

Fehlerbehebung bei Paketverlusten mit Paketeinfärbungsverfahren oder Plattformzählern

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Topologie](#)

[Option 1. ERSPAN-Einrichtung mit Flow-ID](#)

[Schritt 1. Einrichtung des ESPAN-Ziels](#)

[Schritt 2a: Erstellen einer Spanning Source für den Datenverkehr, der direkt mit dem SRC verbunden ist](#)

[Schritt 2b. Erstellen einer Spanning Source für den Datenverkehr, der direkt mit dem DST verbunden ist](#)

[Schritt 3: Schnelle Wireshark-Analyse](#)

[Option 2. Plattformzähler](#)

[Plattformzähler löschen](#)

[Identifizieren einer Paketgröße mit niedrigen oder null Paketen](#)

[Datenverkehrsfluss verfolgen](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie ein Netzwerkfluss mithilfe von Paketfarbtechniken nachverfolgt wird.

Voraussetzungen

Anforderungen

- Grundkenntnisse der ACI
- Endpunktgruppen und Vertrag
- Wireshark - Grundkenntnisse

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Hardware- und Softwareversionen beschränkt.

Verwendete Geräte:

- Cisco ACI mit Version 5.3(2)
- Übergreifendes Ziel
- Gen2-Switches

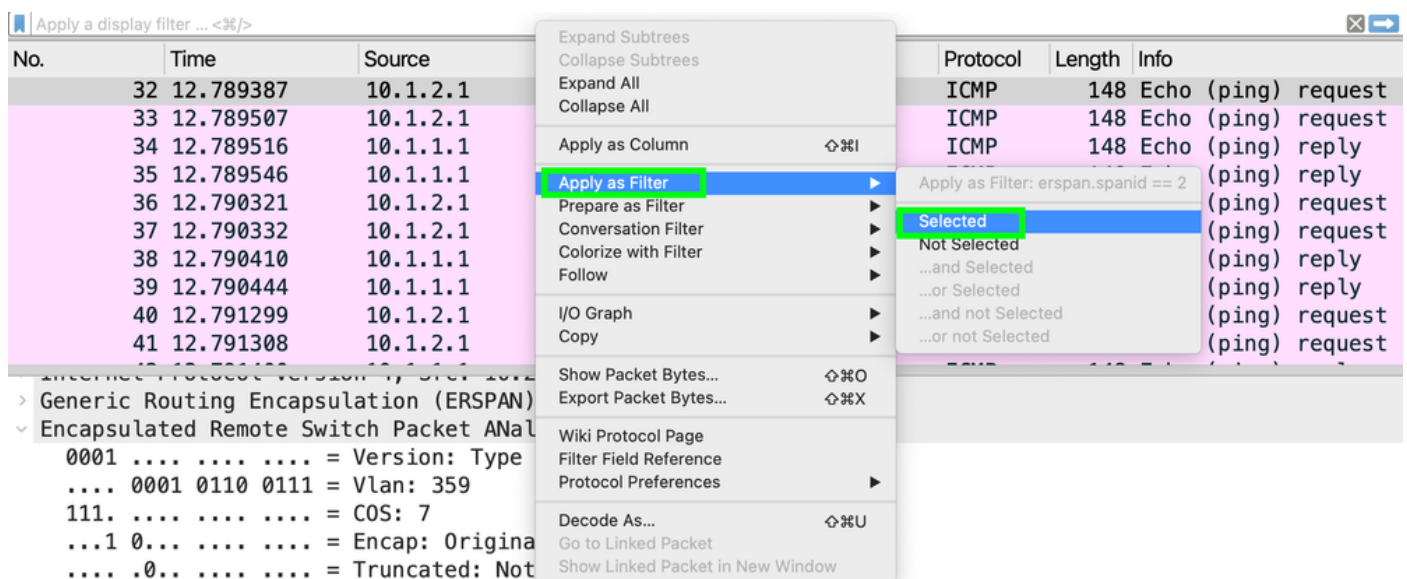
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

