Uso de Wireshark para identificar el tráfico en ráfagas en switches Catalyst

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Antecedentes Metodología de solución de problemas

Introducción

Este documento describe cómo identificar el tráfico de ráfaga en los puertos de switch de los switches Cisco Catalyst.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en la serie de switches Catalyst de Cisco.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si su red está activa, asegúrese de comprender el impacto potencial de cualquier comando antes de ejecutar el comando.

Antecedentes

Las ráfagas de tráfico pueden causar caídas de salida incluso cuando la velocidad de salida de la interfaz es significativamente menor que la capacidad máxima de la interfaz. De forma predeterminada, las velocidades de salida en el comando **show interface** se promedian durante cinco minutos, lo que no es adecuado para capturar ninguna ráfaga de corta duración. Lo mejor es estimarlos en 30 segundos. En este caso, puede utilizar Wireshark para capturar el tráfico de salida con el analizador de puertos conmutados (SPAN), que se analiza para identificar las ráfagas.

Metodología de solución de problemas

1. Identifique una interfaz que tenga caídas de salida incrementales. Por ejemplo, observa caídas de salida en un link de 100 Mb mientras que el uso promedio del link es solamente de 55 Mb. Aquí está el resultado del comando:

```
Switch#show int fa1/1 | i duplex output drops rate
 Full-duplex, 100Mb/s, media type is 10/100BaseTX
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 5756
  5 minute input rate 55343353 bits/sec, 9677 packets/sec
  5 minute output rate 55456293 bits/sec, 9878 packets/sec
```

2. Configure SPAN en el switch para capturar el tráfico transmitido (TX). Para capturar este tráfico, conecte una PC que ejecute Wireshark y capture paquetes en el puerto de destino SPAN.

```
Switch#config t
   Switch(conf) #monitor session 1 source interface fa1/1 tx
   Switch(conf) #monitor session 1 destination interface fa1/2
Abra el archivo capturado en Wireshark y grabe un gráfico de E/S como este.
                                                                                        ark 1.8.5 (SVN Rev 47350 from /trunk-1.8)
                                                                         art22.pca
   Eile Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
   🗒 👹 😂 😂 🛍 ⊨ 🗔 🗶 🚭 Summary
                                                                     🗏 🖪 । ९, ९, ९, 🖭 🔐 🕅 🝢 🐒 🔛
                                         Protocol Hierarchy
    Filter:
                                      Conversations
                                                                     ar Apply Save
                        Source
                                      Endpoints
           Time
                                                                     Protocol Length Info
                                         Packet Lengths.
                                                                                  1970.9/
        9968 47
                                                                      LIDP
                                                                                                    ginkvo-1 Destination pr
                                                                                         rce port: ze
                                                                                                                        ort: fet
                                        10 Graph
                                                                      UDP
         370 47.23
                                                                                  1370 St
                                                                                        urce port: zenginkyo-1 Destination port: fntp
                                         Conversation List
                                                                      LIDP
                                                                                              et: cis
                                                                                                         c n
                                                                                                           Destination p
          71 47.2
                                                                                                                        ++ N
                                         Endpoint List
                                         Service Response Time
                                                                      LDF
                                                                                             ort: zer
                                                                                                    ginkvo-1 Destination port: fmt
                                         ANCP
                                         BACnet
                                         BOOTP-DHCP...
                                                                                  1370 Source port: zenginkyo-1 Destination port: fntp
1370 Source port: zenginkyo-1 Destination port: fntp
      186379 47.241703000
                                         Collectd...
                                                                      UDP
      195380 47.241951000
                        100.000.070
                                                                      LIDE
                                         Compare...
                                       Flow Graph...
                                                                                  1370 Source port: zenginkyo-1 Destination port: fmtp
```

UDP

LIDP

UDP

UDP

bits) on interface O

05 [00:90:f9:1b:ef:05]

1.1.2 (192.168.1.2)

ort: cisco-s

1370 Source port: zenginkyo-1 Destination port: fmt

1370 Source port: zenainkvo-1 Destination port: fmtp

Destination

186382 47.242512000

6 47,243

Data (1328 bytes)

3 47, 242514000

6000

186387 47.243661000

Frame 186377: 1370 bytes on wire (109)

Ethernet II, Src: Leitch_1c:10:05 [00:

Internet Protocol Version 4, Src: 192. User Datagram Protocol, Src Port: zeng

120.00.00.00.77

HART-IP HTTP

Sametime

IP Addresses...

IP Destinations...

IP Protocol Types..

ONC-RPC Programs

TCP StreamGraph

UDP Multicast Streams WLAN Traffic

4. En la escala predeterminada, parece que no hay tráfico saturado. Sin embargo, un segundo es un intervalo muy grande cuando se considera la velocidad a la que ocurre el almacenamiento en búfer y el switching de paquetes. En un período de un segundo, un link a100 Mb/s puede alojar 100 Mb de tráfico a través de la interfaz en un perfil en forma clara con una necesidad mínima de almacenar en búfer cualquier paquete.

