Wireshark用于识别Catalyst交换机上的突发流量

目录

简介

本文档介绍如何识别Cisco Catalyst交换机交换机端口上的突发流量。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于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。如果您的网络处于活动状态，请确保在执行命令之前了解任何命令的潜在影响。

背景信息

即使接口输出速率显着低于最大接口容量，流量突发也会导致输出丢弃。默认情况下，**show interface**命令的输出速率平均在五分钟内，这不足以捕获任何短时突发。最好在30秒内将其平均化。在这种情况下，您可以使用Wireshark通过交换端口分析器(SPAN)捕获出口流量，该分析用于识别突发流量。

故障排除方法

1. 识别输出丢弃递增的接口。例如，您注意到100Mb链路上的输出丢弃，而链路的平均利用率仅为55Mb。以下是命令的输出：

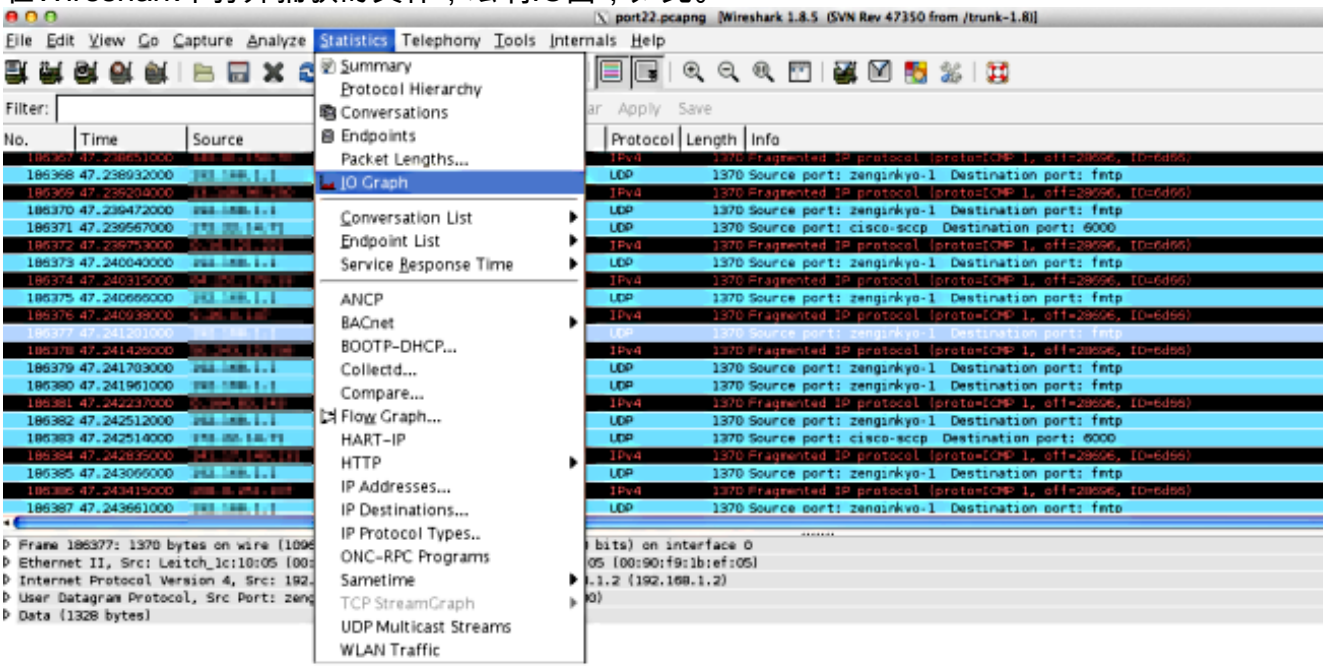
```
Switch#show int fa1/1 | i duplex|output drops|rate
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 5756
  5 minute input rate 55343353 bits/sec, 9677 packets/sec
  5 minute output rate 55456293 bits/sec, 9878 packets/sec
```

