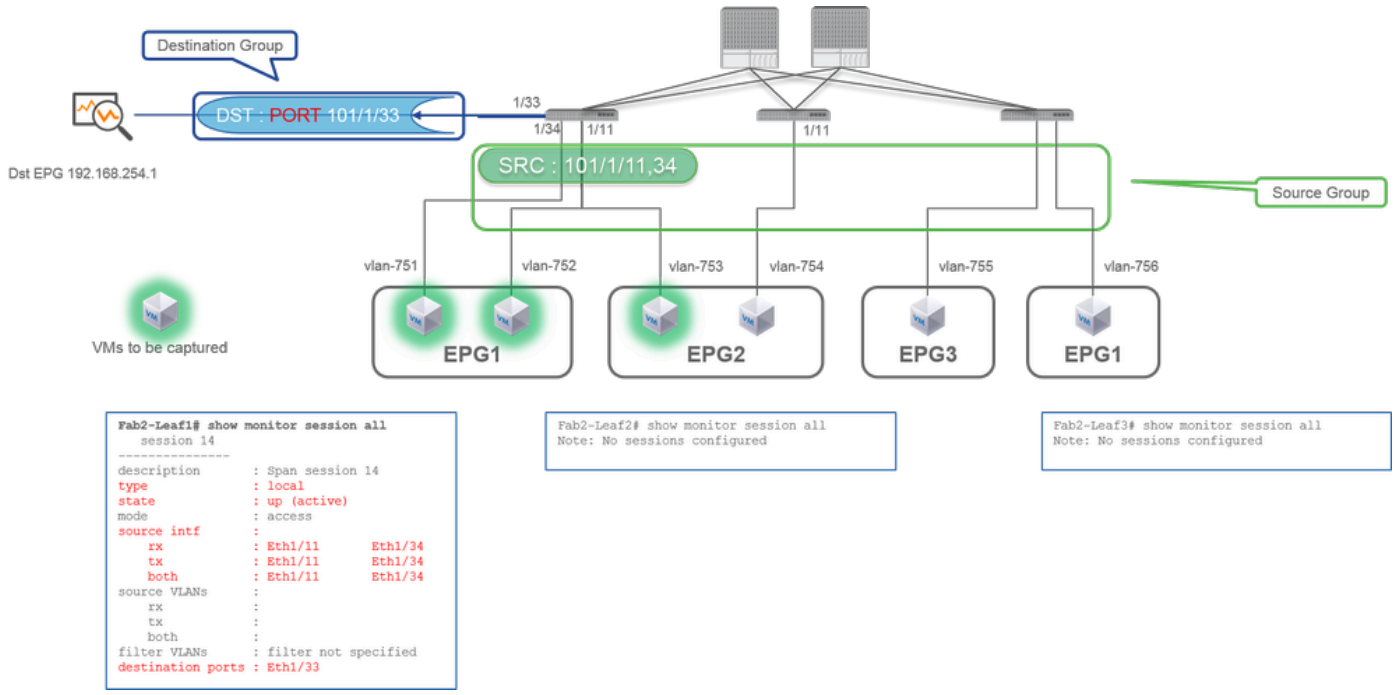
- **Gruppo di destinazione**

  - 192.168.254.1 su EPG X

Quando l'interfaccia vPC è configurata come origine, la destinazione deve essere un indirizzo IP remoto (ERSPAN) e non l'interfaccia (SPAN locale)

Access SPAN (Local SPAN)

Caso 1. Src "Leaf1 e1/1 e1/34" | Dst "Leaf1 e1/3"



- **Gruppo di origine**

  - Foglia 1 e1/11

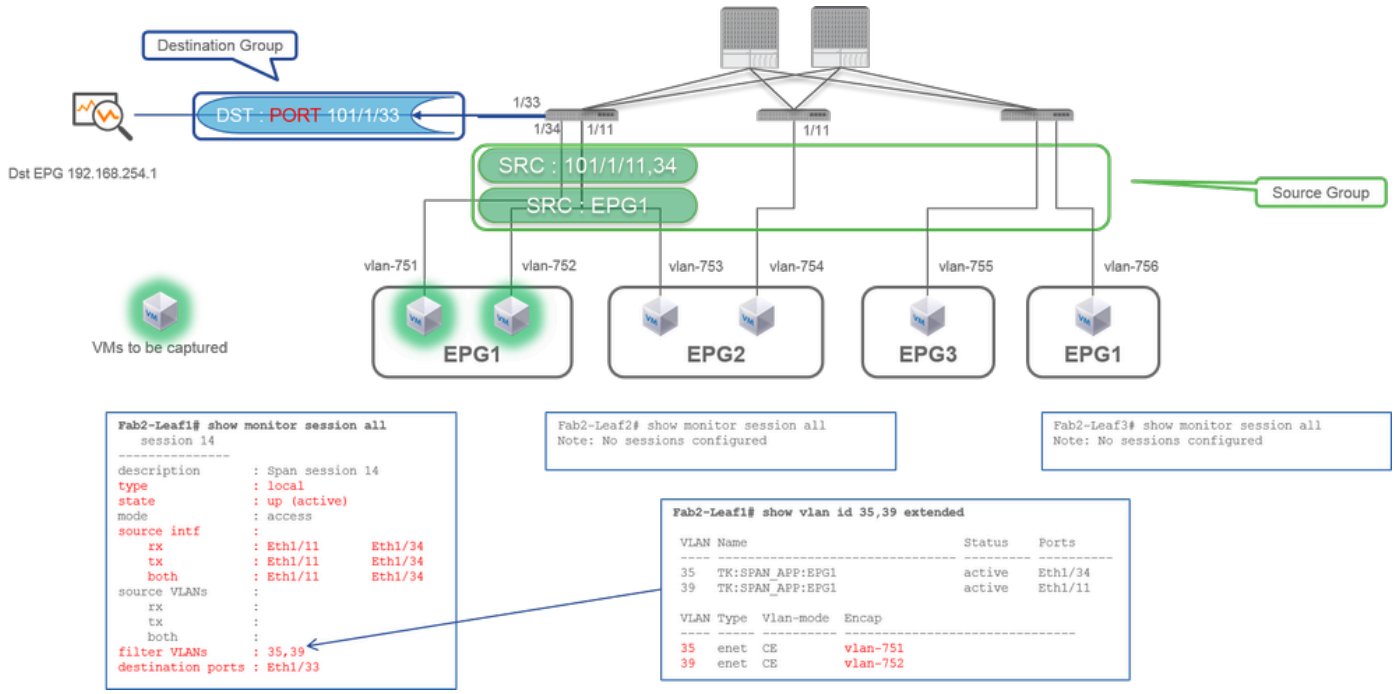
  - Foglia 1 e1/34

- **Gruppo di destinazione**
  - Foglia 1 e1/3

Access SPAN può anche utilizzare Local SPAN (ossia un'interfaccia specifica come destinazione)

Tuttavia, in questo caso, le interfacce di origine devono trovarsi sulla stessa foglia dell'interfaccia di destinazione.

Caso 2. Src "Leaf1 e1/11 e1/34 & filtro EPG1 | Dst " Leaf1 e1/3"



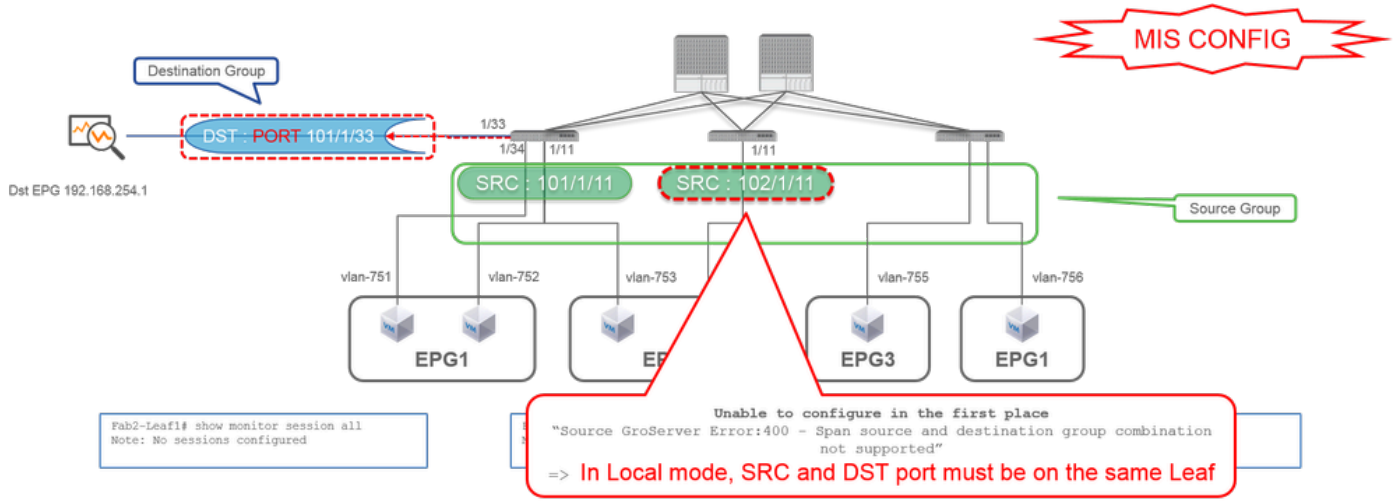
- **Gruppo di origine**
  - Foglia 1 e1/11
  - Foglia 1 e1/34
  - Filtro EPG1

