

Risoluzione dei problemi relativi alle perdite di pacchetti con le tecniche di colorazione dei pacchetti o i contatori della piattaforma

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Topologia](#)

[Opzione 1. Impostazione di ERSPAN con Flow-id](#)

[Passaggio 1. Impostazione destinazione ESPAN](#)

[Passaggio 2a. Crea Span Source per il traffico connesso direttamente a SRC](#)

[Passaggio 2b. Crea origine span per il traffico connesso direttamente a DST](#)

[Passaggio 3. Analisi rapida di Wireshark](#)

[Opzione 2. Contatori della piattaforma](#)

[Cancella contatori piattaforma](#)

[Identificazione delle dimensioni di un pacchetto con pacchetti bassi o zero](#)

[Traccia flusso traffico](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive come tenere traccia di un flusso di rete utilizzando le tecniche di colorazione dei pacchetti.

Prerequisiti

Requisiti

- Conoscenze base di ACI
- Gruppi di endpoint e contratto
- Conoscenze base di Wireshark

Componenti usati

Il documento può essere consultato per tutte le versioni hardware o software.

Dispositivi usati:

- Cisco ACI con versione 5.3(2)
- Destinazione Span
- Switch Gen2

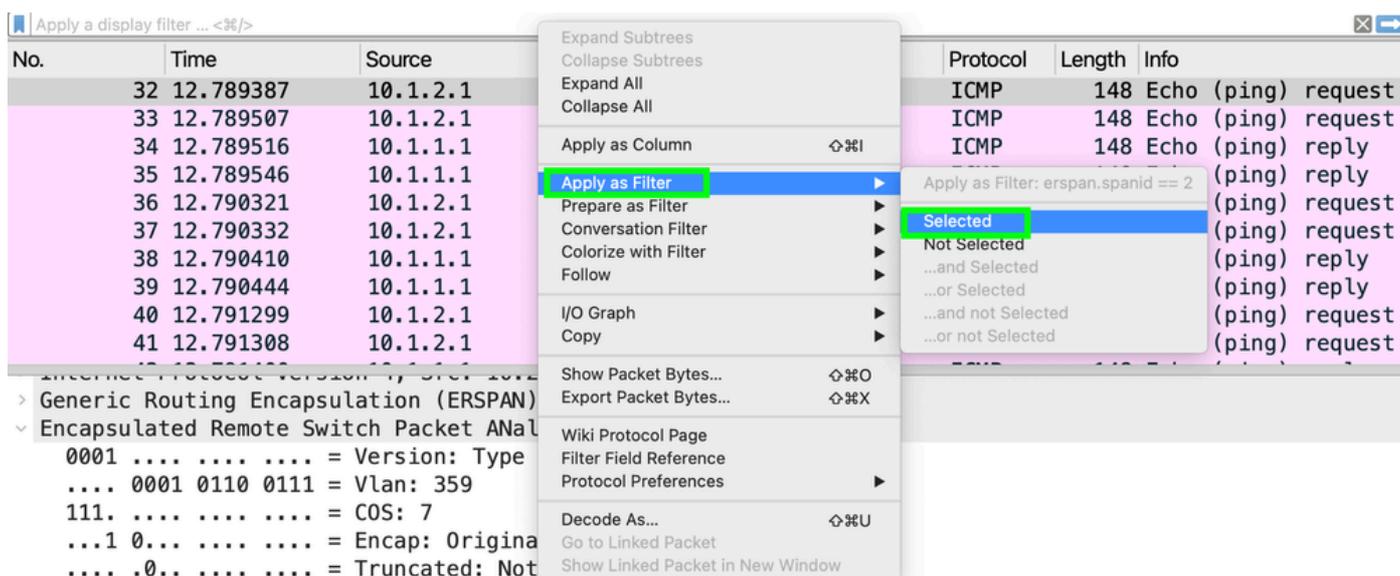
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