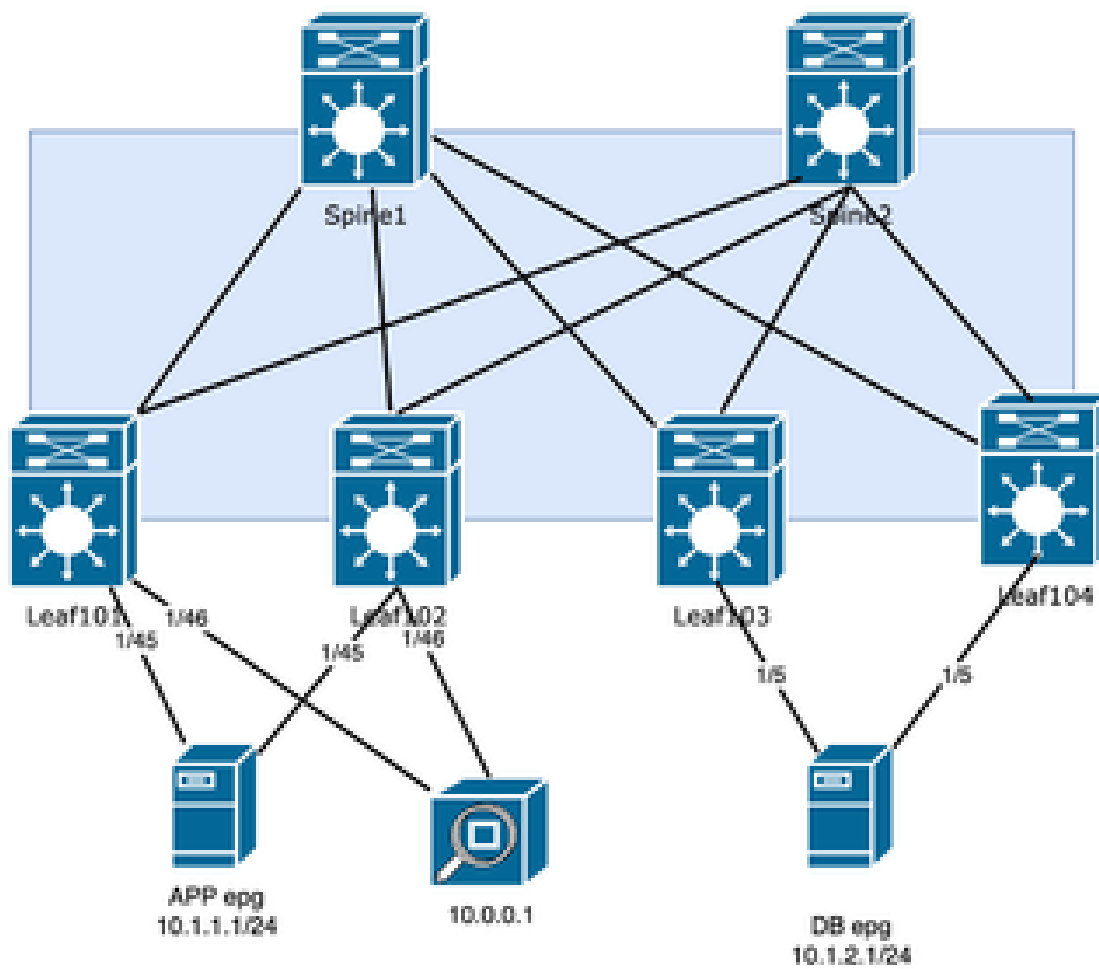
Erstellen von Filtern in Wireshark

Öffnen Sie die Erfassung. Wählen Sie mithilfe eines Frames innerhalb des Encapsulated Remote Switch Packet die Zeile SpanID aus, und klicken Sie mit der rechten Maustaste.

Wählen Sie Anwenden als Filter > Ausgewählt, wie das Bild zeigt:



Topologie



Option 1. ERSPAN-Einrichtung mit Flow-ID

Wenn ein Zielsystem den gesamten Datenverkehr verarbeiten kann, enthält der ERSPAN-Header eine Option zur Definition einer Flow-ID. Diese Flow-ID kann so konfiguriert werden, dass eingehender Datenverkehr an die Fabric identifiziert wird, während eine andere Flow-ID für ausgehenden Datenverkehr eingerichtet werden kann.

