ACI SPAN-Leitfaden

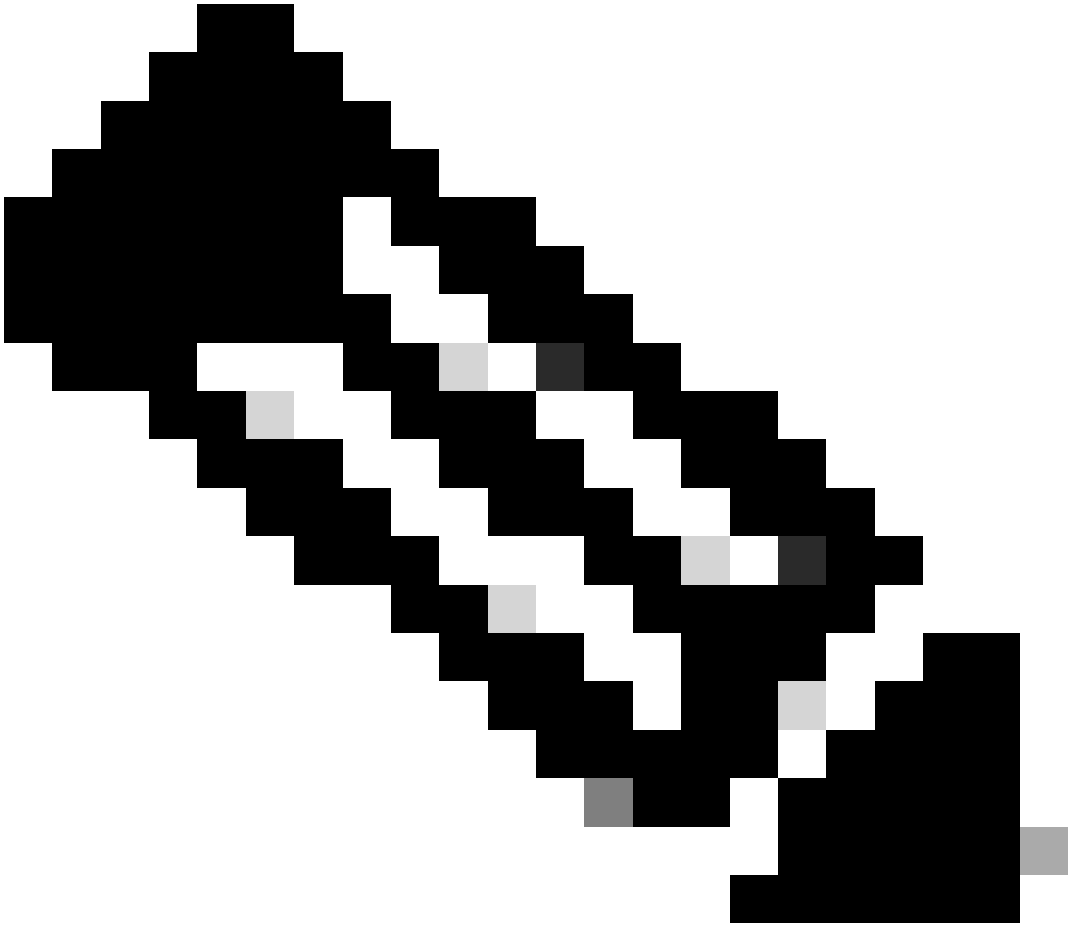
Inhalt

Einleitung

In diesem Dokument wird die Konfiguration von Switched Port Analyzer (SPAN) auf der Cisco Application Centric Infrastructure (ACI) beschrieben.

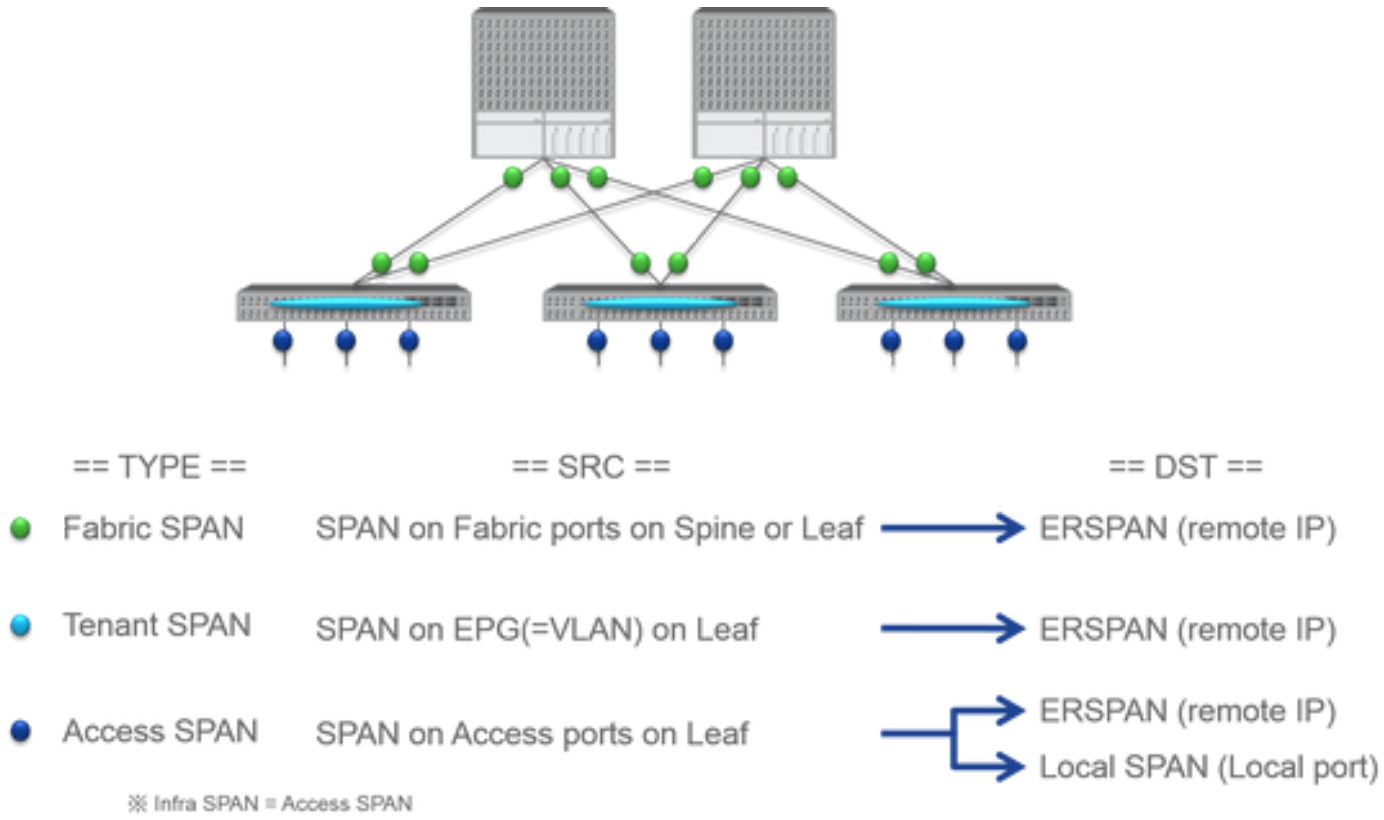
Hintergrundinformationen

Im Allgemeinen gibt es drei Arten von SPAN. Lokales SPAN, Remote SPAN (RSPAN) und Encapsulated Remote SPAN (ERSPAN). Die Unterschiede zwischen diesen SPANs sind hauptsächlich das Ziel von Kopierpaketen. Die Cisco ACI unterstützt Local SPAN und ERSPAN.



Hinweis: In diesem Dokument wird davon ausgegangen, dass die Leser SPAN bereits im Allgemeinen kennen, z. B. lokale SPAN- und ERSPAN-Unterschiede.

SPAN-Typ in Cisco ACI



Die Cisco ACI umfasst drei SPAN-Typen: Fabric SPAN, Tenant SPAN und Access SPAN. Der Unterschied zwischen den einzelnen SPANs ist die Quelle der Kopierpakete.

Wie bereits erwähnt,

- **Fabric SPAN** ist das Erfassen von Paketen, die ein- und ausgehen **interfaces between Leaf and Spine switches**.
    - Access SPAN ist die Erfassung von Paketen, die ein- und ausgeheninterfaces between Leaf switches and external devices.
    - Tenant SPAN ist die Erfassung von Paketen, die ein- und ausgehenEndPoint Group (EPG) on ACI Leaf switches.

Dieser SPAN-Name entspricht dem auf der Cisco ACI-GUI zu konfigurierenden Standort.

- Fabric SPAN wird konfiguriert unter Fabric > Fabric Policies
    - Access SPAN wird konfiguriert unter Fabric > Access Policies

- Tenant-SPAN wird konfiguriert unter Tenants > {each tenant}

Was das Ziel jedes SPAN angeht, so kann nurAccess SPAN sowohl als auch Local SPAN ERSPAN verwendet werden. Die beiden anderen SPANs (Fabric und Tenant) sind nur in der Lage, ERSPAN dies zu tun.

Einschränkungen und Richtlinien

Lesen Sie die Einschränkungen und Richtlinien im Cisco APIC-Fehlerbehebungshandbuch. Sie wird in Troubleshooting Tools and Methodology > Using SPAN erwähnt.

Konfiguration

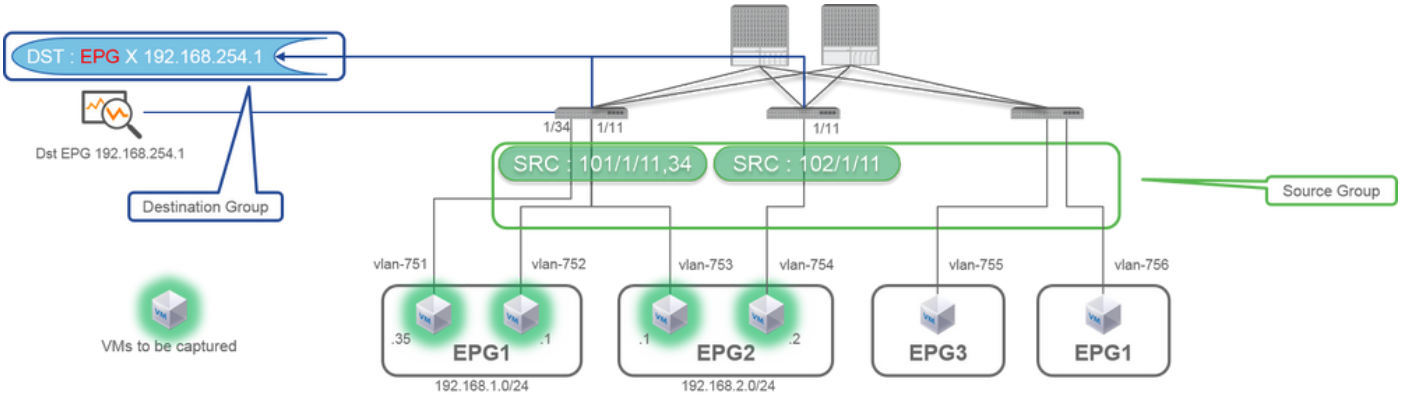
In diesem Abschnitt werden kurze Beispiele vorgestellt, die sich auf die Konfiguration für die einzelnen SPAN-Typen beziehen. Im nachfolgenden Abschnitt finden Sie Beispiele für die Auswahl des Spannentyps.

Die SPAN-Konfiguration wird auch im Cisco APIC Troubleshooting Guide: Troubleshooting Tools and method > Using SPAN beschrieben.

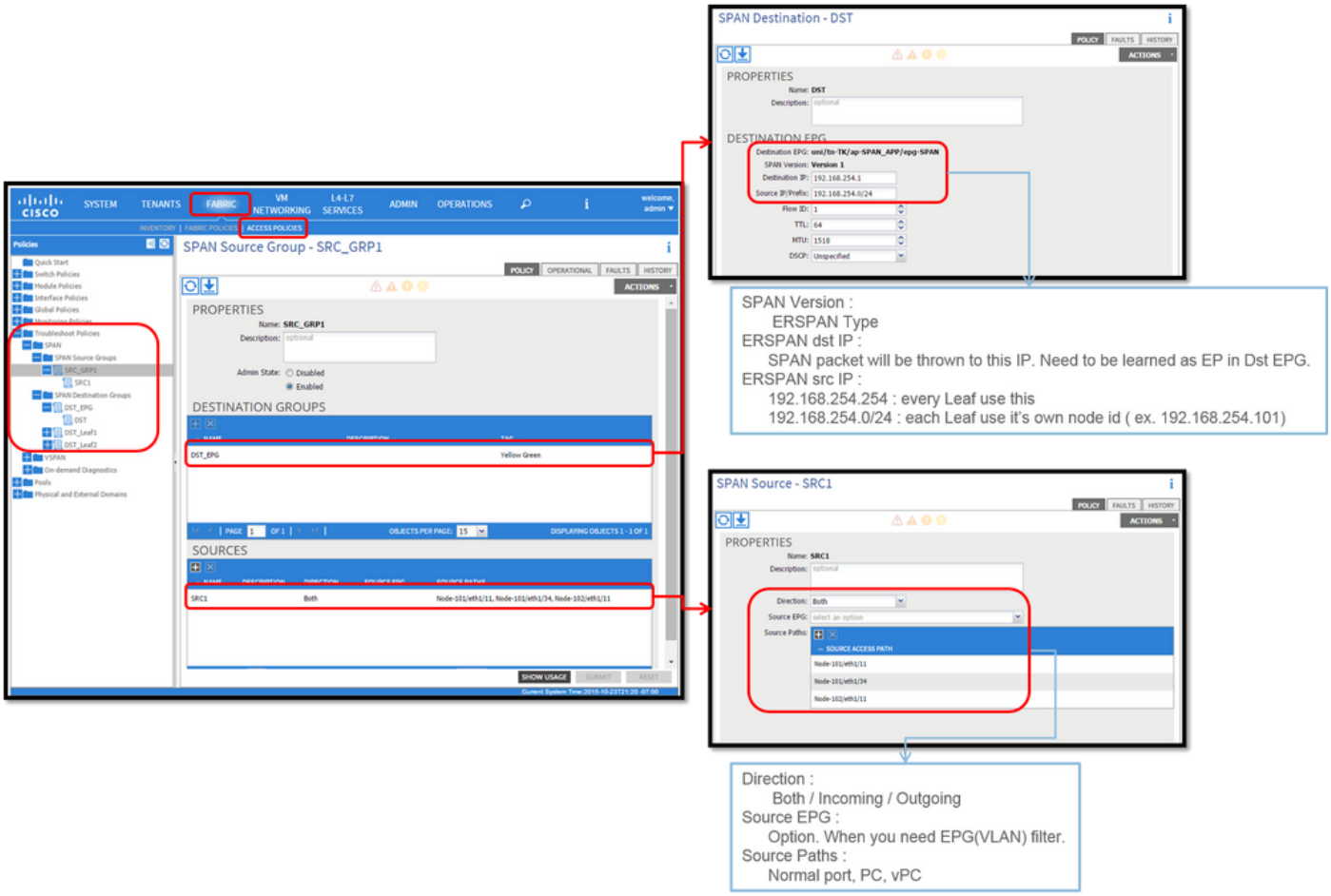
Die Benutzeroberfläche kann sich von der aktuellen Version unterscheiden, die Konfigurationsmethode ist jedoch dieselbe.

Zugangs-SPAN (ERSPAN)

Beispieltopologie



Konfigurationsbeispiel



Dabei gilt:

Navigieren Sie zu FABRIC > ACCESS POLICIES > Troubleshoot Policies > SPAN.

- SPAN Source Groups
    - SPAN Destination Groups

SPAN Source Group Verbindungen Destination und Sources.

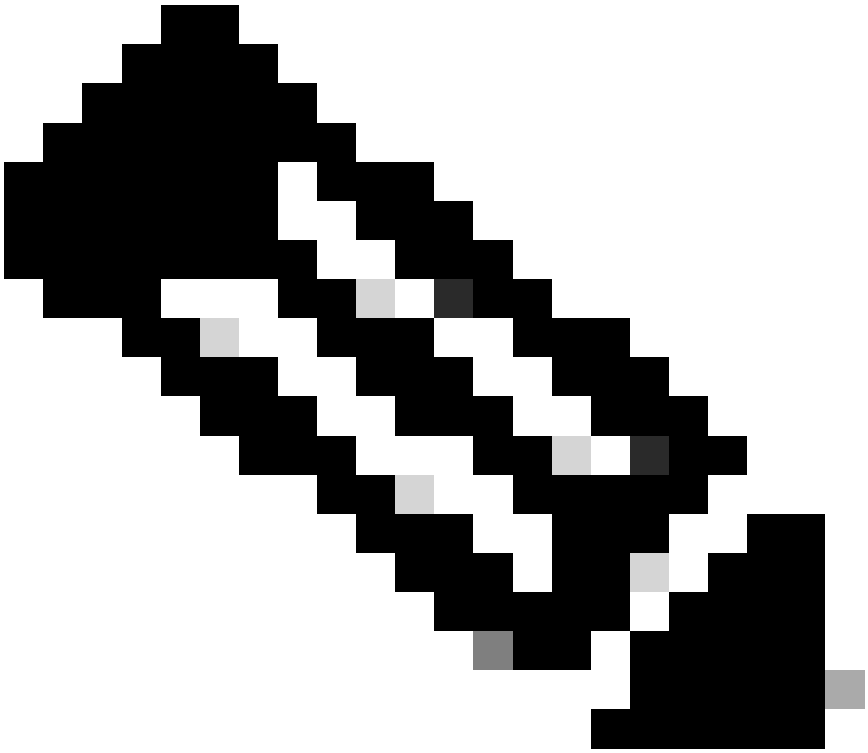
Vorgehensweise:

1. Erstellen SPAN Source Group (SRC_GRP1).

- Erstellen Sie SPAN Source (SRC1) unter SPAN Source Group (SRC_GRP1).

- Konfigurieren Sie diese Parameter für SPAN Source (SRC1).

- Richtung - Quell-EPG (optional)
- Quellpfade (können mehrere Schnittstellen sein)



Hinweis: Details zu den einzelnen Parametern finden Sie im Bild.

- Erstellen SPAN Destination Group (DST_EPG).

- Erstellen SPAN Destination (DST).

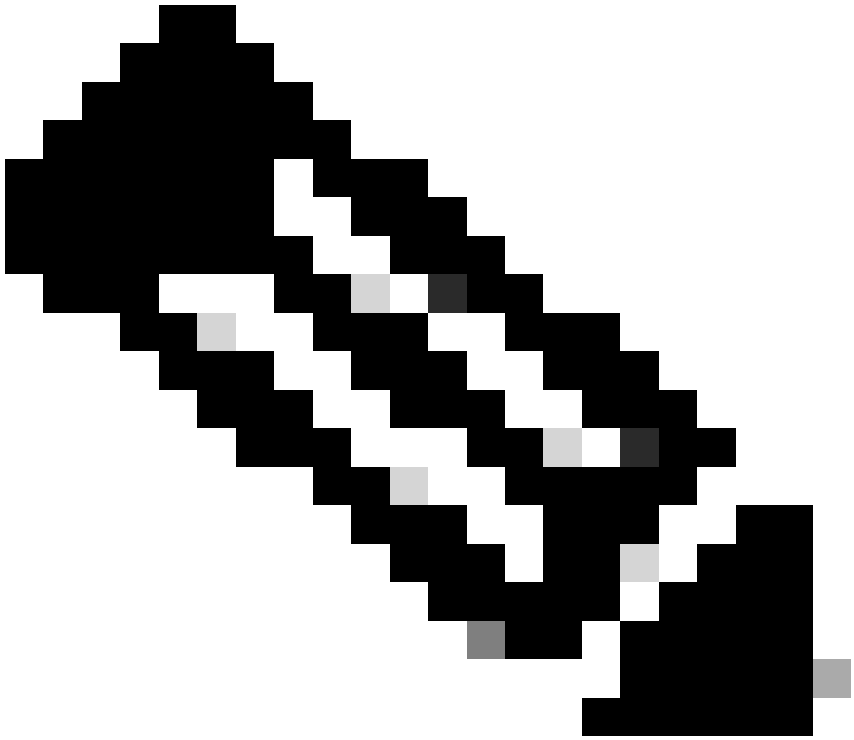
- Konfigurieren Sie diese Parameter für SPAN Destination (DST).

