

Wireshark使用识别在Catalyst交换机的突发数据流

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[故障排除方法](#)

简介

本文描述如何识别在Cisco Catalyst交换机连接孔的突发传输数据流。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文的信息根据Cisco Catalyst交换机系列。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络实际，请切记您在执行命令前了解所有命令的潜在影响。

背景信息

流量突发能导致输出下落，既使当接口输出费率比最大接口容量显着低。默认情况下，在**show interface**命令的输出速率被平均五分钟，不是足够的捕获任何短期的突发传输。平均为他们30秒是最佳的。在这种情况下，您能使用Wireshark为了捕获与交换端口分析器(SPAN)的出口流量，分析为了识别突发传输。

故障排除方法

1. 识别有递增输出下落的一个接口。例如，当链路的平均利用率是仅55Mb时，您注意在100Mb链路的输出下落。这是命令的输出：

```
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

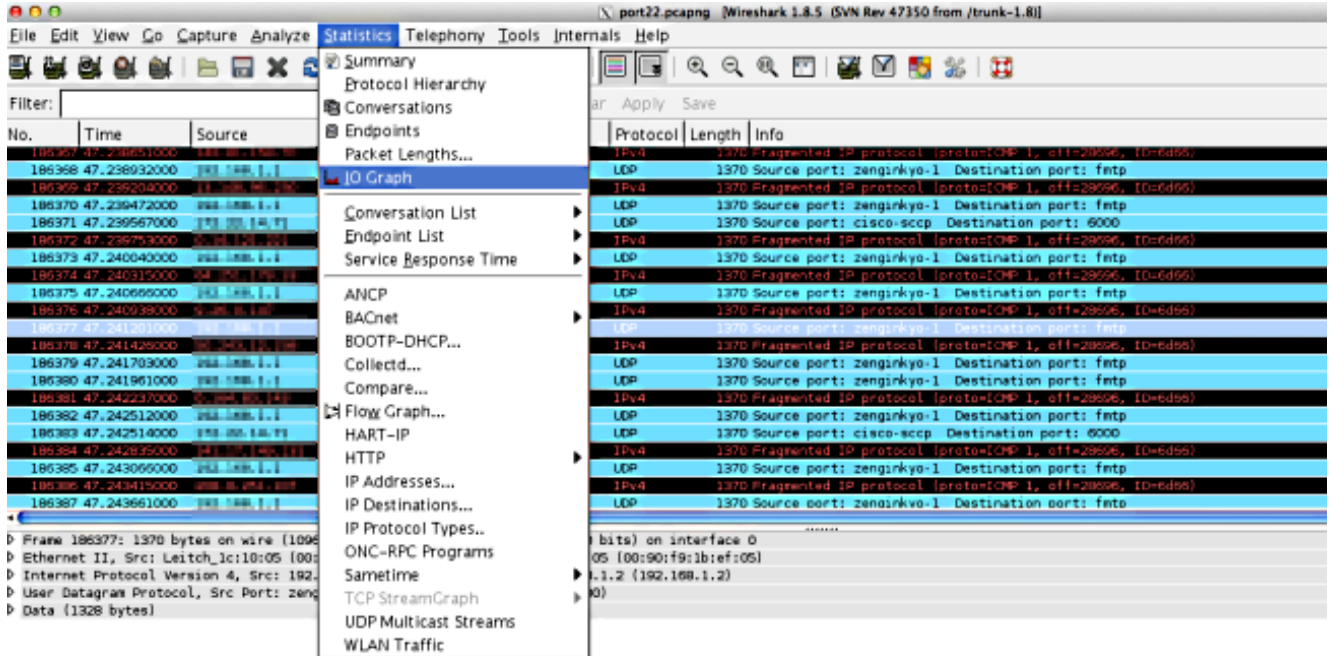
- 配置在交换机的SPAN为了捕获被传输的(TX)数据流。为了捕获此数据流，请连接传输Wireshark和捕获信息包在SPAN目的地端口的PC。

Switch#config t

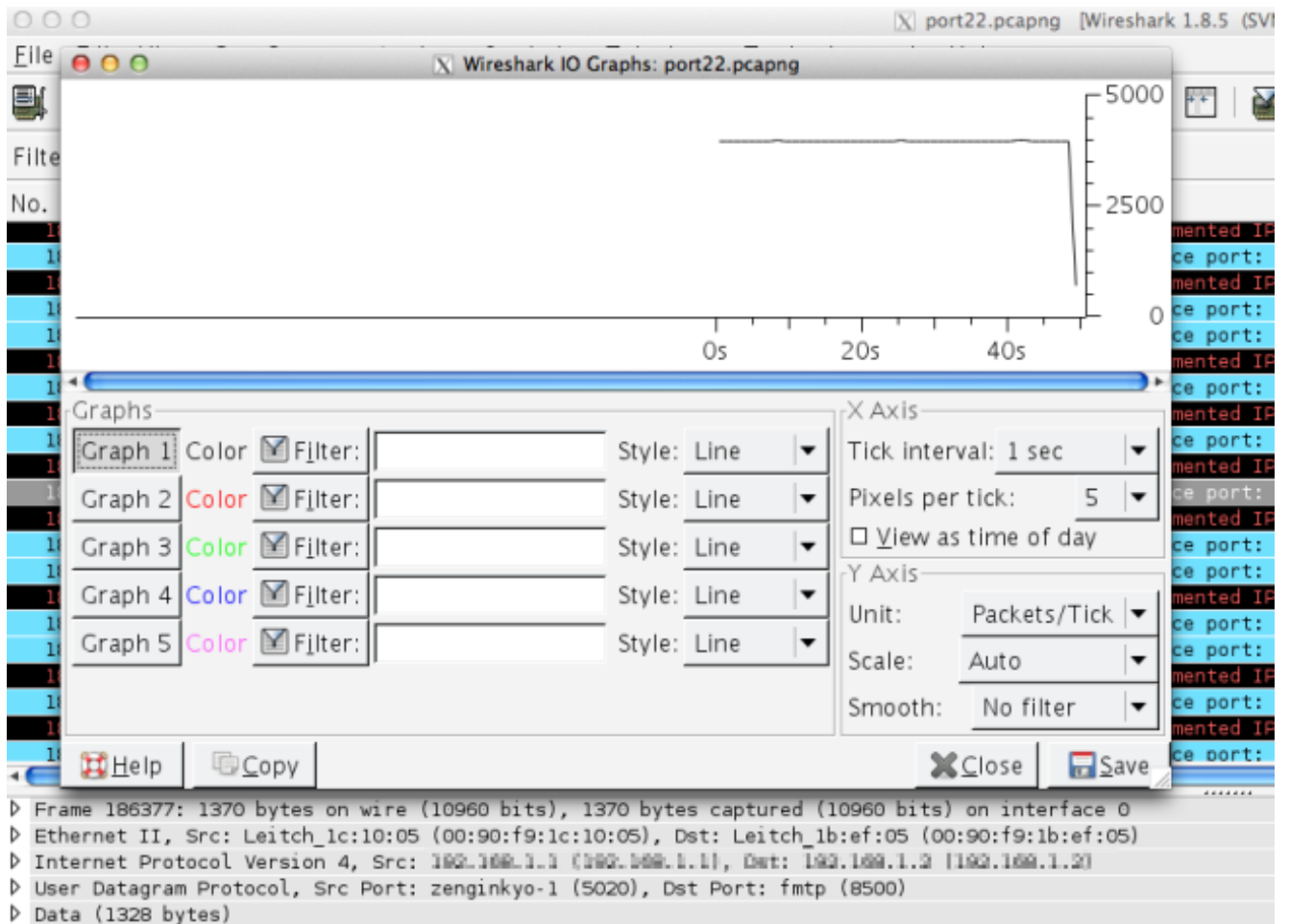
Switch(conf)#monitor session 1 source interface fal/1 tx

Switch(conf)#monitor session 1 destination interface fal/2

- 打开在Wireshark的捕获文件并且密谋一个IO图形类似这一个。



- 在默认缩放，看来没有突发数据流。然而，一秒钟是一个非常大大间隔，当您考虑缓冲和数据包交换发生的费率时。在一秒钟的周期，a100 Mb/s链路能适应数据流100 Mb在接口间的在一个整形型配置文件以最低的需要缓冲所有信息包。



