Wireshark: utilizzo per identificare rotture di traffico sugli switch Catalyst

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Premesse](#)
[Metodologia di risoluzione dei problemi](#)

Introduzione

Questo documento descrive come identificare il traffico burst sulle porte degli switch Cisco Catalyst.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per la stesura del documento, sono stati usati switch Cisco Catalyst serie 700.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi prima di eseguirli.

Premesse

I picchi di traffico possono causare perdite di output anche quando la velocità di output dell'interfaccia è significativamente inferiore alla capacità massima dell'interfaccia. per impostazione predefinita, le velocità di output nel comando **show interface** vengono calcolate su una media di cinque minuti, un valore non sufficiente per acquisire eventuali burst di breve durata. È meglio fare una media di 30 secondi. In questo caso, è possibile usare Wireshark per catturare il traffico in uscita con SPAN (Switched Port Analyzer), analizzato per identificare i burst.

Metodologia di risoluzione dei problemi

1. Identificare un'interfaccia che presenta interruzioni di output incrementali. Ad esempio,

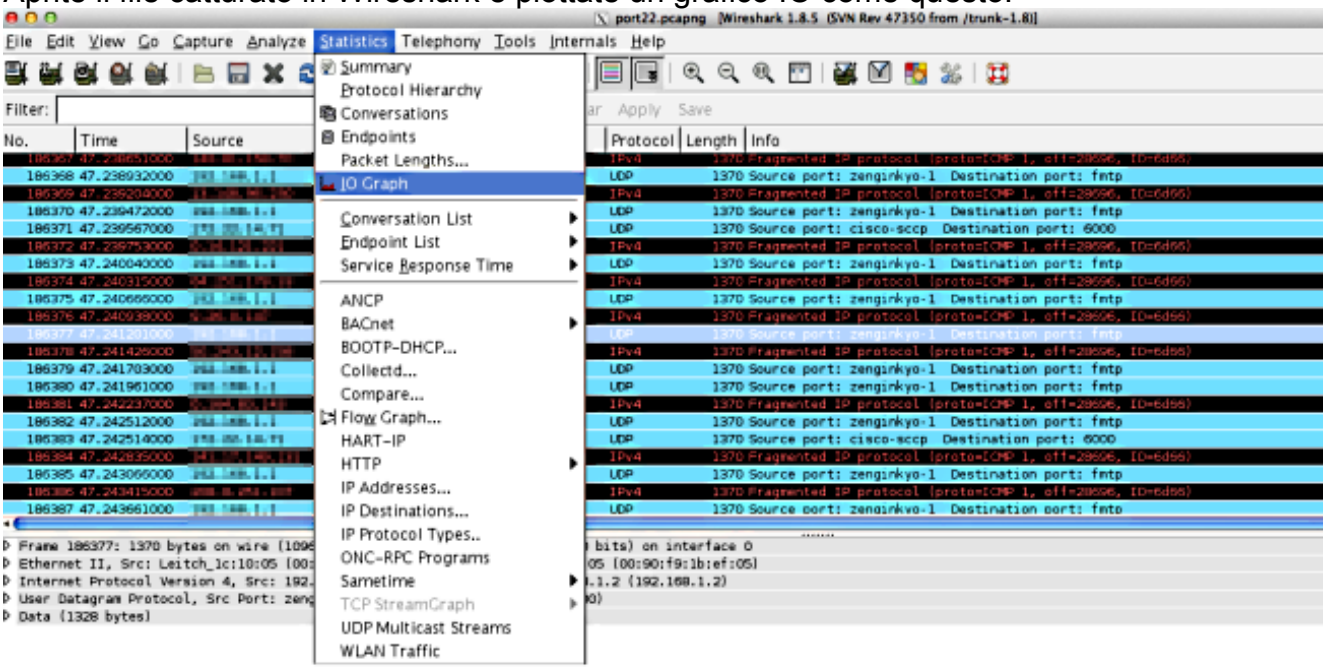
l'output di un collegamento a 100 MB diminuisce mentre l'utilizzo medio del collegamento è di soli 55 MB. Di seguito è riportato l'output del comando:

```
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
```

