Uso do Wireshark para identificar tráfego em surtos em switches Catalyst

Contents

Introduction

Este documento descreve como identificar o tráfego de pico nas portas de switch dos switches Cisco Catalyst.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas na série de switches 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. Se sua rede estiver ativa, certifique-se de que você entendeu o impacto potencial de qualquer comando antes de executar o comando.

Informações de Apoio

As intermitências de tráfego podem causar quedas de saída mesmo quando a taxa de saída da interface é significativamente inferior à capacidade máxima da interface. Por padrão, as taxas de saída no comando **show interface** são médias em cinco minutos, o que não é adequado para capturar quaisquer rajadas de vida curta. É melhor mediá-los em 30 segundos. Nesse caso, você pode usar o Wireshark para capturar o tráfego de saída com o Switched Port Analyzer (SPAN), que é analisado para identificar as rajadas.

Metodologia de solução de problemas

1. Identifique uma interface que tenha quedas de saída incrementais. Por exemplo, você

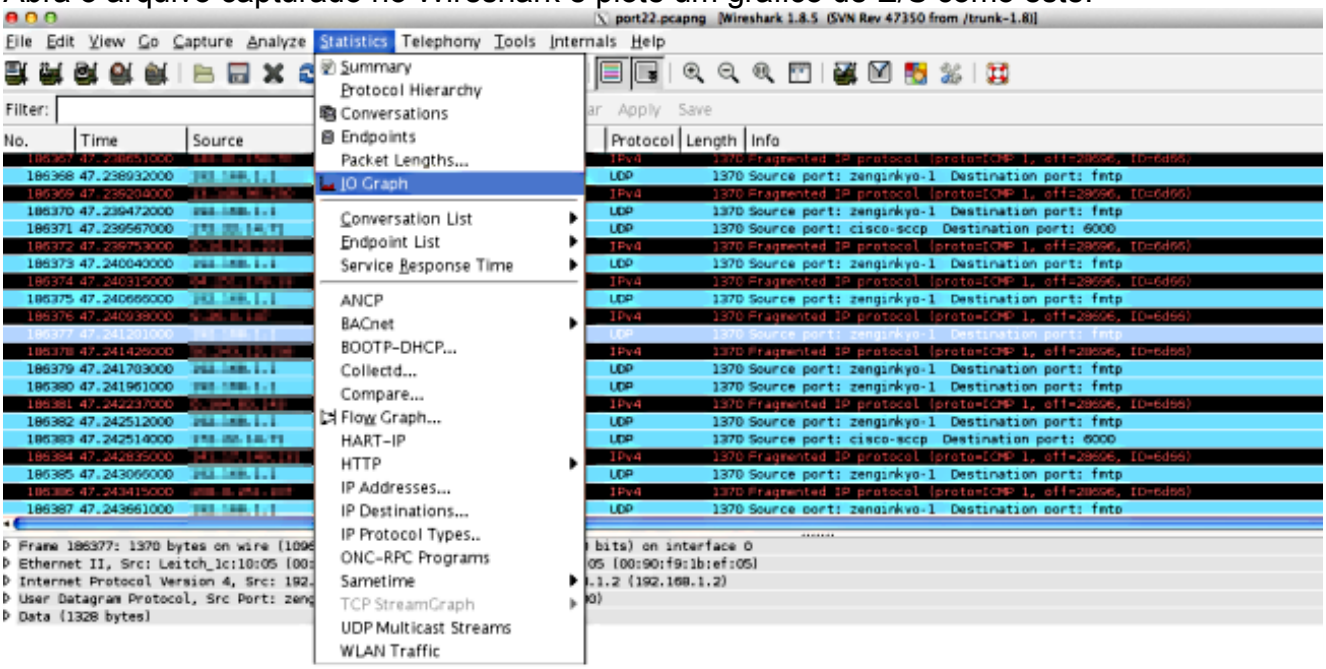
percebe quedas de saída em um link de 100 Mb, enquanto a utilização média do link é de apenas 55 Mb. Aqui está a saída do comando:

```
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
```

