

L'utilisation de Wireshark d'identifier le trafic de Bursty sur le Catalyst commute

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Informations générales](#)

[Dépannage de la méthodologie](#)

Introduction

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

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

[Composants utilisés](#)

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

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande avant d'exécuter la commande.

[Informations générales](#)

Les rafales du trafic peuvent entraîner des suppressions de sortie même lorsque le débit de sortie d'interface est sensiblement inférieur que la capacité maximum d'interface. Par défaut, les débits sortants dans la **commande d'interface d'exposition** sont ramenés à une moyenne plus de cinq minutes, qui n'est pas adéquate pour ne capturer aucune rafale de courte durée. Il est le meilleur de faire la moyenne de eux plus de 30 secondes. Dans ce cas, vous pouvez employer Wireshark afin de capturer le trafic en sortie avec le Fonction Switched Port Analyzer (SPAN), qui est analysé afin d'identifier les rafales.

Dépannage de la méthodologie

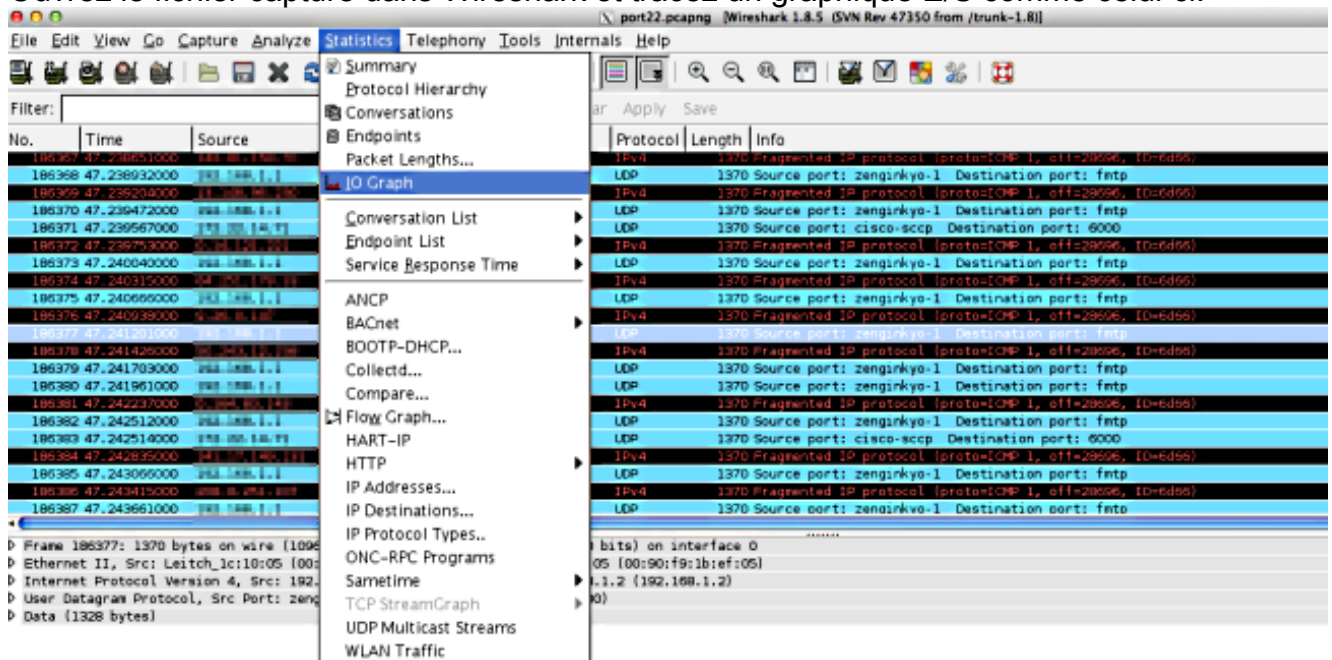
1. Identifiez une interface qui a les suppressions de sortie incrémentales. Par exemple, vous notez des suppressions de sortie sur un lien 100Mb tandis que l'utilisation moyenne du lien est seulement 55Mb. Voici la sortie de la commande :

```
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
```