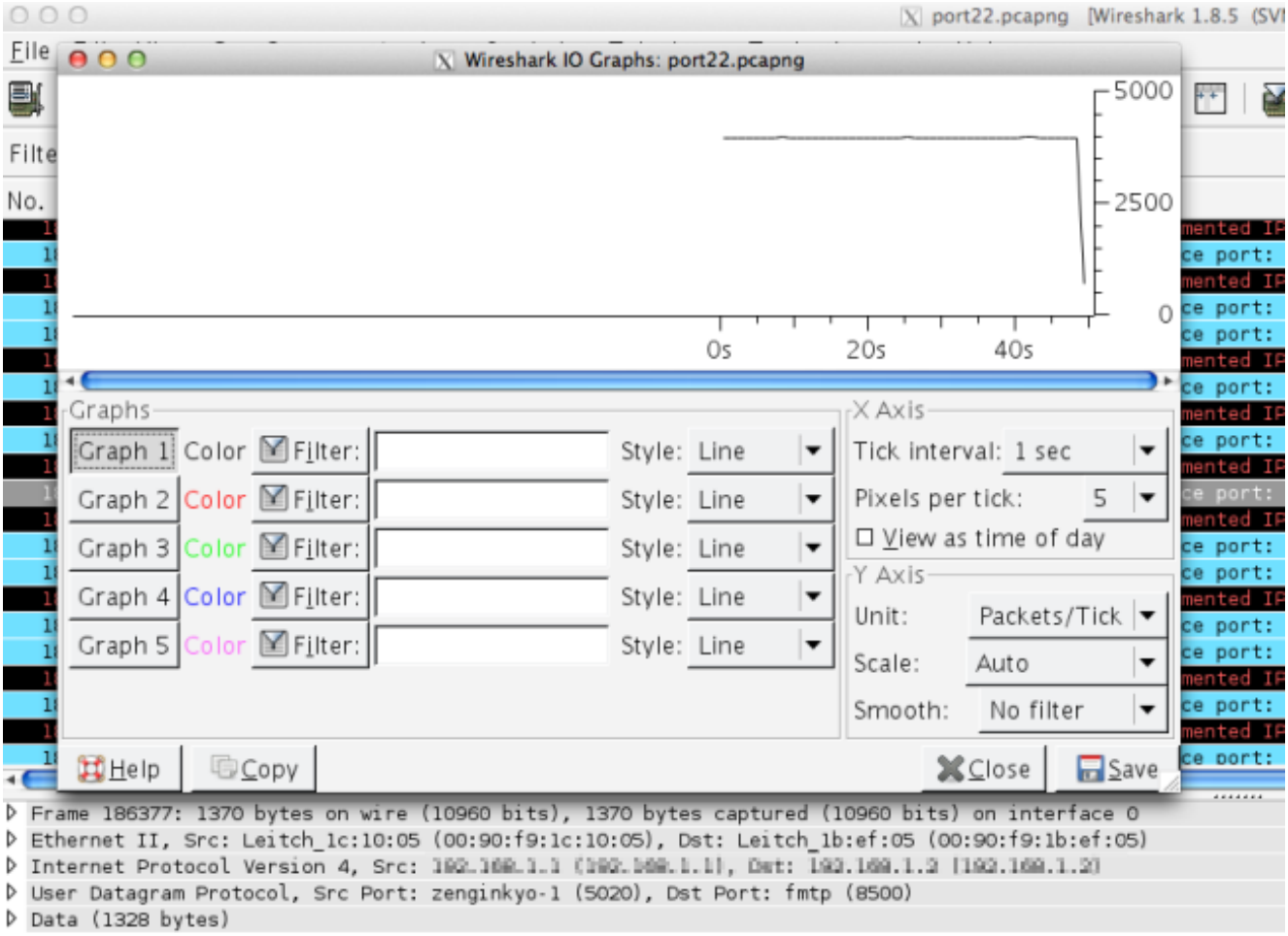
2. Configurare SPAN sullo switch per acquisire il traffico trasmesso (TX). Per acquisire il traffico, connettere un PC con Wireshark e catturare i pacchetti sulla porta di destinazione SPAN.

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

3. Aprite il file catturato in Wireshark e plottate un grafico IO come questo.



4. Nella scala predefinita, non sembra esistere traffico bursty. Tuttavia, un secondo è un intervallo molto ampio se si considera la velocità con cui si verifica il buffering e la commutazione di pacchetto. In un secondo, un collegamento a 100 Mb/s può gestire 100 Mb di traffico sull'interfaccia in un profilo ordinato con la necessità di memorizzare almeno un pacchetto.