- Ziel-EPG

-Ziel-IP

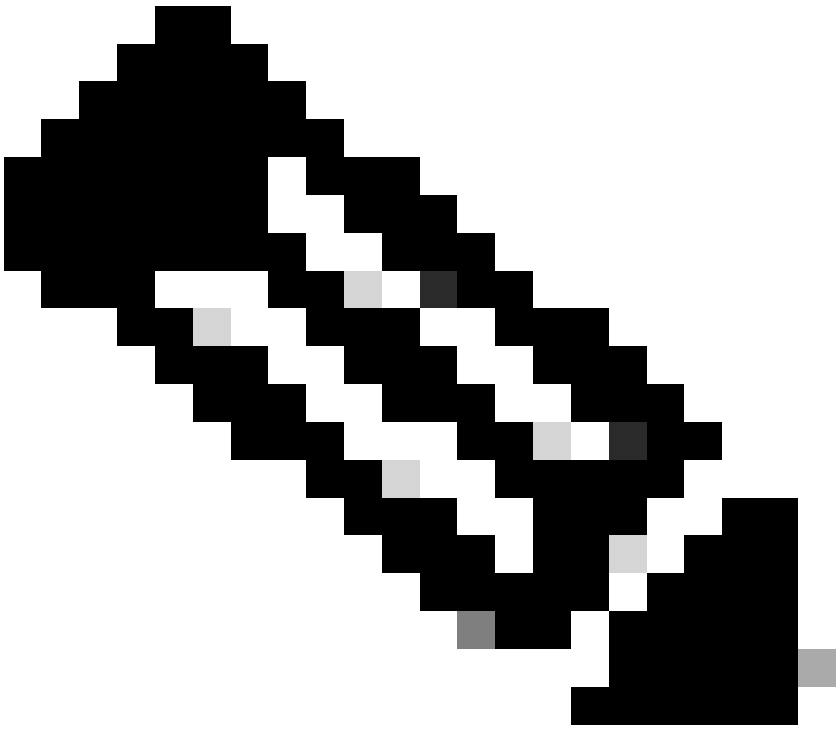
- Quell-IP/Präfix (Dies kann eine beliebige IP sein. Wenn das Präfix verwendet wird, wird die Knoten-ID des Quellknotens für die nicht definierten Bits verwendet. Beispiel: prefix: 1.0.0.0/8 on node-101 => src IP 1.0.0.101)

- Andere Parameter können als Standard beibehalten werden.



Hinweis: Details zu den einzelnen Parametern finden Sie im Bild.

- Stellen Sie sicher,SPAN Destination Group dass eine Bindung zum SPAN Source Group besteht.
- Stellen Sie sicher, Admin Statedass aktiviert ist.

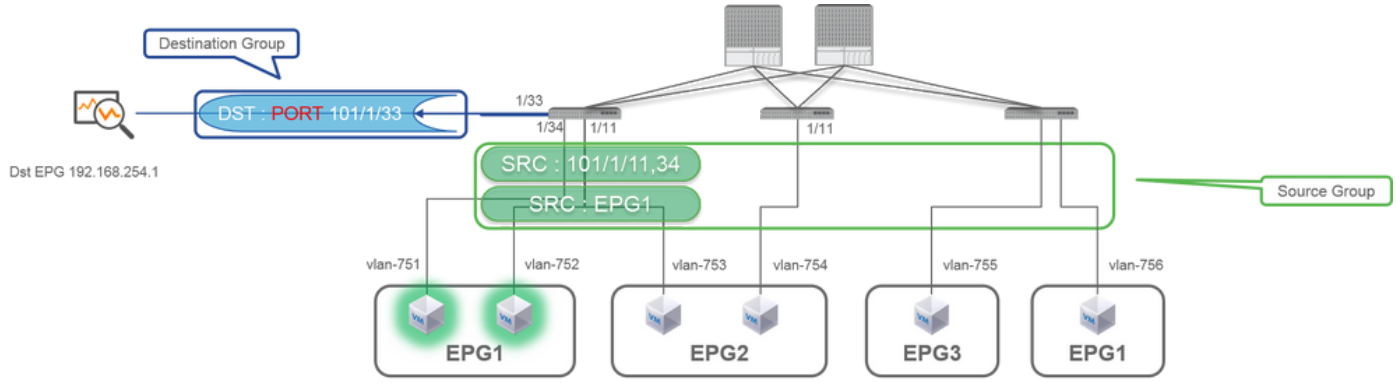


Hinweis: SPAN wird beendet, wenn Sie in diesem Admin-Status Disabled (Deaktiviert) auswählen. Es müssen nicht alle Richtlinien gelöscht werden, wenn Sie sie später wiederverwenden.

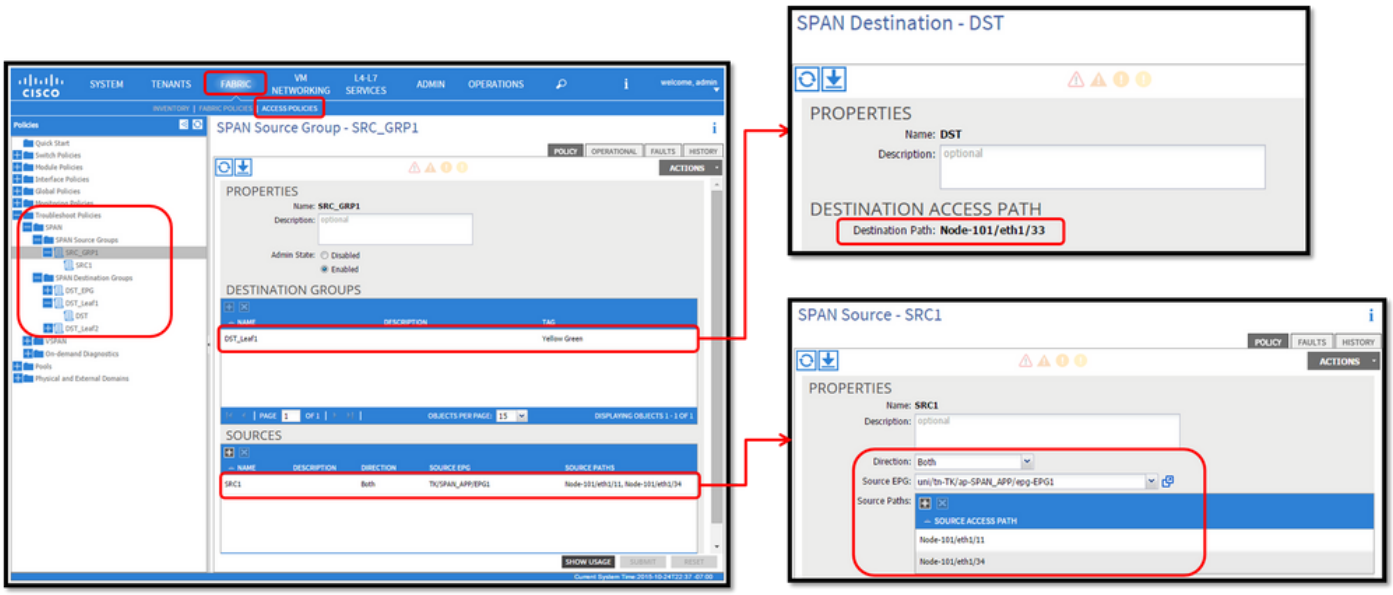
Stellen Sie außerdem sicher, dass die Ziel-IP-Adresse für ERSPAN als Endpunkt in der angegebenen Ziel-EPG erfasst wird. Im oben genannten Beispiel ist 192.168.254.1 unter Tenant TK > Application profile SPAN_APP > EPG SPAN zu erlernen. Die Ziel-IP-Adresse kann auch als statischer Endpunkt unter dieser EPG konfiguriert werden, wenn es sich bei dem Zielgerät um einen unbeaufsichtigten Host handelt.

Zugangs-SPAN (Lokal)

Beispieltopologie



Konfigurationsbeispiel



- Dabei gilt:

Fabric > ACCESS POLICIES > Troubleshoot Policies > SPAN

- SPAN Source Groups

- SPAN Destination Groups

SPAN Source Group Bindungen Destination und Sources.

- Vorgehensweise:

1. Erstellen SPAN Source Group (SRC_GRP1)

   - Erstellen SPAN Source(SRC1) unter SPAN Source Group (SRC_GRP1)

   - Konfigurieren Sie diese Parameter für SPAN Source (SRC1).
   - Richtung
   - Quell-EPG (optional)
   - Quellpfade (können mehrere Schnittstellen sein)
   ※ Details zu den einzelnen Parametern finden Sie im Bild.

   - Erstellen (SPAN Destination GroupDST_Leaf1)

   - Erstellen (SPAN DestinationDST)

   - Konfigurieren Sie diese Parameter für SPAN Destination (DST).
   - Zielschnittstelle und Knoten.

   - Stellen Sie sicher,SPAN Destination Group dass eine Bindung zum SPAN Source Group besteht.

   -

   Stellen Sie sicher,Admin State dass aktiviert ist.
   ※ SPAN wird beendet, wenn Sie in diesem Admin-Status Disabled (Deaktiviert) auswählen. Es müssen nicht alle Richtlinien gelöscht werden, wenn Sie sie später wiederverwenden.

Die Zielschnittstelle muss nicht nach Schnittstellen-Richtliniengruppen konfiguriert werden. Sie funktioniert, wenn Sie ein Kabel an die Schnittstelle der ACI-Leaf anschließen.

Einschränkungen:

- Für Local SPAN müssen eine Ziel- und eine Quellschnittstelle auf demselben Leaf konfiguriert werden.

- Für die Zielschnittstelle muss sie sich nicht in einer EPG befinden, solange sie aktiviert ist.

- Wenn die vPC-Schnittstelle (Virtual Port-Channel) als Quellport angegeben ist, kann kein lokales SPAN verwendet werden.
  Es gibt jedoch einen Workaround. Auf einem Leaf der ersten Generation kann ein einzelner physischer Port, der zu vPC oder PC gehört, als SPAN-Quelle konfiguriert werden. Dadurch kann Local SPAN für den Datenverkehr an vPC-Ports verwendet werden.
  Diese Option ist jedoch auf einem Leaf der zweiten Generation (CSCvc11053) nicht verfügbar. Stattdessen wurde die SPAN-Unterstützung für "VPC-Komponenten-PC" über CSCvc44643 in 2.1(2e), 2.2(2e) und weiter hinzugefügt. Auf diese Weise kann ein beliebiger Generationsknoten einen Port-Channel, der zu vPC gehört, als SPAN-Quelle konfigurieren. Auf diese Weise kann ein beliebiges Generations-Leaf Local SPAN für den Datenverkehr an vPC-Ports verwenden.

- Wenn Sie die einzelnen Ports eines Port-Channels für die zweite Generation festlegen, wird nur eine Teilmenge der Pakete überbrückt (auch aufgrund von CSCvc11053).

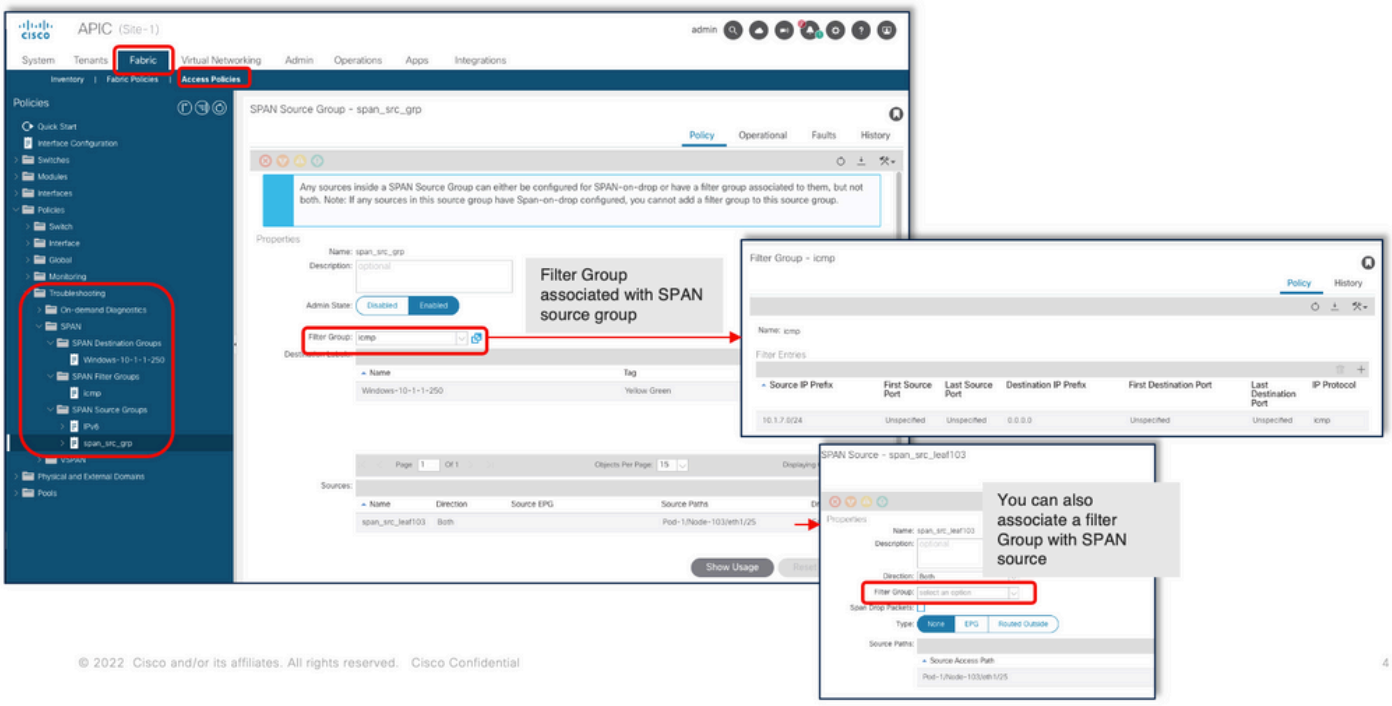
- PC und vPC können nicht als Zielport für das lokale SPAN verwendet werden. Ab 4.1(1) kann der PC als Zielport für Local SPAN verwendet werden.

Access SPAN - mit ACL-Filtern

Sie können ACL-Filter für Access Span-Quellen verwenden. Diese Funktion bietet die Möglichkeit, einen bestimmten Datenfluss oder -fluss innerhalb/außerhalb einer SPAN-Quelle per SPAN zu regeln.
Benutzer können die SPAN-ACLs auf eine Quelle anwenden, wenn SPAN-Datenverkehr für bestimmte Datenströme erforderlich ist.
Sie wird in Fabric SPAN- und Tenant Span-Quellgruppen/-quellen nicht unterstützt.
Beim Hinzufügen von Filtereinträgen in einer Filtergruppe ist Vorsicht geboten, da für jede Quelle, die derzeit die Filtergruppe verwendet, tcam-Einträge hinzugefügt werden können.

Eine Filtergruppe kann zugeordnet werden zu:
-Span Source (Spannenquelle): Die Filtergruppe wird verwendet, um Datenverkehr auf ALLEN Schnittstellen zu filtern, die unter dieser Spannenquelle definiert sind.
-Span Source Group (Spannen-Quellgruppe): Die Filtergruppe (z. B. x) wird verwendet, um Datenverkehr auf ALLEN Schnittstellen zu filtern, die unter jeder Spanne Source(s) dieser Spanne Source Group (Spannen-Quellgruppe) definiert sind.

In diesem Konfigurations-Snapshot wird die Filtergruppe auf die Span-Quellgruppe angewendet.

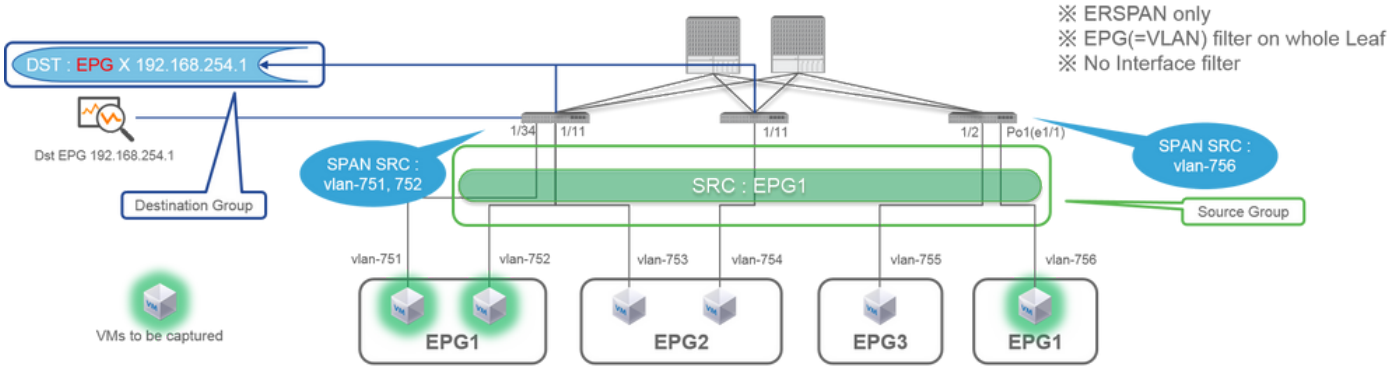


Wenn eine bestimmte Spanning Source bereits einer Filtergruppe zugeordnet ist (z. B. y), wird stattdessen die Filtergruppe (y) verwendet, um die Gruppe auf allen Schnittstellen unter dieser Spanning Source zu filtern.

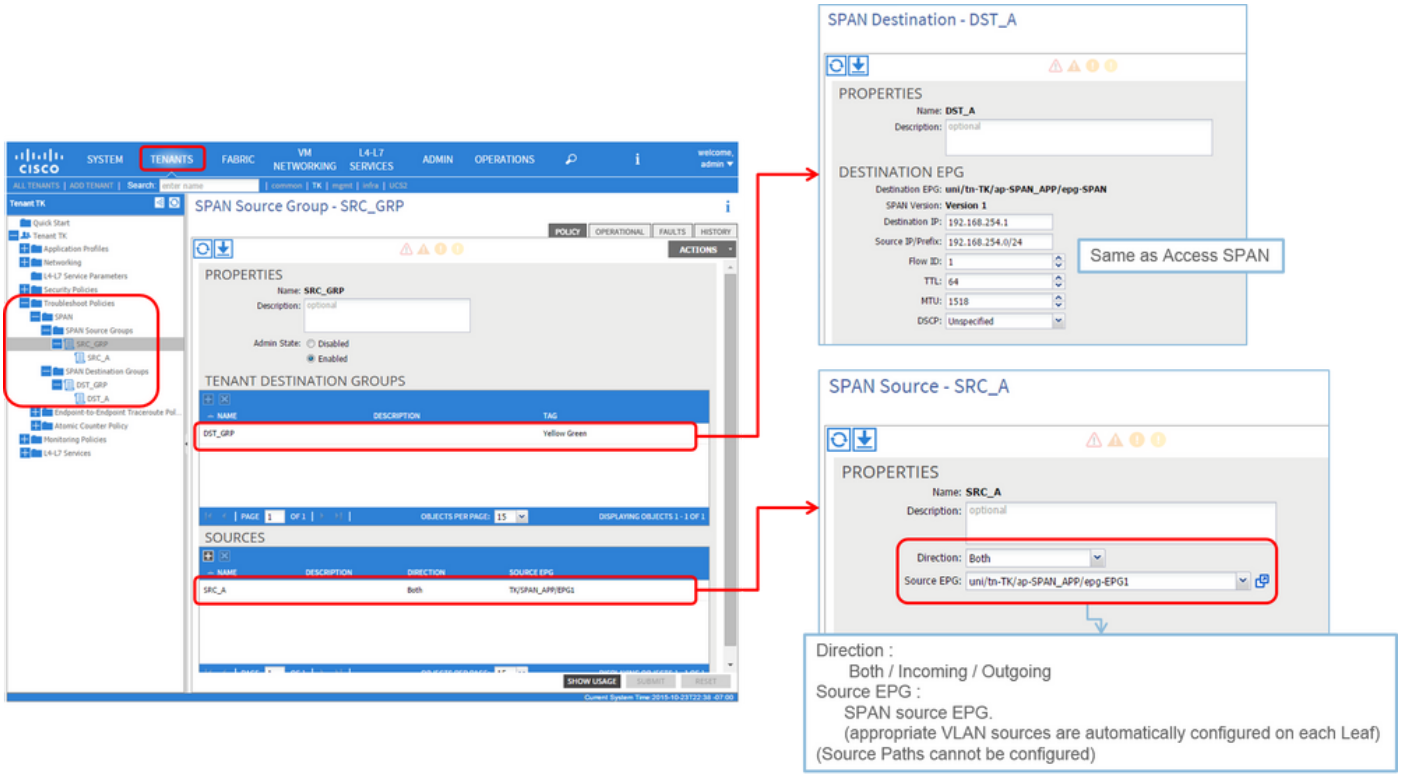
- Eine Filtergruppe, die in einer Quellgruppe angewendet wird, wird automatisch auf alle Quellen in dieser Quellgruppe angewendet.
- Eine Filtergruppe, die an einer Quelle angewendet wird, gilt nur für diese Quelle.
- Eine Filtergruppe wird sowohl in der Quellgruppe als auch in einer Quelle in dieser Quellgruppe angewendet, wobei die Filtergruppe, die an der Quelle angewendet wird, Vorrang hat.
- Eine an einer Quelle angewendete Filtergruppe wird gelöscht, und die an der übergeordneten Quellgruppe angewendete Filtergruppe wird automatisch angewendet.
- Eine Filtergruppe, die in einer Quellgruppe angewendet wird, wird gelöscht. Sie wird aus allen Quellen gelöscht, die derzeit in dieser Quellgruppe erben.