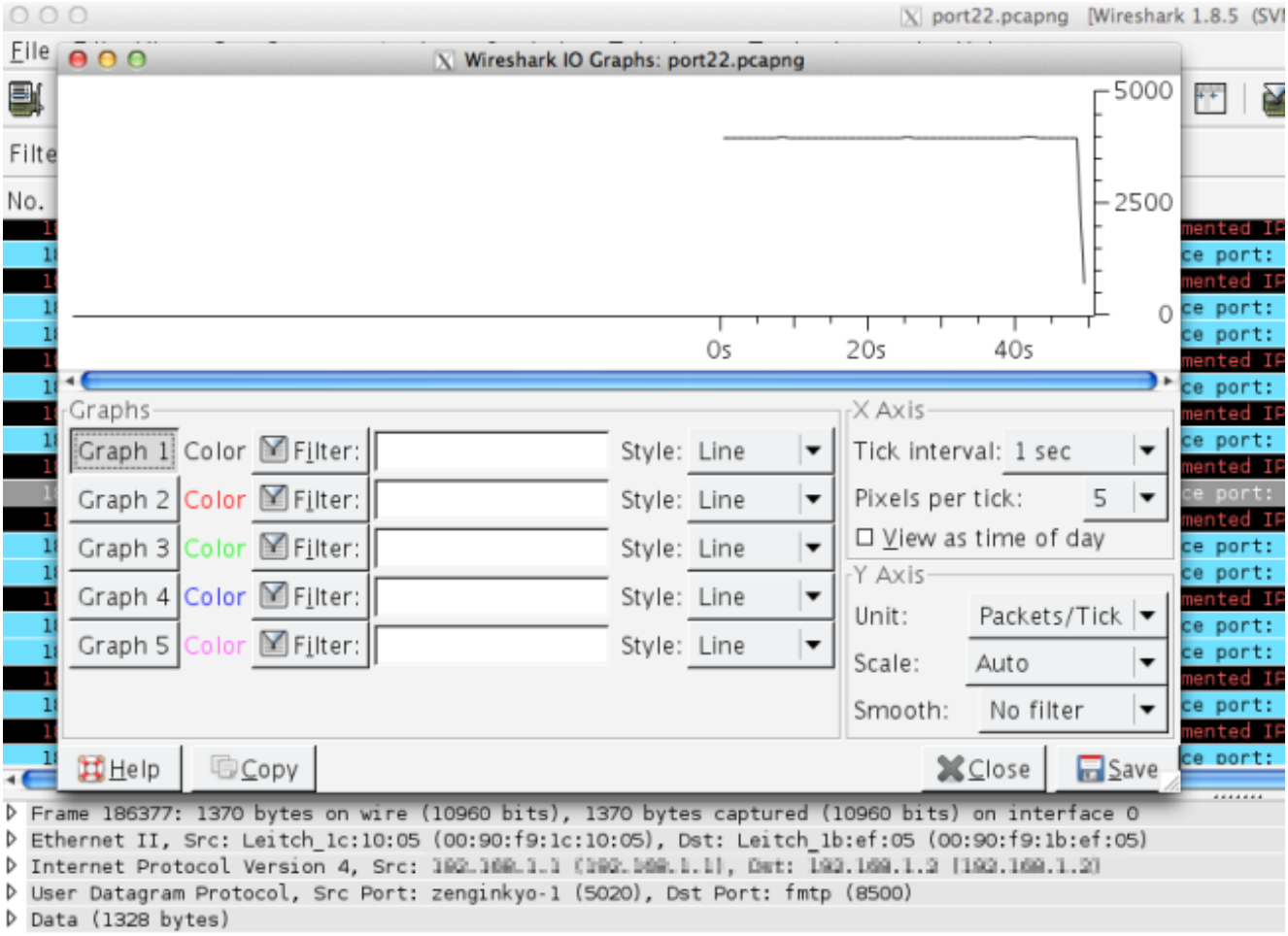
2. Configure o SPAN no switch para capturar o tráfego transmitido (TX). Para capturar esse tráfego, conecte um PC que executa o Wireshark e capture pacotes na porta de destino do SPAN.

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

3. Abra o arquivo capturado no Wireshark e plote um gráfico de E/S como este.



4. Na escala padrão, parece que não há tráfego de pico. No entanto, um segundo é um intervalo muito grande quando você considera a taxa na qual o buffer e a comutação de pacotes ocorrem. Em um período de um segundo, um link de 100 Mb/s pode acomodar 100 Mb de tráfego através da interface em um perfil em forma de rede com uma necessidade mínima de armazenar em buffer qualquer pacote.



