Utilisation de Wireshark pour identifier le trafic en rafale sur les commutateurs Catalyst

Contenu

Introduction Conditions préalables Conditions requises Components Used Informations générales Méthodologie de dépannage

Introduction

Ce document décrit comment identifier le trafic en rafale sur les ports de commutation des commutateurs Cisco Catalyst.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations de ce document sont basées sur la gamme de commutateurs Cisco Catalyst.

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 votre réseau est actif, assurez-vous de bien comprendre l'impact potentiel d'une commande avant d'exécuter la commande.

Informations générales

Les rafales de trafic peuvent entraîner des pertes de sortie même lorsque le débit de sortie de l'interface est significativement inférieur à la capacité maximale de l'interface. Par défaut, les débits de sortie de la commande **show interface** sont en moyenne sur cinq minutes, ce qui n'est pas suffisant pour capturer des rafales de courte durée. Il est préférable de les calculer en moyenne sur 30 secondes. Dans ce cas, vous pouvez utiliser Wireshark afin de capturer le trafic de sortie avec l'analyseur de port commuté (SPAN), qui est analysé afin d'identifier les rafales.

Méthodologie de dépannage

1. Identifiez une interface qui possède des pertes de sortie incrémentielles. Par exemple, vous

remarquerez des pertes de sortie sur une liaison de 100 Mo alors que l'utilisation moyenne de la liaison est seulement de 55 Mo. Voici le résultat de la commande :

```
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
```

 Configurez SPAN sur le commutateur afin de capturer le trafic transmis (TX). Afin de capturer ce trafic, connectez un PC qui exécute Wireshark et capture des paquets au port de destination SPAN.

```
Switch#config t
Switch(conf)#monitor session 1 source interface fa1/1 tx
Switch(conf)#monitor session 1 destination interface fa1/2
```