Tenant-SPAN (ERSPAN)

Beispieltopologie



Konfigurationsbeispiel



- Dabei gilt:

Tenants > {tenant name} > Troubleshoot Policies > SPAN

- SPAN Source Groups

- SPAN Destination Groups

※ SPAN-Quellgruppen-Verbindungen Destination und Sources.

- Vorgehensweise:

1. Erstellen SPAN Source Group (SRC_GRP)

- Erstellen SPAN Source (SRC_A) unter SPAN Source Group (SRC_GRP)

- Konfigurieren Sie diese Parameter für SPAN Source (SRC_A).
  - Richtung
  - Quell-EPG

※ Details zu den einzelnen Parametern finden Sie im Bild.

- Erstellen SPAN Destination Group (DST_GRP)

- Erstellen SPAN Destination (DST_A)

- Konfigurieren Sie diese Parameter für (SPAN DestinationDST_A).
  - Ziel-EPG
  -Ziel-IP
  - Quell-IP/Präfix
  - Andere Parameter können als Standard beibehalten werden.

※ Details zu den einzelnen Parametern finden Sie im Bild.

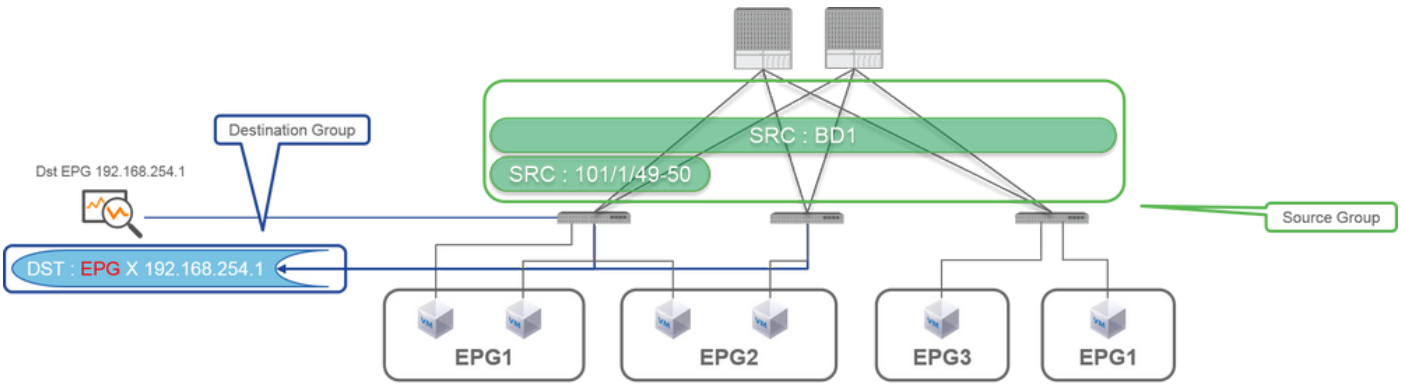
- Stellen Sie sicher,SPAN Destination Group dass an einen geeigneten SPAN Source Group gebunden ist.

- Stellen Sie sicher,Admin State dass aktiviert ist.

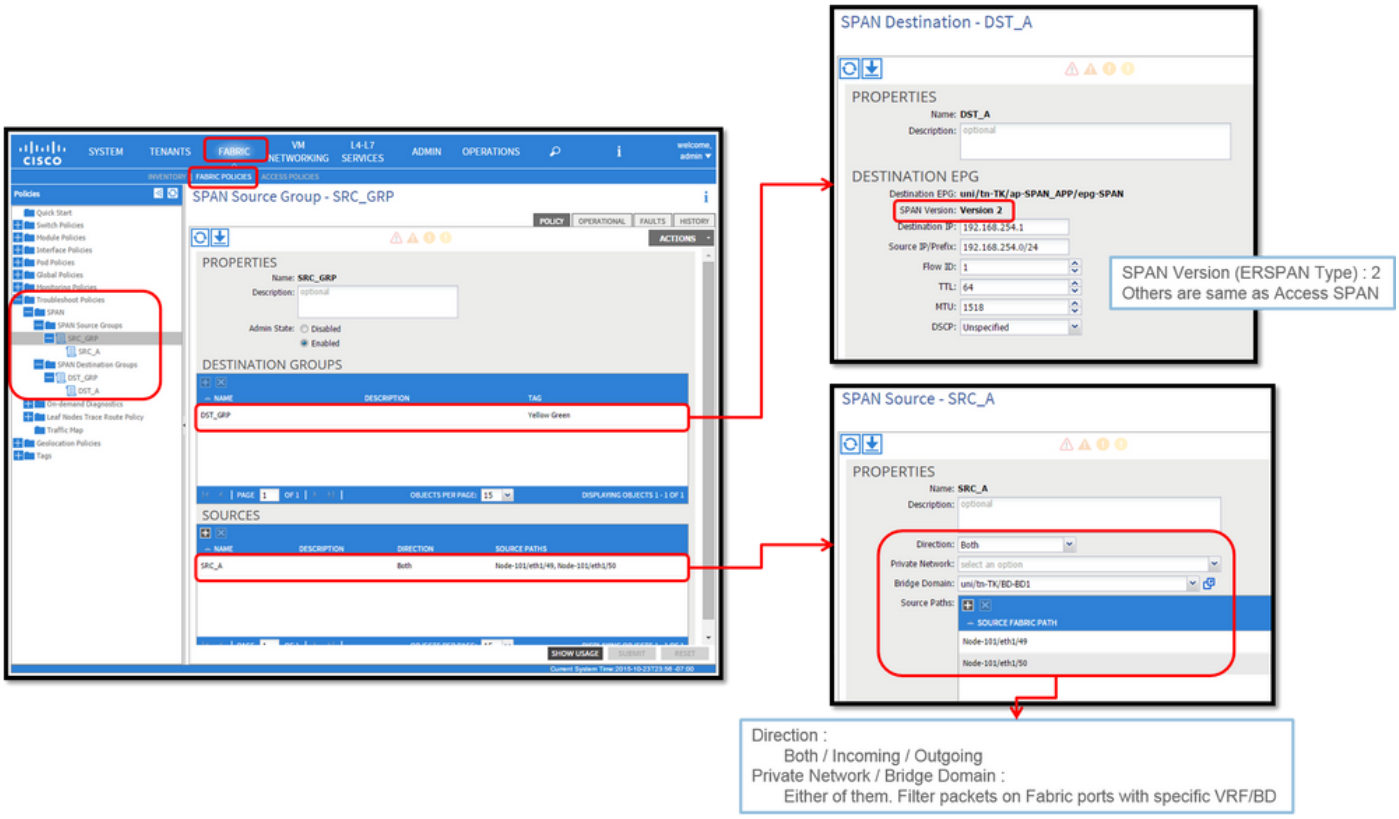
※ SPAN wird beendet, wenn Sie in diesem Admin-Status Disabled (Deaktiviert) auswählen. Es müssen nicht alle Richtlinien gelöscht werden, wenn Sie sie später wiederverwenden.

Fabric-SPAN (ERSPAN)

Beispieltopologie



Konfigurationsbeispiel



- Dabei gilt:

Fabric > FABRIC POLICIES > Troubleshoot Policies > SPAN

- Fabric

- SPAN Destination Groups

※ SPAN Source Group Verbindungen Destination und Sources

- Vorgehensweise:

1. Erstellen SPAN Source Group (SRC_GRP)

- Erstellen SPAN Source (SRC_A) unter SPAN Source Group (SRC_GRP)

- Konfigurieren Sie diese Parameter für SPAN Source (SRC_A).
  - Richtung
  - Privates Netzwerk (optional)
  - Bridge-Domäne (optional)
  - Quellpfade (können mehrere Schnittstellen sein)

※ Details zu den einzelnen Parametern finden Sie im Bild.

- Erstellen SPAN Destination Group (DST_GRP)

- Erstellen SPAN Destination (DST_A)

- Konfigurieren Sie diese Parameter für SPAN Destination (DST_A)
  - Ziel-EPG
  -Ziel-IP
  - Quell-IP/Präfix
  - Andere Parameter können als Standard beibehalten werden.

※ Details zu den einzelnen Parametern finden Sie im Bild.

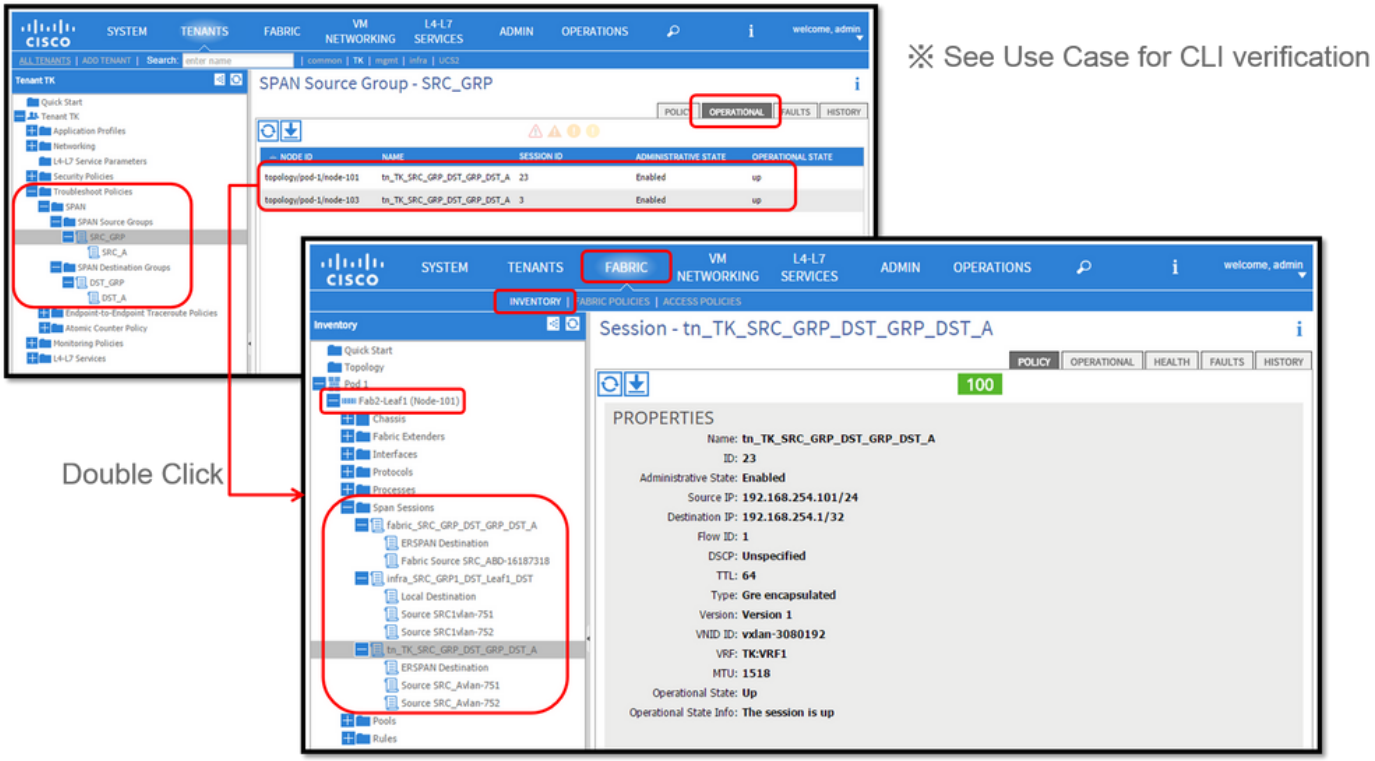
- Stellen Sie sicher,SPAN Destination Group dass an einen geeigneten SPAN Source Group gebunden ist.

- Stellen Sie sicher, Admin State dass aktiviert ist.

※ SPAN wird beendet, wenn Sie auf diesem Admin State die Option Disabled (Deaktiviert) auswählen. Es müssen nicht alle Richtlinien gelöscht werden, wenn Sie sie später wiederverwenden.

Obwohl sie in einem späteren Abschnitt "ERSPAN-Version (Typ)" beschrieben wird, können Sie feststellen, dass ERSPAN-Version II für Fabric SPAN und Version I für Tenant und Access SPAN verwendet wird.

GUI-Überprüfung



- Überprüfen der SPAN-Konfigurationsrichtlinie

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

Stellen Sie sicher, dass der Betriebsstatus aktiv ist.

- Überprüfung der SPAN-Sitzung auf dem Knoten selbst

1. Doppelklicken Sie auf jede Sitzung von SPAN Configuration Policyoder Fabric > INVENTORY > Node > Span Sessions > { SPAN session name }

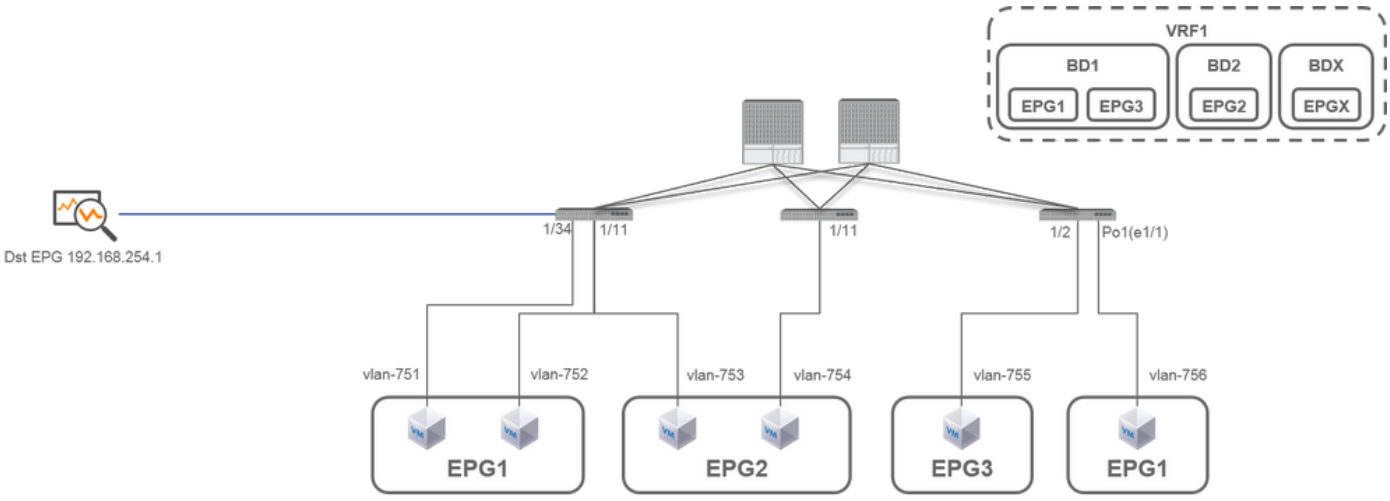
Stellen Sie sicher, dass der Betriebsstatus aktiv ist.

Namenskonvention für SPAN-Sitzungen:

- Fabric-SPAN: Fabric_xxxx

- Zugriff auf SPAN: infra_xxxx
- Tenant-SPAN: tn_xxxx

ACI-SPAN-Typ auswählen

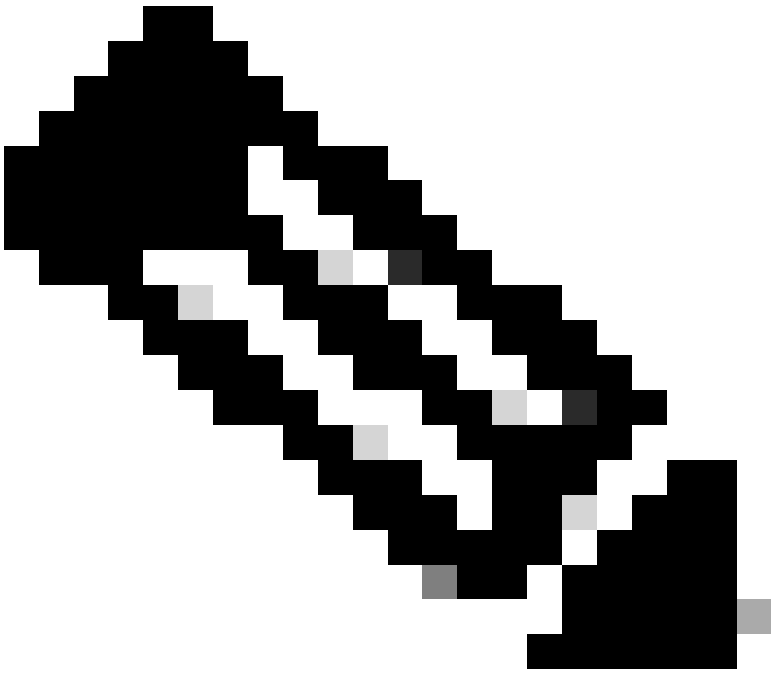


In diesem Abschnitt werden detaillierte Szenarien für jeden ACI-SPAN-Typ beschrieben (Access, Tenant, Fabric). Die Basistopologie für jedes Szenario wird im vorherigen Abschnitt beschrieben.

Wenn Sie diese Szenarien verstehen, können Sie den für Ihre Anforderungen geeigneten ACI-SPAN-Typ auswählen. Beispielsweise müssen Pakete nur auf bestimmten Schnittstellen oder alle Pakete auf einer bestimmten EPG unabhängig von den Schnittstellen erfasst werden.

In der Cisco ACI wird SPAN mit dem source group und destination group konfiguriert. Die Quellgruppe enthält mehrere Quellfaktoren, z. B. Schnittstellen oder EPG. Die Zielgruppe enthält Zielinformationen wie die Zielschnittstelle für Local SPAN oder Ziel-IP für ESPAN.