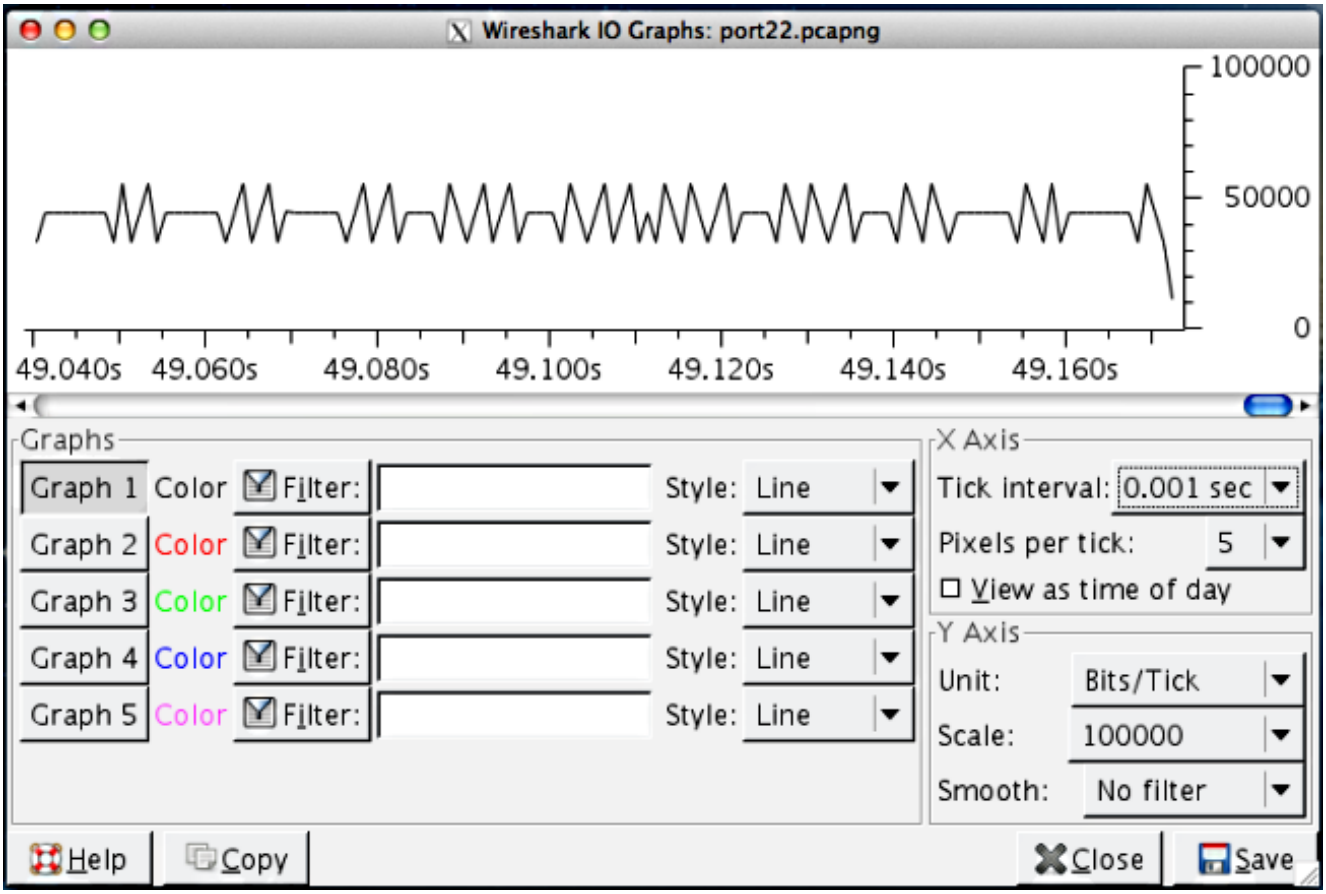
No entanto, se uma grande parte desse tráfego tentar deixar a interface em uma fração de segundo, o switch precisará armazenar em buffer os pacotes extensivamente e descartá-los quando os buffers estiverem cheios. Se você tornar as escalas mais granulares, verá uma imagem mais precisa do perfil de tráfego real. Altere o eixo **Y** para bits/tique porque as interfaces mostram taxas de saída em bits/s.

