El uso de Wireshark de identificar el tráfico de Bursty en el catalizador cambia

Contenido

Introducción

Este documento describe cómo identificar el tráfico de la explosión en los switchports del Switches del Cisco Catalyst.

Prerequisites

Requisitos

No hay requisitos específicos para este documento.

Componentes usados

La información en este documento se basa en la serie del conmutador del Cisco Catalyst.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si su red está viva, asegúrese de que usted entienda el impacto potencial del comando any antes de ejecutar el comando.

Antecedentes

Las ráfagas de tráfico pueden hacer hacer salir los descensos incluso cuando la tarifa de salida de la interfaz es perceptiblemente más baja que la capacidad máxima del interfaz. Por abandono, las velocidades de salida en el **comando show interface** se hacen un promedio durante cinco minutos, que no es adecuado capturar ninguna explosiones efímera. Es el mejor hacer un promedio de ellas durante 30 segundos. En este caso, usted puede utilizar Wireshark para capturar el tráfico de salida con el Switched Port Analyzer (SPAN), que se analiza para identificar las explosiones.

Resolver problemas la metodología

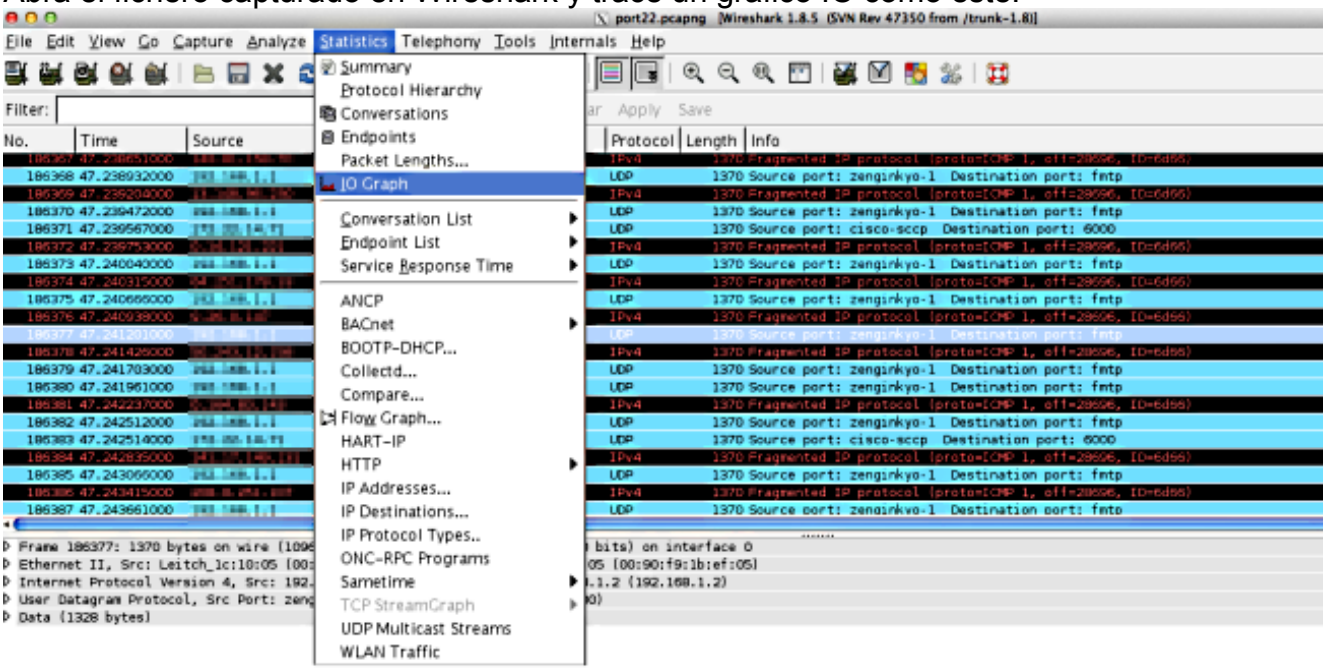
1. Identifique un interfaz que tenga descensos de la salida ampliada. Por ejemplo, usted nota los descensos de la salida en un link 100Mb mientras que el Uso promedio del link es solamente 55Mb. Aquí está la salida del comando:

```
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
```

