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

Contenu

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

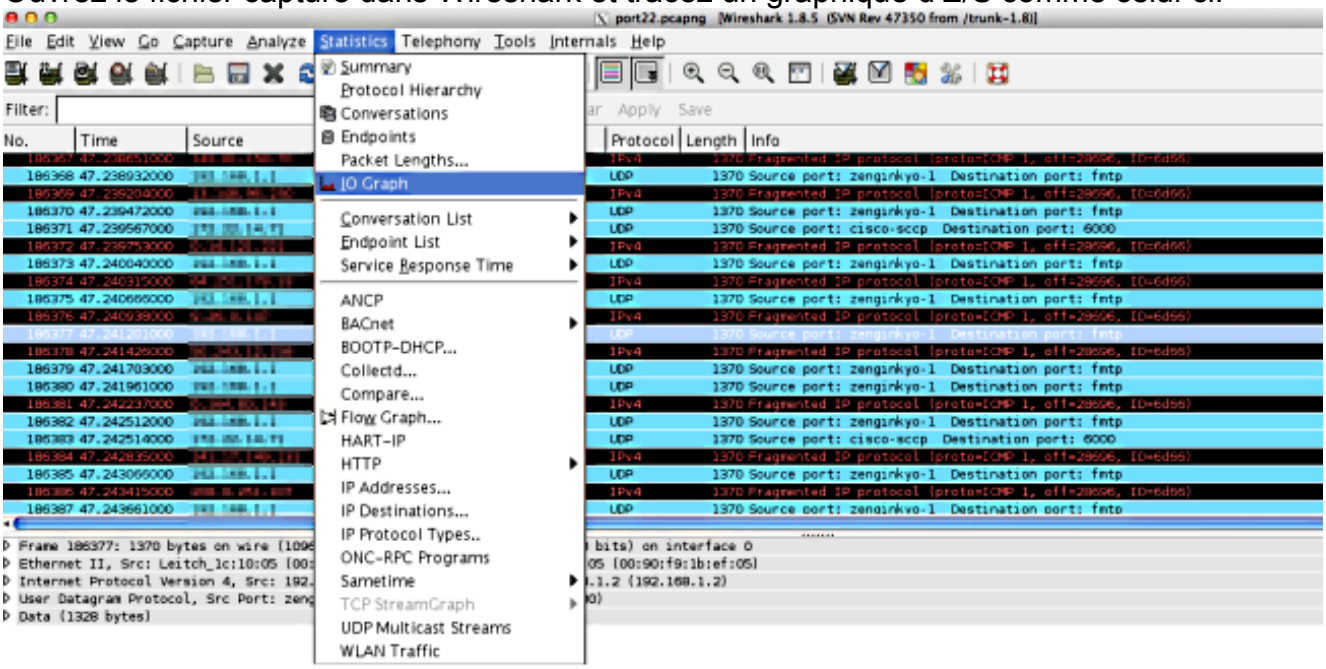
remarquerez des pertes de sortie sur une liaison de 100 Mo alors que l'utilisation moyenne de la liaison est seulement de 55 Mo. Voici le résultat de la commande :

```
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