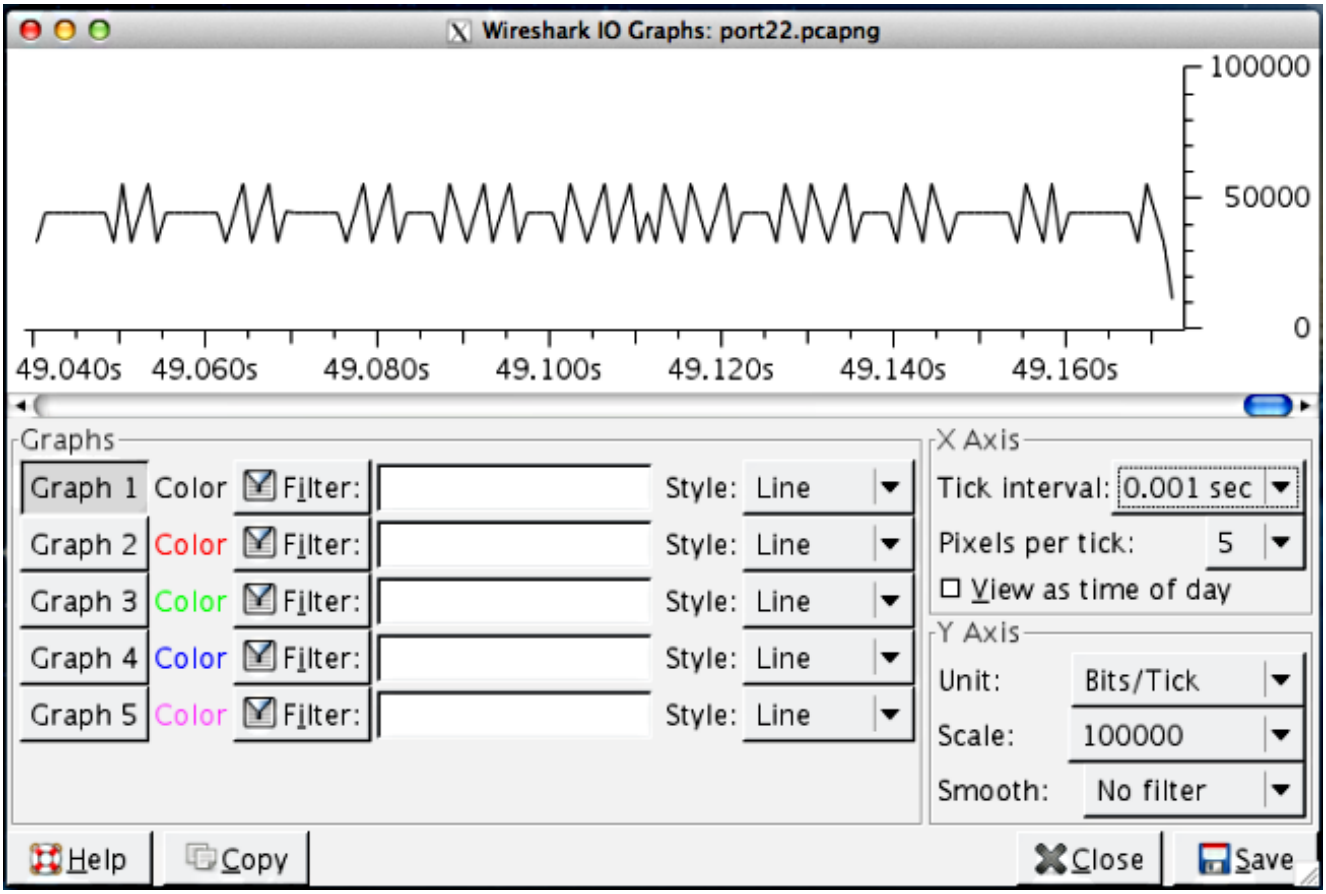
Tuttavia, se la maggior parte del traffico tenta di uscire dall'interfaccia in una frazione di secondo, lo switch deve inserire in un buffer esteso i pacchetti e scartarli quando i buffer sono pieni. Se si rendono le scale più granulari, si ottiene un'immagine più accurata del profilo del traffico effettivo. Modificare l'asse **Y** in bit/tick perché le interfacce mostrano le velocità di output in bit/sec.