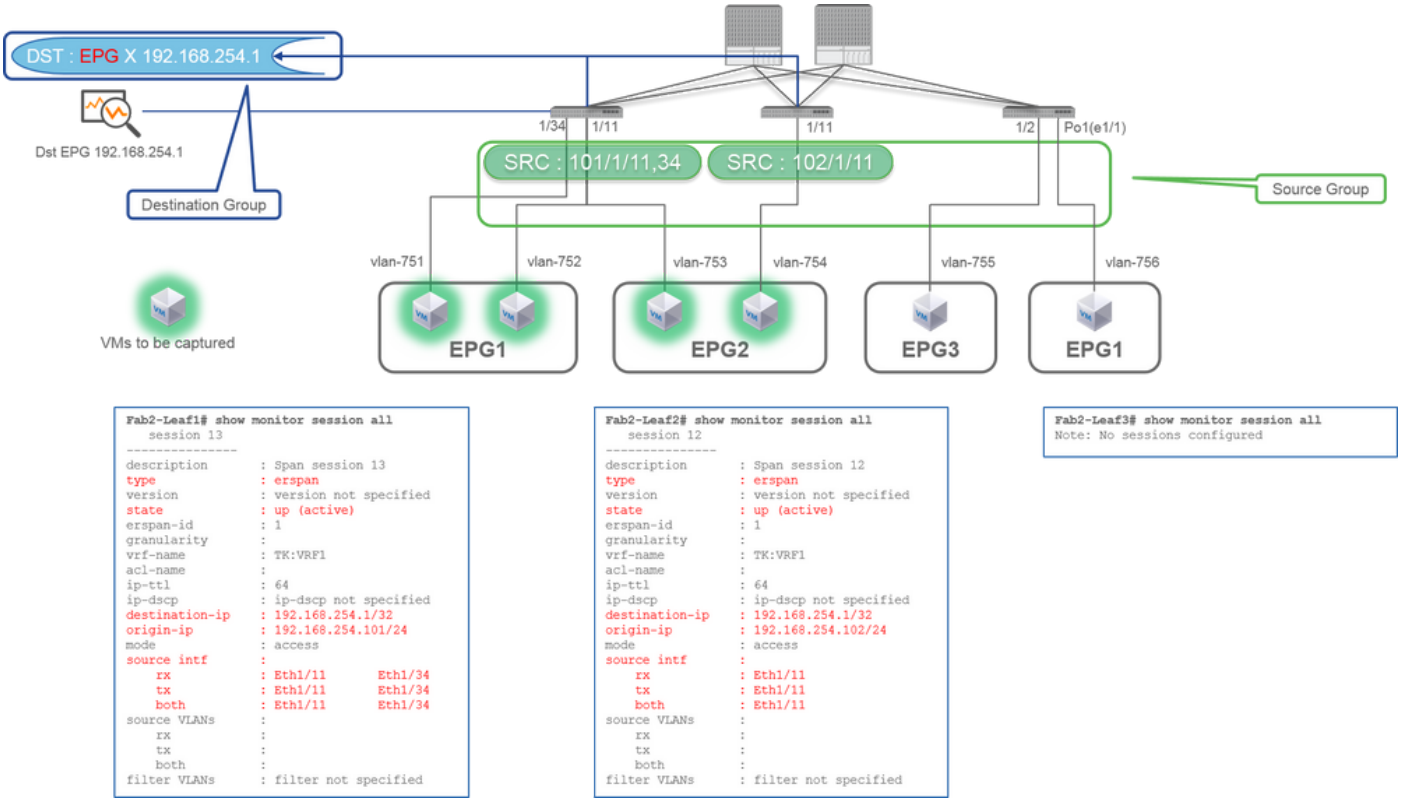
Nachdem die Pakete erfasst wurden, lesen Sie den Abschnitt "Lesen von SPAN-Daten", um die erfassten Pakete zu dekodieren.



Hinweis: Bitte konzentrieren Sie sich auf VMs, die in jeder Topologie mit einem grünen Licht markiert sind. In jedem Szenario werden Pakete von diesen hervorgehobenen virtuellen Systemen erfasst.

Zugangs-SPAN (ERSPAN)

Fall 1: Quelle "Leaf1 e1/11 e1/34 & Leaf2 e1/11" | Ziel "192.168.254.1"



- Source Group
  - Leaf1 e1/11
  - Leaf1 e1/34
  - Leaf2 e1/11
- Destination Group
  - 192.168.254.1 für EPG X

Access-SPAN kann mehrere Schnittstellen für eine einzelne SPAN-Sitzung angeben. Er kann alle Pakete erfassen, die über bestimmte Schnittstellen eingehen oder austreten, unabhängig von ihrer EPG.

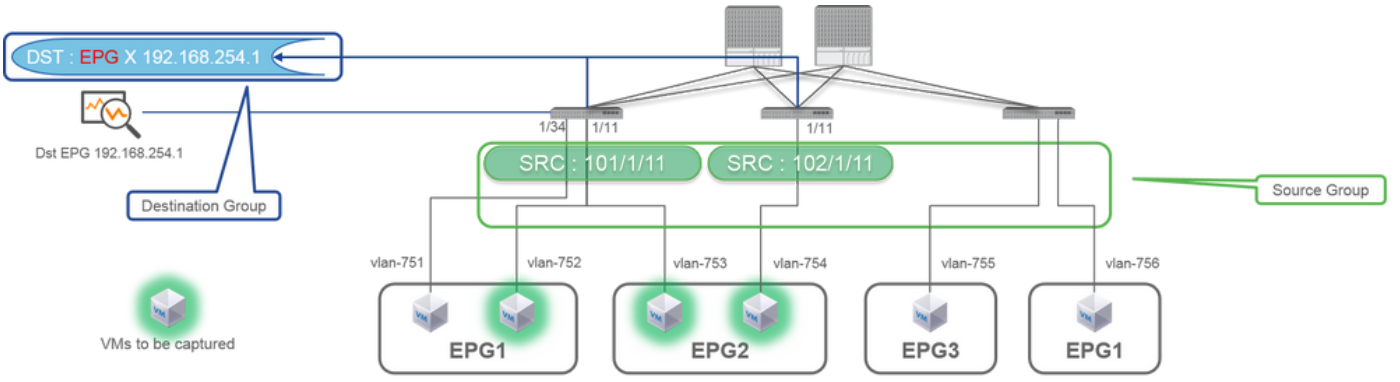
Wenn mehrere Schnittstellen von mehreren Leaf-Switches als Quellgruppe angegeben werden, muss es sich bei der Zielgruppe um ERSPAN und nicht um Local SPAN handeln.

In diesem Beispiel werden Pakete von allen VMs in EPG1 und EPG2 kopiert.

CLI-Prüfpunkt

- Vergewissern Sie sich, dass der Status "up (active)" lautet.
- "destination-ip" ist die Ziel-IP für ERSPAN
    - "origin-ip" ist Quell-IP für ERSPAN

Fall 2: Quelle "Leaf1 e1/11 & Leaf2 e1/11" | Ziel "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
```

- **Quellgruppe**
    - Leaf1 e1/11
    - Leaf2 e1/11
- **Zielgruppe**
    - 192.168.254.1 für EPG X

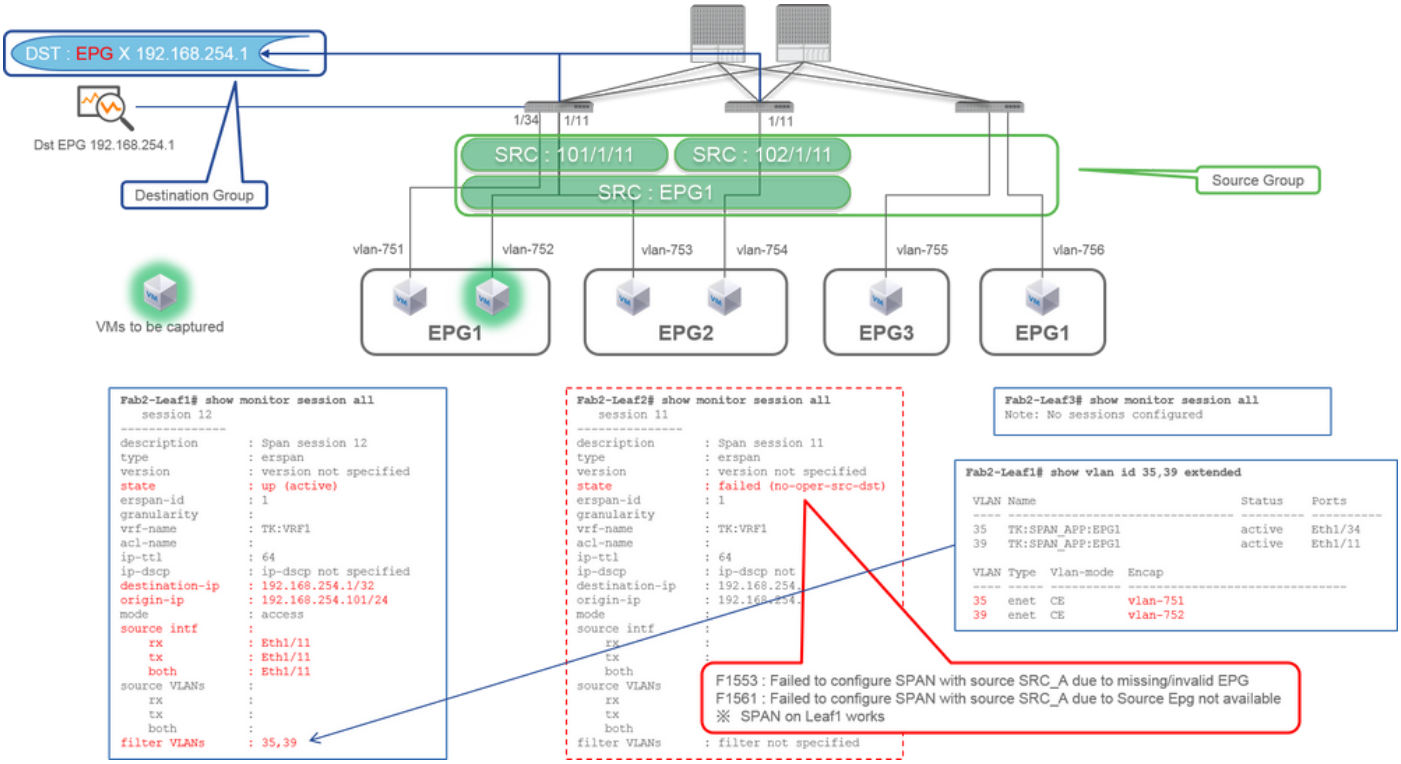
In diesem Beispiel wird Leaf1 e1/34 aus der SPAN-Quellgruppe entfernt, die in der vorherigen Case1-Konfiguration konfiguriert wurde.

Der zentrale Punkt in diesem Beispiel ist, dass Access SPAN Quellschnittstellen unabhängig von der EPG angeben kann.

CLI-Prüfpunkt

- Die Quellschnittstelle auf Leaf1 wird von "Eth1/11 Eth1/34" in "Eth1/11 Eth1/11" geändert.

Fall 3: Quelle: "Leaf1 e1/11 & Leaf2 e1/11 & EPG1 filter" | Ziel "192.168.254.1"



- **Quellgruppe**
  - Leaf1 e1/11
  - Leaf2 e1/11
  - Filter-EPG1
- **Zielgruppe**
  - 192.168.254.1 für EPG X

Dieses Beispiel zeigt, dass Access SPAN auch eine bestimmte EPG auf den Quell-Ports angeben kann. Dies ist nützlich, wenn mehrere EPGs auf einer Schnittstelle übertragen werden und der Datenverkehr nur für EPG1 auf dieser Schnittstelle erfasst werden muss.

Da EPG1 auf Leaf2 nicht bereitgestellt wird, schlägt SPAN für Leaf2 mit den Fehlern F1553 und F1561 fehl. SPAN auf Leaf1 funktioniert jedoch weiterhin.

Außerdem werden automatisch zwei VLAN-Filter für die SPAN-Sitzung auf Leaf1 hinzugefügt, da EPG1 zwei VLANs (VLAN-751.752) auf Leaf1 verwendet.

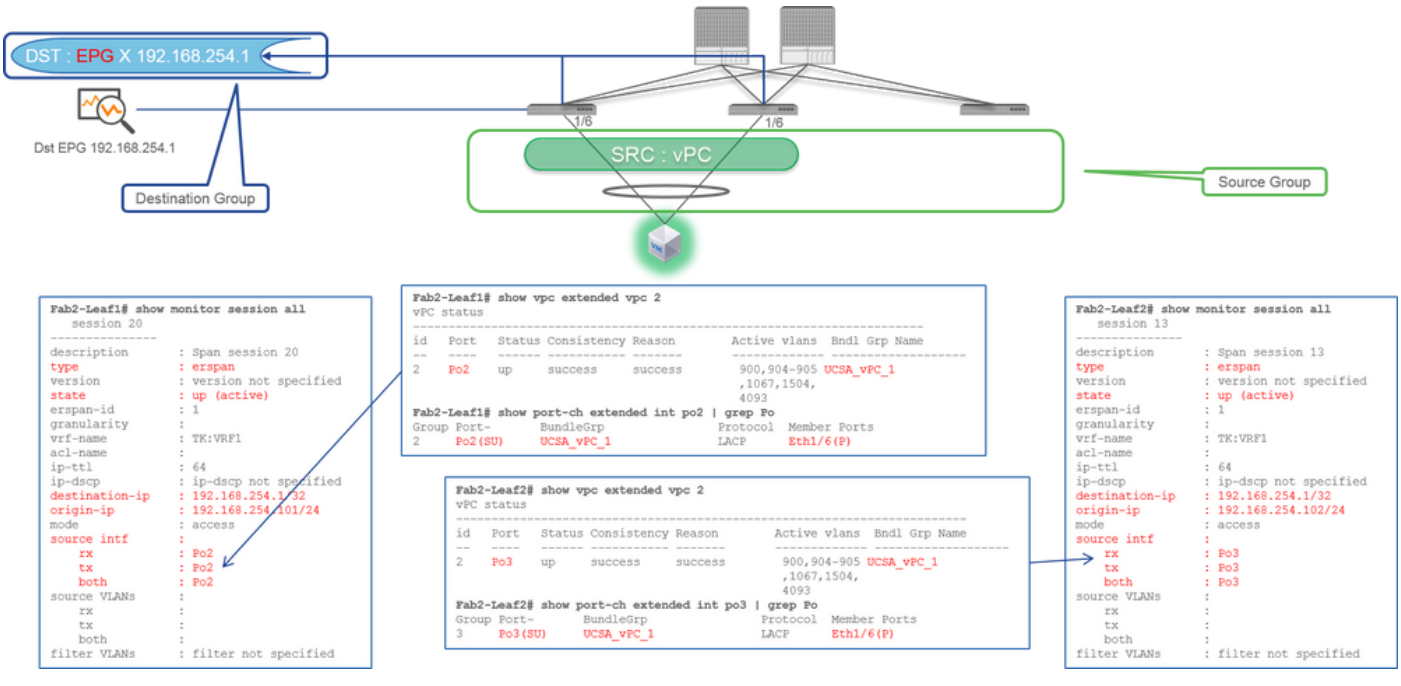
Beachten Sie, dass die VLAN-ID auf CLI (35, 39) die interne VLAN-ID (PI-VLAN (Platform Independent VLAN)) ist, die nicht die tatsächliche ID auf der Leitung ist. Wie in der Abbildung dargestellt, zeigt der Befehl **show vlan extended** die Zuordnung der tatsächlichen VLAN-ID des Encaps und des IP-VLAN.

Mit dieser SPAN-Sitzung können Pakete nur für EPG1 (VLAN-752) auf Leaf1 e1/11 erfasst werden, obwohl EPG2 (VLAN-753) über dieselbe Schnittstelle übertragen wird.

CLI-Prüfpunkt

- Filter-VLANs werden gemäß den für den Filter verwendeten EPGs hinzugefügt.
- Wenn auf dem Leaf keine entsprechenden EPGs vorhanden sind, schlägt die SPAN-Sitzung auf diesem Leaf fehl.

Fall 4: Quelle "Leaf1-Leaf2 vPC" | Ziel "192.168.254.1"

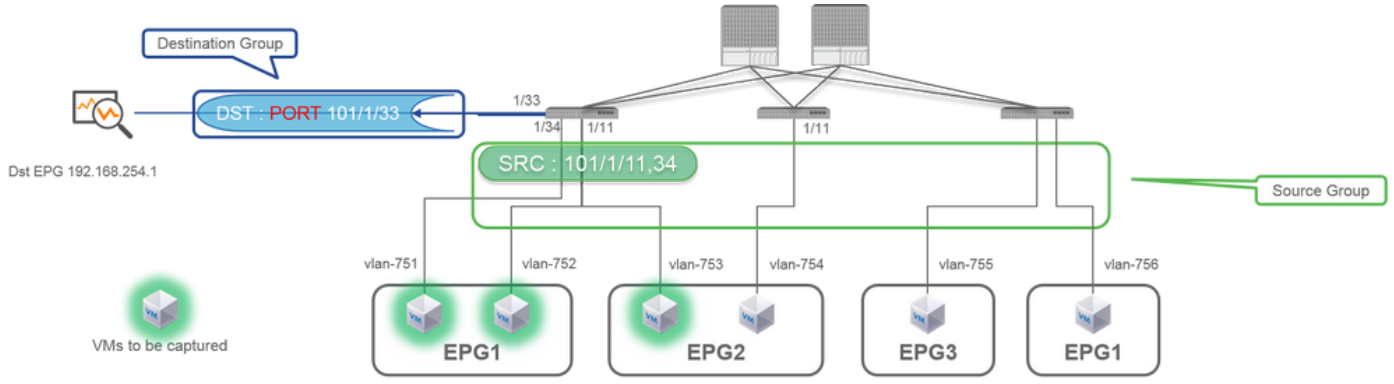


- **Quellgruppe**
    - Leaf1 - 2e1/11
- **Zielgruppe**
    - 192.168.254.1 für EPG X

Wenn die vPC-Schnittstelle als Quelle konfiguriert ist, muss ein Ziel die Remote-IP (ERSPAN) und nicht die Schnittstelle (Local SPAN) sein

Zugangs-SPAN (Lokales SPAN)

Fall 1: Quelle "Leaf1 e1/11 e1/34" | Ziel "Leaf1 e1/33"




```
Fab2-Leaf1# show monitor session all
    session 14
---------------
description       : Span session 14
type              : local
state             : up (active)
mode              : access
source intf       :
    rx            : Eth1/11       Eth1/34
    tx            : Eth1/11       Eth1/34
    both          : Eth1/11       Eth1/34
source VLANs      :
    rx            :
    tx            :
    both          :
filter VLANs      : filter not specified
destination ports : Eth1/33
```