3. Ouvrez le fichier capturé dans Wireshark et tracez un graphique d'E/S comme celui-ci.

Elle Edit View Co Capture Analyze Statistics Telephony Tools Internals Help Image: Construct Analyze Statistics Telephony Tools Internals Image: Construct Analyze Conversation			A house-beahing famesuary rear fame wer available really
Iter: Protocol Hierarchy No. Time Source Idexard/Y=zelex/locol Endpoints Packet Lengths Endpoints Idexard/Y=zelex/locol Endpoints Packet Lengths Endpoint List Idexard/Y=zelex/locol Endpoint List Idexard/Y=z	Eile Edit View Go Capture Analyze	Statistics Telephony Tools	Internals Help
165366 47.259932000 100 Graph 165366 47.259932000 100 Graph 165367 47.259932000 100 Graph 165375 47.24000000 100 Graph 165375 100 Graph 100 Graph	Filter: No. Time Source	Summary Protocol Hierarchy Conversations Endpoints Packet Lengths	ar Apply Save
180307 47, 23942000 180307 47, 23942000 180307 47, 23942000 180307 47, 23942000 180307 47, 23942000 180307 47, 23942000 180307 47, 23942000 180307 47, 24004000 180307 47, 240440000 180307 47, 240440000 180307 47, 24044000 180307 47, 24044000 180307 47, 24044000 180307 47, 24044000 180307 47, 24044000 180307 47, 24044000 180307 47, 24044000 180307 47, 24044000 180307 47, 24044000 180307 47, 24044000 180307 47, 24044000 180307 47, 24044000 180307 47, 24044000 180307 47, 24044000 180307 47, 24044000 180307 47, 24044000 180307 47, 24044000 180307 47, 24044000 180407 480000 180407 480000	186368 47.238932000	La IO Graph	LDP 1370 Source port: Zenginkyo-1 Destination port: fmtp
	186329 47.239231000 11100 11101 1110 186379 47.239567000 11101 1110 186373 47.239567000 11101 1110 186373 47.24063000 11101 1110 186375 47.24063000 11101 1110 186375 47.24163000 11101 1110 186380 47.24195000 11101 1110 186380 47.24195000 11101 1110 186380 47.24195000 11101 1110 186380 47.24251000 11101 1110 186380 47.24251000 11101 1110 186380 47.24251000 11101 1110 186385 47.24251000 11101 1110 186387 47.24551000 11101 1110 186387 47.24551000 11101 1100 186387 47.24551000 111010 186387 47.24551000 111010 186387 47.24551000 111010 186387 47.24551000 111010 186387 47.24551000 111010 186387 47.24551000 11100 186387 47.24551000 11000 186387 47.2455000 11000 186387 47.245500 110000 186387 47.245500 1100000 186387 47.245500 1100000	Conversation List Endpoint List Service Besponse Time ANCP BACnet BOOTP-DHCP Collectd Compare E Flow Graph HART-IP HTTP IP Addresses IP Destinations IP Protocol Types ONC-RPC Programs Sametime TCP StreamGraph UDP Multicast Streams WLAN Traffic	<pre>IPv4 1300 Fragmented IP protocol [srotosCGMP 1, off=200006, [CoEd00] UDP 1370 Source port: cisco-sccp Destination port: fntp UDP 1370 Source port: cisco-sccp Destination port: fntp IPv4 1370 Errorpented IP protocol [srotosCGMP 1, off=20000, [CoEd00] UDP 1370 Source port: renginkyo-1 Destination port: fntp IPv4 1370 Errorpented IP protocol [srotosCGMP 1, off=20000, [CoEd00] UDP 1370 Source port: renginkyo-1 Destination port: fntp IPv4 1370 Errorpented IP protocol [srotosCGMP 1, off=20000, [CoEd00] UDP 1370 Source port: renginkyo-1 Destination port: fntp IPv4 1370 Errorpented IP protocol [srotosCGMP 1, off=20000, [CoEd00] UDP 1370 Source port: renginkyo-1 Destination port: fntp IPv4 1370 Errorpented IP protocol [srotosCGMP 1, off=20000, [CoEd00] UDP 1370 Source port: renginkyo-1 Destination port: fntp IPv4 1370 Errorpented IP protocol [srotosCGMP 1, off=20000, [Desd00] UDP 1370 Source port: renginkyo-1 Destination port: fntp IPv4 1370 Errorpented IP protocol [srotosCGMP 1, off=20000, [Desd00] UDP 1370 Source port: renginkyo-1 Destination port: fntp IPv4 1370 Errorpented IP protocol [srotosCMP 1, off=20000, [Desd00] UDP 1370 Source port: renginkyo-1 Destination port: fntp IPv4 1370 Errorpented IP protocol [srotosCMP 1, off=20000, [Desd00] UDP 1370 Source port: renginkyo-1 Destination port: fntp IPv4 1370 Errorpented IP protocol [srotosCMP 1, off=20000, [Desd00] UDP 1370 Source port: renginkyo-1 Destination port: fntp IPv4 1370 Errorpented IP protocol [srotosCMP 1, off=20000, [Desd00] UDP 1370 Source port: renginkyo-1 Destination port: fntp IPv4 1370 Source port: renginkyo-1 Destination port: fntp IPv4 1370 Errorpented IP protocol [srotosCMP 1, off=20000, [Desd00] UDP 1370 Source port: renginkyo-1 Destination port: fntp IPv4 1370 Source port: renginkyo-1 Destination port: fntp IPv4</pre>

4. Àl'échelle par défaut, il semble qu'il n'y ait pas de trafic en rafale. Cependant, une seconde est un très grand intervalle lorsque vous considérez le taux auquel la mise en mémoire tampon et la commutation de paquets ont lieu. En une seconde, une liaison de 100 Mbits/s peut accueillir 100 Mbits/s de trafic sur l'interface dans un profil en forme propre avec un besoin minimal de tampon de paquet.