Schritt 1. Einrichtung des ESPAN-Ziels

Eine Zielgruppe hat die Flow-ID 1.

Unter Fabric > Access Policies > Policies > Troubleshooting > SPAN > SPAN Destination Groups

Create SPAN Destination Group



Name: All-dst-jr-flowid

Description: optional

Destination Type: **EPG** Access Interface

Destination EPG: jr ALL monitor

Tenant Application Profile EPG

SPAN Version: **Version 1** Version 2

Enforce SPAN Version: ☐

Destination IP: 10.0.0.1

Source IP/Prefix: 10.255.0.0/16

Flow ID: 1

TTL: 64

MTU: 8000

DSCP: Unspecified

Cancel

Submit

Konfigurieren Sie für die zweite Zielgruppe die Fluss-ID 2:

Create SPAN Destination Group

Name:

Description:

Destination Type: EPG Access Interface

Destination EPG:
Tenant Application Profile EPG

SPAN Version: Version 1 Version 2

Enforce SPAN Version: ☐

Destination IP:

Source IP/Prefix:

Flow ID:

TTL:

MTU:

DSCP:

Cancel

Submit

Schritt 2a: Erstellen einer Spanning Source für den Datenverkehr, der direkt mit dem SRC verbunden ist

Unter Fabric > Access Policies > Policies > Troubleshooting > SPAN > SPAN Source Groups

Create SPAN Source Group

Name:

Description:

Admin State: Disabled Enabled

Filter Group:

Destination Group:

Create Sources

Name	Direction	Source EPG	Source Paths
------	-----------	------------	--------------

Filtern Sie den Datenverkehr mehr, indem Sie den Pfad und die EPG hinzufügen. Das

Übungsbeispiel ist Tenant jr Application Profile ALL und EPG app.

Create SPAN Source



Name:

Description:

Direction: Both Incoming Outgoing

Filter Group:

Span Drop Packets: ☐

Type: None EPG Routed Outside

Source EPG:

Tenant Application Profile EPG

Add Source Access Paths

Source Access Path
Pod-1/Node-101/VPC-ESX-169
Pod-1/Node-102/VPC-ESX-169

Cancel OK

Schritt 2b. Erstellen einer Spanning Source für den Datenverkehr, der direkt mit dem DST verbunden ist

Unter Fabric > Access Policies > Policies > Troubleshooting > SPAN > SPAN Source Groups

Create SPAN Source

Description: optional

Direction: **Both** Incoming Outgoing

Filter Group: select an option

Span Drop Packets: ☐

Type: None **EPG** Routed Outside

Source EPG: jr Tenant  ALL Application Profile db EPG

Add Source Access Paths

	 
Source Access Path	
Pod-1/Node-103/eth1/6	

Filtern Sie den Datenverkehr stärker, indem Sie nicht nur den Pfad, sondern auch die EPG-DB hinzufügen:

Create SPAN Source Group

Name: Src-epg-2

Description: optional

Admin State: Disabled **Enabled**

Filter Group: select an option

Destination Group: All-dst-jr-flowid2 

Create Sources

			 
Name	Direction	Source EPG	Source Paths

Schritt 3: Schnelle Wireshark-Analyse

In diesem Beispiel überprüfen Sie, ob die Anzahl der ICMP-Anforderungspakete mit der Anzahl der ICMP-Antwortpakete übereinstimmt, und stellen sicher, dass es in der ACI-Fabric keine Paketverluste gibt.

Öffnen Sie die Erfassung in Wireshark, um den Filter mithilfe der zusammen mit SRC und DST IP konfigurierten SPAN-ID/Flow-ID zu erstellen:

```
<#root>
```

```
(erspan.spanid ==
```

```
and
```

```
) && (ip.src==
```

```
and ip.dst ==
```

```
)
```

Filter für den getesteten Fluss:

```
<#root>
```

```
(erspan.spanid == 1 and icmp) && (ip.src== 10.1.2.1 and ip.dst == 10.1.1.1)
```

Vergewissern Sie sich, dass das angezeigte Paket den gleichen Betrag wie gesendet hat:

(erspan.spanid == 1 and icmp) && (ip.src == 10.1.2.1 and ip.dst == 10.1.1.1)

No.	Time	Source	Destination	Protocol	Length	Info
33	12.789507	10.1.2.1	10.1.1.1	ICMP	148	Echo (ping) request
37	12.790332	10.1.2.1	10.1.1.1	ICMP	148	Echo (ping) request
41	12.791308	10.1.2.1	10.1.1.1	ICMP	148	Echo (ping) request
45	12.792088	10.1.2.1	10.1.1.1	ICMP	148	Echo (ping) request
49	12.792891	10.1.2.1	10.1.1.1	ICMP	148	Echo (ping) request
53	12.793663	10.1.2.1	10.1.1.1	ICMP	148	Echo (ping) request
57	12.794455	10.1.2.1	10.1.1.1	ICMP	148	Echo (ping) request
61	12.795259	10.1.2.1	10.1.1.1	ICMP	148	Echo (ping) request
65	12.796080	10.1.2.1	10.1.1.1	ICMP	148	Echo (ping) request
69	12.796812	10.1.2.1	10.1.1.1	ICMP	148	Echo (ping) request

> Frame 33: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits)
 > Ethernet II, Src: Cisco_f8:19:ff (00:22:bd:f8:19:ff), Dst: VMware_b7:4c:66 (00:50:56:b7:4c:66)
 > Internet Protocol Version 4, Src: 10.255.0.102, Dst: 10.0.0.1
 > Generic Routing Encapsulation (ERSPAN)
 > Encapsulated Remote Switch Packet Analysis Type II
 0001 = Version: Type II (1)
 1010 0111 1110 = Vlan: 2686
 000. = COS: 0
 ...1 0... = Encap: Originally 802.1Q encapsulated (2)
 0... = Truncated: Not truncated (0)
00 0000 0001 = SpanID: 1
 0000 0000 0000 = Reserved: 0

SpanID (erspan.spanid), 10 bits Packets: 4109 Displayed: 1000 (24.3%) Profile:

Die nächste SPAN-ID muss den gleichen Betrag aufweisen. Andernfalls wurde das Paket innerhalb der Fabric verworfen.

Filter:

(erspan.spanid == 2 and icmp) && (ip.src == 10.1.2.1 and ip.dst == 10.1.1.1)

Wireshark packet capture interface showing an ERSPAN filter: `(erspan.spanid == 2 and icmp) && (ip.src == 10.1.2.1 and ip.dst == 10.1.1.1)`.

No.	Time	Source	Destination	Protocol	Length	Info
32	12.789387	10.1.2.1	10.1.1.1	ICMP	148	Echo (ping) request
36	12.790321	10.1.2.1	10.1.1.1	ICMP	148	Echo (ping) request
40	12.791299	10.1.2.1	10.1.1.1	ICMP	148	Echo (ping) request
44	12.792076	10.1.2.1	10.1.1.1	ICMP	148	Echo (ping) request
48	12.792880	10.1.2.1	10.1.1.1	ICMP	148	Echo (ping) request
52	12.793654	10.1.2.1	10.1.1.1	ICMP	148	Echo (ping) request
56	12.794434	10.1.2.1	10.1.1.1	ICMP	148	Echo (ping) request
60	12.795250	10.1.2.1	10.1.1.1	ICMP	148	Echo (ping) request
64	12.796038	10.1.2.1	10.1.1.1	ICMP	148	Echo (ping) request
68	12.796797	10.1.2.1	10.1.1.1	ICMP	148	Echo (ping) request

Packet details for Frame 32:

- Frame 32: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits)
- Ethernet II, Src: Cisco_f8:19:ff (00:22:bd:f8:19:ff), Dst: VMware_b7:4c:66 (00:50:56:b7:4c:66)
- Internet Protocol Version 4, Src: 10.255.0.103, Dst: 10.0.0.1
- Generic Routing Encapsulation (ERSPAN)
- Encapsulated Remote Switch Packet Analysis Type II
 - 0001 = Version: Type II (1)
 - 0001 0110 0111 = Vlan: 359
 - 111. = COS: 7
 - ...1 0... = Encap: Originally 802.1Q encapsulated (2)
 -0.. = Truncated: Not truncated (0)
 -00 0000 0010 = SpanID: 2
 - 0000 0000 0000 = Reserved: 0

Status bar: Packets: 4109 Displayed: 1000 (24.3%)

Option 2. Plattformzähler

Diese Methode nutzt den Vorteil, dass Nexus die Leistung einzelner Schnittstellen mit unterschiedlichen Paketgrößen verfolgt, dass jedoch mindestens eine Warteschlange einen geringen Datenverkehr, wenn nicht gar null, aufweisen muss.