```
Fab2-Leaf2# show monitor session all
Note: No sessions configured
```

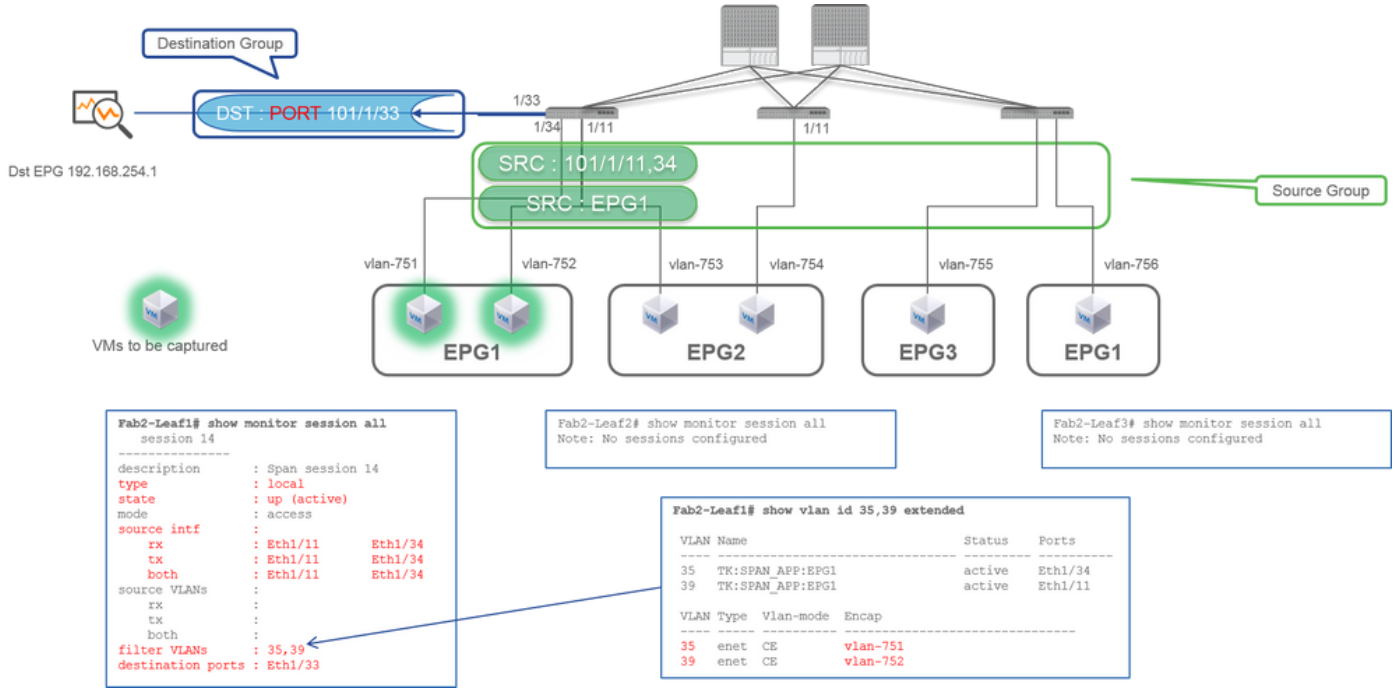
```
Fab2-Leaf3# show monitor session all
Note: No sessions configured
```

- **Quellgruppe**
  - Leaf1 e1/11
  - Leaf1 e1/34
- **Zielgruppe**
  - Leaf1 e1/33

Access SPAN kann auch Local SPAN verwenden (d. h. eine bestimmte Schnittstelle als Ziel).

In diesem Fall müssen sich die Quellschnittstellen jedoch auf demselben Leaf befinden wie die Zielschnittstelle.

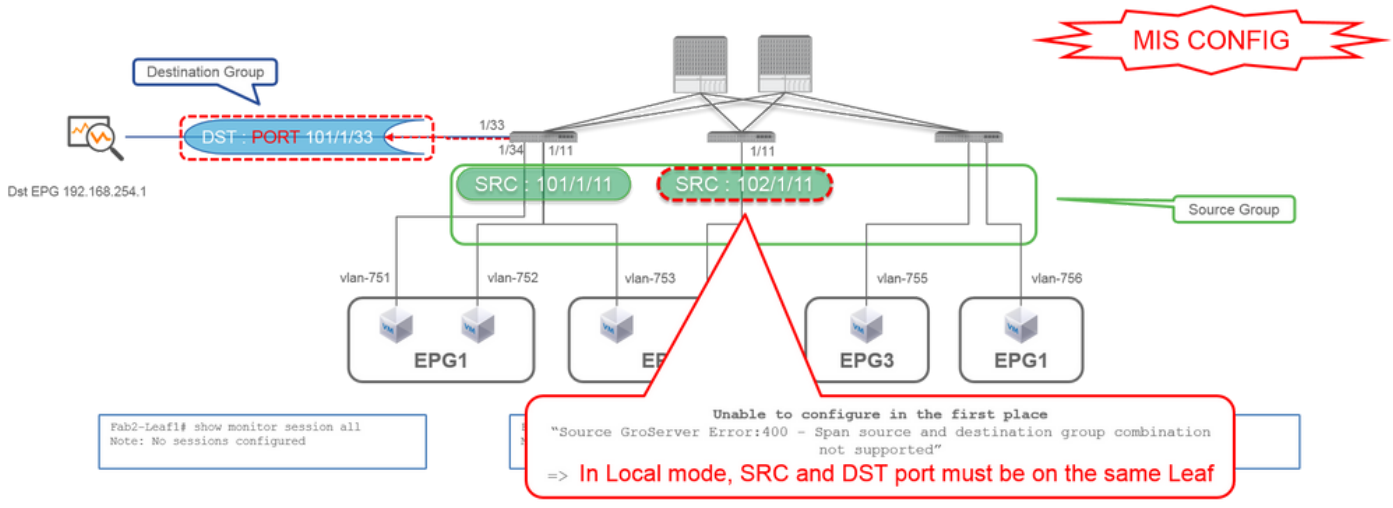
Fall 2: Quelle "Leaf1 e1/11 e1/34 & EPG1 filter | Ziel " Blatt 1 e1/33"



- **Quellgruppe**
    - Leaf1 e1/11
    - Leaf1 e1/34
    - EPG1-Filter
- **Zielgruppe**
    - Leaf1 e1/33

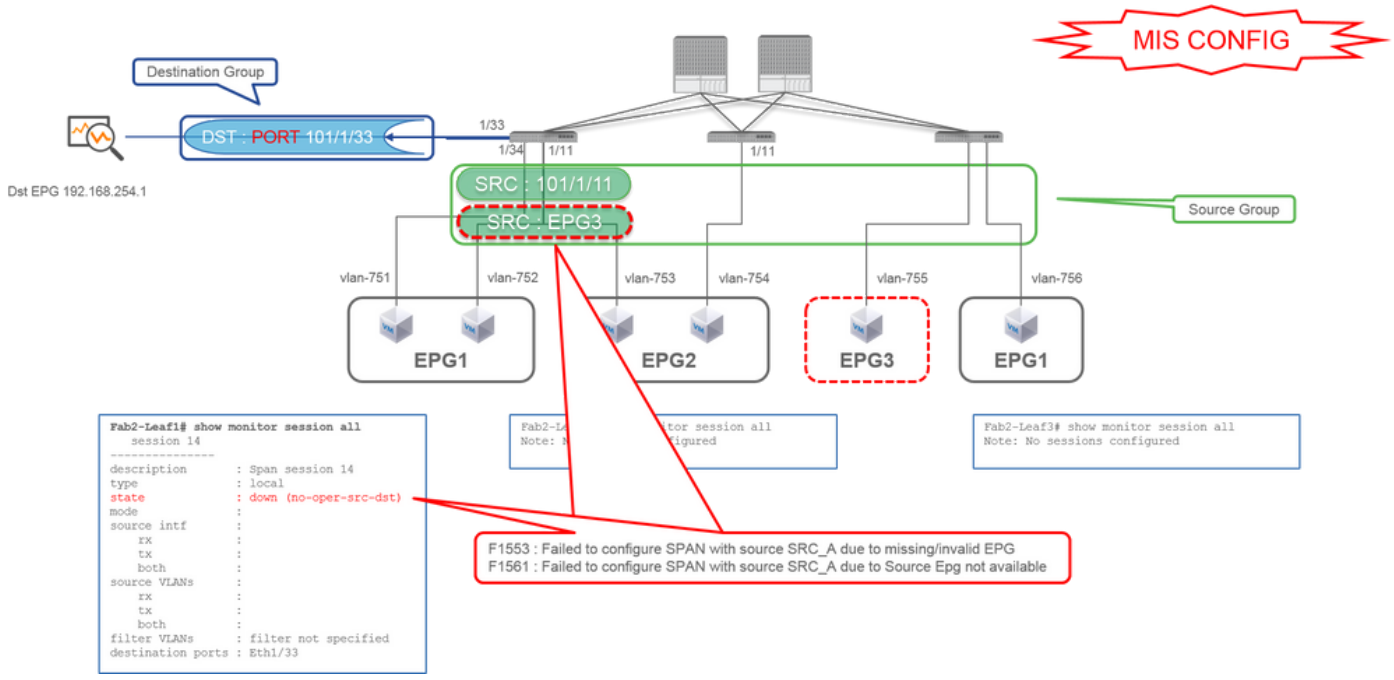
Access SPAN mit Local SPAN kann auch den EPG-Filter sowie ERSPAN verwenden.

Fall 3: Quelle "Leaf1 e1/11 & Leaf2 e/11" | Dst "Leaf1 e1/33" (schlechter Fall)



- **Quellgruppe**
    - Leaf1 e1/11
    - Leaf2 e1/11
- **Zielgruppe**
    - Leaf1 e1/33

Fall 4: Quelle: "Leaf1 e1/11 & EPG3 filter" | Dst "Leaf1 e1/33" (schlechter Fall)



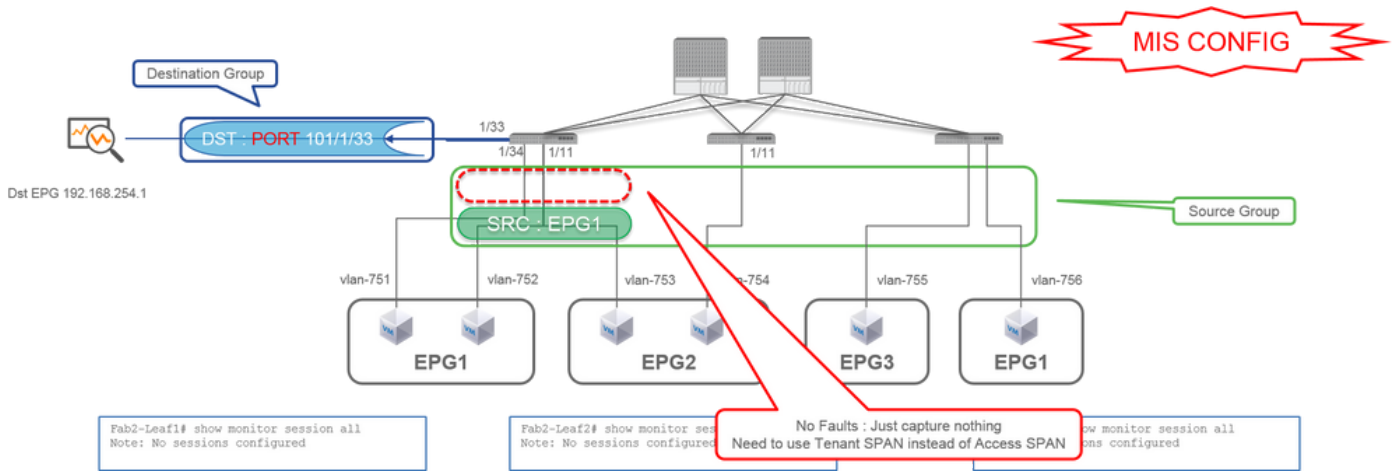
- **Quellgruppe**

- Leaf1 e1/11
- EPG3-Filter

- **Zielgruppe**
  - Leaf1 e1/33

Dies ähnelt Fall 3 bei Access SPAN (ERSPAN), in diesem Beispiel schlägt jedoch die einzige SPAN-Sitzung auf Leaf1 fehl, da EPG3 auf Leaf1 nicht vorhanden ist. SPAN funktioniert also überhaupt nicht.

Fall 5: Quelle "EPG1 filter" | Dst "Leaf1 e1/33" (schlechter Fall)

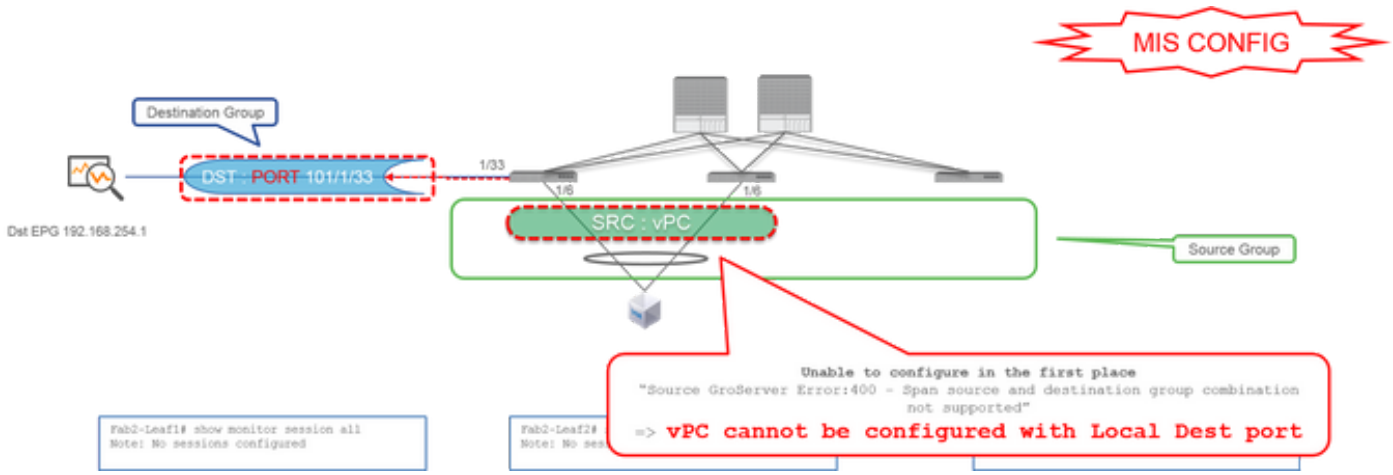


- **Quellgruppe**
  - EPG1-Filter

- **Zielgruppe**
    - Leaf1 e1/33

Der EPG-Filter für Access SPAN funktioniert nur, wenn Quell-Ports konfiguriert sind. Wenn EPG als einzige Quelle angegeben wird, muss Tenant-SPAN anstelle von Access-SPAN verwendet werden.

Fall 6: Quelle "Leaf1 - Leaf2 vPC" | Dst "Leaf1 e1/33" (schlechter Fall)

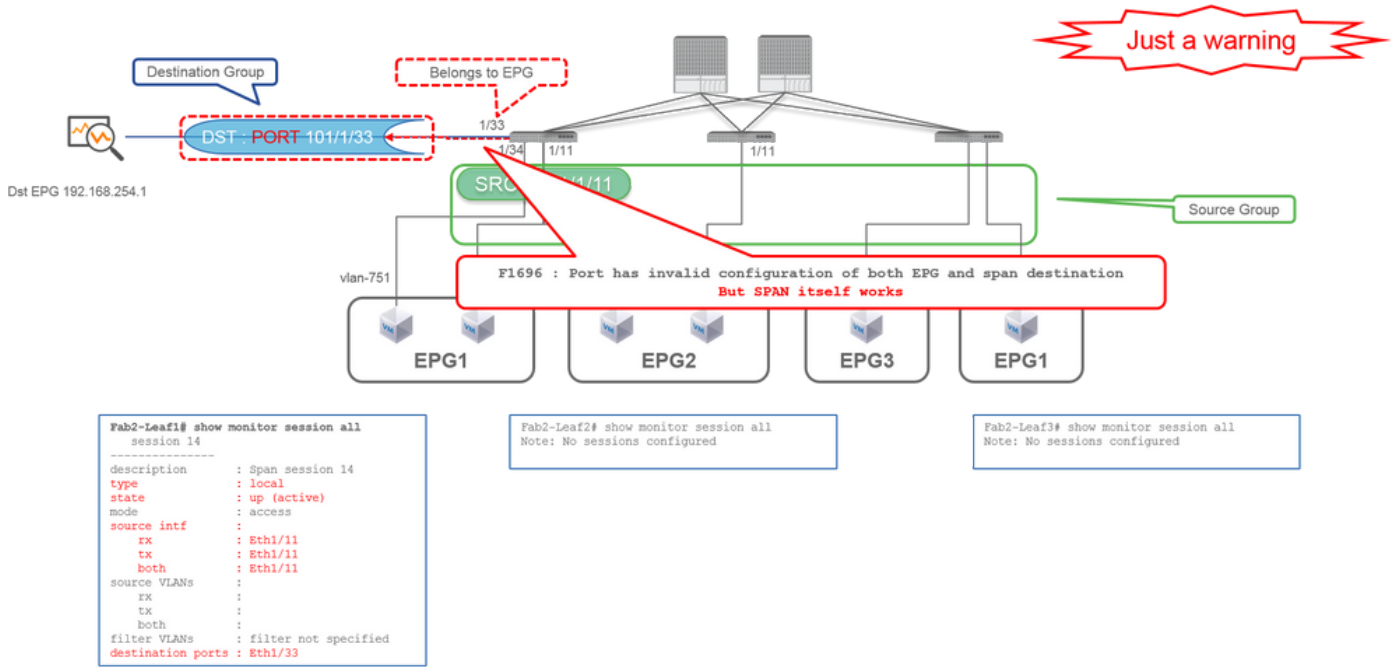


- **Quellgruppe**
    - Leaf1-2 vPC

- **Zielgruppe**
    - Leaf1 e1/33

Eine vPC-Schnittstelle kann nicht als Quelle mit Local SPAN konfiguriert werden. Verwenden Sie ERSPAN. Informationen zu Access SPAN (ERSPAN) finden Sie in case4.

Fall 7: Quelle "Leaf1 e1/11 | Dst "Leaf1 e1/33 & e1/33 gehört zur EPG" (funktioniert fehlerhaft)

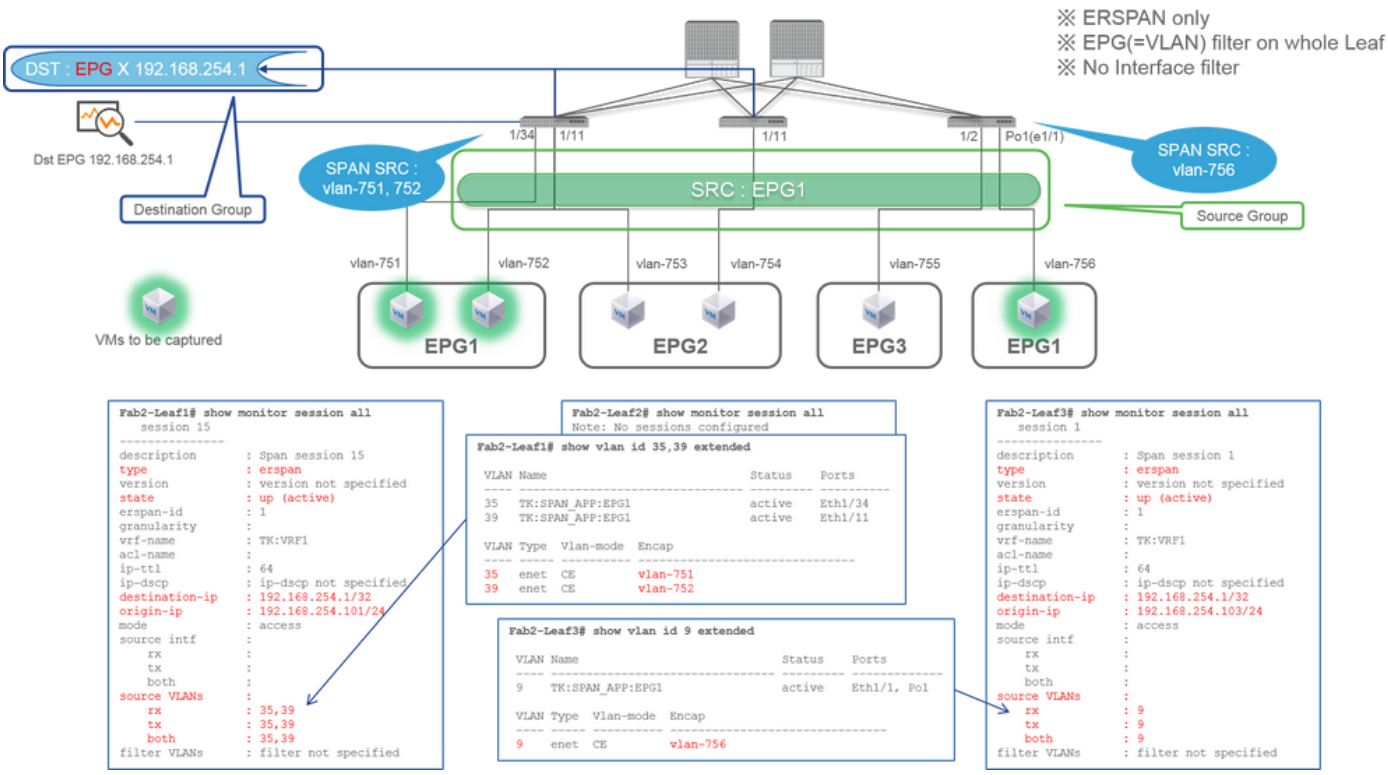


Wenn ein Ziel-I/F für SPAN bereits zur EPG gehört, wird der Fehler "F1696 : Port has an invalid configuration of both EPG and span destination" (F1696: Port hat eine ungültige Konfiguration von EPG- und Span-Ziel) unter dem physischen I/F ausgelöst.

Aber selbst bei diesem Fehler funktioniert SPAN problemlos. Dieser Fehler ist nur eine Warnung vor zusätzlichem Datenverkehr, der durch SPAN verursacht wird, da er sich auf den normalen EPG-Datenverkehr von Kunden auf derselben E/A-Schnittstelle auswirken kann.

Tenant-SPAN (ERSPAN)

Fall 1: Quelle "EPG1" | Ziel "192.168.254.1"



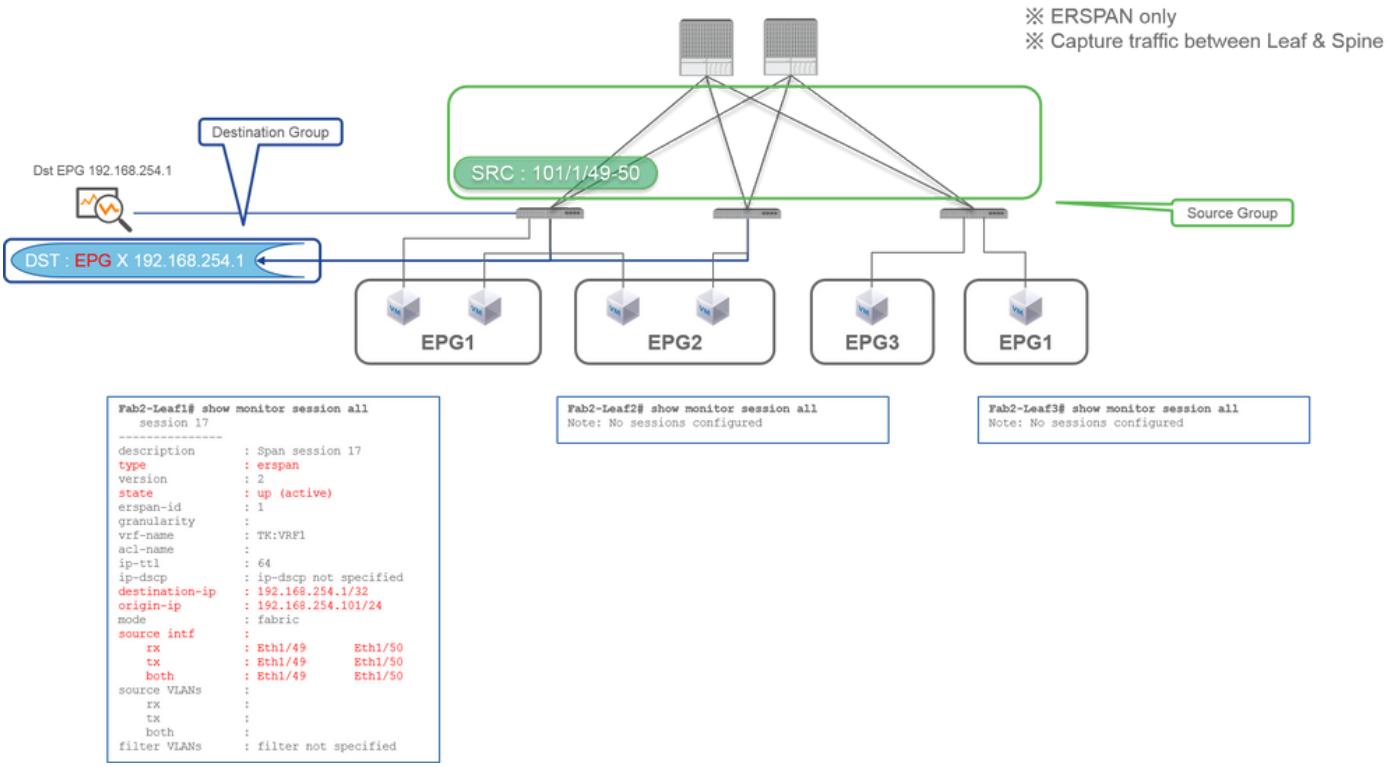
- **Quellgruppe**
  - EPG1 (kein Filter)
- **Zielgruppe**
  - 192.168.254.1 für EPG X

Tenant-SPAN verwendet die EPG selbst als Quelle, während Access-SPAN die EPG nur als Filter verwendet.

Der Hauptvorteil von Tenant SPAN besteht darin, dass Sie nicht jeden einzelnen Port angeben müssen, und dass die ACI automatisch die entsprechenden VLANs auf jedem Leaf-Switch erkennt. Dies ist nützlich, wenn alle Pakete für eine bestimmte EPG überwacht werden müssen und die Endpunkte für diese EPG mehreren Schnittstellen über Leaf-Switches angehören.

Fabric-SPAN (ERSPAN)

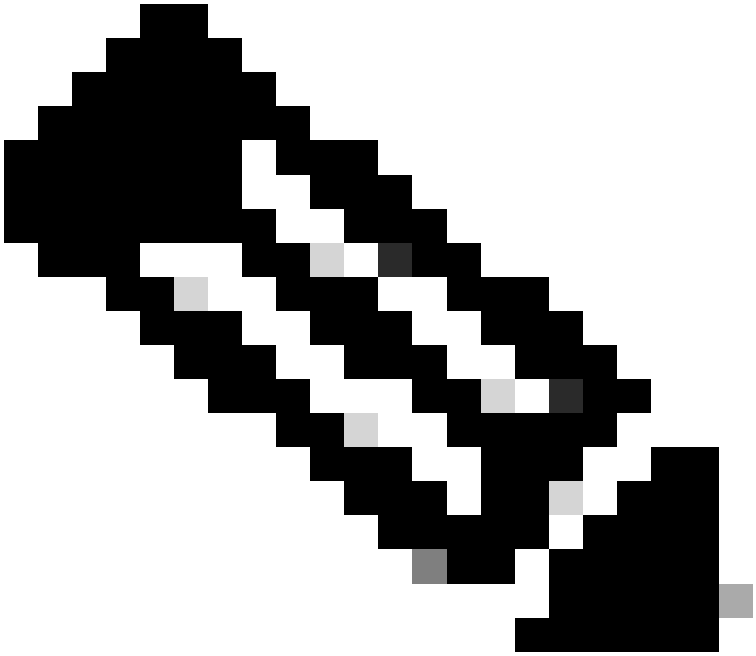
Fall 1: Quelle "Leaf1 e1/49-50" | Ziel "192.168.254.1"



- **Quellgruppe**
  - Leaf1 e1/49-50
- **Zielgruppe**
  - 192.168.254.1 für EPG X

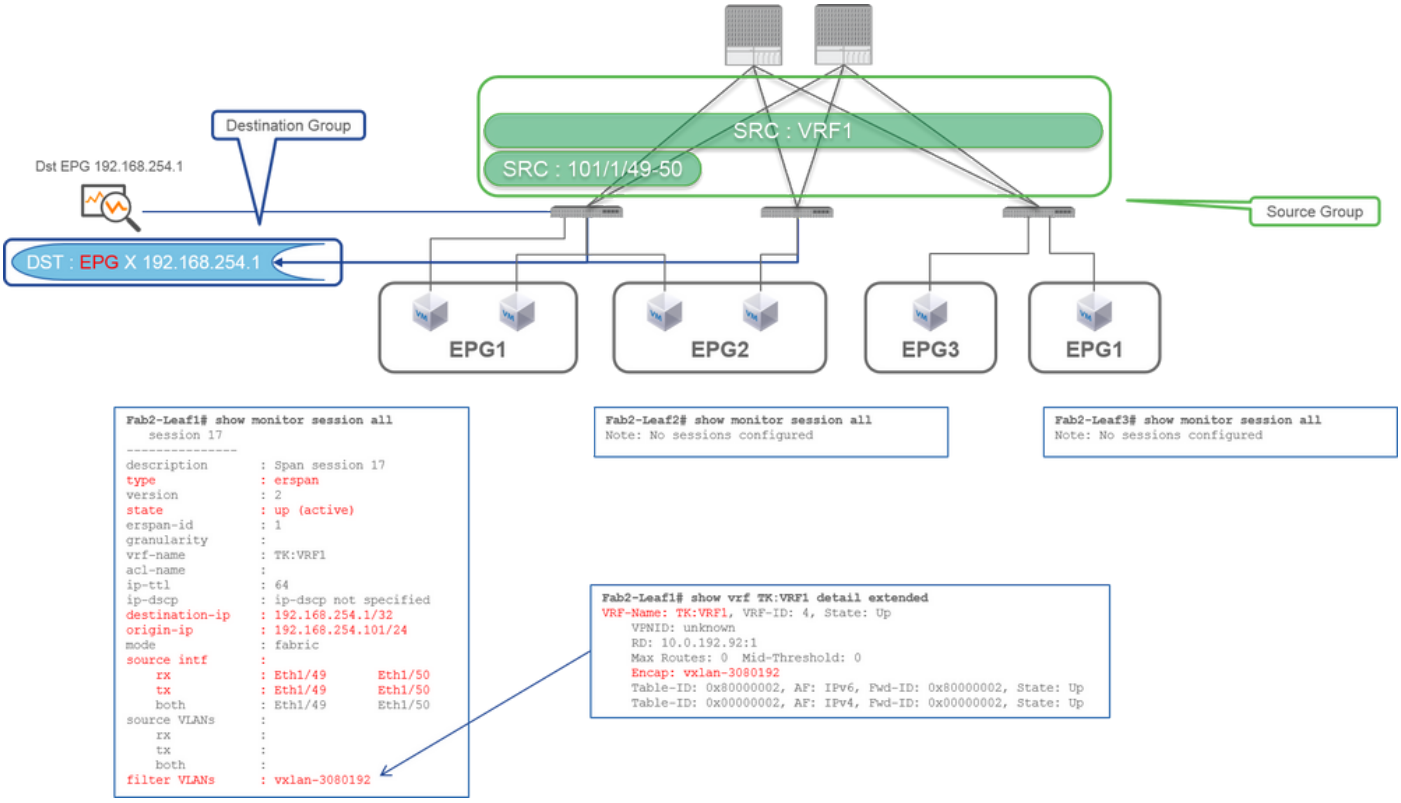
Fabric SPAN gibt Fabric-Ports als Quelle an, wobei Fabric-Ports Schnittstellen zwischen Leaf- und Spine-Switches sind.

Dieses SPAN ist nützlich, wenn Pakete zwischen Leaf- und Spine-Switches kopiert werden müssen. Pakete zwischen Leaf- und Spine-Switches werden jedoch mit dem iVxLAN-Header gekapselt. Es ist also ein kleiner Trick nötig, um es zu lesen. Weitere Informationen finden Sie unter "Lesen von SPAN-Daten".



Hinweis: Der iVxLAN-Header ist ein erweiterter VxLAN-Header, der nur zur internen Verwendung in der ACI-Fabric verwendet wird.

Fall 2: Quelle: "Leaf1 e1/49-50 & VRF-Filter" | Ziel "192.168.254.1"



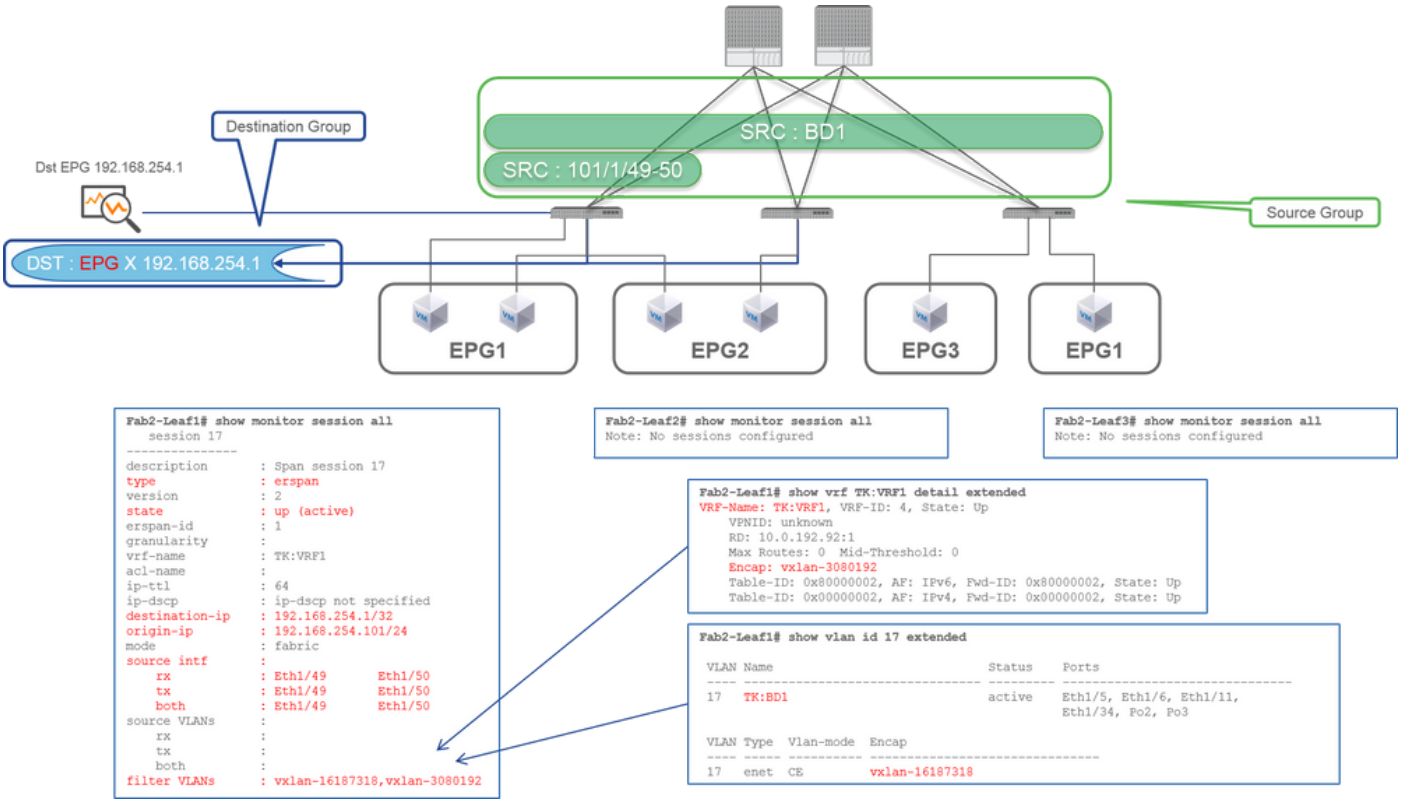
- **Quellgruppe**
  - Leaf1 e1/49-50
  - VRF-Filter
- **Zielgruppe**
  - 192.168.254.1 für EPG X

Fabric SPAN kann Filter sowie Access SPAN verwenden. Der Filtertyp ist jedoch anders. Fabric SPAN verwendet Virtual Routing and Forwarding (VRF) oder BD als Filter.

Wie bereits beschrieben, werden in der Cisco ACI Pakete, die Fabric-Ports durchlaufen, mit einem iVxLAN-Header verkapselt. Dieser iVxLAN-Header enthält VRF- oder BD-Informationen als Virtual Network Identifier (VNID). Wenn Pakete als Layer 2 (L2) weitergeleitet werden, steht "iVxLAN VNID" für "BD". Wenn Pakete als Layer 3 (L3) weitergeleitet werden, steht iVxLAN VNID für VRF.