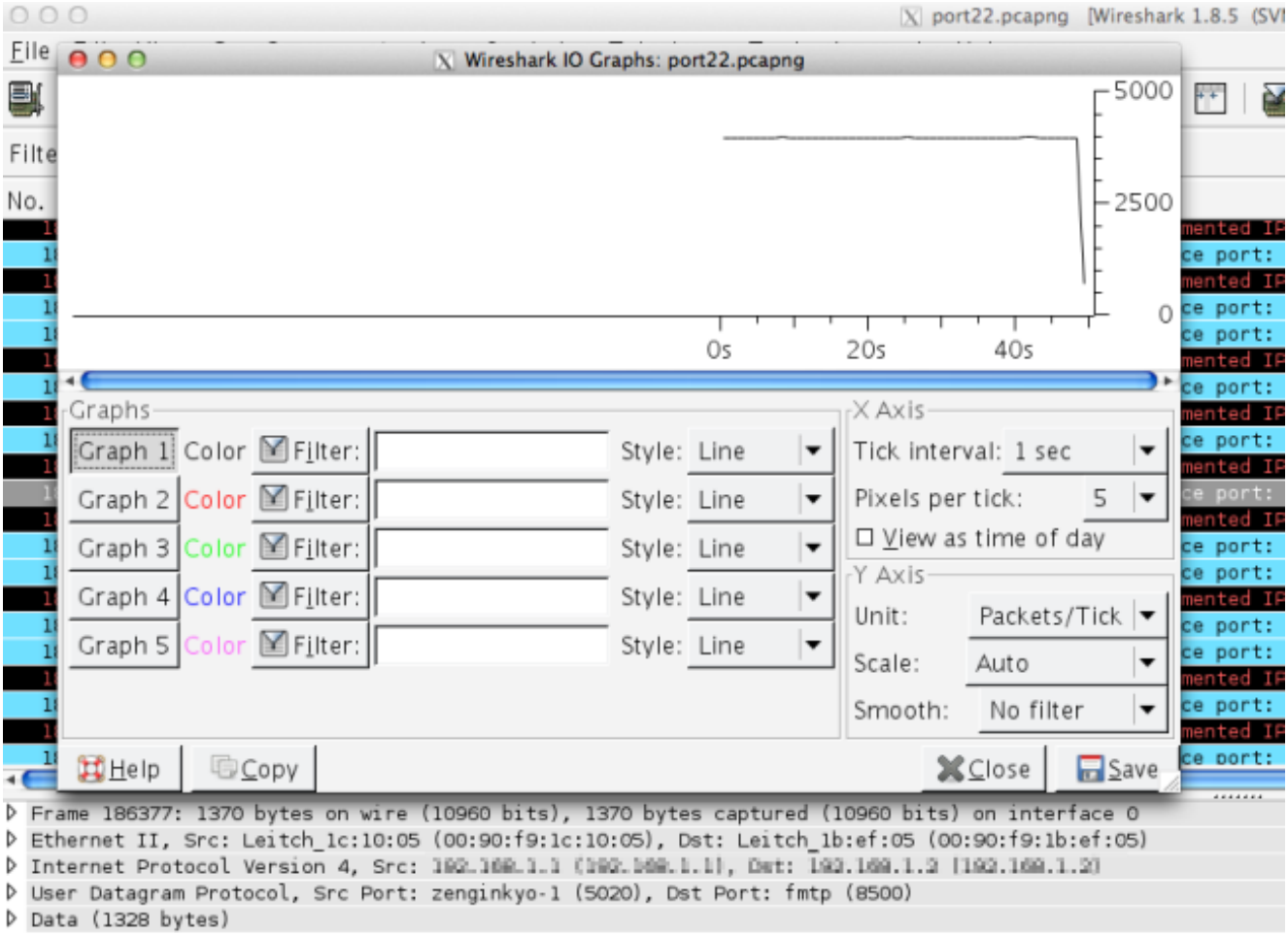
2. Configure el SPAN en el conmutador para capturar el tráfico transmitido (TX). Para capturar este tráfico, conecte una PC que funcione con Wireshark y los paquetes de la captura en el puerto de destino del SPAN.

```
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 fichero capturado en Wireshark y trace un gráfico IO como éste.



4. En la escala del valor por defecto, aparece que no hay tráfico bursty. Sin embargo, el segundo es un intervalo muy grande cuando usted considera la tarifa en la cual el buffering y el packet switching sucede. En un período de segundo, el link a100 Mb/s puede acomodar el 100 Mb del tráfico a través del interfaz en un perfil aseado-formado con una necesidad mínima de proteger cualquier paquete.