La velocità di collegamento è di 100 Mb/s

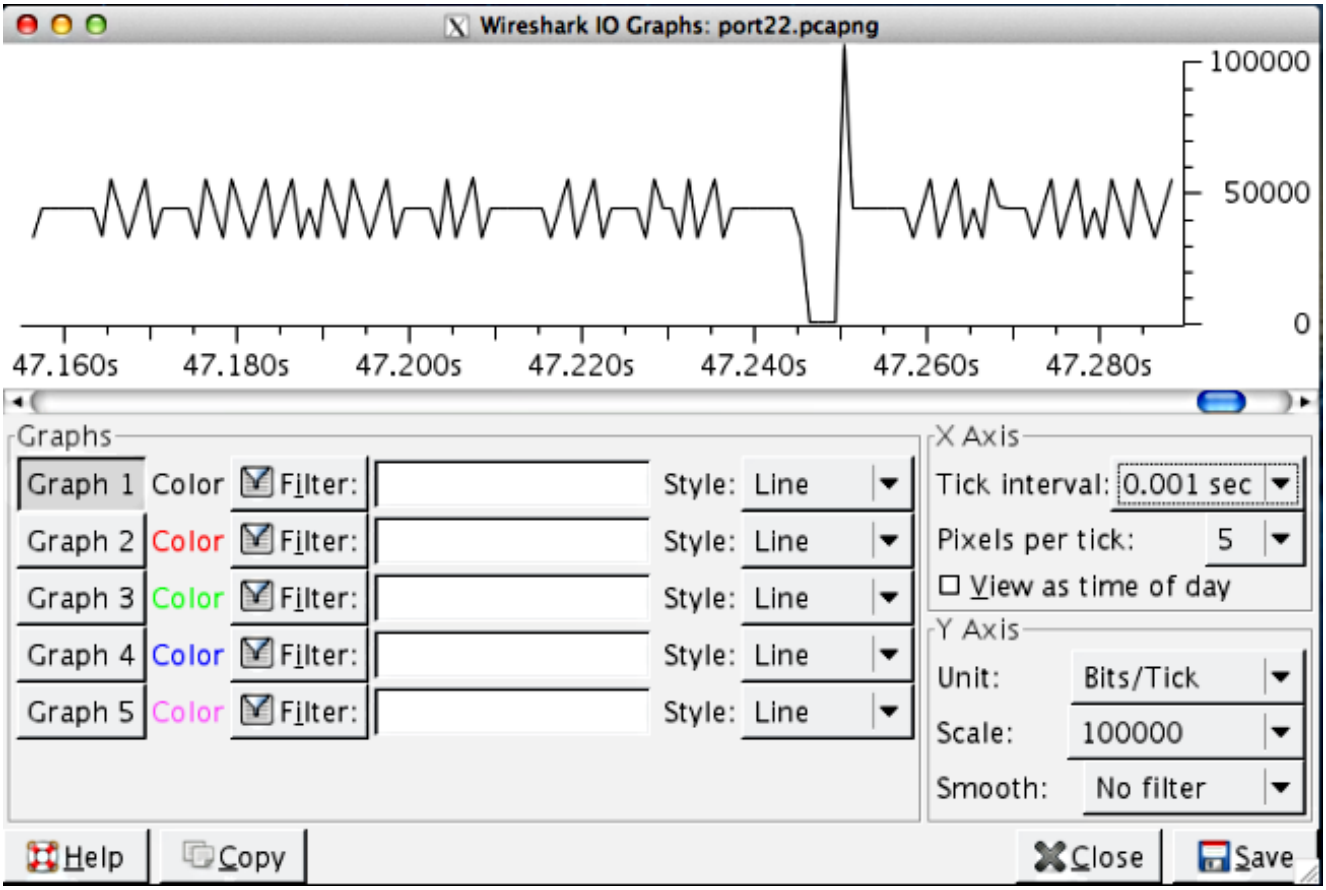
= 100.000.000 bit/s

= 100.000 bit/0,001 s

Ricalcolate le scale sugli assi **X** e **Y**. Impostate l'intervallo di graduazione su **Asse X=0.001 sec** e la scala su **Asse Y=00.000 (bit/tick)**.



5. Scorrere il grafico per identificare i burst. Nell'esempio, potete vedere una sequenza di traffico che supera i 100.000 bit su una scala di 0,001 secondi. Ciò conferma che il traffico è bursty al livello del secondo ed è previsto che venga scartato dallo switch quando i buffer sono pieni.
6. Fare clic sul picco di traffico sul grafico per visualizzare il pacchetto nell'acquisizione di Wireshark. L'analisi della cattura è un modo utile per scoprire quale traffico costituisce lo burst.


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