- **Gruppo di destinazione**

- Foglia 1 e1/3

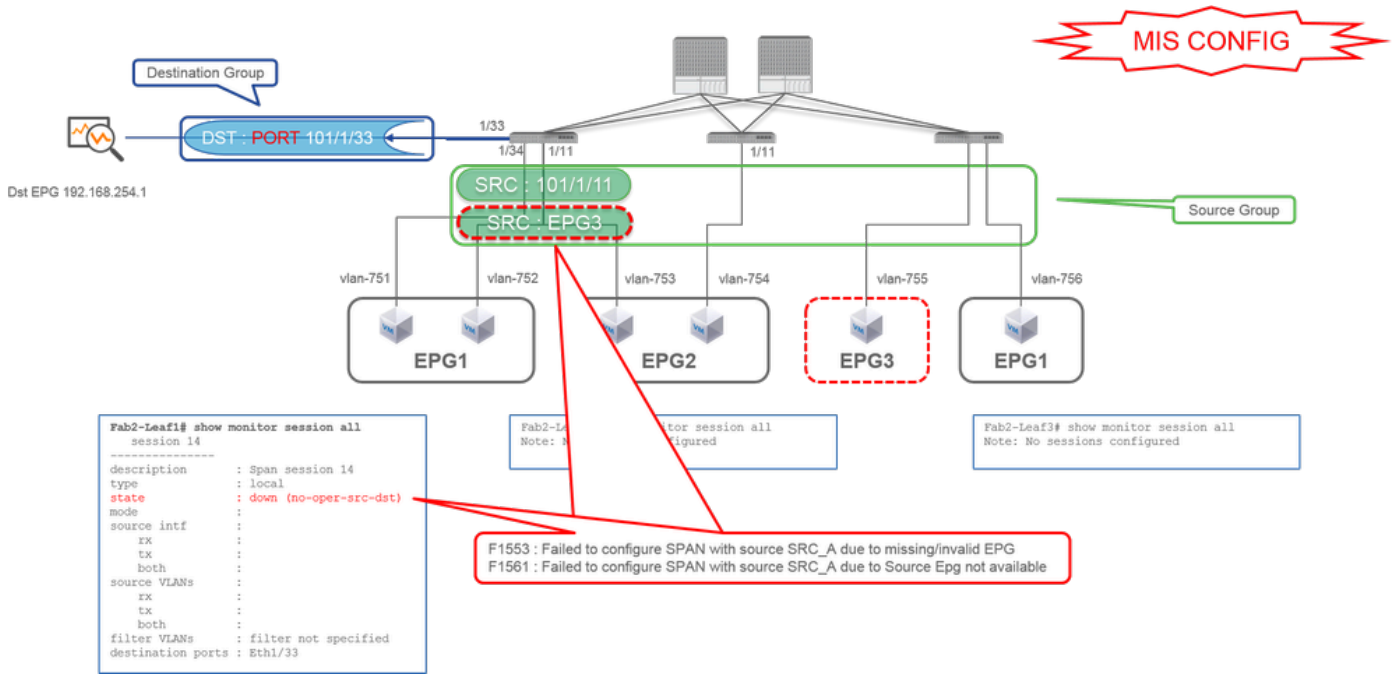
Access SPAN con Local SPAN può anche usare EPG Filter ed ERSPAN.

Caso 3. Src "Leaf1 e1/11 & Leaf2 e/11" | Dst "Leaf1 e1/3" (custodia non valida)



- **Gruppo di origine**
  - Foglia 1 e1/11
  - Foglia2 e1/11
- **Gruppo di destinazione**
  - Foglia 1 e1/3

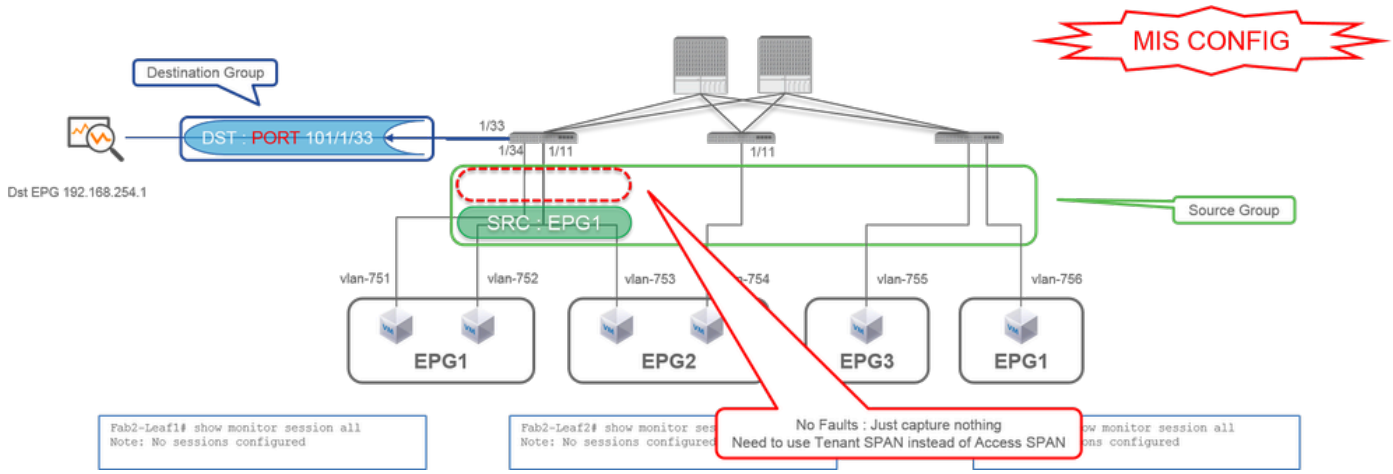
Caso 4. Src "Filtro Leaf1 e1/11 & EPG3" | Dst "Leaf1 e1/3" (custodia non valida)



- **Gruppo di origine**
  - Foglia 1 e1/11
  - Filtro EPG3
- **Gruppo di destinazione**
  - Foglia 1 e1/3

È simile al caso 3 su Access SPAN (ERSPAN), ma in questo esempio, l'unica sessione SPAN su Leaf1 ha esito negativo perché EPG3 non esiste su Leaf1. Quindi SPAN non funziona affatto.

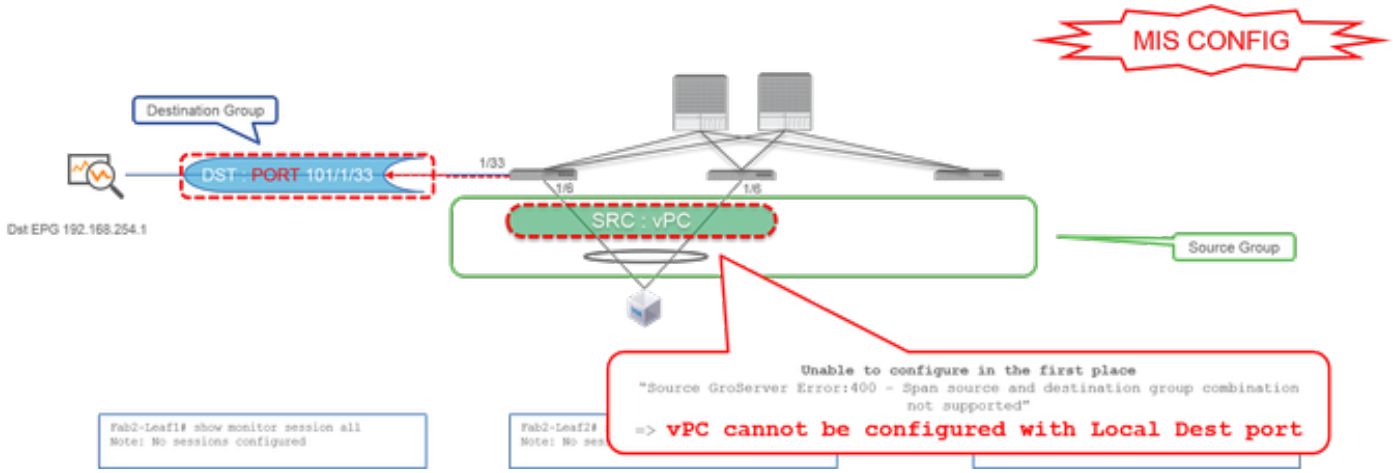
Caso 5: Src "EPG1 filter" | Dst "Leaf1 e1/3" (custodia non valida)



- **Gruppo di origine**
  - Filtro EPG1
- **Gruppo di destinazione**
  - Foglia 1 e1/3

Il filtro EPG su Access SPAN funziona solo quando le porte di origine sono configurate. Se EPG è l'unica origine da specificare, utilizzare Tenant SPAN anziché Access SPAN.

Caso 6. Src "Leaf1 - Leaf2 vPC" | Dst "Leaf1 e1/3" (custodia non valida)

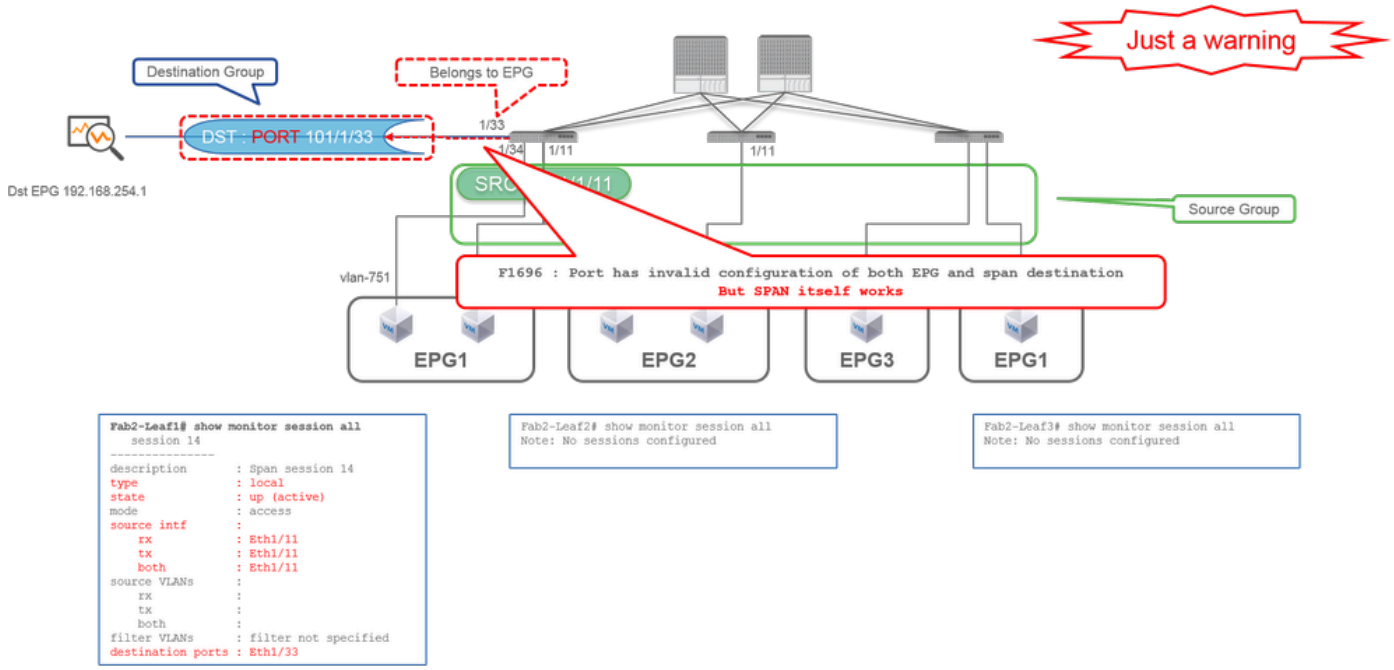


- **Gruppo di origine**
  - vPC foglia1-2

- **Gruppo di destinazione**
  - Foglia 1 e1/3

Impossibile configurare un'interfaccia vPC come origine con SPAN locale. Utilizzare ERSPAN. Fare riferimento alla richiesta case4 per Access SPAN (ERSPAN).