A velocidade do link é 100 Mb/s

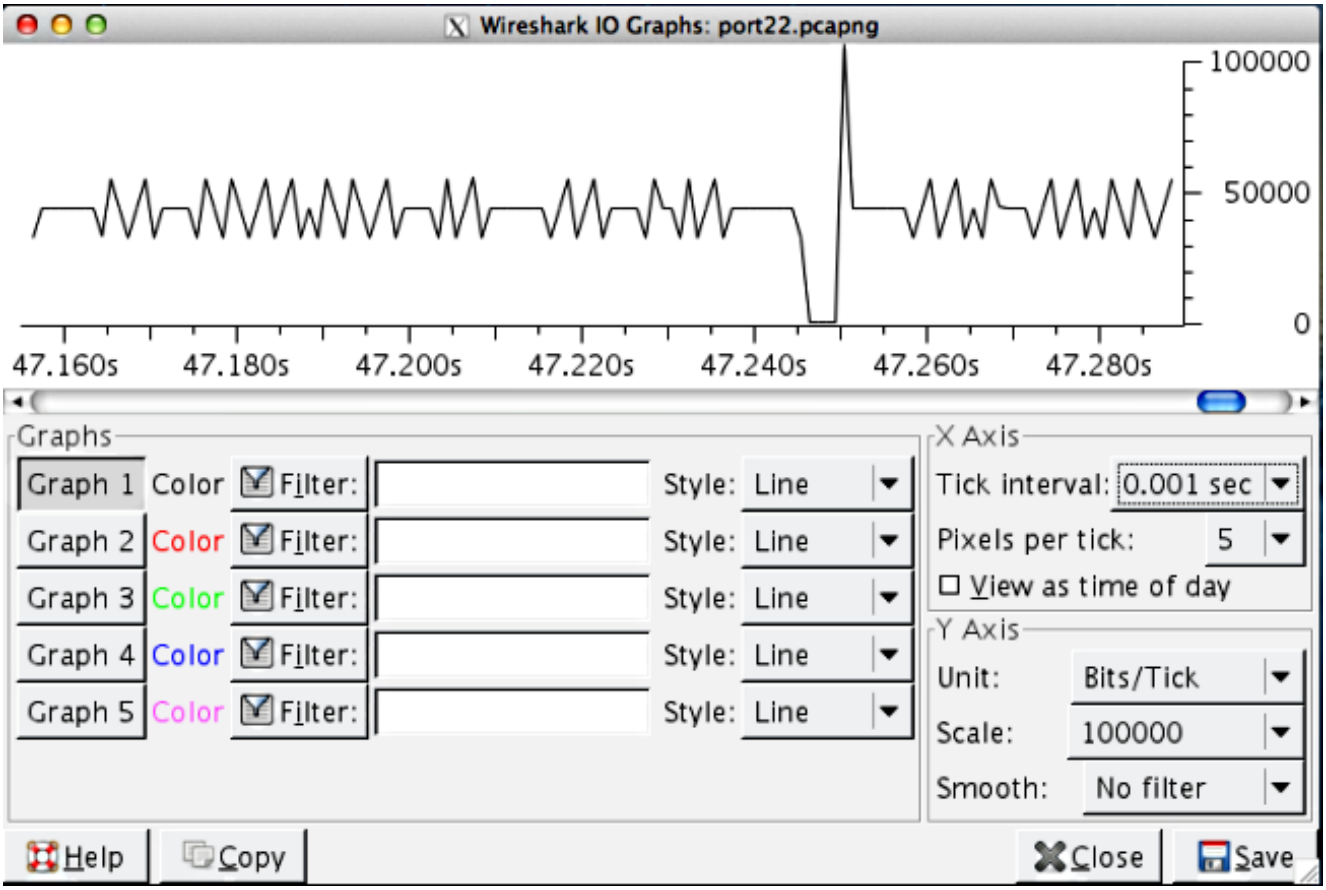
= 100.000.000 bits/s

= 100.000 bits/0,001 s

Recalcular as escalas nos eixos **X** e **Y**. Altere o intervalo de escala para **X Eixo=0,001 s** e ajuste para o **eixo Y=00.000 (bits/tique)**.



5. Percorra o gráfico para identificar rajadas. Neste exemplo, você pode ver que há uma intermitência de tráfego que excedeu 100.000 bits em uma segunda escala de 0.001. Isso confirma que o tráfego está intermitente no nível de subsegundo e espera-se que seja descartado pelo switch quando os buffers estiverem cheios para acomodar essas intermitências.
6. Clique no pico de tráfego no gráfico para visualizar esse pacote na captura do Wireshark. A análise de captura é uma forma útil de descobrir o tráfego que constitui a intermitência.


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