```

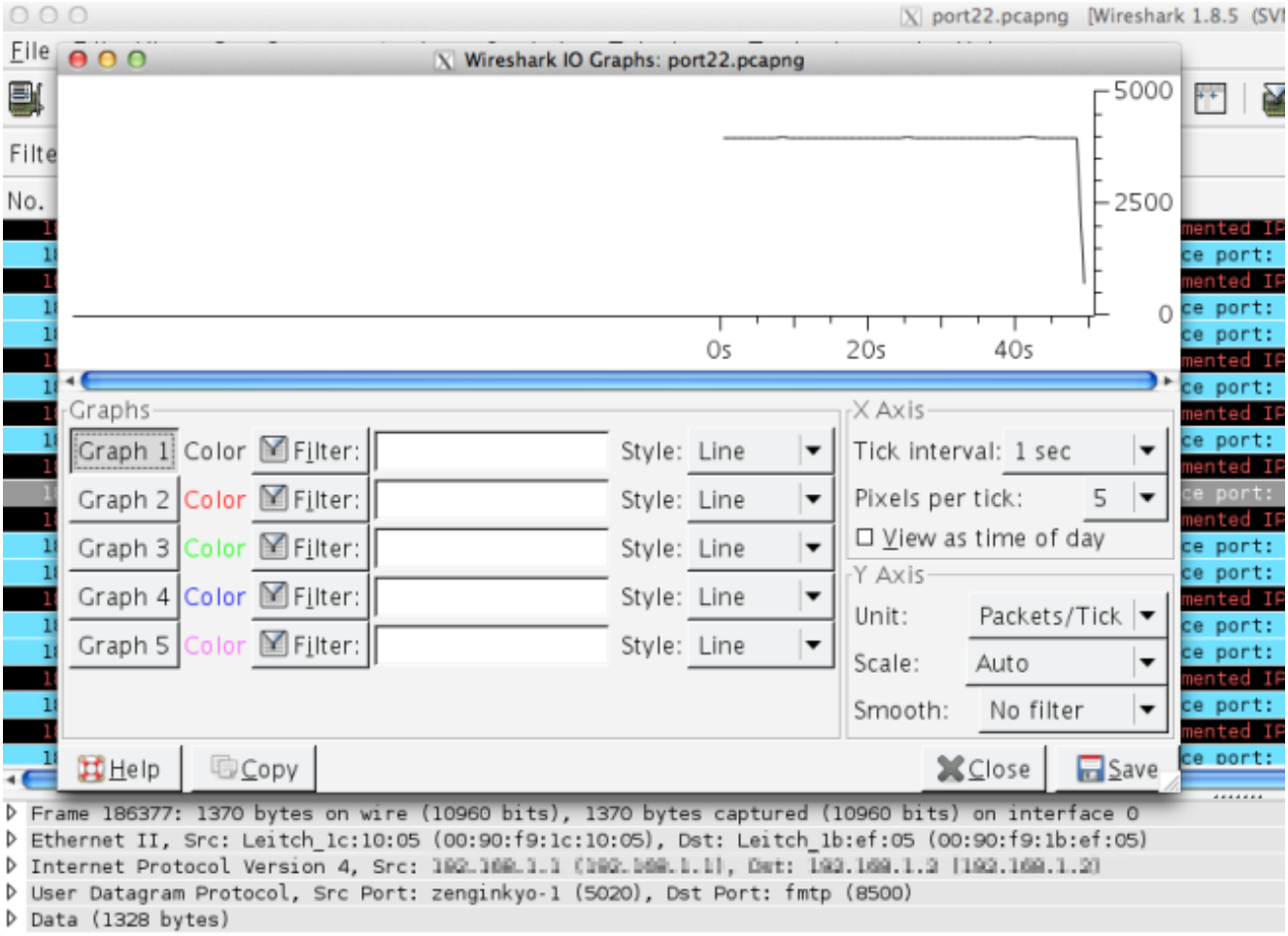
2. Configurez SPAN sur le commutateur afin de capturer le trafic transmis (TX). Afin de capturer ce trafic, connectez un PC qui exécute Wireshark et capture des paquets au port de destination SPAN.

```
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.



4. À l'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.



