

Resolución de problemas de paquetes descartados con técnicas de coloreado de paquetes o contadores de plataforma

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Topología](#)

[Opción 1. Configuración de ERSPAN con Flow-id](#)

[Paso 1. Configuración de destino de ESPAN](#)

[Paso 2a. Creación de un Origen de Tramo para el Tráfico Directamente Conectado al SRC](#)

[Paso 2b. Crear origen de expansión para el tráfico conectado directamente al DST](#)

[Paso 3. Análisis rápido de Wireshark](#)

[Opción 2. Contadores de plataforma](#)

[Borrar contadores de plataforma](#)

[Identificar un tamaño de paquete con paquetes bajos o nulos](#)

[Seguimiento del flujo de tráfico](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo realizar un seguimiento de un flujo de red mediante técnicas de coloreado de paquetes.

Prerequisites

Requirements

- Conocimientos básicos de ACI
- Grupos de terminales y contratos
- Conocimientos básicos de Wireshark

Componentes Utilizados

Este documento no se limita a versiones específicas de hardware y software.

Dispositivos utilizados:

- Cisco ACI versión 5.3(2)
- Destino de extensión
- Switches Gen2

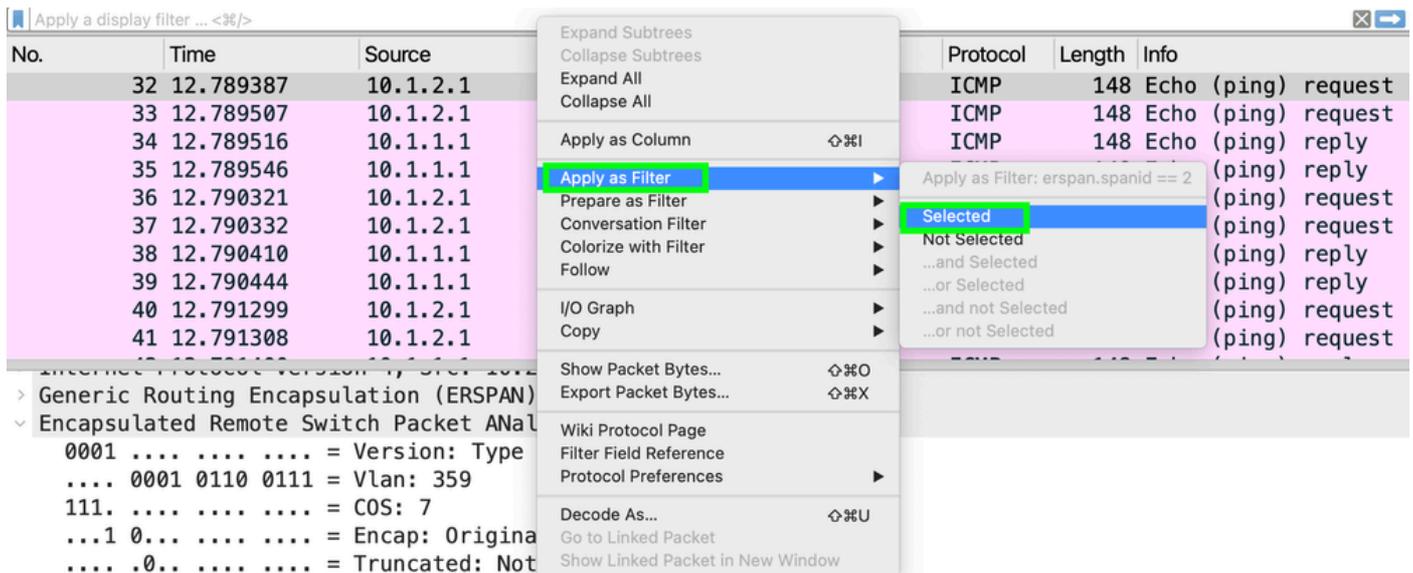
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

