

Solucione problemas de quedas de pacotes com técnicas de colorir pacotes ou contadores de plataforma

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Topologia](#)

[Opção 1. Configuração de ERSPAN com Flow-id](#)

[Etapa 1. Configuração do destino ESPAN](#)

[Passo 2a. Criar fonte de abrangência para o tráfego diretamente conectado ao SRC](#)

[Passo 2b. Crie uma origem de abrangência para o tráfego diretamente conectado ao DST](#)

[Etapa 3. Análise Rápida do Wireshark](#)

[Opção 2. Contadores de plataforma](#)

[Limpar Contadores de Plataforma](#)

[Identificar um tamanho de pacote com pacotes baixos ou zero](#)

[Fluxo de tráfego de rastreamento](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como rastrear um fluxo de rede usando técnicas de colorir de pacotes.

Pré-requisitos

Requisitos

- Conhecimento básico da ACI
- Grupos de endpoints e contrato
- Conhecimento básico do Wireshark

Componentes Utilizados

Este documento não está restrito a versões específicas de hardware e software.

Dispositivos usados:

- Cisco ACI executando a versão 5.3(2)
- Destino da abrangência
- Switches Gen2

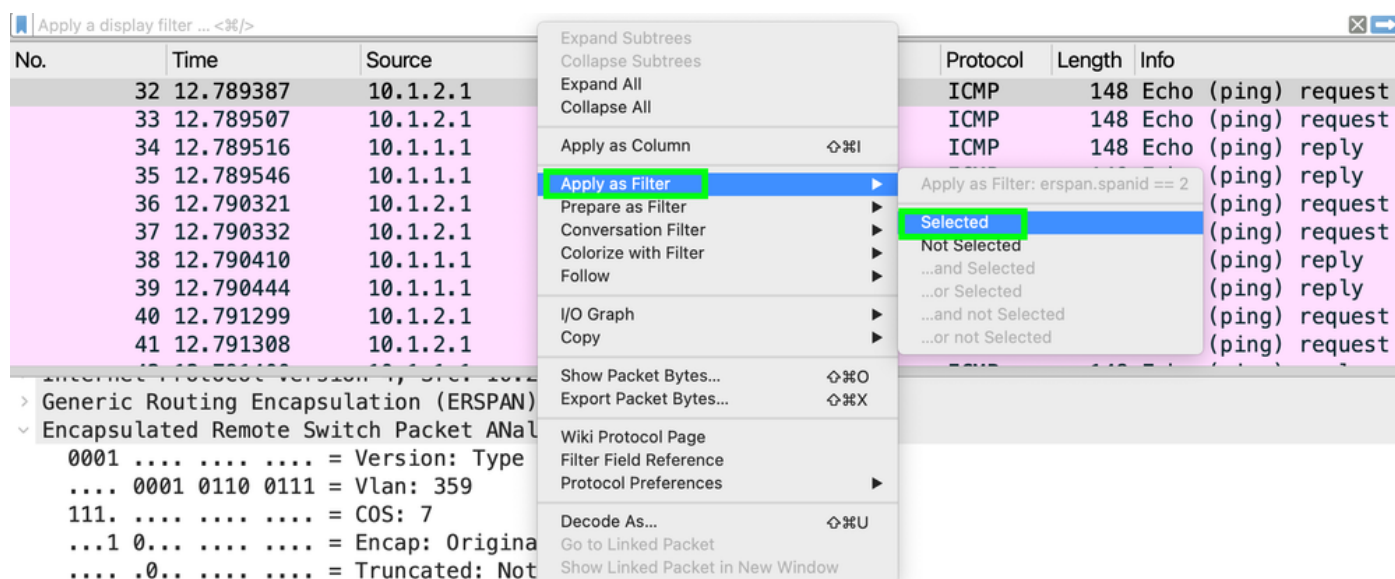
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