Wenn es also erforderlich ist, gerouteten Verkehr an Fabric-Ports zu erfassen, sollten Sie VRF als Filter verwenden.

Fall 3: Quelle: "Leaf1 e1/49-50 & BD filter" | Ziel "192.168.254.1"

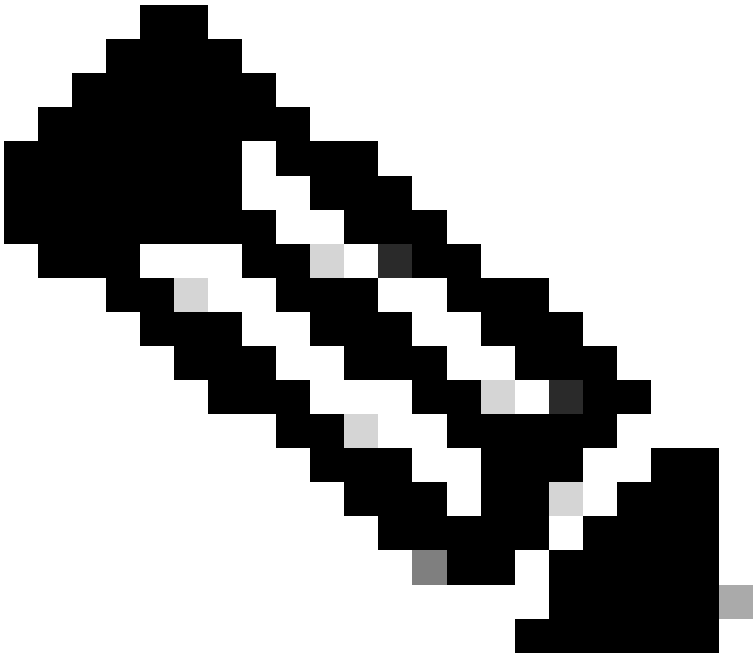


- **Quellgruppe**
  - Leaf1 e1/49-50
  - BD-Filter
- **Zielgruppe**

- 192.168.254.1 für EPG X

Wie im vorherigen Fall 2 beschrieben, kann Fabric SPAN BD als Filter verwenden.

Wenn Bridge-Datenverkehr an Fabric-Ports erfasst werden soll, sollte BD als Filter verwendet werden.



Hinweis: Es kann jeweils nur ein Filter für BD oder VRF konfiguriert werden.

Was benötigen Sie für das SPAN-Zielgerät?

Führen Sie einfach eine Paketerfassungsanwendung wie tcpdump, wireshark auf ihr aus. Es ist nicht erforderlich, die ERSPAN-Zielsitzung zu konfigurieren.

Für ERSPAN

Stellen Sie sicher, dass auf der Schnittstelle mit der Ziel-IP für ERSPAN ein Erfassungstool ausgeführt wird, da SPAN-Pakete an die Ziel-IP weitergeleitet werden.

Das empfangene Paket wird mit einem GRE-Header gekapselt. Informationen zum Decodieren des ERSPAN GRE-Headers finden Sie im Abschnitt "Lesen von ERSPAN-Daten".

Für lokales SPAN

Stellen Sie sicher, dass auf der Schnittstelle, die mit der SPAN-Zielschnittstelle auf dem ACI-Leaf verbunden ist, ein Erfassungstool ausgeführt wird.

Rohpakete werden an dieser Schnittstelle empfangen. Für den ERSPAN-Header ist keine Verarbeitung erforderlich.

Lesen von ERSPAN-Daten

ERSPAN-Version (Typ)

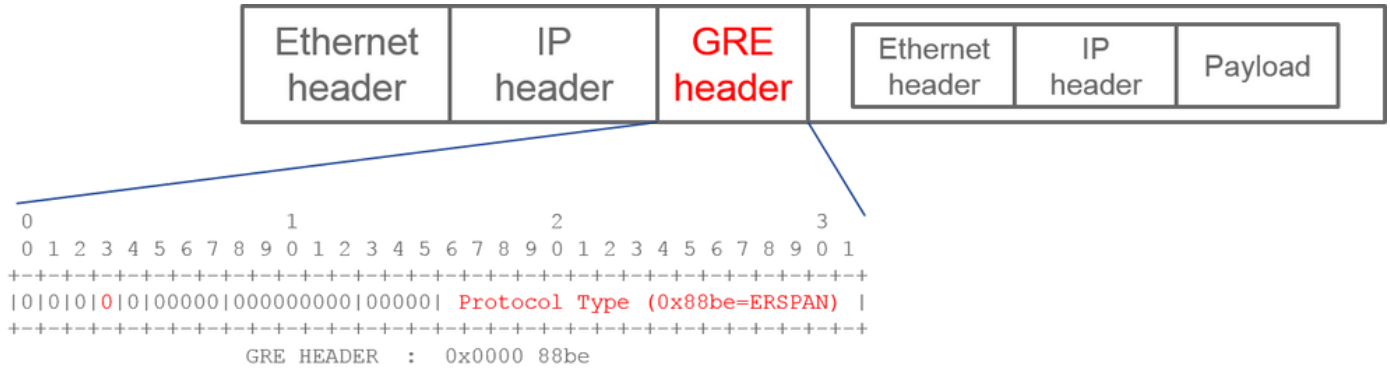
ERSPAN kapselt kopierte Pakete, um sie an das Remote-Ziel weiterzuleiten. GRE wird für diese Kapselung verwendet. Der Protokolltyp für ERSPAN auf dem GRE-Header ist 0x88be.

Im Dokument der Internet Engineering Task Force (IETF) wird die ERSPAN-Version als Typ und nicht als Version beschrieben.

Es gibt drei Arten von ERSPAN. I, II und III. Der ERSPAN-Typ wird in diesem RFC-Entwurf erwähnt. Außerdem kann dieser GRE-RFC1701 hilfreich sein, um jeden ERSPAN-Typ zu verstehen.

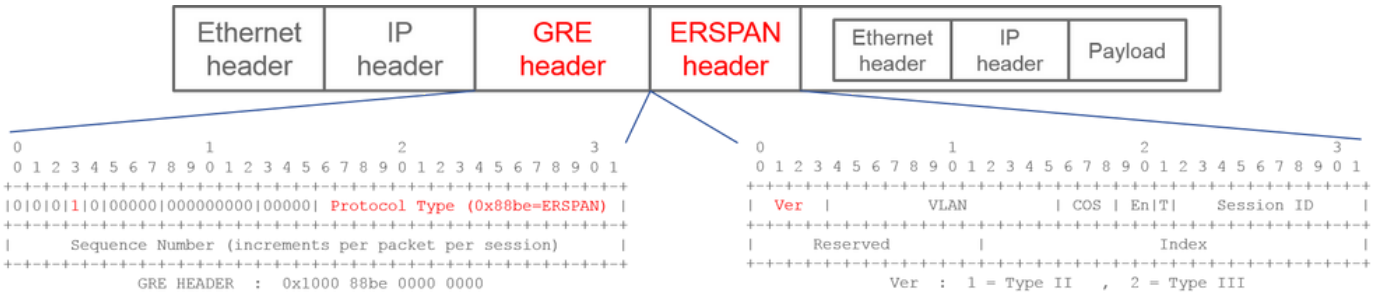
Nachfolgend finden Sie das Paketformat der einzelnen Typen:

ERSPAN Typ I (von Broadcom Trident 2 verwendet)



Bei Typ I wird das Sequenzfeld im GRE-Header nicht verwendet. Er verwendet nicht einmal den ERSPAN-Header, der dem GRE-Header folgen muss, wenn es sich um ERSPAN Typ II und III handelt. Broadcom Trident 2 unterstützt nur diesen ERSPAN Typ I.

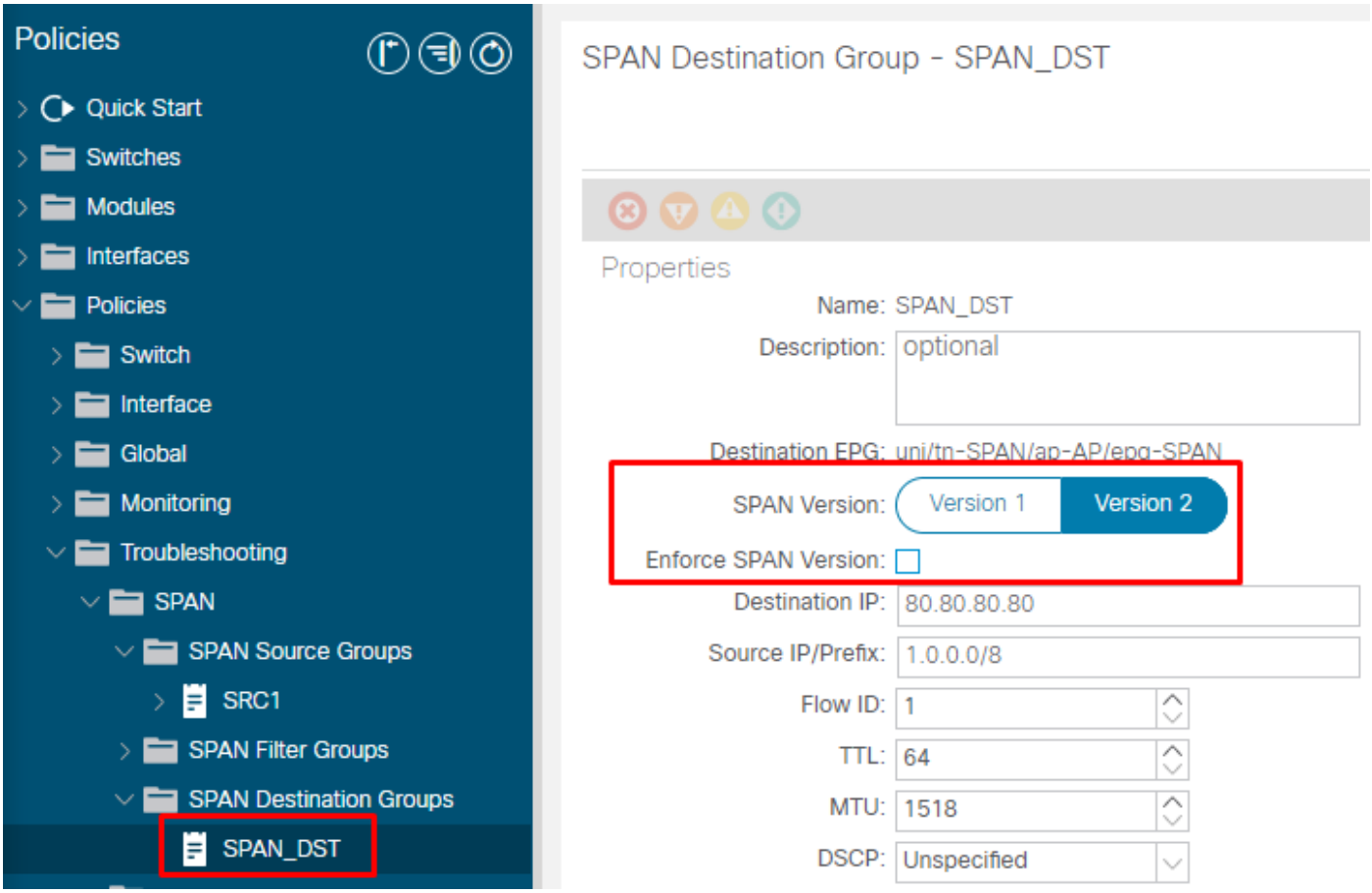
ERSPAN Typ II oder III



Wird das Sequenzfeld durch das S-Bit aktiviert, so muss dies ERSPAN Typ II oder III sein. Das Versionsfeld im ERSPAN-Header gibt den ERSPAN-Typ an. In der ACI wird Typ III ab dem 20.03.2016 nicht mehr unterstützt.

Wenn eine SPAN-Quellgruppe für Access- oder Tenant-SPAN Quellen auf Knoten der 1. und 2. Generation aufweist, empfängt das ERSPAN-Ziel sowohl ERSPAN-Pakete vom Typ I als auch von Typ II von jeder Generation von Knoten. Wireshark kann jedoch jeweils nur einen der ERSPAN-Typen decodieren. Standardmäßig wird nur ERSPAN Typ II dekodiert. Wenn Sie die Dekodierung von ERSPAN Typ I aktivieren, dekodiert Wireshark ERSPAN Typ II nicht. Weitere Informationen zum Decodieren von ERSPAN Typ I in Wireshark finden Sie im nachfolgenden Abschnitt.

Um diese Art von Problem zu vermeiden, können Sie den ERSPAN-Typ für eine SPAN-Zielgruppe konfigurieren.



- SPAN-Version (Version 1 oder Version 2): Bezieht sich auf ERSPAN Typ I oder II

- Erzwingen der SPAN-Version (aktiviert oder deaktiviert): Diese Option entscheidet, ob die SPAN-Sitzung fehlschlagen muss, wenn der konfigurierte ERSPAN-Typ nicht von der Quellknotenhardware unterstützt wird.

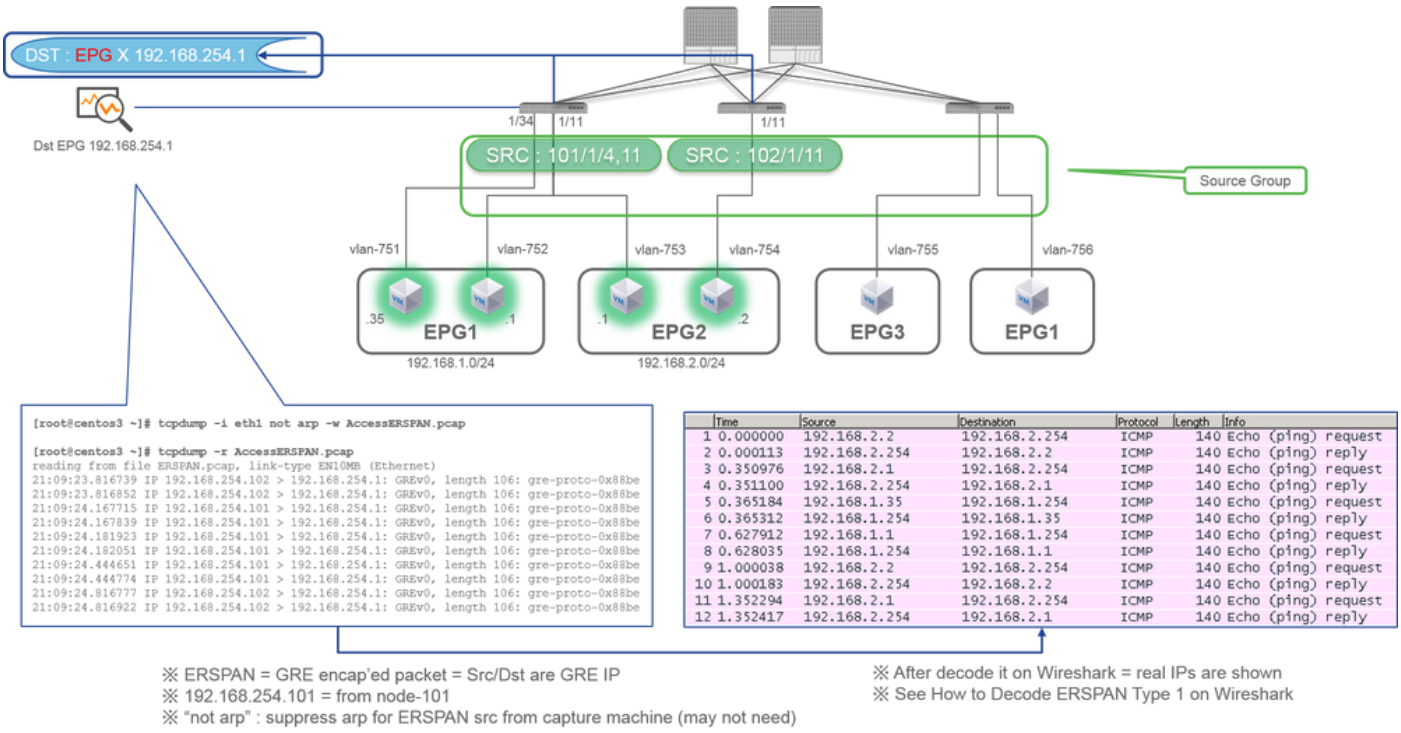
Standardmäßig ist SPAN-Version 2, und SPAN-Version erzwingen ist deaktiviert. Wenn es sich beim Quellknoten um einen Knoten der 2. Generation oder höher handelt, der ERSPAN Typ II unterstützt, generiert er ERSPAN mit Typ II. Wenn der Quellknoten der 1. Generation angehört, die ERSPAN Typ II nicht unterstützt (mit Ausnahme von Fabric SPAN), fällt er auf Typ I zurück, da die SPAN-Version erzwingen nicht aktiviert ist. Dadurch erhält das ERSPAN-Ziel einen gemischten ERSPAN-Typ.

In dieser Tabelle werden die einzelnen Kombinationen für Access und Tenant-SPAN erläutert.

SPAN-Version	SPAN-Version erzwingen	Quellknoten der 1. Generation	Quellknoten der 2. Generation
Version 2	Deaktiviert	Verwendet Typ I	Verwendet Typ II
Version 2	Aktiviert	Fehlschläge	Verwendet Typ II
Version 1	Deaktiviert	Verwendet Typ I	Verwendet Typ I
Version 1	Aktiviert	Verwendet Typ I	Verwendet Typ I

ERSPAN-Datenbeispiel

Tenant-SPAN/Zugangs-SPAN (ERSPAN)



Pakete müssen decodiert werden, da sie von ERSPAN Typ I gekapselt werden. Dies ist mit Wireshark möglich. Weitere Informationen finden Sie im Abschnitt "Decodierung von ERSPAN-Typ 1".

Details des erfassten Pakets (ERSPAN-Typ 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
```