Caso 7. Src "Leaf1 e1/11 | Dst "Leaf1 e1/33 & e1/33 appartiene a EPG" (funziona con errore)

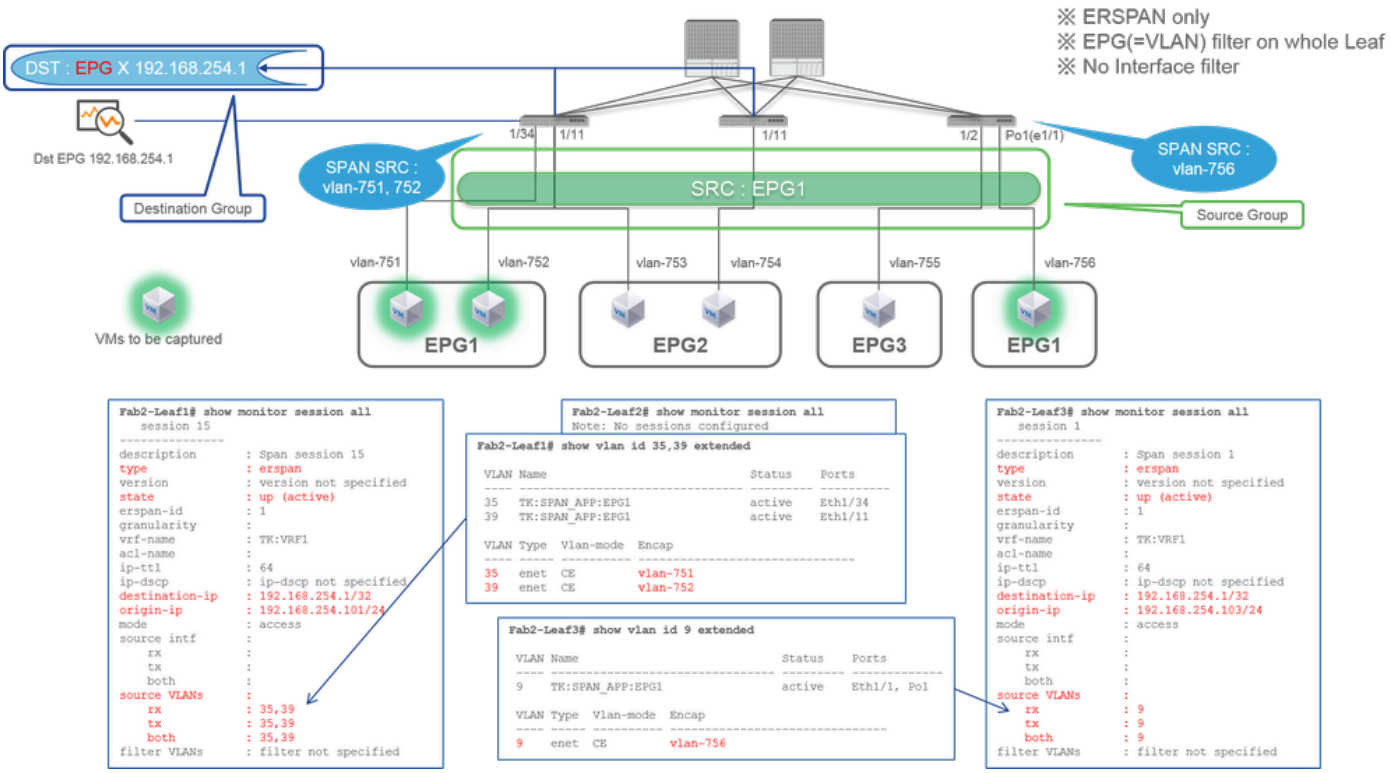


Se un I/F di destinazione per SPAN appartiene già a EPG, viene generato un errore "F1696 : Port has an invalid configuration of both EPG and span destination" (F1696: la porta ha una configurazione non valida sia di EPG che di span destination) nell'I/F fisico.

Ma anche con questo errore, SPAN funziona senza alcun problema. Questo errore è solo un avviso relativo al traffico aggiuntivo causato dall'SPAN, in quanto può influire sul normale traffico EPG dei clienti sullo stesso I/F.

ERSPAN (Tenant SPAN)

Caso 1. Src EPG1 | Dst "192.168.254.1"



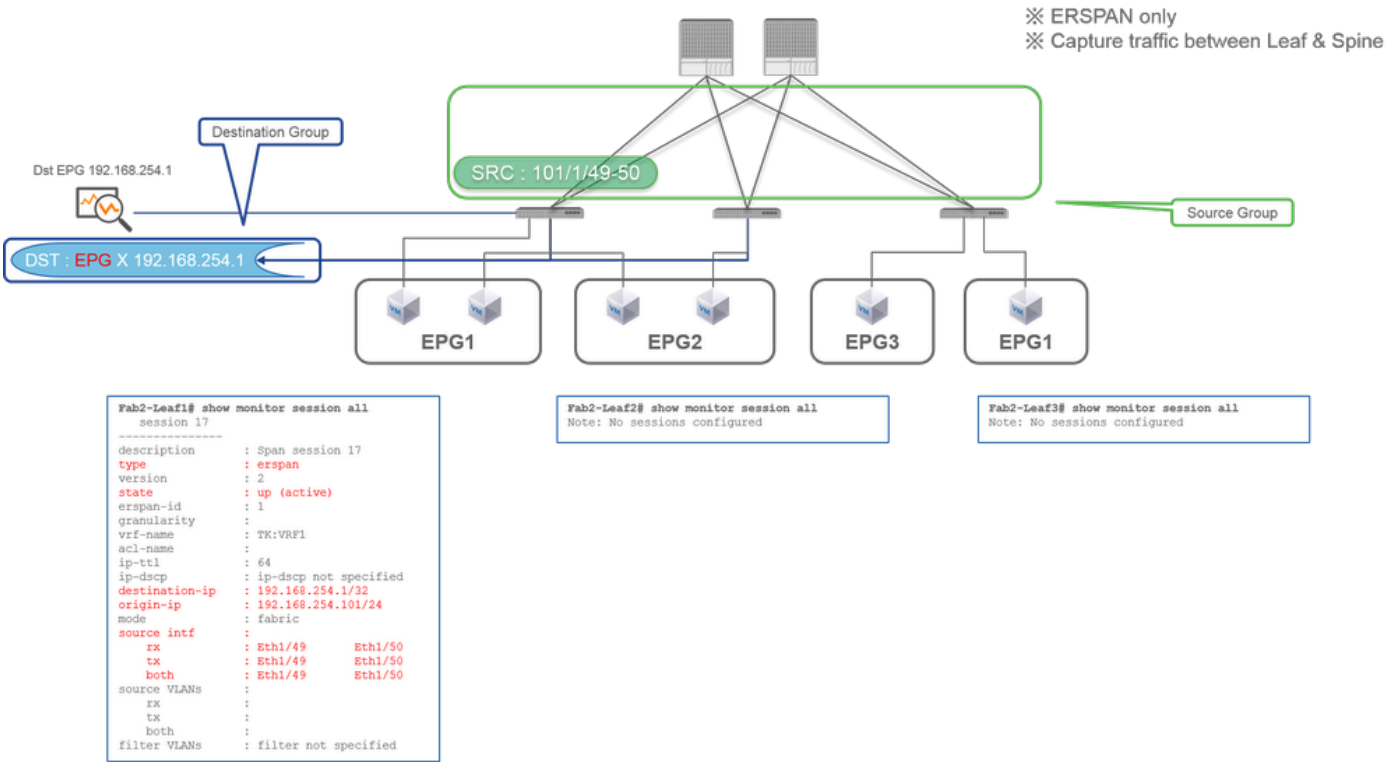
- **Gruppo di origine**
  - EPG1 (nessun filtro)
- **Gruppo di destinazione**
  - 192.168.254.1 su EPG X

L'SPAN tenant utilizza lo stesso EPG come origine mentre l'SPAN di Access utilizza EPG solo per un filtro.

Il punto chiave dell'SPAN tenant è che non è necessario specificare ciascuna porta e l'ACI rileva automaticamente le VLAN appropriate su ciascuno switch foglia. Ciò è utile quando tutti i pacchetti per EPG specifici devono essere monitorati e gli endpoint per EPG specifico appartengono a più interfacce su switch foglia.

ERSPAN (Fabric SPAN)

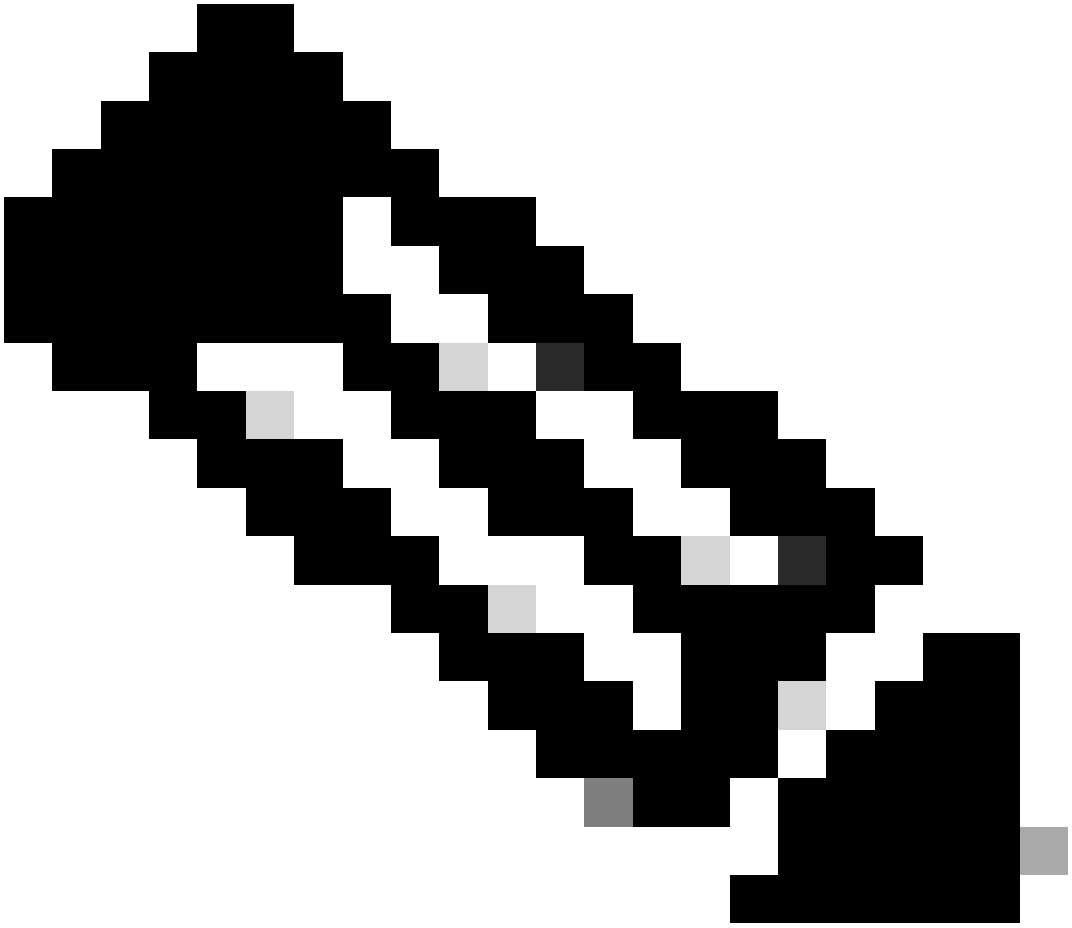
Caso 1. Src "Leaf1 e1/49-50" | Dst "192.168.254.1"