Plattformzähler löschen

Öffnen Sie den individuellen Switch, und deaktivieren Sie die Schnittstelle, die mit den Geräten verbunden ist.

```
<#root>
```

```
Switch#
```

```
vsh_lc -c "clear platform internal counters port
```

```
"
```

```
<#root>
```

```
LEAF3#
```

```
vsh_lc -c "clear platform internal counters port 6"
```

```
LEAF1#
```

```
vsh_lc -c "clear platform internal counters port 45"
```

```
LEAF2#
```

```
vsh_lc -c "clear platform internal counters port 45"
```

Identifizieren einer Paketgröße mit niedrigen oder null Paketen

Suchen Sie nach einer Paketgröße, die möglicherweise keine Zähler in allen Leafs für RX und TX enthält:

```
<#root>
```

```
vsh_lc -c 'show platform internal counters port
```

```
' | grep X_PKT
```

Im nächsten Beispiel ist die Paketgröße größer als 512 und kleiner als 1024:

```
<#root>
```

```
LEAF101#
```

```
vsh_lc -c "show platform internal counters port 45 " | grep X_PKT
```

RX_PKTOK	1187
RX_PKTTOTAL	1187
RX_PKT_LT64	0
RX_PKT_64	0
RX_PKT_65	1179
RX_PKT_128	8
RX_PKT_256	0
RX_PKT_512	0 <<
RX_PKT_1024	0
RX_PKT_1519	0
RX_PKT_2048	0
RX_PKT_4096	7

RX_PKT_8192	43
RX_PKT_GT9216	0
TX_PKT0K	3865
TX_PKTTOTAL	3865
TX_PKT_LT64	0
TX_PKT_64	0
TX_PKT_65	3842
TX_PKT_128	17
TX_PKT_256	6
TX_PKT_512	0 <<
TX_PKT_1024	10
TX_PKT_1519	3
TX_PKT_2048	662
TX_PKT_4096	0
TX_PKT_8192	0
TX_PKT_GT9216	0

Der Schritt muss in der Verbindung ausgeführt werden, an die die Pakete weitergeleitet werden.

Datenverkehrsfluss verfolgen

Vom Server 10.1.2.1 werden 1.000 Pakete mit einer Paketgröße von 520 gesendet.

Überprüfen Sie auf der Leaf 103-Schnittstelle 1/6, wo der Datenverkehr auf RX initiiert wird:

```
<#root>
```

```
MXS2-LF103#
```

```
vsh_lc -c "show platform internal counters port 6 " | grep X_PKT_512
```

RX_PKT_512	1000
TX_PKT_512	647

1000 Paket RX, aber nur 647 wurden als Antwort gesendet.

Der nächste Schritt besteht darin, die ausgehenden Schnittstellen der anderen Server zu überprüfen:

Für Leaf102:

```
<#root>
```

```
MXS2-LF102#
```

```
vsh_lc -c "show platform internal counters port 45 " | grep X_PKT_512
```

RX_PKT_512	0
TX_PKT_512	1000

Die Anforderung wurde vom Fabric nicht verworfen.

Für Leaf 101 ist RX mit 647 verbunden und entspricht der Anzahl an Paketen TX von ACI.

<#root>

MXS2-LF101#

```
vsh_lc -c "show platform internal counters port 45 " | grep X_PKT_512
```

RX_PKT_512	647
TX_PKT_512	0

Zugehörige Informationen

[Fehlerbehebung: ACI Intra-Fabric Forwarding - zeitweilige Unterbrechungen](#)

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.