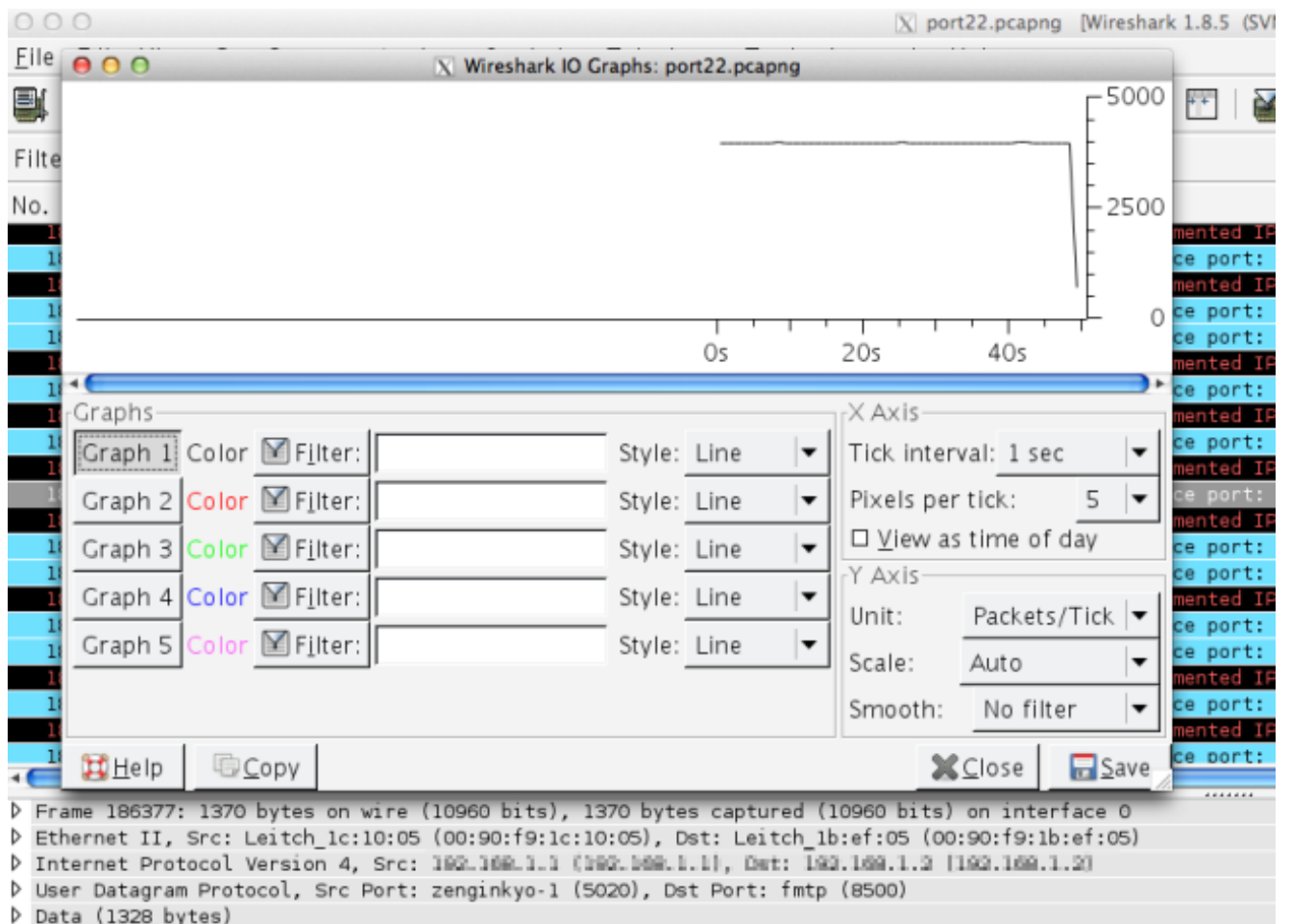
2. Configurez l'ENVERGURE sur le commutateur afin de capturer le trafic (TX) transmis. Afin de capturer ce trafic, connectez un PC qui exécute Wireshark et paquets de capture à la destination port d'ENVERGURE.

```
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 E/S comme celui-ci.



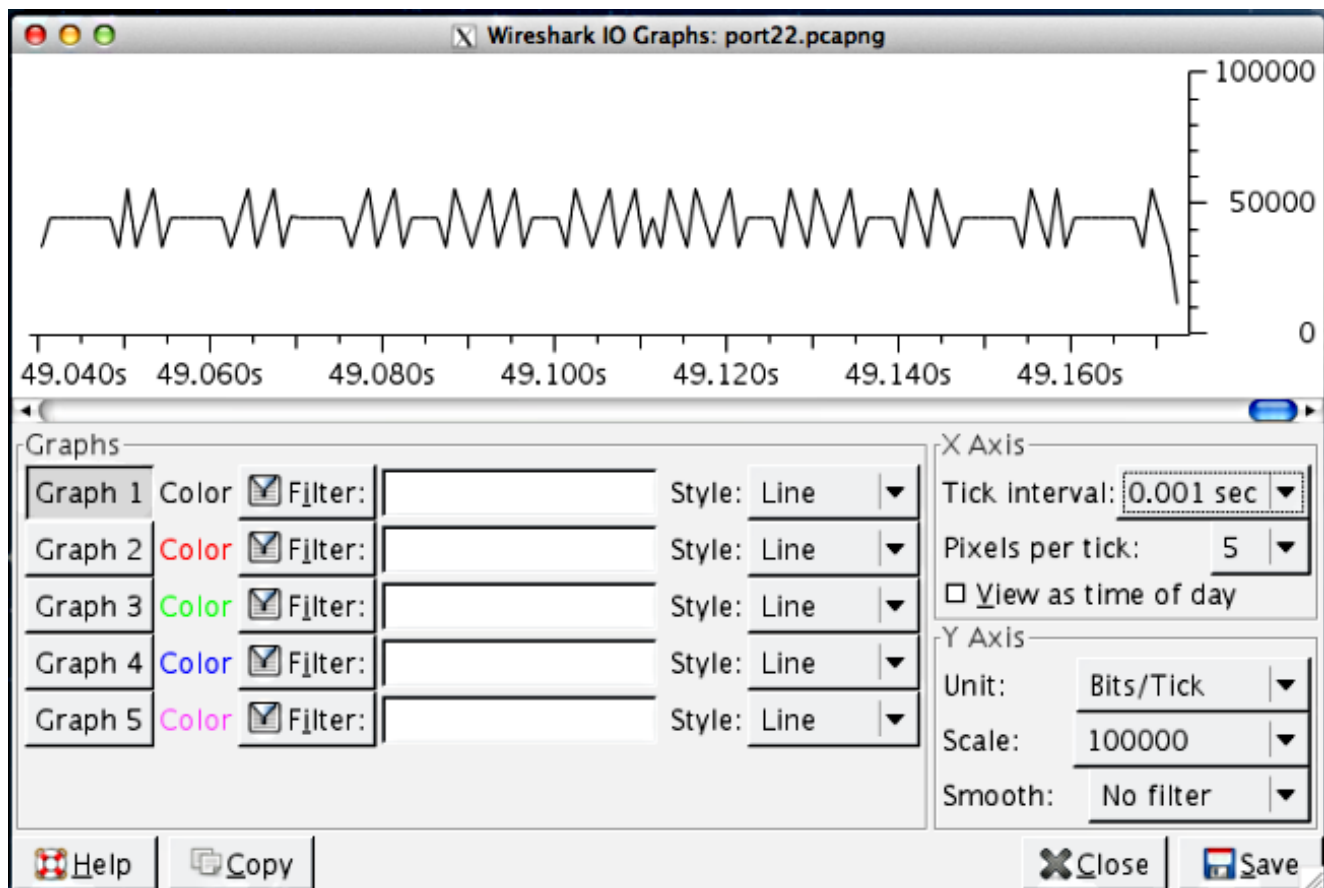
4. À l'échelle par défaut, il s'avère qu'il n'y a aucun trafic bursty. Cependant, une seconde est un intervalle très grand quand vous considérez le débit auquel la mise en mémoire tampon et la commutation de paquets se produit. Dans une période d'une seconde, le lien a 100 Mb/s peut faciliter la mi-bande 100 du trafic à travers l'interface dans un profil en forme ordonnée avec un besoin minimum de mettre en mémoire tampon n'importe quel paquet.



Cependant, si une partie importante de tentatives de ce trafic de laisser l'interface dans une fraction de seconde, le commutateur doit mettre en mémoire tampon intensivement des paquets et les relâcher quand les mémoires tampons sont pleines. Si vous rendez les échelles plus granulaires, vous voyez une image plus précise du profil réel du trafic. Changez l'**axe des ordonnées** aux bits/coutil parce que les interfaces affichent des débits sortants dans le bits/seconde.

La vitesse de liaison est 100 Mb/s
 = 100,000,000 bits/s
 = 100,000 bits/0.001 s

Recalculez les échelles sur le **X** et les **axes des ordonnées**. Changez l'intervalle de coutil à **sec X Axis=0.001** et l'échelle à **Y axis=00,000 (bits/coutil)**.



5. Parcourez le graphique afin d'identifier des rafales. Dans cet exemple, vous pouvez voir qu'il y a une rafale de trafic qui a dépassé 100,000 bits sur une 0.001 seconde échelle. Ceci confirme qu'on s'attend à ce que le trafic est bursty au niveau fraction de seconde et obtienne relâché par le commutateur quand les mémoires tampons sont pleines afin de faciliter ces rafales.
6. Cliquez sur en fonction le pic du 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.