- **Gruppo di origine**
  - Foglia1 e1/49-50
- **Gruppo di destinazione**
  - 192.168.254.1 su EPG X

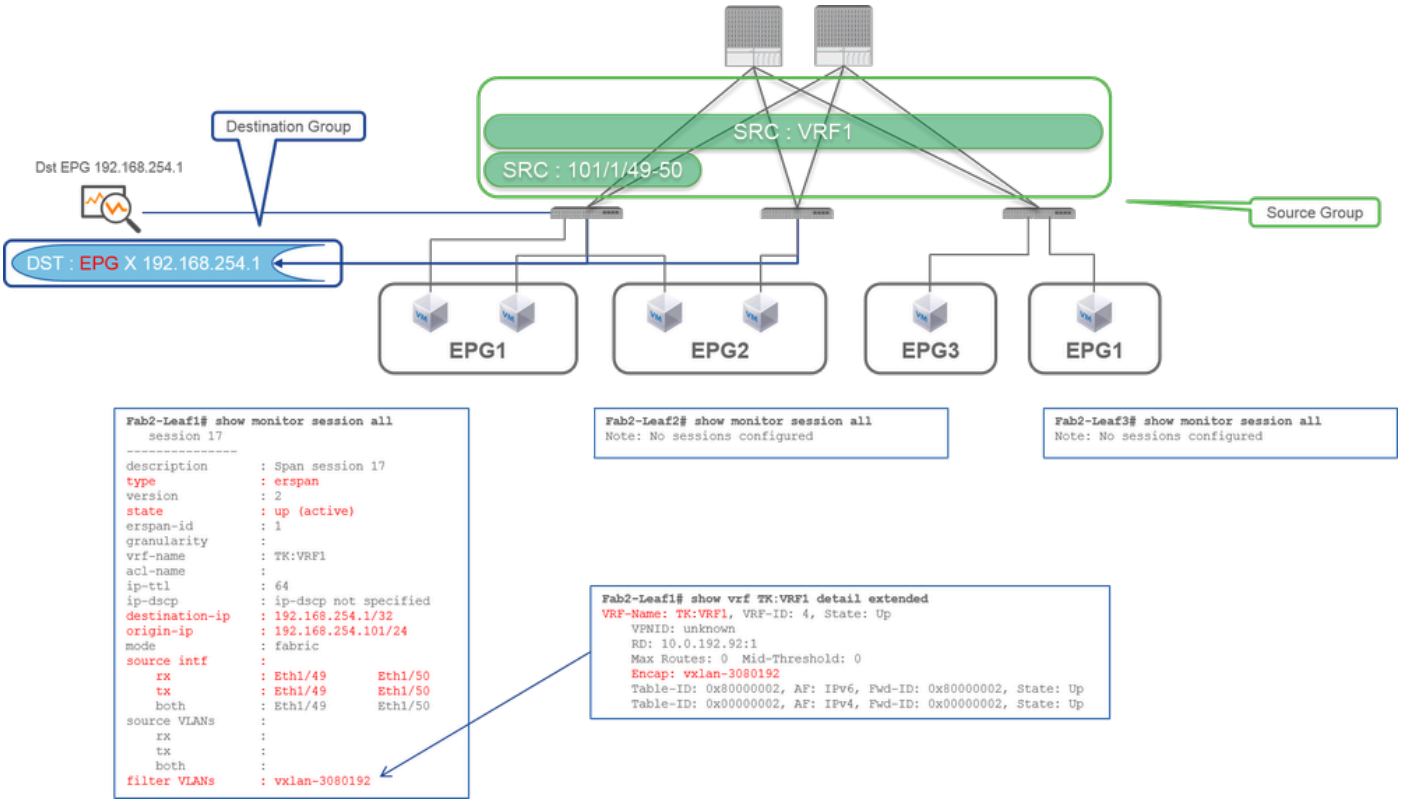
Fabric SPAN specifica le porte Fabric come origine in cui le porte Fabric sono interfacce tra switch Leaf e Spine.

Questo SPAN è utile quando è necessario copiare pacchetti tra switch Leaf e Spine. Tuttavia, i pacchetti tra gli switch Leaf e Spine sono incapsulati con intestazione ViXLAN. Per leggerlo è necessario un po' di trucco. Consultare "Come leggere i dati SPAN".



Nota: l'intestazione iVxLAN è un'intestazione VxLAN migliorata solo per uso interno ACI Fabric.

Caso 2. Src "Leaf1 e1/49-50 & VRF filter" | Dst "192.168.254.1"



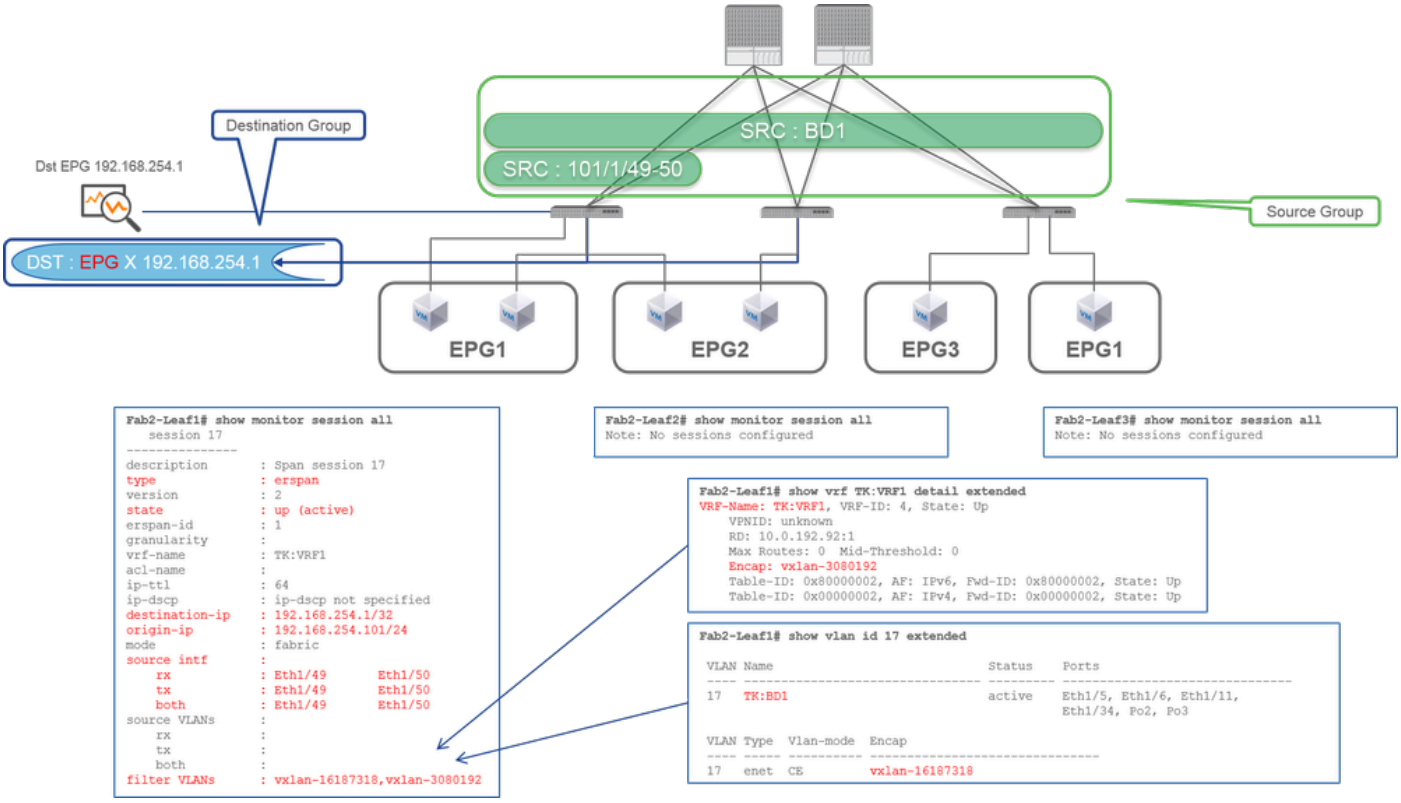
- **Gruppo di origine**
  - Foglia1 e1/49-50
  - Filtro VRF
- **Gruppo di destinazione**
  - 192.168.254.1 su EPG X

Fabric SPAN può utilizzare filtri oltre ad Access SPAN. Ma il tipo di filtro è diverso. L'SPAN del fabric utilizza il routing e l'inoltro virtuali (VRF) o BD come filtro.

In Cisco ACI, come descritto sopra, i pacchetti che passano attraverso le porte Fabric sono incapsulati con l'intestazione ViXLAN. Questa intestazione iVxLAN contiene informazioni VRF o BD come VNID (Virtual Network Identifier). Quando i pacchetti vengono inoltrati come layer 2 (L2), iVxLAN VNID è l'acronimo di BD. Quando i pacchetti vengono inoltrati come layer 3 (L3), iVxLAN VNID è l'acronimo di VRF.

Pertanto, quando è necessario acquisire il traffico indirizzato sulle porte Fabric, utilizzare VRF come filtro.