Fabric-SPAN (ERSPAN)

```
[root@centos3 ~]# tcpdump -r FabricERSPAN.pcap
reading from file FabricERSPAN.pcap, link-type EN10MB (Ethernet)
23:25:00.777331 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 54227, length 127: gre-proto-0x88be
23:25:00.777445 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 53328, length 82: gre-proto-0x88be
23:25:00.777567 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 54228, length 187: gre-proto-0x88be
23:25:00.777580 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 53329, length 82: gre-proto-0x88be
23:25:00.778068 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 53330, length 127: gre-proto-0x88be
23:25:00.817915 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 54229, length 82: gre-proto-0x88be
23:25:00.829676 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 54230, length 82: gre-proto-0x88be
23:25:00.829691 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 53331, length 82: gre-proto-0x88be
23:25:00.873953 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 54231, length 82: gre-proto-0x88be
23:25:00.873968 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 53332, length 82: gre-proto-0x88be
```

ERSPAN Type 2 is automatically decoded by Wireshark
※ be noted that this is still iVxLAN header

Filter: ip.addr==10.0.192.92 Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
26	0.184754	10.0.192.92	10.0.32.66	UDP	198	Source port: 7248 Destination port: 48879
27	0.184893	10.0.192.95	10.0.192.92	UDP	198	Source port: 25168 Destination port: 48879
32	0.262735	10.0.192.92	10.0.32.65	UDP	160	Source port: 62672 Destination port: 48879
34	0.262855	10.0.192.92	239.255.255.255	UDP	156	Source port: 38745 Destination port: 48879
35	0.262868	10.0.192.92	239.255.255.255	UDP	156	Source port: 38745 Destination port: 48879
38	0.263458	10.0.192.92	225.0.213.250	UDP	160	Source port: 43738 Destination port: 48879
148	0.768367	10.0.0.1	10.0.192.92	TCP	116	56210-12151 [ACK] Seq=1 Ack=1 Win=770 Len=0
149	0.768486	10.0.192.92	10.0.0.1	TCP	116	[TCP ACKed unseen segment] 12151-56210 [ACK]
152	0.856142	10.0.192.92	225.0.213.248	UDP	164	Source port: 45334 Destination port: 48879
175	0.875130	10.0.192.92	10.0.0.1	TCP	116	[TCP Keep-Alive] [TCP ACKed unseen segment]
176	0.875252	10.0.0.1	10.0.192.92	TCP	116	[TCP Previous segment not captured] 56210-12
234	1.185477	10.0.192.92	10.0.32.66	UDP	198	Source port: 7248 Destination port: 48879
235	1.185606	10.0.192.95	10.0.192.92	UDP	198	Source port: 25168 Destination port: 48879
253	1.259119	10.0.192.92	10.0.0.1	TCP	116	57294-12375 [ACK] Seq=1 Ack=1 Win=270 Len=0

Wireshark decodiert automatisch ERSPAN Typ II. Sie wird jedoch weiterhin vom iVxLAN-Header gekapselt.

Standardmäßig versteht Wireshark den iVxLAN-Header nicht, da es sich um einen internen ACI-Header handelt. Weitere Informationen finden Sie unter "So dekodieren Sie den iVxLAN-Header".

Details des erfassten Pakets (ERSPAN Typ II)

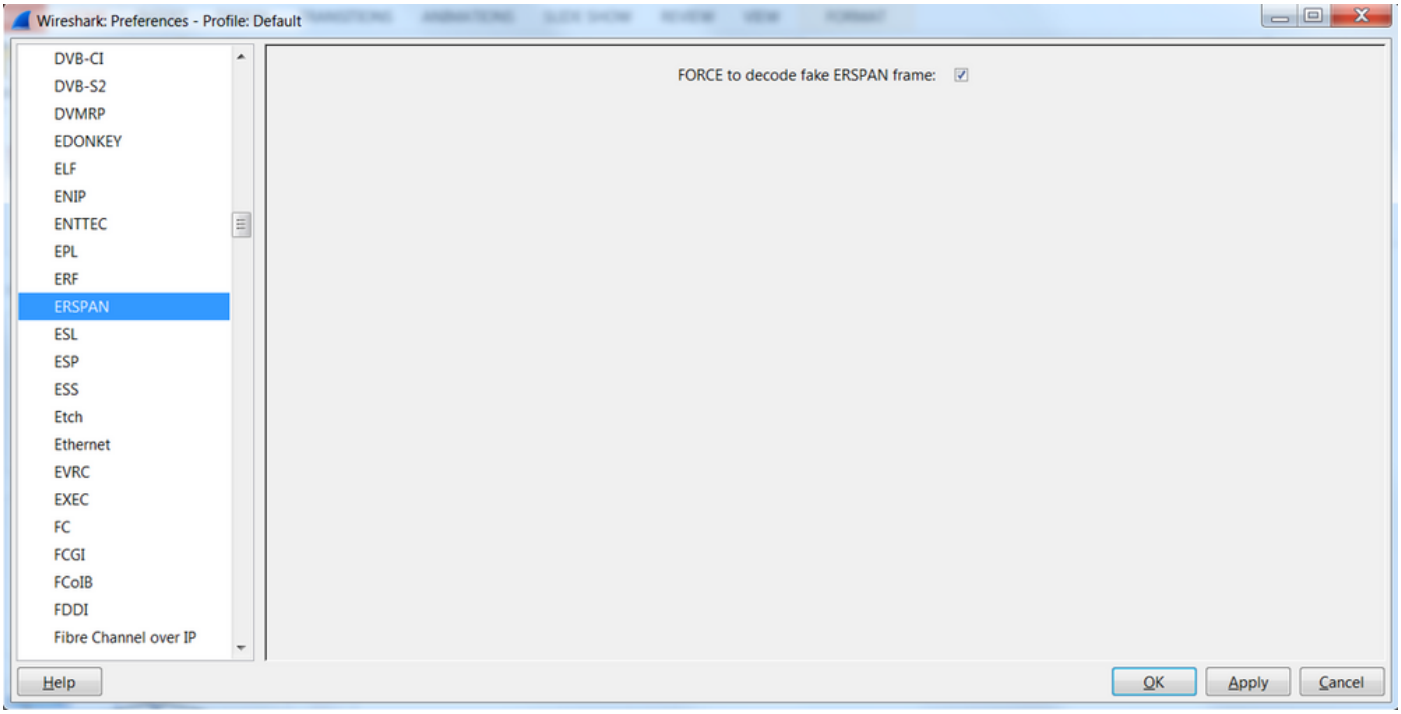
```
[root@centos3 ~]# tcpdump -xxr FabricERSPAN.pcap -c 1
reading from file FabricERSPAN.pcap, link-type EN10MB (Ethernet)
23:25:00.962224 IP 192.168.254.101 > 192.168.254.1: GREv0, seq 53341, length 164: gre-proto-0x88be
        0x0000:  0050 56bb 3096 0022 bdf8 19ff 0800 4500
        0x0010:  00b8 0580 0000 3e2f f8de c0a8 fe65 c0a8
        0x0020:  fe01 1000 88be 0000 d05d 1002 1001 0001
        0x0030:  abcb 000c 0c0c 0c0c 0000 0000 0000 0800
        0x0040:  4500 0086 55aa 0000 1f11 b101 0a00 c05f
        0x0050:  0a00 c05c 6250 beef 0072 0000 c8a0 c007
        0x0060:  fd7f 8200 0050 56bb d95f 0050 56bb d6c2
        0x0070:  0800 4500 0054 799b 0000 4001 7bba c0a8
        0x0080:  0202 c0a8 0201 0000 4f21 b749 0027 3d24
        0x0090:  2b56 0000 0000 c720 0b00 0000 0000 1011
        0x00a0:  1213 1415 1617 1819 1a1b 1c1d 1e1f 2021
        0x00b0:  2223 2425 2627 2829 2a2b 2c2d 2e2f 3031
        0x00c0:  3233 3435 3637

ESPAN Ethernet header          : Dst 0050.56bb.3096 , Src 0022.bdf8.19.ff
ERSPAN IP header               : Dst 192.168.254.1  , Src 192.168.254.101
GRE header (= ERSPAN Type II)  : 0x88be = ERSPAN (S bit on 0x1000)
ERSPAN Type II header          : VLAN 2, ERSPAN ID 1
Ethernet header                : Dst 0022.bdf8.19ff , Src 0050.56bb.d6c2
IP header                      : Dst 10.0.192.95    , Src 10.0.192.92
UDP header                     : Dst 0xbeef(48879)  , Src 0x6250(25168)
iVXLAN header                  : sclass 0xc007 , VNID 0xfd7f82
Ethernet header                : Dst 0050.56bb.d95f , Src 0050.56bb.d6c2
IP header                      : Dst 192.168.2.254  , Src 192.168.2.2
```