000	X port22.pcapng	[Wireshark 1.8.5 (SVI				
Elle e o o	X Wireshark IO Graphs: port22.pcapng					
		⊂ ⁵⁰⁰⁰ 🖽 🗑				
Filto		1				
Fille						
No.		- 2500				
1		ce port:				
1		mented IP				
1	05 205 405	ce port:				
	03 203 403	mented IP				
Graphs	XAxis	mented IP				
Graph 1 Color Filter:	Style: Line 🔽 Tick interval: 1 sec	↓ ce port: mented IP				
Graph 2 Color 🗹 Filter:	Style: Line 🔻 Pixels per tick:	5 - ce port:				
Graph 3 Color 📓 Filter:	Style: Line 🔽 🗆 View as time of d	day ce port:				
1 Graph 4 Color M Filter:	Style: Line VAXIS	ce port: mented IP				
Graph 5 Color Filter:	Style: Line V	Ce port:				
	Scale: Auto	mented IP				
10	Smooth: No filte	r v ce port:				
 ↓ United the second s	≋ ⊆lose	Save ce port:				
> Frame 186377: 1370 bytes on wire	(10960 bits), 1370 bytes captured (10960 bits) on inter	face 0				
Ethernet II, Src: Leitch_1c:10:05 (00:90:f9:1c:10:05), Dst: Leitch_1b:ef:05 (00:90:f9:1b:ef:05)						

User Datagram Protocol, Src Port: zenginkyo-1 (5020), Dst Port: fmtp (8500)

Data (1328 bytes)

Sin embargo, si una parte importante de este tráfico intenta salir de la interfaz en una fracción de segundo, el switch necesita almacenar paquetes en búfer extensamente y descartarlos cuando las memorias intermedias están llenas. Si hace que las escalas sean más granulares, verá una imagen más precisa del perfil de tráfico real. Cambie el eje Y a bits/tic porque las interfaces muestran las velocidades de salida en bits/seg.

La velocidad del enlace es de 100 Mb/s

- = 100 000 000 bits/s
- = 100 000 bits/0,001 s

Recalcular las escalas en los ejes X e Y. Cambie el intervalo de graduación a **Eje X=0,001 s** y la escala a **Eje Y=00,000 (bits/tic)**.

\varTheta 🖸 🖸 🛛 🕅 🕅 🕅 🕅	raphs: port22.pcapng			
				F ¹⁰⁰⁰⁰⁰
				È i
		٨	۸۸ ۸	L 50000
/////////////////////////////	~~~~~~~~~~~	\sim	/\//\	1
				١Ŀ
		· ·		L 0
49.040s 49.060s 49.080s 49.100s	49.120s 49.140	Os 4	49.160s	
Graphs		_[X Axis		
Graph 1 Color 🗹 F <u>i</u> lter:	Style: Line 🛛 🔻	Tick in	nterval: 0.0	01 sec 🔻
Graph 2 Color 🛛 F <u>i</u> lter:	Style: Line 🛛 🔫	Pixels	per tick:	5 🔫
Graph 3 Color 📓 Filter:	Style: Line 🛛 🔻	□ <u>V</u> iev	w as time o	f day
Graph 4 Color 🖾 Filter:	Style: Line 🔽	Y Axis		
Graph 5 Color MEilter	Style: Line 🔻	Unit:	Bits/T	ick 🗸 🔻
	Style: Line	Scale:	10000	0 🔻
		Smoot	h: No fil	ter 🔻
<mark>Щ</mark> Help [©] ⊆opy			XClose	Save

- 5. Desplácese por el gráfico para identificar ráfagas. En este ejemplo, puede ver que hay una ráfaga de tráfico que excedió los 100.000 bits en una escala de 0,001 segundos. Esto confirma que el tráfico está saturado en el nivel de subsegundos y se espera que el switch lo descarte cuando las memorias intermedias estén llenas para acomodar estas ráfagas.
- 6. Haga clic en el pico de tráfico en el gráfico para ver ese paquete en la captura de Wireshark. El análisis de captura es una forma útil de descubrir qué tráfico constituye la ráfaga.

	X WI	resnark to Graphs: port22.pcaphg			
/	MMM-M-		- / W/-	- ///// /	/ _ 50000
47.160s 47	.180s 47.200s	47.220s 47.240s	47.260s	47.280s	0
Graphs					• •
Graph 1 Color	r ⊠F <u>i</u> lter:	Style: Line	▼ Tick in	nterval: 0.0	01 sec 🔻
Graph 2 Color	Filter:	Style: Line	▼ Pixels	per tick:	5 🔫
Graph 3 Color	Filter:	Style: Line		w as time o	f day
Graph 4 Color	Filter:	Style: Line	▼ Y Axis	Rite /T	ick 🖵
Graph 5 Color	Filter:	Style: Line	▼ Scale:	10000	
			Smoot	th: No fi	ter ∣▼
<mark>₿</mark> Help 💿	<u>C</u> opy			XClose	Save