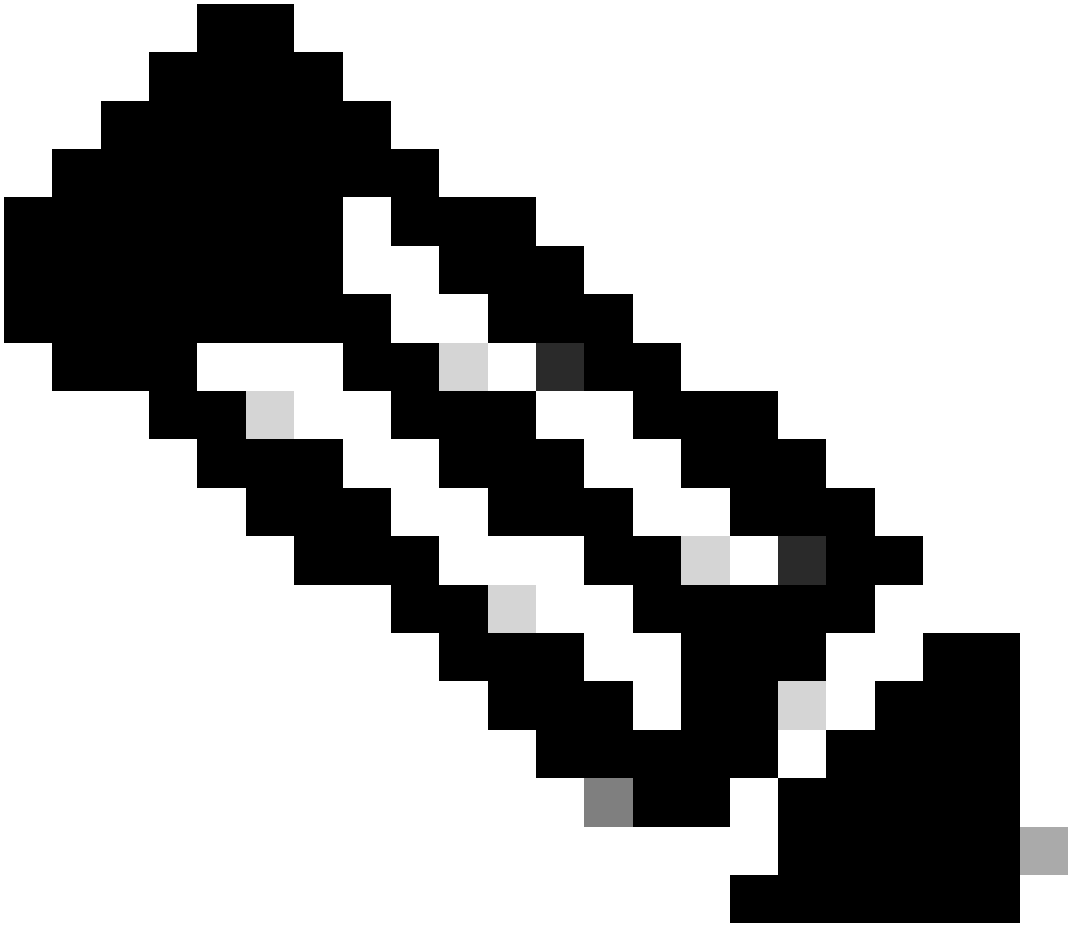
Caso 3. Src "Leaf1 e1/49-50 & BD filter" | Dst "192.168.254.1"



- **Gruppo di origine**
  - Foglia1 e1/49-50
  - Filtro BD
- **Gruppo di destinazione**
  - 192.168.254.1 su EPG X

Come descritto nel caso precedente 2, Fabric SPAN può utilizzare BD come filtro.

Quando è necessario per acquisire il traffico con bridging sulle porte Fabric, utilizzare BD come filtro.



Nota: è possibile configurare un solo filtro di BD o VRF alla volta.

Di cosa avete bisogno sul dispositivo di destinazione SPAN?

È sufficiente eseguire un'applicazione di acquisizione dei pacchetti come quellatcpdump, wireshark. Non è necessario configurare la sessione di destinazione ERSPAN o altro.

Per ERSPAN

Assicurarsi di eseguire uno strumento di acquisizione sull'interfaccia con l'IP di destinazione per ERSPAN, poiché i pacchetti SPAN vengono inoltrati all'IP di destinazione.

Il pacchetto ricevuto è incapsulato con un'intestazione GRE. Consultare questa sezione "Come leggere i dati ERSPAN" su come decodificare l'intestazione GRE ERSPAN.

Per Local SPAN

Assicurarsi di eseguire uno strumento di acquisizione sull'interfaccia che si connette all'interfaccia di destinazione SPAN su ACI Leaf.

Pacchetti non elaborati ricevuti in questa interfaccia. Non è necessario gestire l'intestazione ERSPAN.

Come leggere i dati ERSPAN

Versione ERSPAN (tipo)

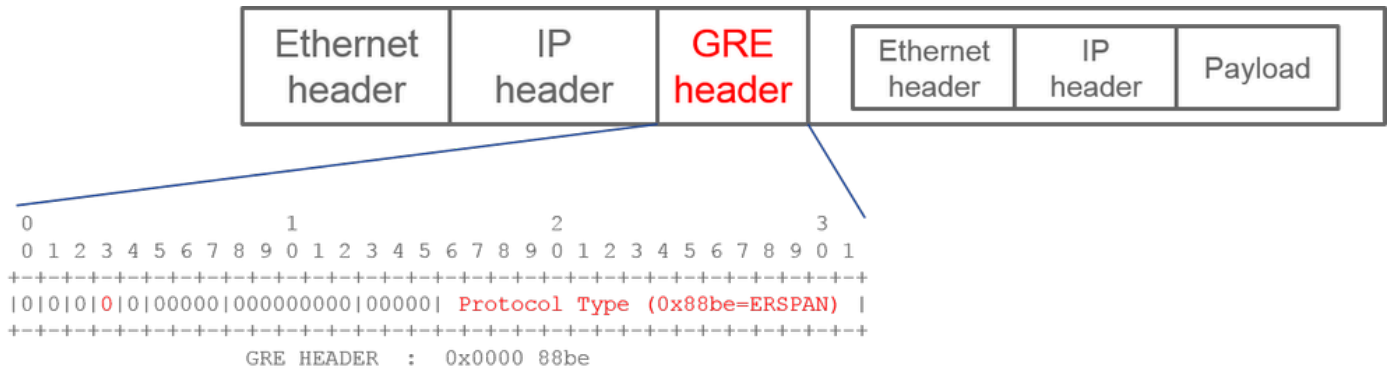
ERSPAN incapsula i pacchetti copiati per inoltrarli alla destinazione remota. GRE viene usato per questo incapsulamento. Il tipo di protocollo per ERSPAN sull'intestazione GRE è 0x88be.

Nel documento della Internet Engineering Task Force (IETF), la versione ERSPAN è descritta come tipo anziché versione.

Esistono tre tipi di ERSPAN. I, II e III. Il tipo ERSPAN è menzionato in questa bozza RFC. Inoltre, questa RFC1701 del GRE può essere utile per comprendere anche ciascun tipo ERSPAN.

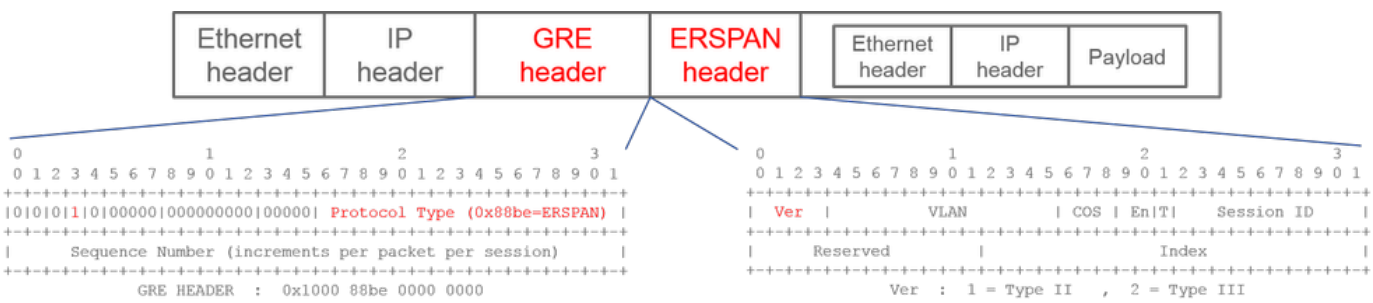
Di seguito viene riportato il formato di ciascun tipo di pacchetto:

ERSPAN tipo I (utilizzato da Broadcom Trident 2)



Il tipo I non utilizza il campo della sequenza nell'intestazione GRE. Non utilizza nemmeno l'intestazione ERSPAN che deve essere sostituita dall'intestazione GRE se si tratta di ERSPAN di tipo II e III. Broadcom Trident 2 supporta solo questo ERSPAN di tipo I.