Dekodierung von ERSPAN Typ I

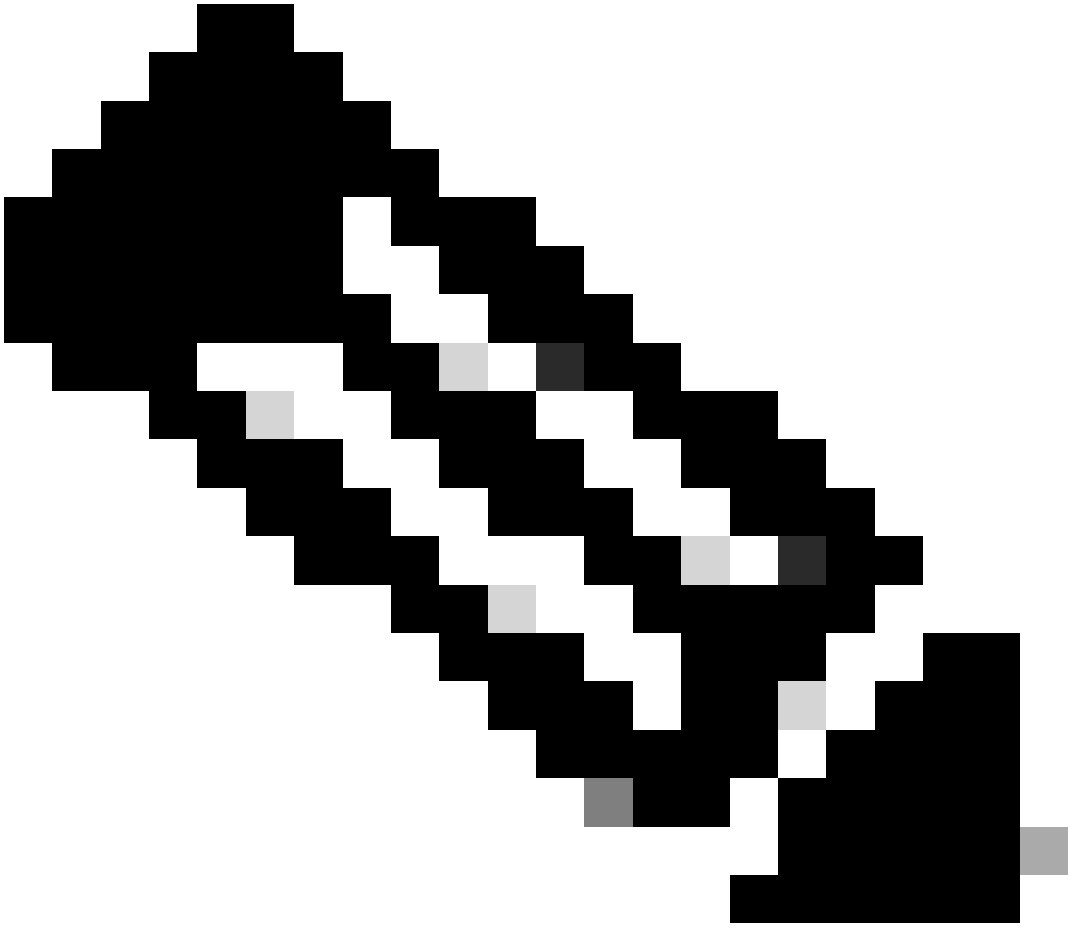
Option 1: Navigieren Sie zu, Edit > Preference > Protocols > ERSPAN und aktivieren Sie FORCE, um den gefälschten ERSPAN-Frame zu decodieren.

- Wireshark (GUI)



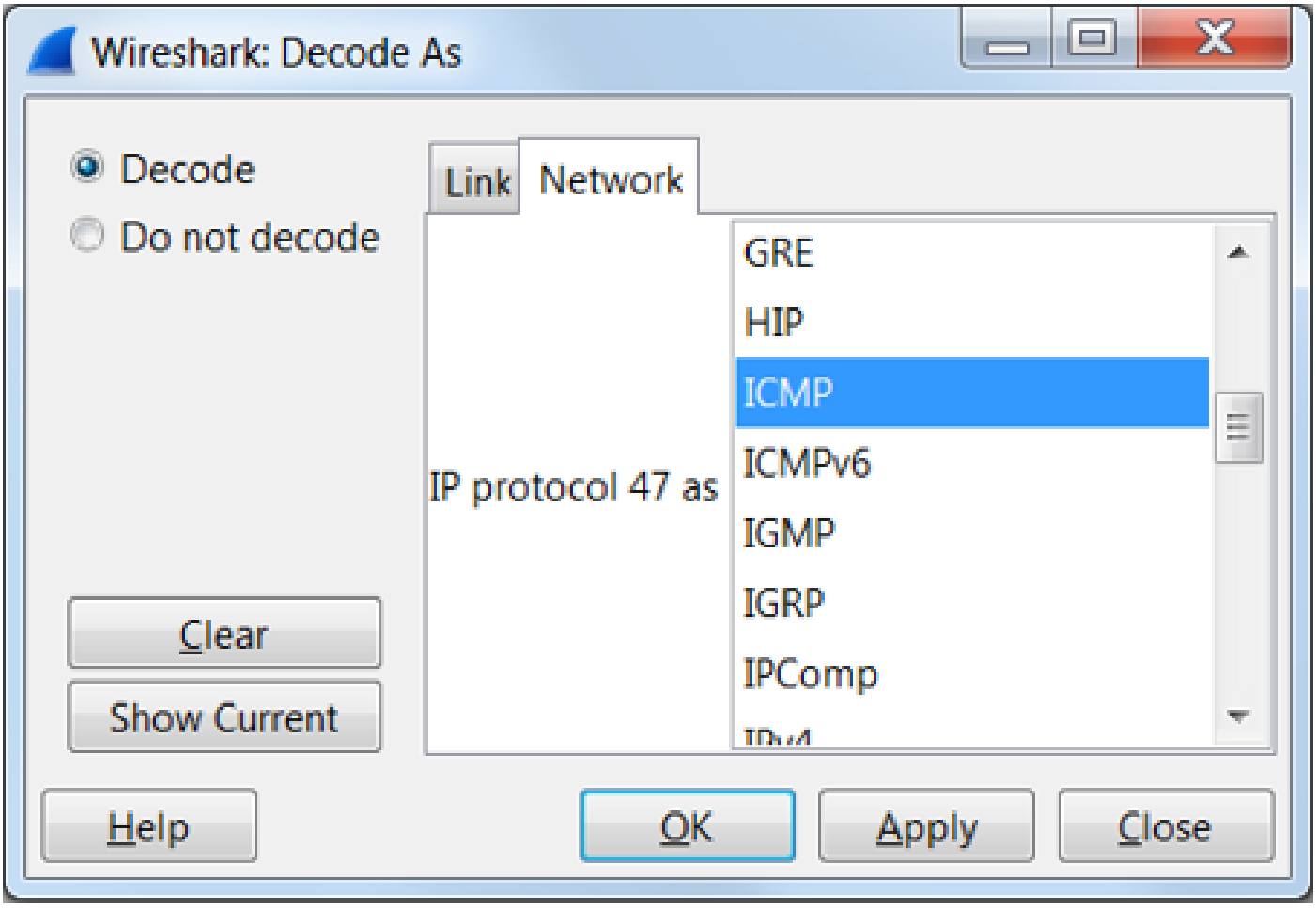
- Tshark (CLI-Version von Wireshark):

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

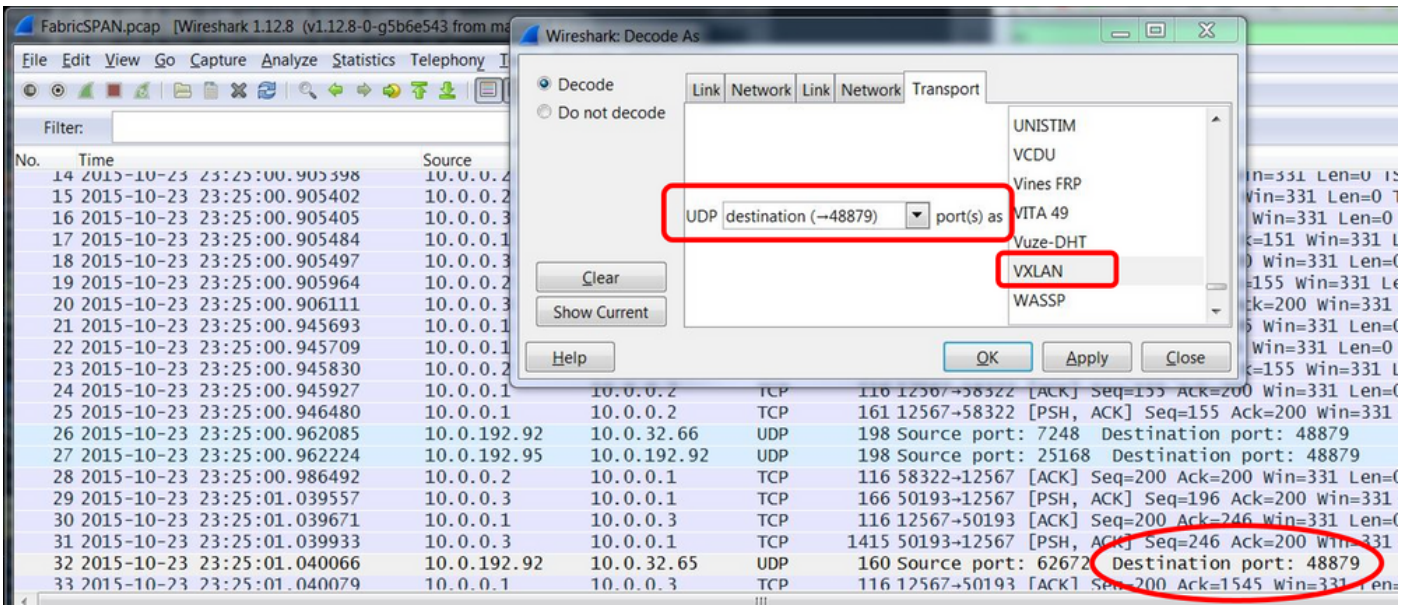


Hinweis: Stellen Sie sicher, dass diese Option beim Lesen von ERSPAN Typ II oder III deaktiviert ist.

Option 2: Navigieren Sie zu Decode As > Network > ICMP (if it’s ICMP).



So dekodieren Sie den iVxLAN-Header

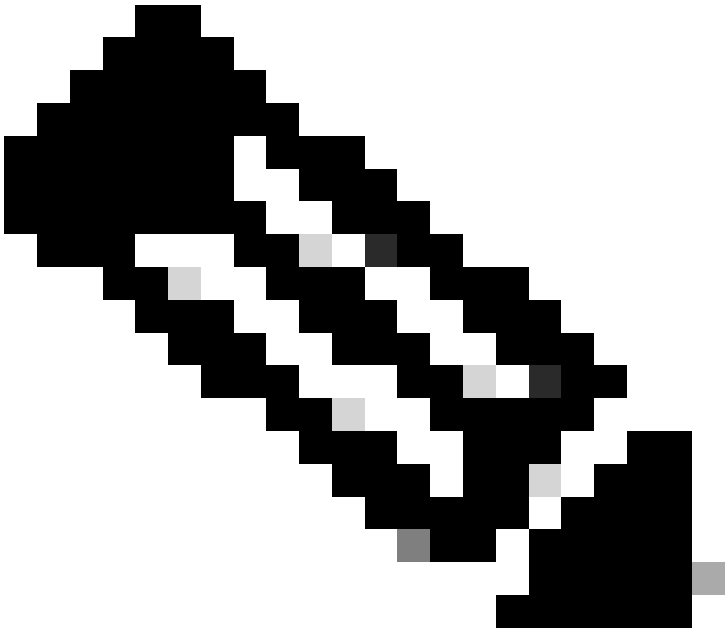


Der iVxLAN-Header verwendet den Zielport 48879. Sie können also sowohl den iVxLAN-Header als auch das VxLAN dekodieren, wenn Sie den UDP-Zielport 48879 in Wireshark als VxLAN konfigurieren.

1. Stellen Sie sicher, dass Sie zuerst VLAN-gekapselte Pakete auswählen.

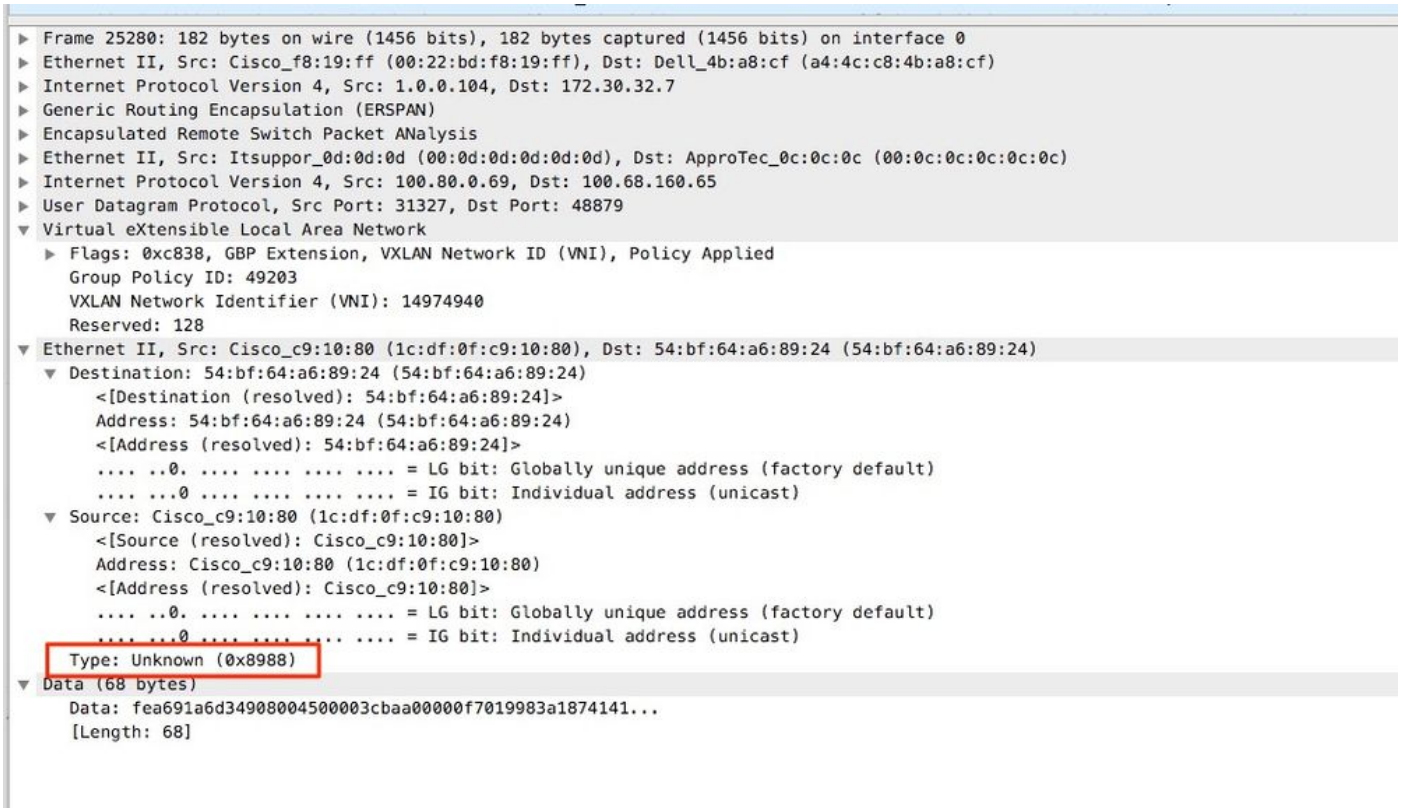
2. Navigieren Sie zu Analyze > Decode As > Transport > UDP destination (48879) > VxLAN.

   - Und dann Apply.



Hinweis: Zwischen den APICs an den Fabric-Ports bestehen Kommunikationspakete. Diese Pakete werden nicht vom iVxLAN-Header gekapselt.

Wenn Sie eine Spanning-Erfassung in einem Anwendernetzwerk durchführen, in dem Precision Time Protocol (PTP) ausgeführt wird, kann es vorkommen, dass Wireshark die Daten aufgrund eines unbekannten Ethertyps innerhalb des GRE-Encaps (0x8988) nicht interpretiert. 0x8988 ist der Ethertyp für das Zeitkennzeichen, das bei aktiviertem PTP in Dataplane-Pakete eingefügt wird. Decodieren Sie den Ethertyp 0x8988 als "Cisco Tag", um die Paketdetails aufzudecken.


Frame 25280: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits) on interface 0
Ethernet II, Src: Cisco_f8:19:ff (00:22:bd:f8:19:ff), Dst: Dell_4b:a8:cf (a4:4c:c8:4b:a8:cf)
Internet Protocol Version 4, Src: 1.0.0.104, Dst: 172.30.32.7
Generic Routing Encapsulation (ERSPAN)
Encapsulated Remote Switch Packet ANalysis
Ethernet II, Src: Itsuppor_0d:0d:0d (00:0d:0d:0d:0d:0d), Dst: ApproTec_0c:0c:0c (00:0c:0c:0c:0c:0c)
Internet Protocol Version 4, Src: 100.80.0.69, Dst: 100.68.160.65
User Datagram Protocol, Src Port: 31327, Dst Port: 48879
Virtual eXtensible Local Area Network
Flags: 0xc838, GBP Extension, VXLAN Network ID (VNI), Policy Applied
Group Policy ID: 49203
VXLAN Network Identifier (VNI): 14974940
Reserved: 128
Ethernet II, Src: Cisco_c9:10:80 (1c:df:0f:c9:10:80), Dst: 54:bf:64:a6:89:24 (54:bf:64:a6:89:24)
Destination: 54:bf:64:a6:89:24 (54:bf:64:a6:89:24)
<[Destination (resolved): 54:bf:64:a6:89:24]>
Address: 54:bf:64:a6:89:24 (54:bf:64:a6:89:24)
<[Address (resolved): 54:bf:64:a6:89:24]>
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: Cisco_c9:10:80 (1c:df:0f:c9:10:80)
<[Source (resolved): Cisco_c9:10:80]>
Address: Cisco_c9:10:80 (1c:df:0f:c9:10:80)
<[Address (resolved): Cisco_c9:10:80]>
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: Unknown (0x8988)
Data (68 bytes)
Data: fea691a6d34908004500003cbaa00000f7019983a1874141...
[Length: 68]

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.