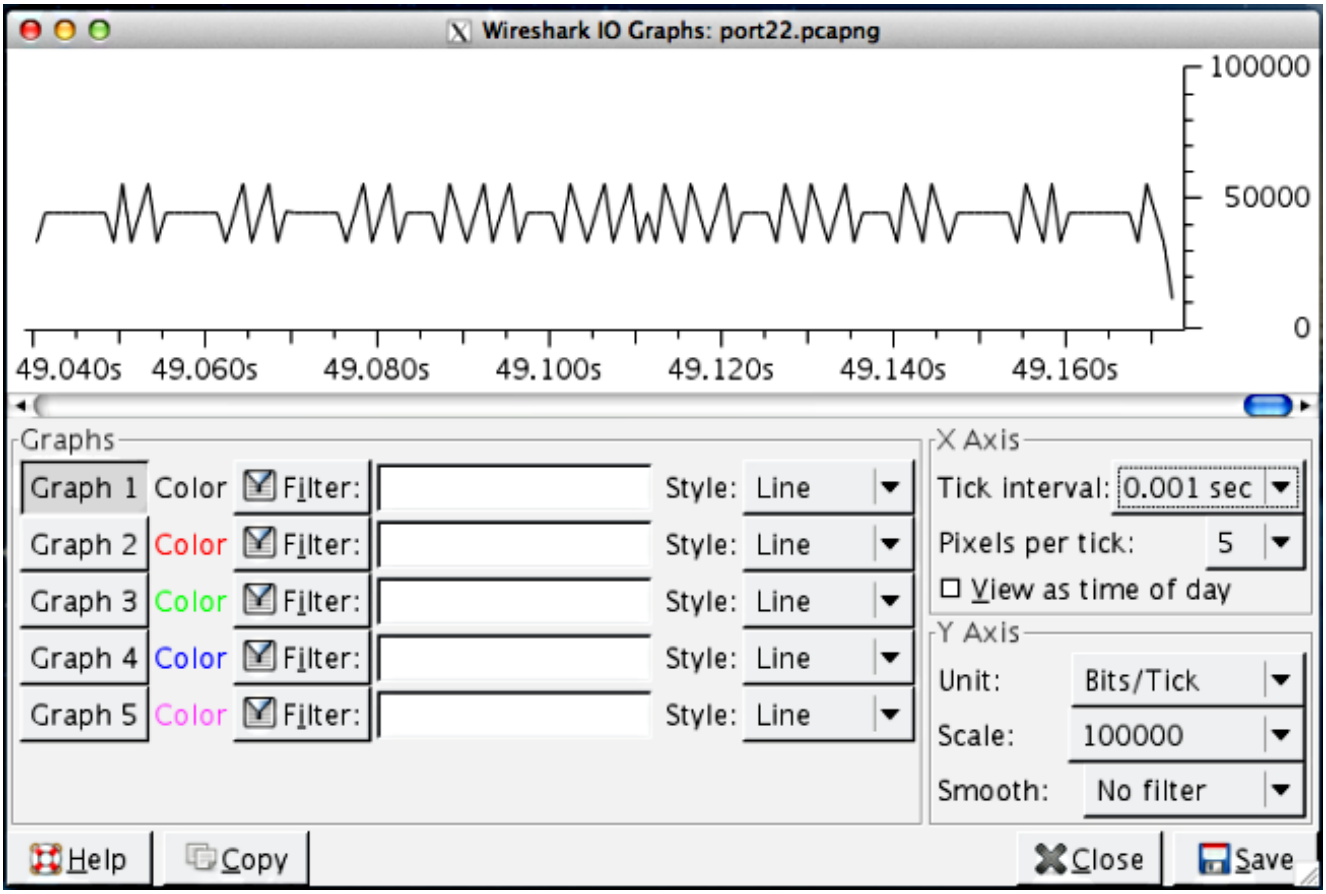
Cependant, si une grande partie de ce trafic tente de quitter l'interface en une fraction de seconde, le commutateur doit considérablement mettre en mémoire tampon les paquets et les abandonner lorsque les tampons sont pleins. Si vous rendez les échelles plus granulaires, vous voyez une image plus précise 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

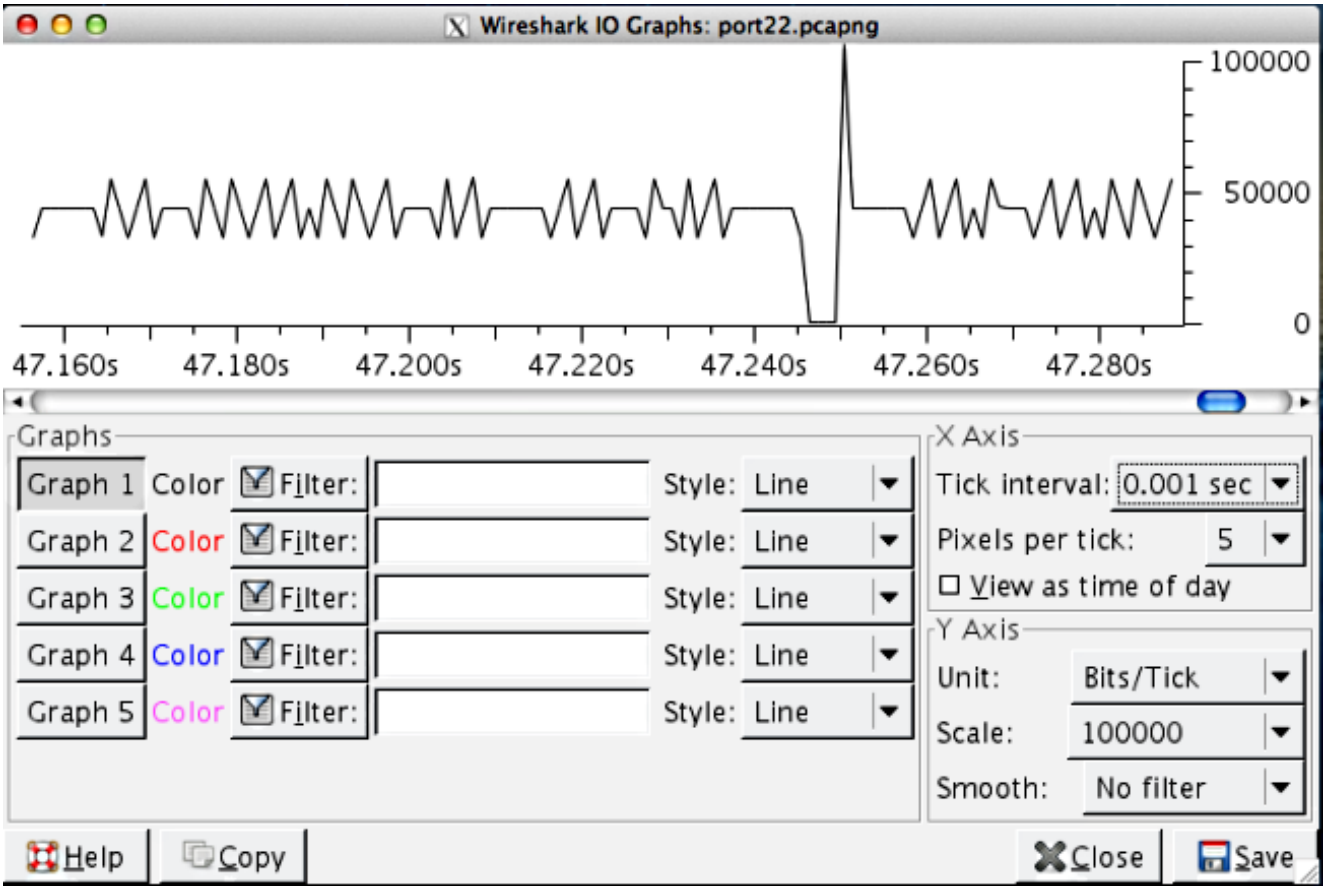
= 100 000 000 bits/s

= 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)**.



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.


Wireshark IO Graphs: port22.pcapng
100000
50000
0
47.160s
47.180s
47.200s
47.220s
47.240s
47.260s
47.280s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: Style: Line
Graph 3 Color Filter: Style: Line
Graph 4 Color Filter: Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 0.001 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Bits/Tick
Scale: 100000
Smooth: No filter
Help
Copy
Close
Save