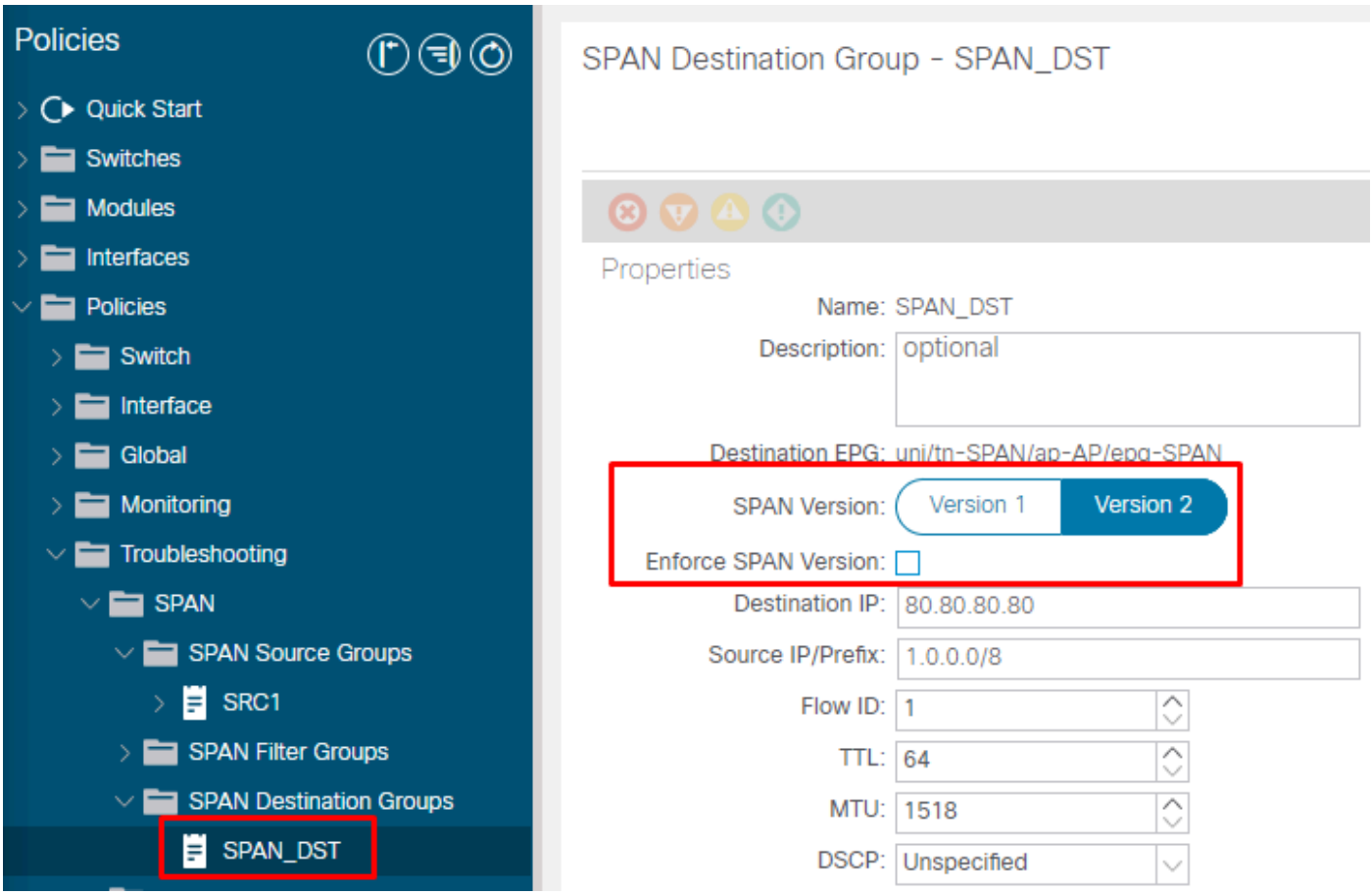
ERSPAN tipo II o III



Se il campo della sequenza è attivato dal bit S, deve essere ERSPAN tipo II o III. Il campo della versione nell'intestazione ERSPAN identifica il tipo ERSPAN. In ACI, il tipo III non è supportato a partire dal 20/03/2016.

Se un gruppo di origini SPAN per Access o Tenant SPAN ha origini sia su nodi di prima generazione che su nodi di seconda generazione, la destinazione ERSPAN riceve entrambi i pacchetti ERSPAN di tipo I e II da ciascuna generazione di nodi. Tuttavia, Wireshark può decodificare solo uno dei tipi ERSPAN alla volta. Per impostazione predefinita, decodifica solo ERSPAN di tipo II. Se si attiva la decodifica di ERSPAN di tipo I, Wireshark non decodifica ERSPAN di tipo II. Vedere la sezione successiva su come decodificare ERSPAN Type I su Wireshark.

Per evitare questo tipo di problema, è possibile configurare il tipo ERSPAN su un gruppo di destinazione SPAN.



- SPAN versione 1 o versione 2: si riferisce a ERSPAN tipo I o II

- Applica versione SPAN (selezionata o deselezionata): questa opzione consente di stabilire se la sessione SPAN deve avere esito negativo nel caso in cui il tipo ERSPAN configurato non sia supportato nell'hardware del nodo di origine.

Per impostazione predefinita, la versione SPAN è la versione 2 e l'opzione Applica versione SPAN è deselezionata. Ciò significa che se il nodo di origine è di seconda generazione o successiva e supporta ERSPAN di tipo II, verrà generato ERSPAN con tipo II. Se il nodo di origine è di prima generazione e non supporta ERSPAN di tipo II (ad eccezione di Fabric SPAN), viene ripristinato il tipo I poiché l'opzione Applica versione SPAN non è selezionata. Di conseguenza, la destinazione ERSPAN riceve un tipo misto di ERSPAN.

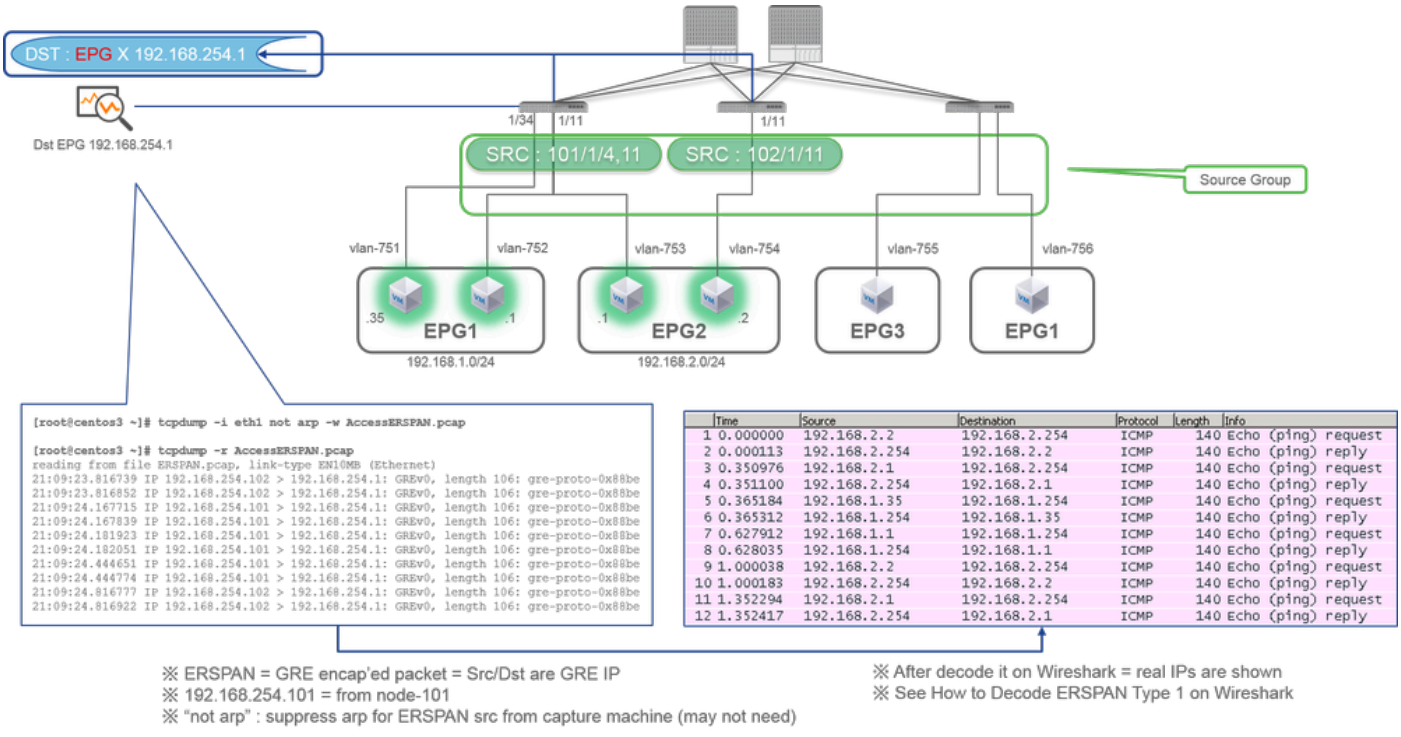
In questa tabella viene illustrata ogni combinazione di Access e Tenant SPAN.

Versione	Imponi versione	nodo di origine di prima	nodo di origine di seconda

SPAN	SPAN	generazione	generazione
Versione 2	Deselezionato	Utilizza tipo I	Utilizza Type II
Versione 2	Controllato	Non riuscito	Utilizza Type II
Versione 1	Deselezionato	Utilizza tipo I	Utilizza tipo I
Versione 1	Controllato	Utilizza tipo I	Utilizza tipo I

Esempio di dati ERSPAN

ERSPAN (Tenant SPAN/Access SPAN)



I pacchetti devono essere decodificati perché sono incapsulati da ERSPAN tipo I. Questa operazione può essere effettuata con Wireshark. Consultare la sezione "Come decodificare ERSPAN tipo 1".

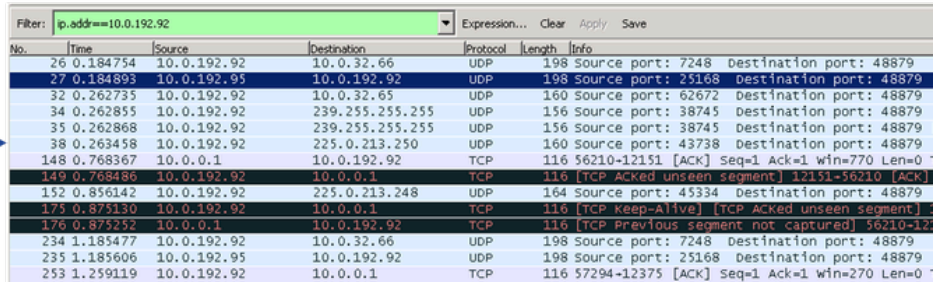
Dettagli del pacchetto catturato (ERSPAN tipo I)

```
[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        ESPAN Ethernet header         : Dst 0050.56bb.3096 , Src 0022.bdf8.19.ff
        0x0020:  fe01 0000 88be 0022 bdf8 19ff 0050 56bb        ERSPAN IP header              : Dst 192.168.254.1  , Src 192.168.254.102
        0x0030:  d6c2 8100 02f2 0800 4500 0054 0000 4000        GRE header (= ERSPAN Type I)  : 0x88be = ERSPAN (S bit off 0x0000)
        0x0040:  4001 b458 c0a8 0202 c0a8 02fe 0800 34cc        Ethernet header               : Dst 0022.bdf8.19ff , Src 0050.56bb.d6c2
        0x0050:  c847 0115 7404 2b56 0000 0000 8da9 0e00        Dot1Q header                  : VLAN 754
        0x0060:  0000 0000 1011 1213 1415 1617 1819 1a1b        IP header                     : Dst 192.168.2.254  , Src 192.168.2.2
        0x0070:  1c1d 1e1f 2021 2223 2425 2627 2829 2a2b
        0x0080:  2c2d 2e2f 3031 3233 3435 3637
```