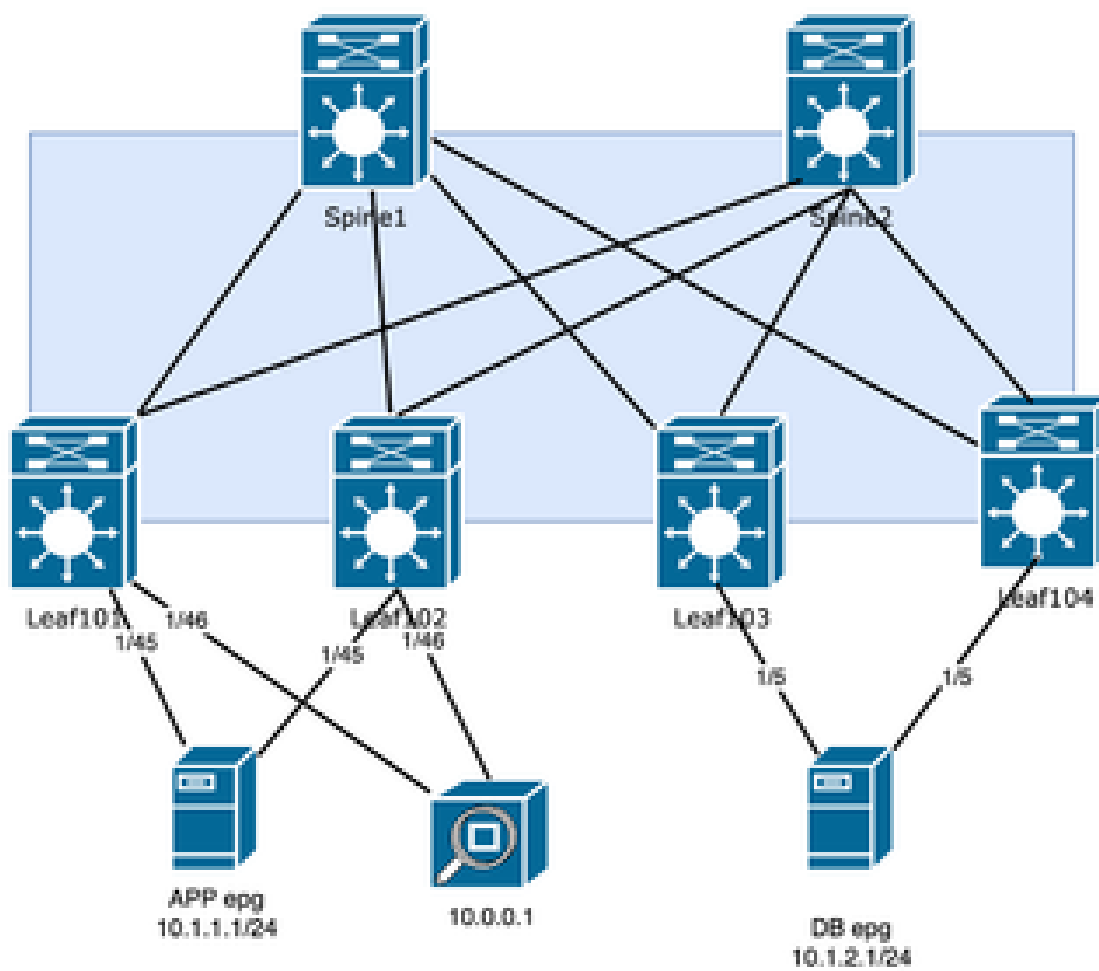
Como criar filtros no Wireshark.

Abra a captura. Usando um quadro dentro do Pacote de Comutador Remoto Encapsulado, selecione a linha SpanID e clique com o botão direito do mouse.

Selecione Aplicar como Filtro > Selecionado conforme mostrado na figura:



Topologia



Opção 1. Configuração de ERSPAN com Flow-id

Se um servidor de destino for capaz de lidar com todo o tráfego, o cabeçalho ERSPAN incluirá uma opção para definir um ID de fluxo. Esse ID de fluxo pode ser configurado para identificar o tráfego de entrada para a estrutura, enquanto um ID de fluxo diferente pode ser configurado para o tráfego de saída.

Etapa 1. Configuração do destino ESPAN

Um grupo de destino terá um flow-id de 1

Em 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

No segundo grupo de destino, configure flow-id como 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

Passo 2a. Crie uma origem de abrangência para o tráfego diretamente conectado ao SRC

Em 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
------	-----------	------------	--------------

Filtre mais o tráfego adicionando o Caminho e o EPG. O exemplo de laboratório é o aplicativo

EPG e o aplicativo ALL do perfil de aplicativo Tenant jr.

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

Passo 2b. Crie uma origem de abrangência para o tráfego diretamente conectado ao DST

Em 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

Filtre mais o tráfego adicionando não apenas o Caminho, mas também o EPG DB:

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
------	-----------	------------	--------------

Etapa 3. Análise Rápida do Wireshark

Neste exemplo, você está verificando se o número de pacotes de solicitação ICMP corresponde ao número de pacotes de resposta ICMP, garantindo que não haja descartes de pacotes na estrutura da ACI.

Abra a captura no Wireshark para criar o filtro usando o SPAN ID /Flow-ID configurado com SRC

e DST IP:

<#root>

(erspan.spanid ==

and

) && (ip.src==

and ip.dst ==

)

Filtro usado para o fluxo testado em laboratório:

<#root>

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

Verifique se o pacote exibido tem a mesma quantidade do pacote enviado:

(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

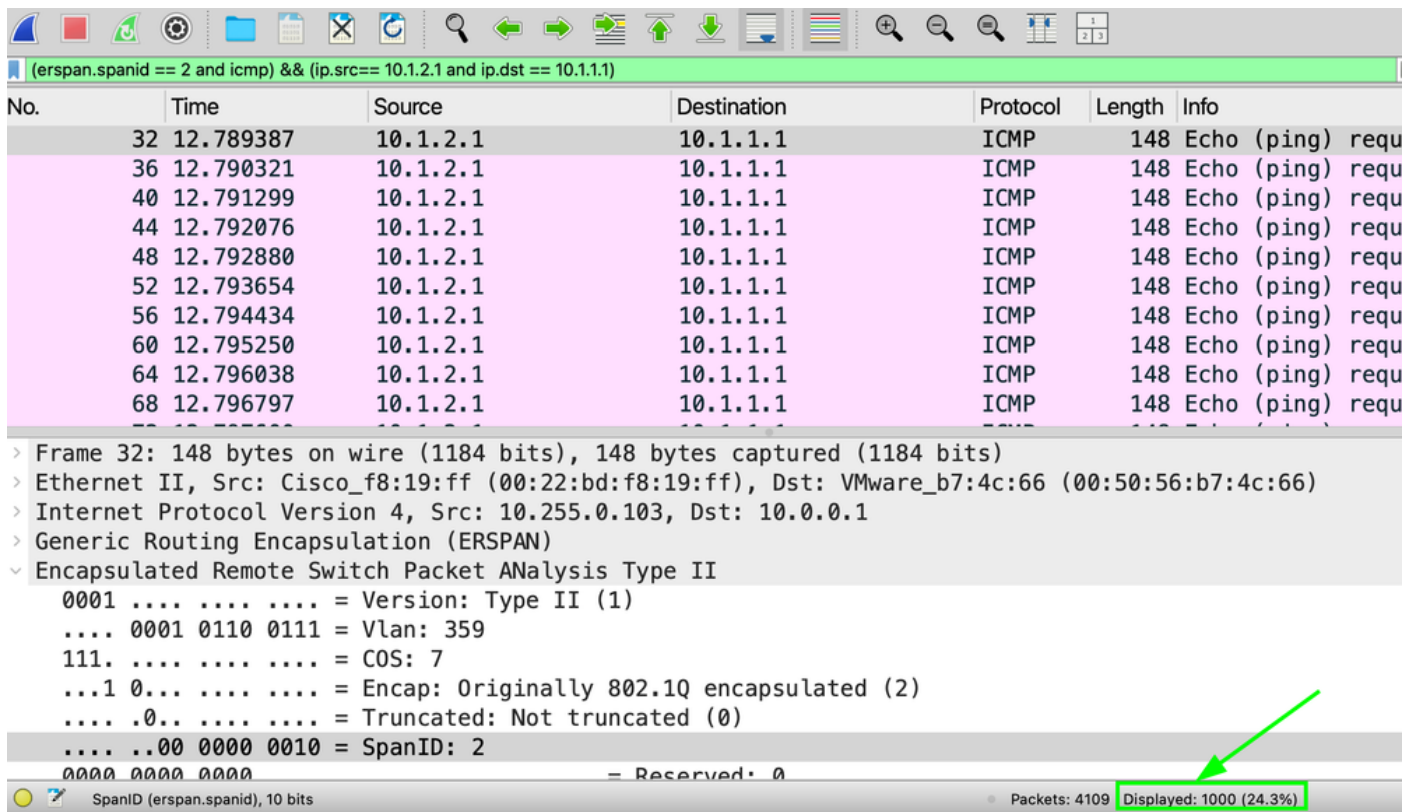
SpanID (erspan.spanid), 10 bits

Packets: 4109 Displayed: 1000 (24.3%) Profile:

O próximo ID de SPAN deve ter o mesmo valor; caso contrário, o pacote foi descartado dentro da estrutura.

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%)

Opção 2. Contadores de plataforma

Esse método aproveita que o Nexus está rastreando o desempenho de interfaces individuais com tamanhos de pacotes diferentes, mas o método exige que pelo menos uma fila tenha uma quantidade baixa de tráfego, se não zero.

Limpar Contadores de Plataforma

Vá até o switch individual e limpe a interface individual que se conecta aos 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 um tamanho de pacote com pacotes baixos ou zero

Localize um tamanho de pacote que possivelmente não tenha contadores em todos os Leafs para RX e TX:

```
<#root>
```

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

```
' | grep X_PKT
```

No próximo exemplo, o tamanho do pacote será maior que 512 e menor que 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

A etapa precisa ser executada no link para o qual os pacotes estão sendo encaminhados.

Fluxo de tráfego de rastreamento

Do servidor 10.1.2.1, 1.000 pacotes são enviados com um tamanho de pacote de 520.

Verifique na Folha 103 interface 1/6, onde o tráfego é iniciado no 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 pacotes RX, mas apenas 647 foram enviados como resposta.

A próxima etapa é verificar as interfaces de saída dos outros 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

A malha não descartou a solicitação.

Para a folha 101, o RX envia pacotes 647 e é a mesma quantidade de pacotes transmitidos pela 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

Informações Relacionadas

[Solução de problemas de encaminhamento entre estruturas da ACI - quedas intermitentes](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.