

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

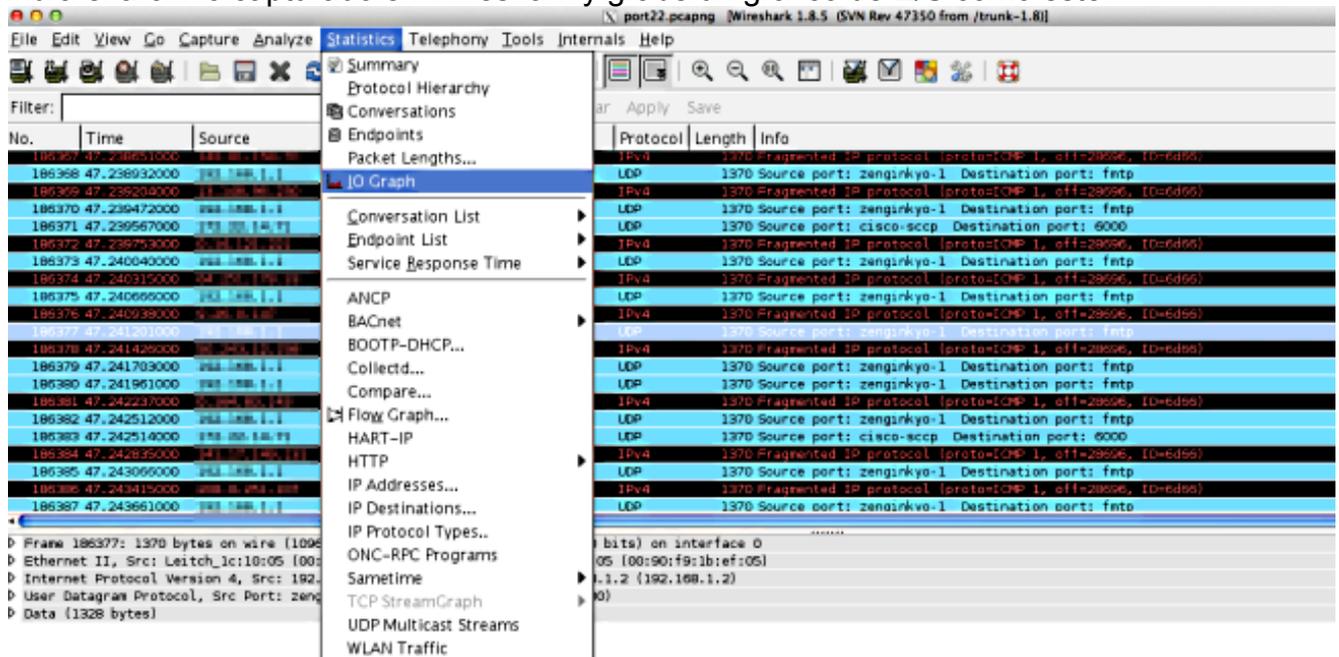
1. Identifique una interfaz que tenga caídas de salida incrementales. Por ejemplo, observa caídas de salida en un link de 100 Mb mientras que el uso promedio del link es solamente de 55 Mb. Aquí está el resultado del comando:

```
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
```

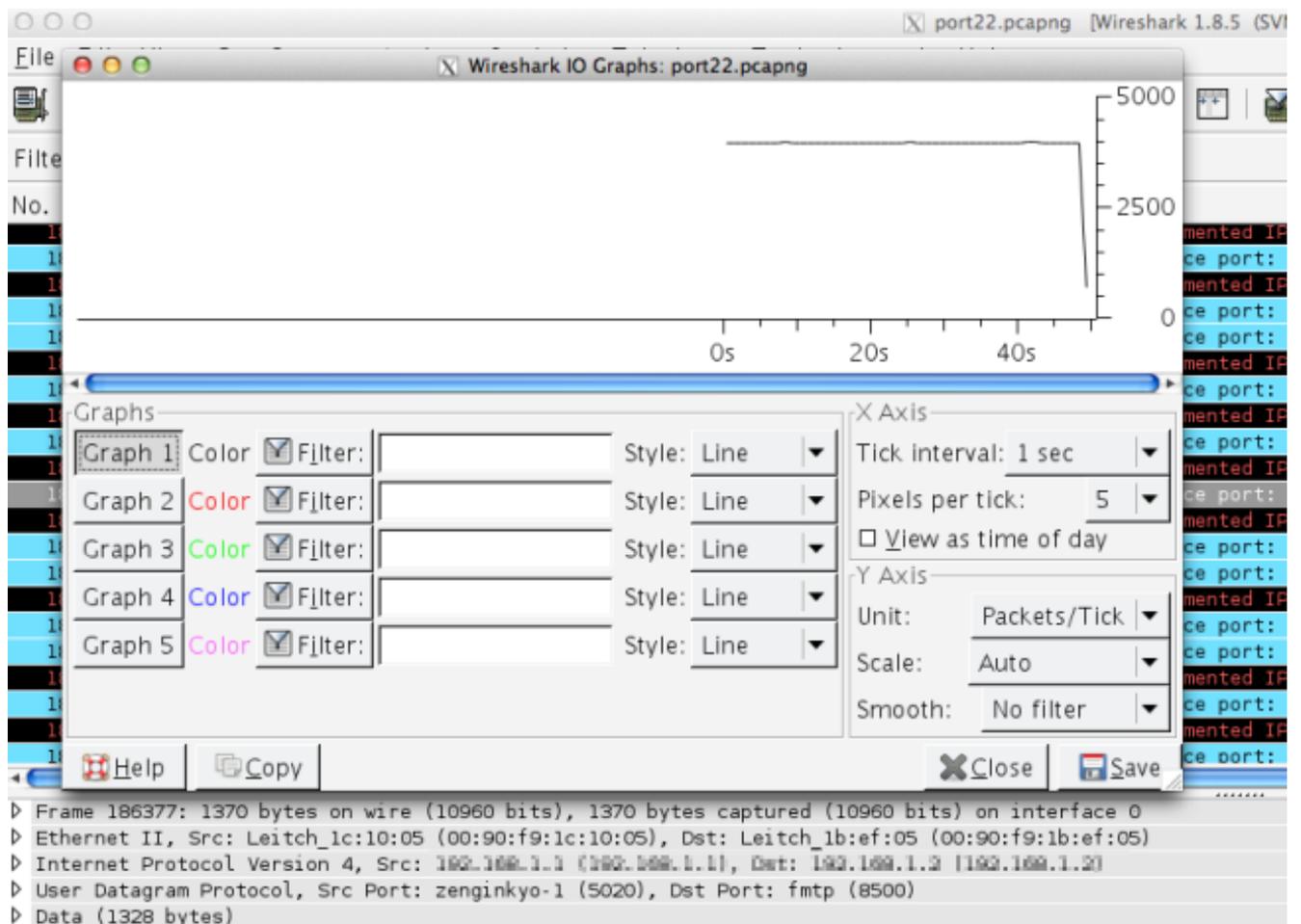
2. Configure SPAN en el switch para capturar el tráfico transmitido (TX). Para capturar este tráfico, conecte una PC que ejecute Wireshark y capture paquetes en el puerto de destino SPAN.