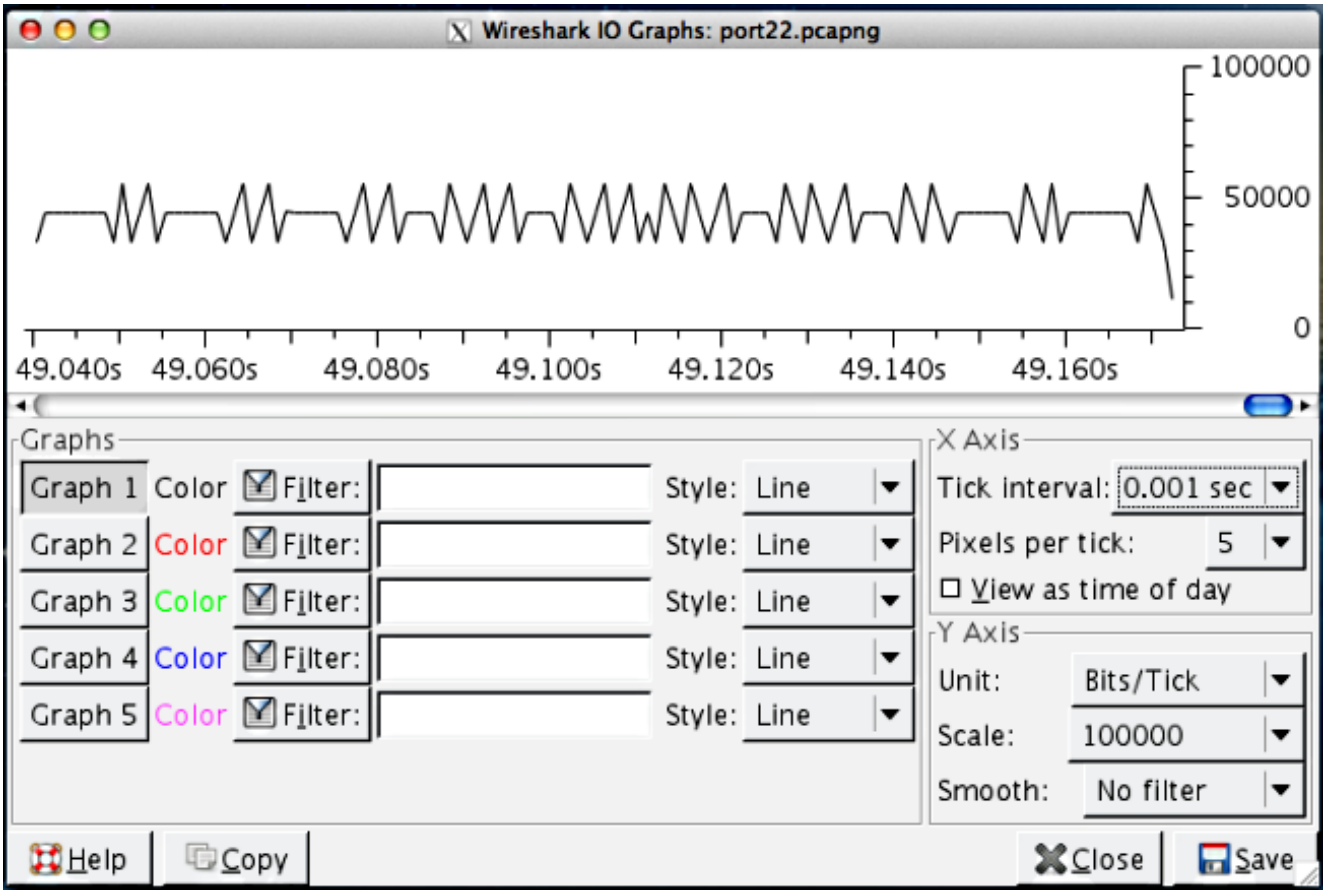
Sin embargo, si una porción importante de este tráfico intenta dejar al interfaz en una parte un segundo, el conmutador necesita extensivamente los paquetes de búfer y los cae cuando los almacenadores intermediarios son llenos. Si usted hace las escalas más granulares, usted ve una imagen más exacta del perfil del tráfico real. Cambie el eje **Y a los** bits/señal porque los interfaces muestran las velocidades de salida en los dígitos por segundo.

La velocidad del link es 100 Mb/s

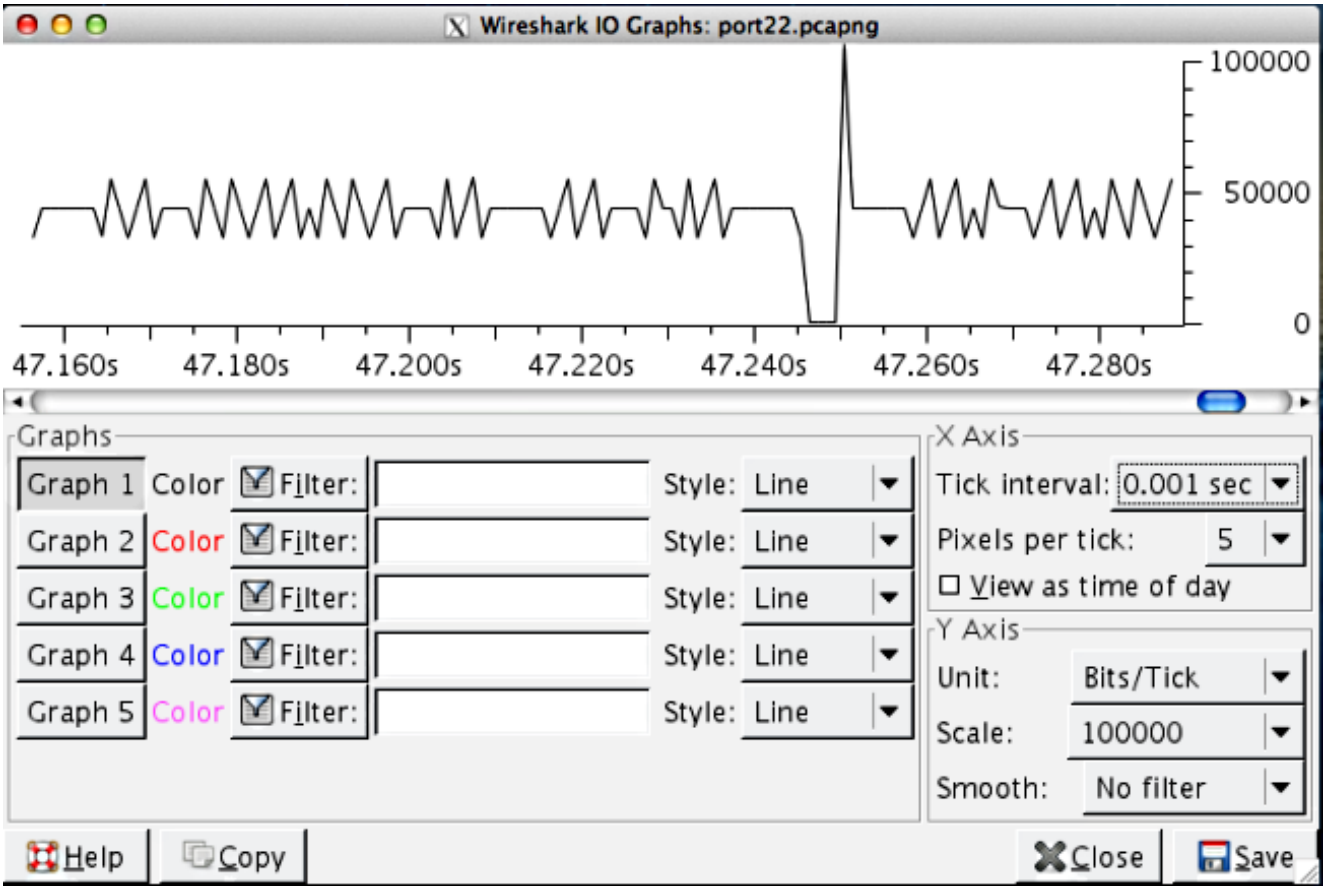
= 100,000,000 bits/s

= 100,000 bits/0.001 s

Recalcule las escalas en las hachas **X** y **Y**. Cambie el intervalo de la señal al **sec X Axis=0.001** y la escala a **Y axis=00,000 (bits/señal)**.



5. Desplazamiento a través del gráfico para identificar las explosiones. En este ejemplo, usted puede ver que hay una explosión del tráfico que excedió 100,000 bits en las 0.001 segundos escalas. Esto confirma que se espera que el tráfico es bursty en el nivel sub-segundo y consiga caído por el conmutador cuando los almacenadores intermediarios son llenos para acomodar estas explosiones.
6. Haga clic en el pico de tráfico en el gráfico para ver que paquete en la captura de Wireshark. El análisis de la captura es una forma útil de descubrir qué tráfico constituye la explosión.


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