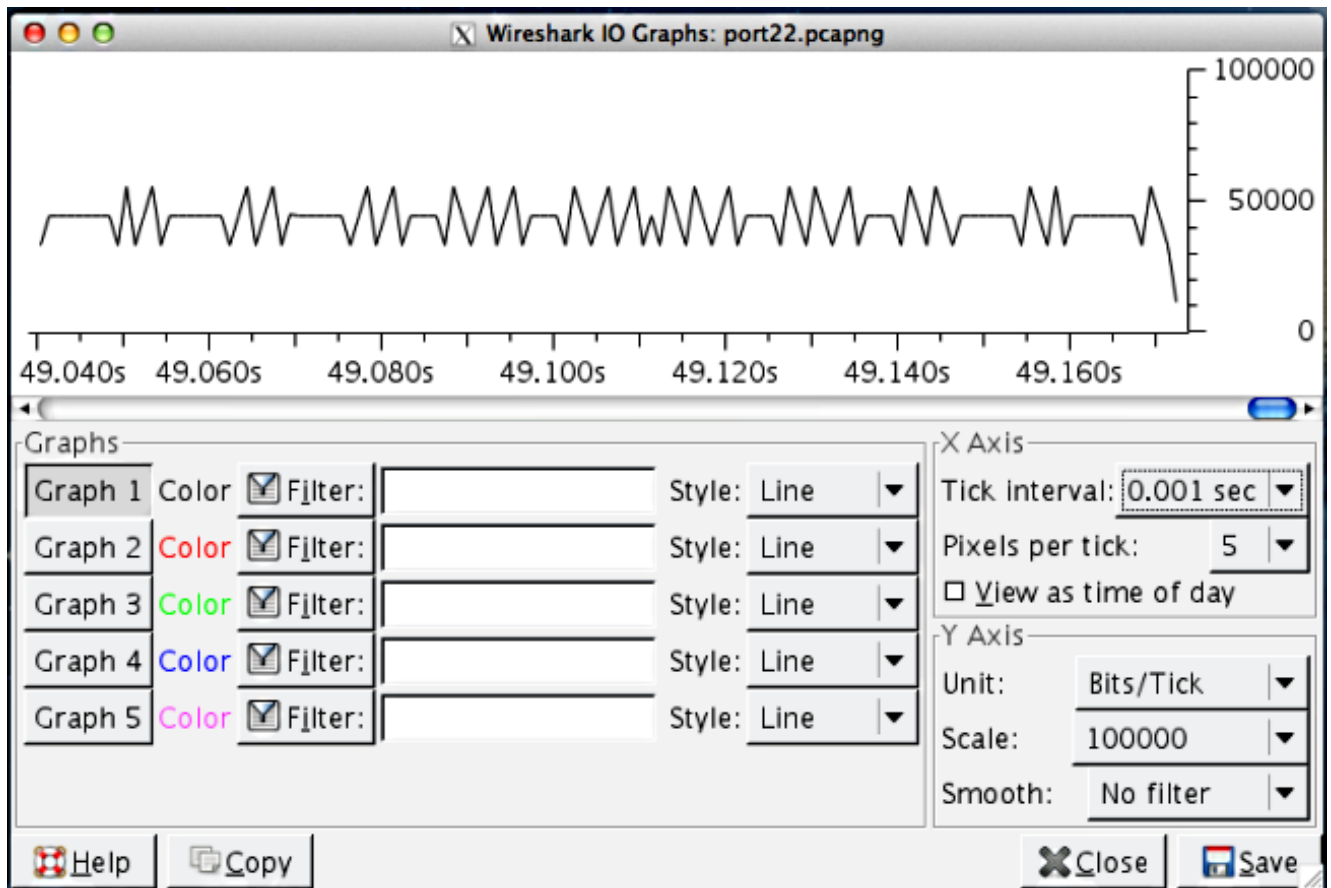
然而，如果此数据流的大部分在一小部分尝试把接口一秒钟留在，交换机广泛地需要缓冲信息包并且丢弃他们，当缓冲区是充分的时。如果使缩放比例更加粒状，您看到实际数据流配置文件的一张更加准确的图片。因为接口在位/秒，显示输出速率请更改Y轴到包/瞬间。

链路速度是100 Mb/s

$$= 100,000,000 \text{ 个bits/s}$$

$$= 100,000 \text{ 个bits/0.001 s}$$

重估在X和Y轴的缩放比例。更改瞬间间隔到X Axis=0.001秒和缩放到Y axis=00,000 (包/瞬间)。



5. 通过图形移动为了识别突发传输。在本例中，您能看到有超出在-0.001秒等级的100,000位的突发数据流。这确认数据流是突变性在分秒的级别和由交换机预计被撤销，当缓冲区是充分的为了适应这些突发传输时。
6. 点击在图形的数据流信号为了查看在Wireshark捕获的信息包。捕获分析是一个有用的方式发现什么数据流构成突发传输。