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

3. Abra el archivo capturado en Wireshark y grabe un gráfico de E/S como este.



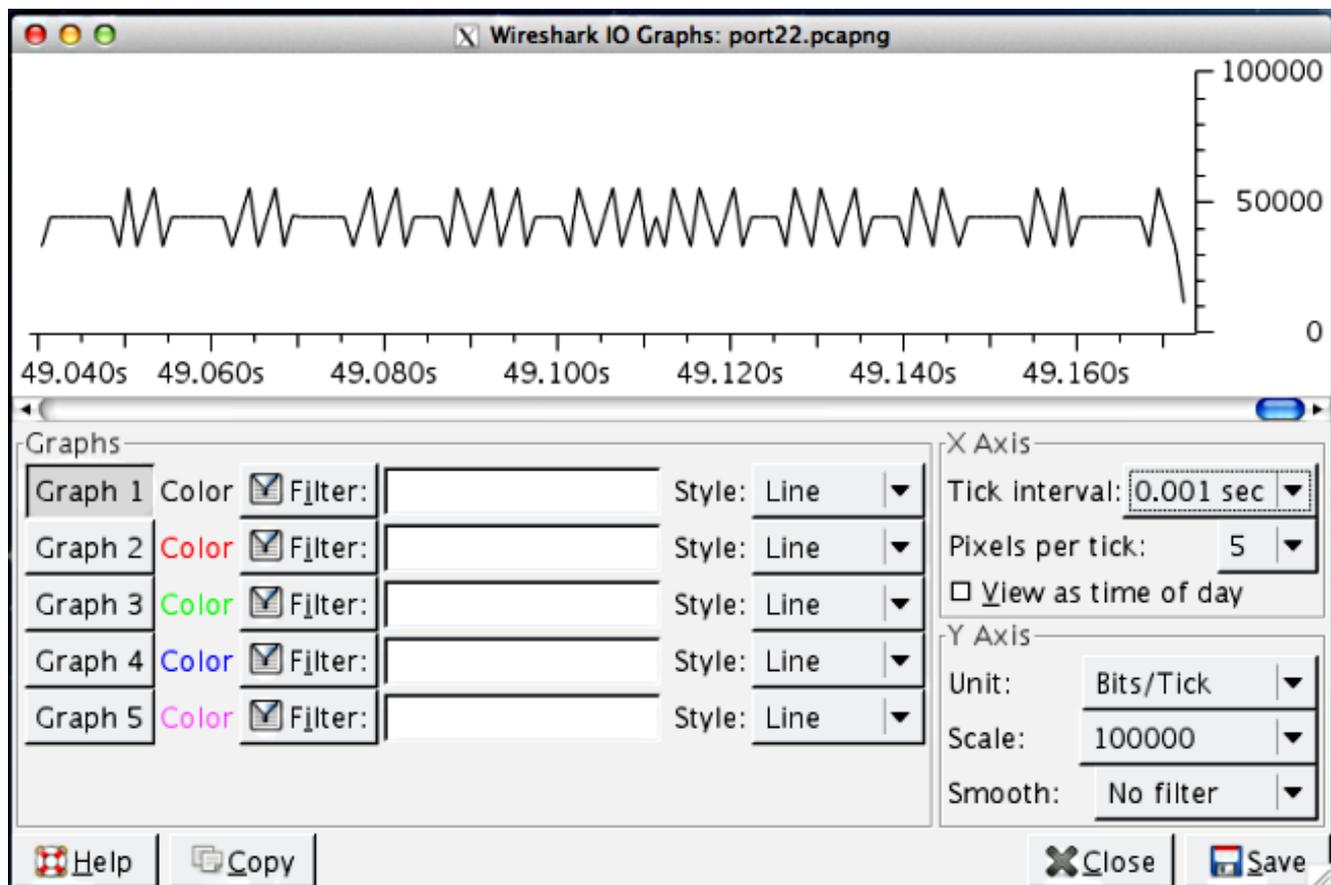
4. En la escala predeterminada, parece que no hay tráfico saturado. Sin embargo, un segundo es un intervalo muy grande cuando se considera la velocidad a la que ocurre el almacenamiento en búfer y el switching de paquetes. En un período de un segundo, un link a 100 Mb/s puede alojar 100 Mb de tráfico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



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)**.



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.