ERSPAN (Fabric SPAN)

```
[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



Wireshark decodifica automaticamente ERSPAN Tipo II. Tuttavia, è ancora incapsulato dall'intestazione iVxLAN.

Per impostazione predefinita, Wireshark non riconosce l'intestazione iVxLAN in quanto è un'intestazione interna ACI. Fare riferimento a "Come decodificare l'intestazione VLAN".

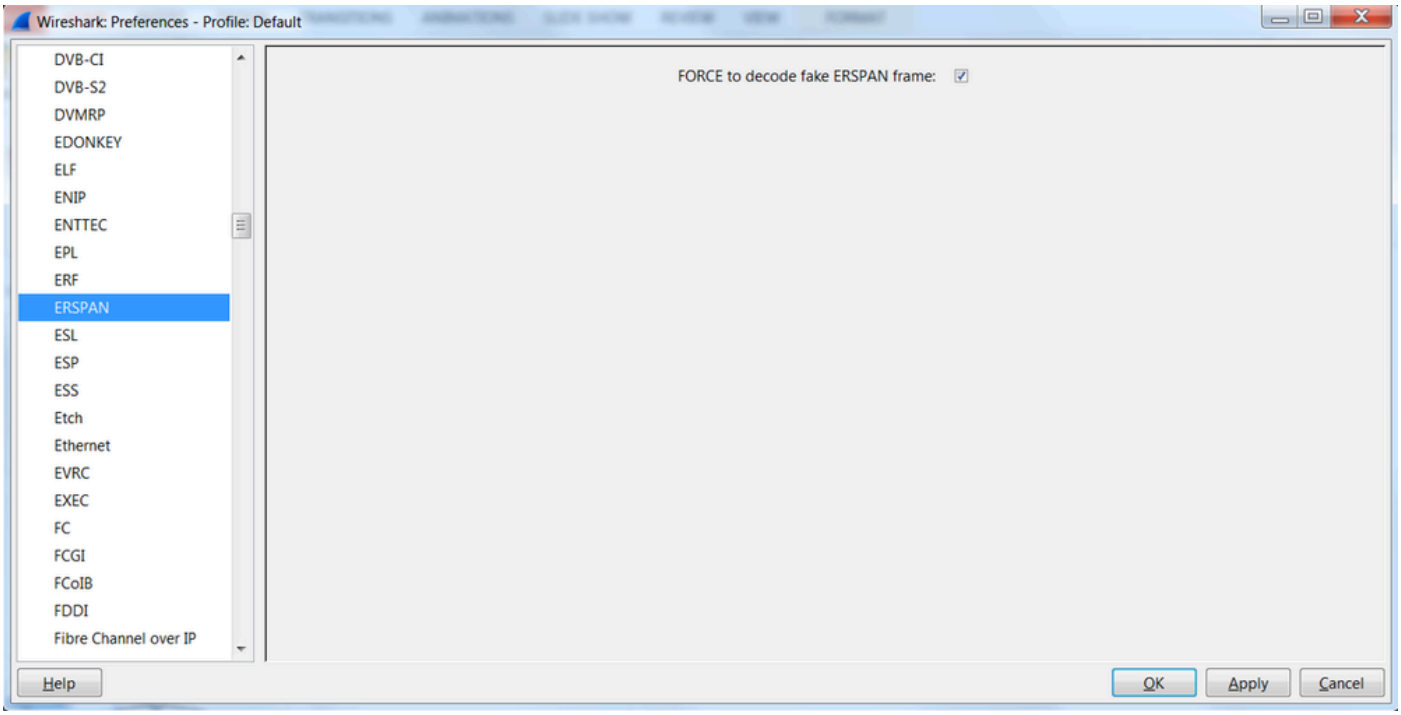
Dettagli del pacchetto catturato (ERSPAN tipo II)

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

Come decodificare ERSPAN Tipo I

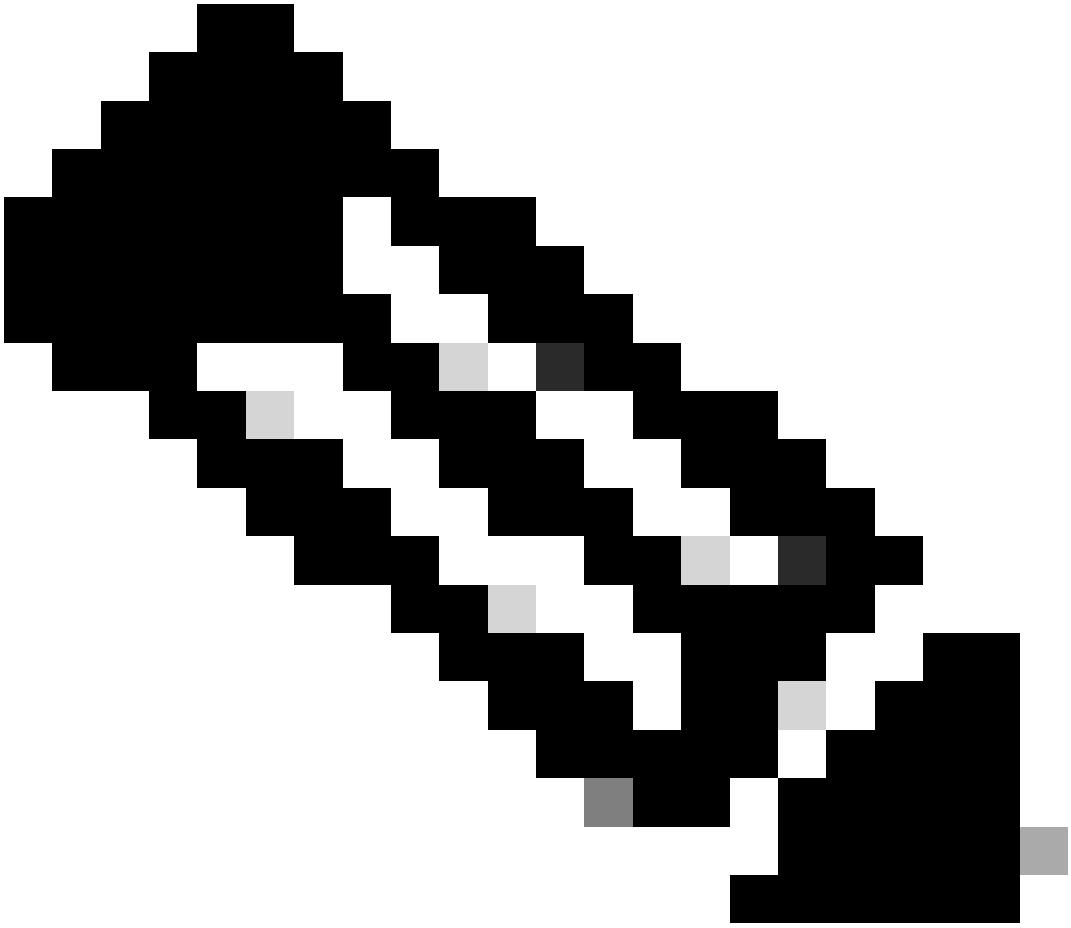
Opzione 1. Individuare Edit > Preference > Protocols > ERSPAN e selezionare FORCE per decodificare il frame ERSPAN falso.

- Wireshark (interfaccia)



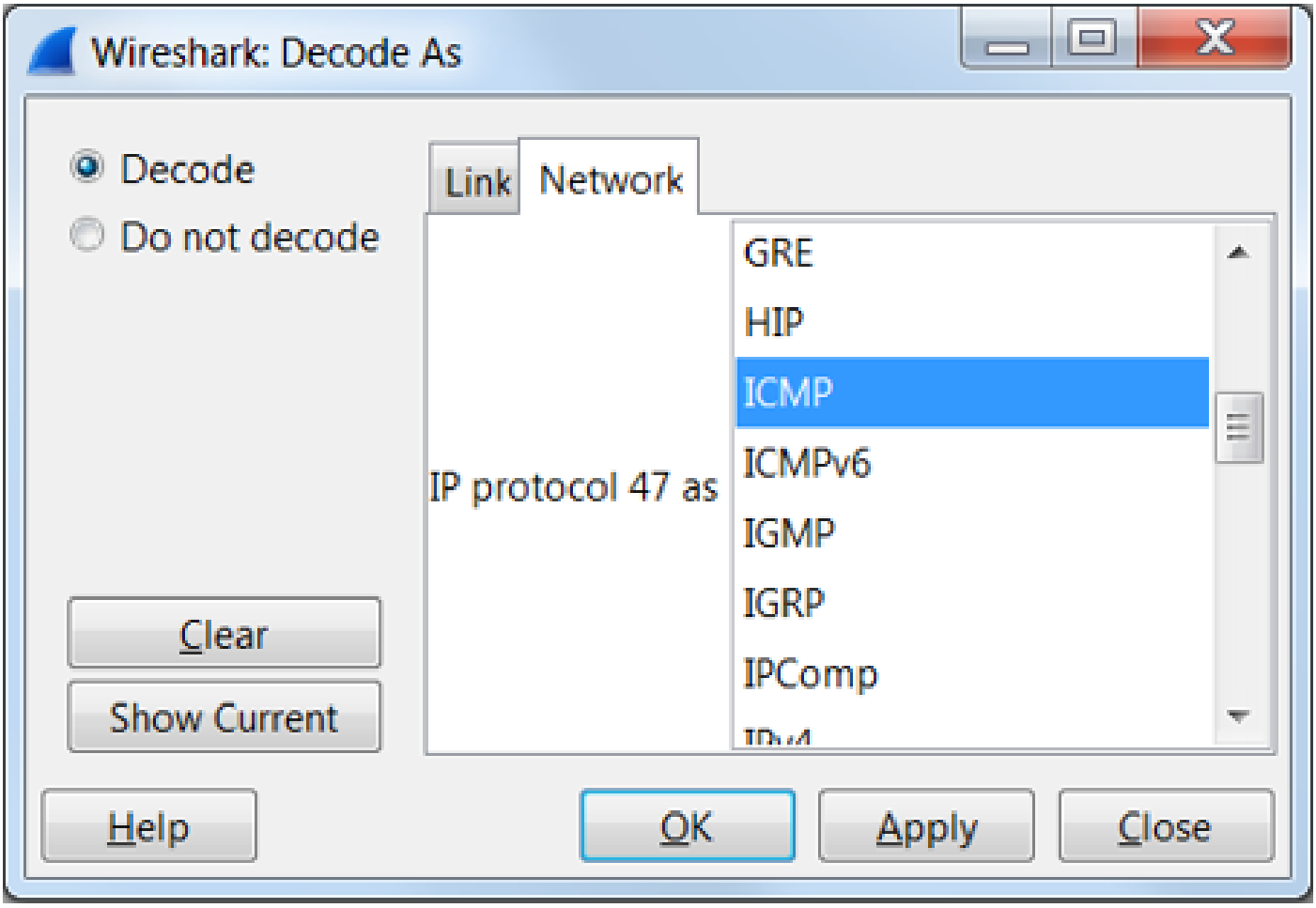
- Tshark (versione CLI di Wireshark):

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

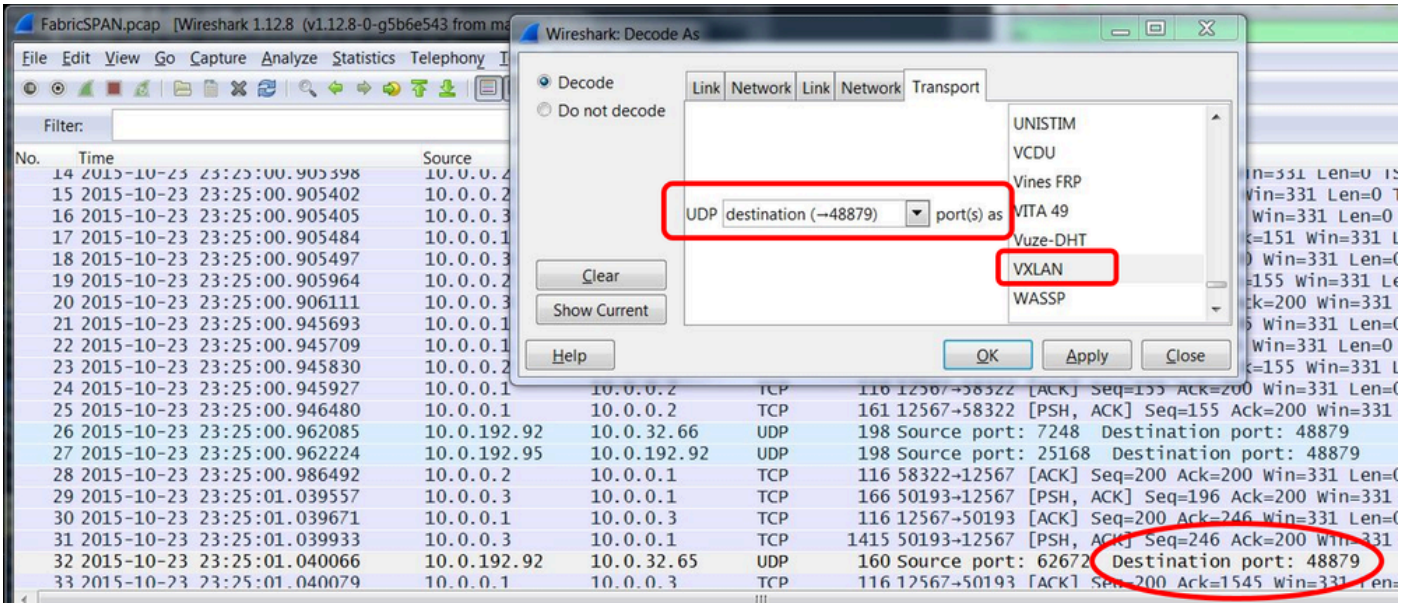


Nota: accertarsi di disattivare questa opzione quando si legge ERSPAN tipo II o III.

Opzione 2. Passa a Decode As > Network > ICMP (if it’s ICMP).



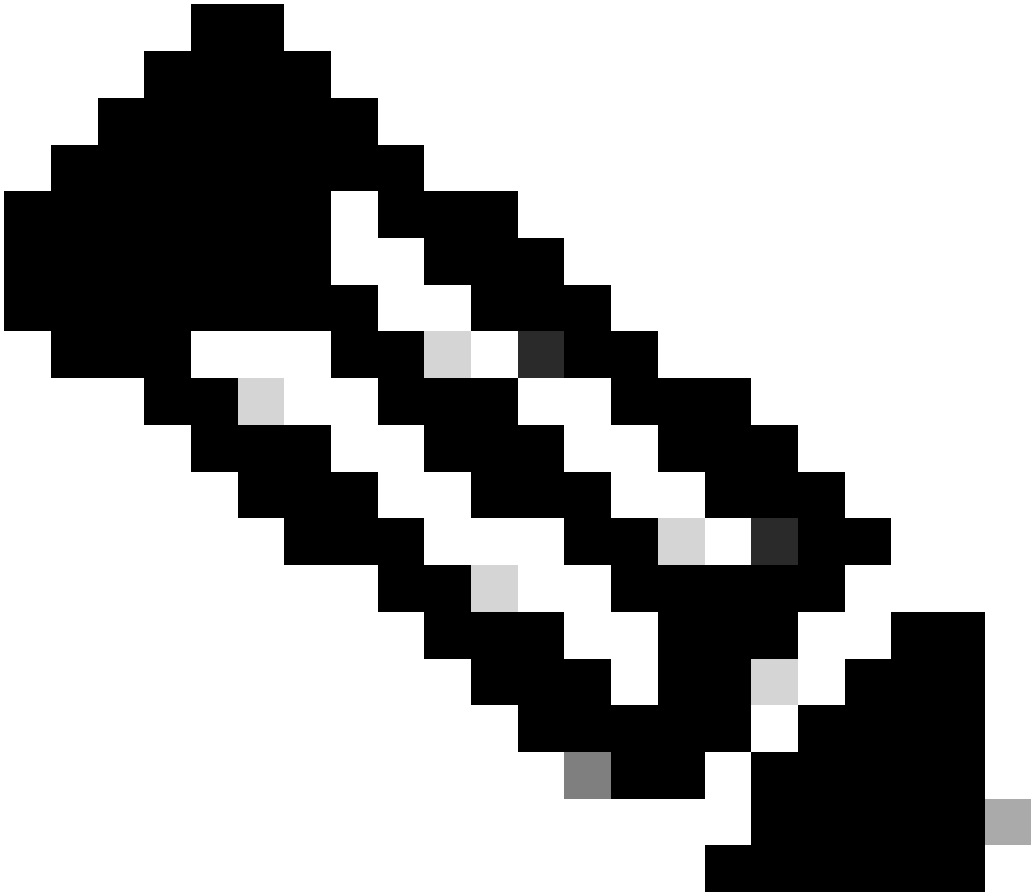