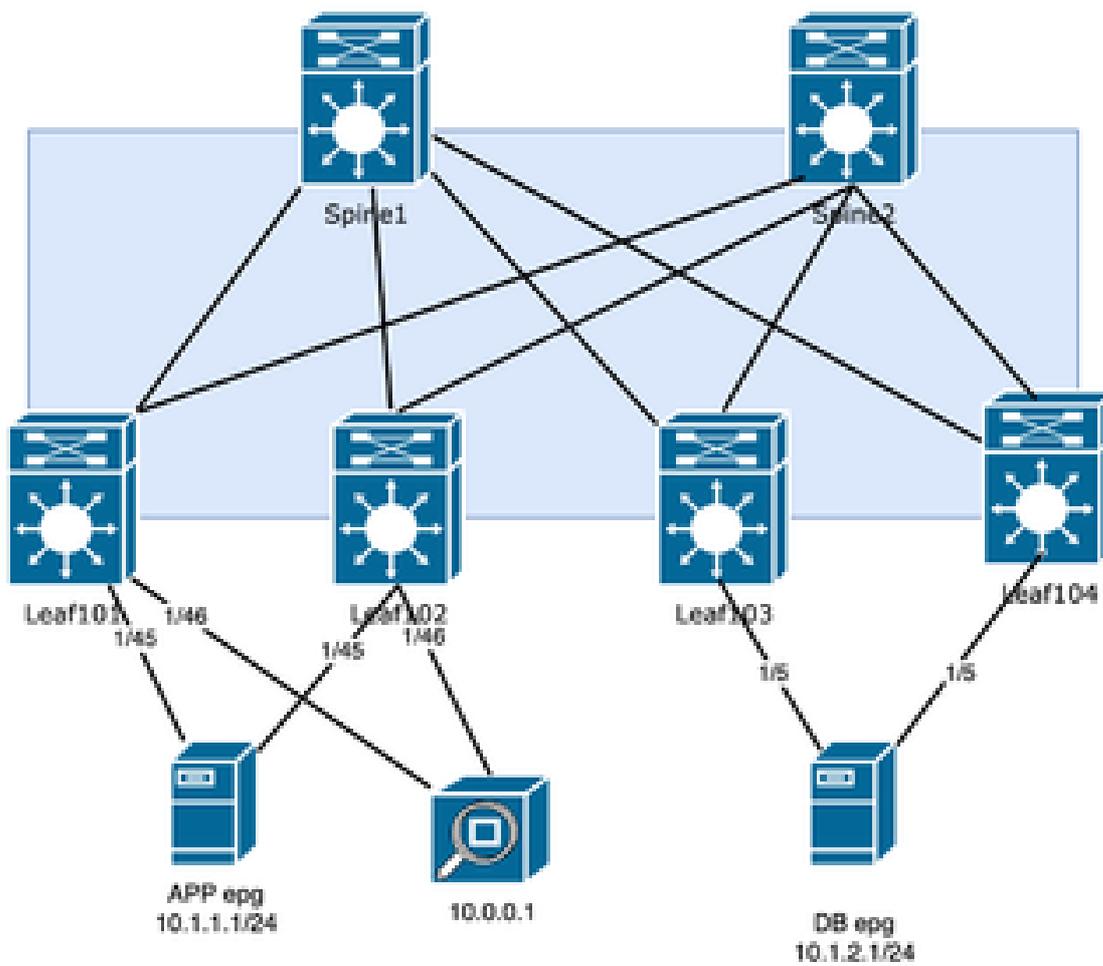
Cómo crear filtros en Wireshark.

Abra la captura. Con un marco dentro del paquete de switch remoto encapsulado, seleccione la línea SpanID y haga clic con el botón derecho.

Seleccione Apply as Filter > Selected como se muestra en la imagen:



Topología



Opción 1. Configuración de ERSPAN con Flow-id

Si un servidor de destino es capaz de manejar todo el tráfico, el encabezado ERSPAN incluye una opción para definir un ID de flujo. Este ID de flujo se puede configurar para identificar el tráfico entrante en el fabric, mientras que se puede configurar un ID de flujo diferente para el tráfico saliente.

Paso 1. Configuración de destino de ESPAN

Un grupo de destino tendrá el id de flujo de 1

En 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

En el segundo grupo de destino, configure flow-id de 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

Paso 2a. Creación del Origen de Tramo para el Tráfico Conectado Directamente al SRC

En Fabric > Access Policies > Políticas > 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
------	-----------	------------	--------------

Filtre más el tráfico agregando la ruta y el EPG. El ejemplo de laboratorio es el perfil de aplicación

de arrendatario jr ALL y la aplicación EPG.

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

Paso 2b. Crear origen de expansión para el tráfico conectado directamente al DST

En Fabric > Access Policies > Políticas > 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	 

Filtre más el tráfico añadiendo no solo la ruta, sino también la base de datos de 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	
				 

Paso 3. Análisis rápido de Wireshark

En este ejemplo, está verificando que el número de paquetes de solicitud ICMP coincida con el número de paquetes de respuesta ICMP, asegurándose de que no haya descartes de paquetes dentro del fabric ACI.

Abra la captura en wireshark para crear el filtro usando el ID de SPAN /Flow-ID configurado junto

con la IP de SRC y DST:

```
<#root>
```

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

```
and
```

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

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

```
)
```

Filtro utilizado para el flujo probado en laboratorio:

```
<#root>
```

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

Verifique que el paquete mostrado tenga la misma cantidad que la enviada:

(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:

El siguiente ID de SPAN debe tener la misma cantidad; si no es así, el paquete se descartó dentro del fabric.

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%)

Opción 2. Contadores de plataforma

Este método aprovecha que Nexus está realizando un seguimiento del rendimiento de interfaces individuales con diferentes tamaños de paquete, pero el método requiere que al menos una cola tenga una cantidad baja de tráfico, si no cero.

Borrar contadores de plataforma

Entre en el switch individual y borre la interfaz individual que se conecta a los dispositivos.

```
<#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"
```

Identificar un tamaño de paquete con paquetes bajos o nulos

Busque un tamaño de paquete que posiblemente no tenga contadores en todas las hojas para RX y TX:

```
<#root>
```

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

```
' | grep X_PKT
```

En el siguiente ejemplo, tamaño de paquete mayor que 512 e inferior a 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

```

El paso debe realizarse en el link donde se le reenvían los paquetes.

Seguimiento del flujo de tráfico

Desde el servidor 10.1.2.1, se envían 1000 paquetes con un tamaño de paquete de 520.

Verifique en la interfaz 1/6 de la hoja 103, donde el tráfico se inicia en 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 paquetes RX, pero solo se enviaron 647 como respuesta.

El siguiente paso es verificar las interfaces salientes de los otros servidores:

Para 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

```

El fabric no descartó la solicitud.

Para la hoja 101, los paquetes RX 647 y es la misma cantidad de paquetes TX por 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

Información Relacionada

[Resolución de problemas de reenvío intrafabric de ACI: caídas intermitentes](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).