000	X port22.pcap	ng [Wireshark 1.8.5 (SVI
Elle e o o	X Wireshark IO Graphs: port22.pcapng	
		□ ⁵⁰⁰⁰ 🕶 🗃
Filte		
No.		-2500
1		ce port:
1		mented IP
1		ce port:
	US 20S 40S	mented IP
1 Graphs	X Axis	mented IP
1 Graph 1 Color I Filter:	Style: Line 🔽 Tick interval: 1 s	ec 🗸 ce port: mented IP
1 Graph 2 Color 🗹 Filter:	Style: Line Vixels per tick:	5 ▼ ce port:
Graph 3 Color I Filter:	Style: Line View as time o	f day ce port:
Graph 4 Color Filter:	Style: Line VIIII: Packet	s/Tick
Graph 5 Color 🗹 Filter:	Style: Line V Scale: Auto	ce port:
1	Smooth: No fi	lter v ce port:
		mented IP
↓ E lp	💥 <u>C</u> lose	Save Ce bort:
> Frame 186377: 1370 bytes on wire	(10960 bits), 1370 bytes captured (10960 bits) on inte	erface O
P Ethernet II, Src: Leitch_1c:10:05 D Internet Protocol Version 4 Src:	5 (00:90:19:16:10:05), Dst: Leitch_lb:ef:05 (00:90:19: • 100 100 1 1 (100 100 1 11 0w+: 100 100 1 0 (100 100	1D:eT:05)

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

Data (1328 bytes)

Cependant, si une grande partie de ce trafic tente de quitter l'interface en une fraction de seconde, le commutateur doit considérablement mettre en mémoire tampon les paquets et les abandonner lorsque les tampons sont pleins. Si vous rendez les échelles plus granulaires, vous voyez une image plus précise du profil de trafic réel. Modifiez l'axe Y en bits/tick, car les interfaces affichent des débits de sortie en bits/s.

La vitesse de liaison est de 100 Mbit/s

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

Recalculer les échelles sur les axes X et Y. Remplacez l'intervalle de graduation par Axe X=0,001 sec et l'échelle par Axe Y=00 000 (bits/tick).

e o o X Wireshark IO Graphs: port22.pcapng										
49.040s 49.060s 49.080s 49.10 Graphs Graph 1 Color Filter: Graph 2 Color Filter: Graph 3 Color Filter: Graph 4 Color Filter: Graph 5 Color Filter:	Style: Line Style: Line Yeiew as time of day Yeiew as time of day Yeiew as time of day Style: Line Line Style: Line Style: Line Line Style: Line Line<									
<u>₩</u> elp <u>©</u> copy	Smooth: No filter 🔻									

- 5. Faites défiler le graphique afin d'identifier les rafales. Dans cet exemple, vous pouvez voir qu'il y a une rafale de trafic qui dépasse 100 000 bits sur une échelle de 0,001 seconde. Ceci confirme que le trafic est en salve au niveau de la sous-seconde et qu'il est attendu que le commutateur abandonne lorsque les tampons sont pleins afin de prendre en charge ces rafales.
- 6. Cliquez sur la pointe de trafic sur le graphique afin de visualiser ce paquet dans la capture Wireshark. L'analyse de capture est un moyen utile de découvrir quel trafic constitue la rafale.

O Wireshark IO Graphs: port22.pcapng									
47.160s 47.180s 47.200s 47.220s	47.240s	47.3	2605	47,2805		0			
•(47.2403			47.2005		•			
Graphs			X Axis			-1			
Graph 1 Color Filter:	Style: Line	▼	Tick in	terval: 0.0	001 sec 🔻	1			
Graph 2 Color 🛛 Filter:	Style: Line		Pixels	per tick:	5 🔫	·			
Graph 3 Color 🖾 Filter:	Style: Line		□ <u>V</u> iew	v as time o	ofday				
Graph 4 Color 🗹 F <u>i</u> lter:	Style: Line	-	Y Axis	Dia / T	iak 🗕	1			
Graph 5 Color Filter:	Style: Line	-	Unit:	Bits/ I		-			
		· ·	Scale:	10000	>0 ▼				
			Smoot	h: No f	ilter 🔻				
<u>Ħ</u> elp <u>□</u> Copy				XClose	<u>∏ S</u> ave				