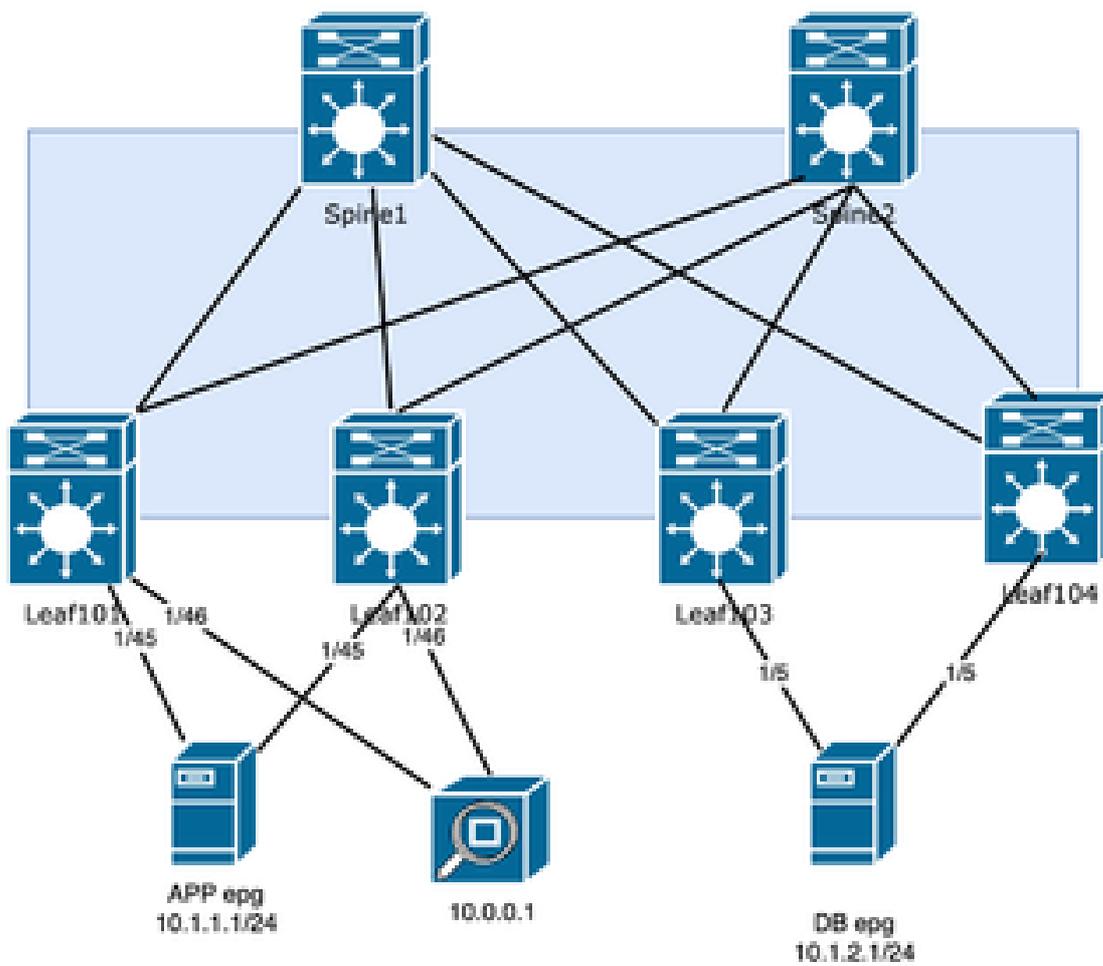
Come creare filtri in Wireshark.

Aprire l'acquisizione. Utilizzando un frame nel pacchetto dello switch remoto incapsulato, selezionare la riga SpanID e fare clic con il pulsante destro del mouse.

Selezionare **Applica come filtro** > **Selezionato come illustrato nell'immagine**:



Topologia



Opzione 1. Impostazione di ERSPAN con Flow-id

Se un server di destinazione è in grado di gestire tutto il traffico, l'installazione ERSPAN include un'opzione per definire un ID flusso. È possibile configurare questo ID di flusso per identificare il traffico in entrata nell'infrastruttura, mentre è possibile impostare un ID di flusso diverso per il traffico in uscita.