Come decodificare l'intestazione VLAN



L'intestazione della VLAN utilizza la porta di destinazione 4879. Pertanto, è possibile decodificare l'intestazione VxLAN e la VxLAN se si configura la porta di destinazione UDP 4879 come VxLAN su Wireshark.

- Accertarsi di selezionare prima i pacchetti incapsulati VLAN.

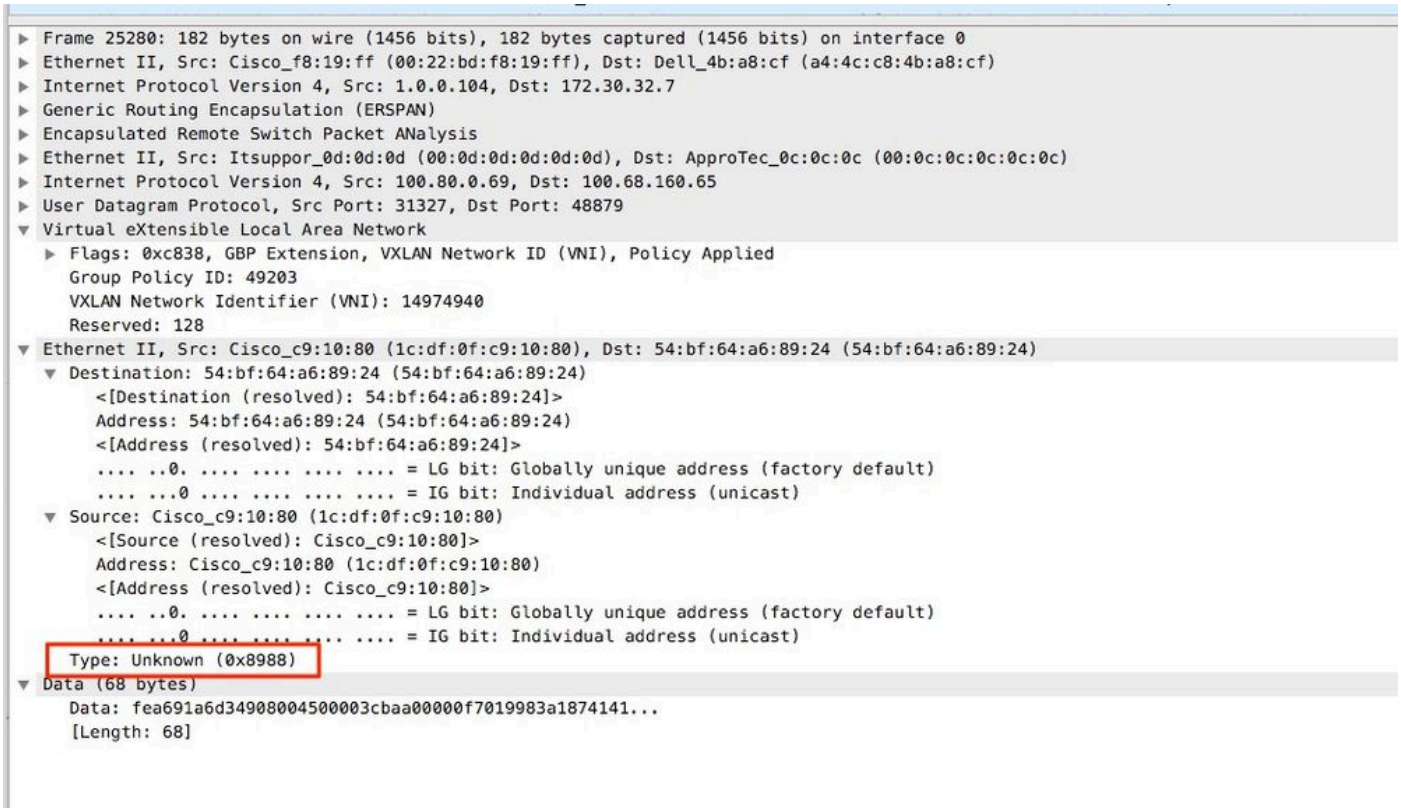
- Passare a Analyze > Decode As > Transport > UDP destination (48879) > VxLAN.
- E poi Apply.



Nota: sono presenti pacchetti di comunicazione tra dispositivi APIC sulle porte dell'infrastruttura. Questi pacchetti non sono incapsulati dall'intestazione ViXLAN.

Quando si esegue un'acquisizione erspan su una rete utente con protocollo PTP (Precision Time Protocol), a volte si rileva che Wireshark non interpreta i dati a causa di un ethertype sconosciuto all'interno dell'encap GRE (0x8988). 0x8988 è l'ethertype del tag time inserito nei pacchetti

del datapane quando PTP è abilitato. Decodificare l'ethertype 0x8988 come "Cisco tag" per esporre i dettagli del pacchetto.



Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).