Passaggio 1. Impostazione destinazione ESPAN

A un gruppo di destinazione verrà assegnato l'ID flusso 1

In Fabric > Criteri di accesso > Criteri > Risoluzione dei problemi > SPAN > Gruppi di destinazione SPAN

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

Sul secondo gruppo di destinazione, configurare l'ID flusso 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

Passaggio 2a. Creazione dell'origine dello span per il traffico connesso direttamente all'SRC

In Fabric > Access Policies > Policies > Troubleshooting > SPAN > SPAN Source Groups (Policy di accesso > Criteri > Risoluzione problemi > SPAN > Gruppi di origini SPAN)

Create SPAN Source Group



Name:

Description:

Admin State: Disabled Enabled

Filter Group:

Destination Group:

Create Sources



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

Filtrare ulteriormente il traffico aggiungendo il Percorso e l'EPG. L'esempio di laboratorio è Tenant jr Application Profile ALL e 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**

Passaggio 2b. Crea origine span per il traffico connesso direttamente a DST

In Fabric > Access Policies > Policies > Troubleshooting > SPAN > SPAN Source Groups (Policy di accesso > Criteri > Risoluzione problemi > SPAN > Gruppi di origini SPAN)

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	 

Filtrare ulteriormente il traffico aggiungendo non solo il percorso ma anche il database EPG:

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	
				 

Passaggio 3. Analisi rapida di Wireshark

Nell'esempio, si sta verificando che il numero di pacchetti di richiesta ICMP corrisponda al numero di pacchetti di risposta ICMP, in modo da verificare che non vi siano perdite di pacchetti all'interno dell'infrastruttura ACI.

Aprire l'acquisizione su wireshark per creare il filtro utilizzando l'ID SPAN /Flow-ID configurato con

SRC e IP DST:

```
<#root>
```

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

```
and
```

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

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

```
)
```

Filtro utilizzato per il flusso testato in laboratorio:

```
<#root>
```

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

Verificare che il pacchetto visualizzato corrisponda alla quantità inviata:

(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:

L'ID SPAN successivo deve avere lo stesso importo; in caso contrario, il pacchetto è stato scaricato all'interno della struttura.

Filtro:

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

(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) requ
36	12.790321	10.1.2.1	10.1.1.1	ICMP	148	Echo (ping) requ
40	12.791299	10.1.2.1	10.1.1.1	ICMP	148	Echo (ping) requ
44	12.792076	10.1.2.1	10.1.1.1	ICMP	148	Echo (ping) requ
48	12.792880	10.1.2.1	10.1.1.1	ICMP	148	Echo (ping) requ
52	12.793654	10.1.2.1	10.1.1.1	ICMP	148	Echo (ping) requ
56	12.794434	10.1.2.1	10.1.1.1	ICMP	148	Echo (ping) requ
60	12.795250	10.1.2.1	10.1.1.1	ICMP	148	Echo (ping) requ
64	12.796038	10.1.2.1	10.1.1.1	ICMP	148	Echo (ping) requ
68	12.796797	10.1.2.1	10.1.1.1	ICMP	148	Echo (ping) requ

> 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

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

Opzione 2. Contatori della piattaforma

Questo metodo sfrutta il fatto che Nexus sta monitorando le prestazioni di singole interfacce con dimensioni del pacchetto diverse, ma richiede che almeno una coda abbia una quantità bassa di traffico, se non zero.

Cancella contatori piattaforma

Accedere allo switch e cancellare il contenuto dell'interfaccia che si connette ai dispositivi.

```
<#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"
```

Identificazione delle dimensioni di un pacchetto con pacchetti bassi o zero

Trovare un pacchetto di dimensioni che potrebbe non avere contatori in tutti i fogli sia per RX che per TX:

```
<#root>
```

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

```
' | grep X_PKT
```

Nell'esempio successivo, le dimensioni del pacchetto sono maggiori di 512 e minori di 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_PKTOK	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

Questa operazione deve essere eseguita nel collegamento dove i pacchetti vengono inoltrati.

Traccia flusso traffico

Dal server 10.1.2.1, vengono inviati 1000 pacchetti con dimensioni pari a 520.

Verificare sull'interfaccia 1/6 di Leaf 103, dove il traffico viene avviato su RX:

```
<#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 pacchetti RX, ma solo 647 sono stati inviati come risposta.

Il passaggio successivo consiste nel controllare le interfacce in uscita degli altri server:

Per 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

L'infrastruttura non ha eliminato la richiesta.

Per Leaf 101, pacchetti RX 647 ed è la stessa quantità di pacchetti TX da parte di 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

Informazioni correlate

[Risoluzione dei problemi di inoltro intra-fabric ACI - Cadute intermittenti](#)

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).