2. 在交换机上配置SPAN以捕获传输(TX)流量。要捕获此流量，请连接运行Wireshark的PC，并

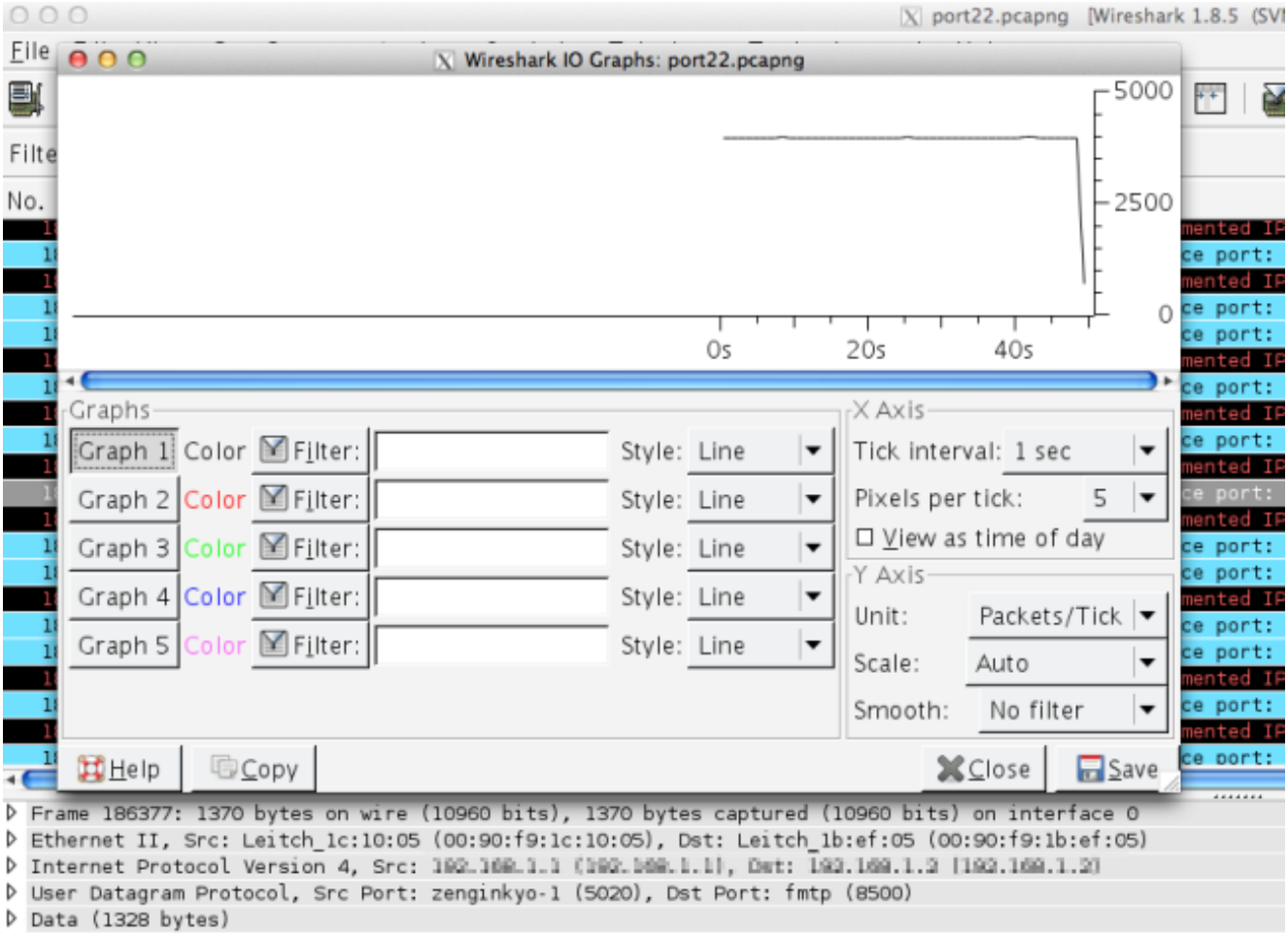
在SPAN目标端口捕获数据包。

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

3. 在Wireshark中打开捕获的文件，绘制IO图，如此。



4. 默认规模下，似乎没有突发流量。但是，当您考虑缓冲和数据包交换的速率时，一秒是非常大的间隔。在一秒内，100 Mb/s链路可以整齐的轮廓中容纳100 Mb的接口流量，最少需要缓冲任何数据包。



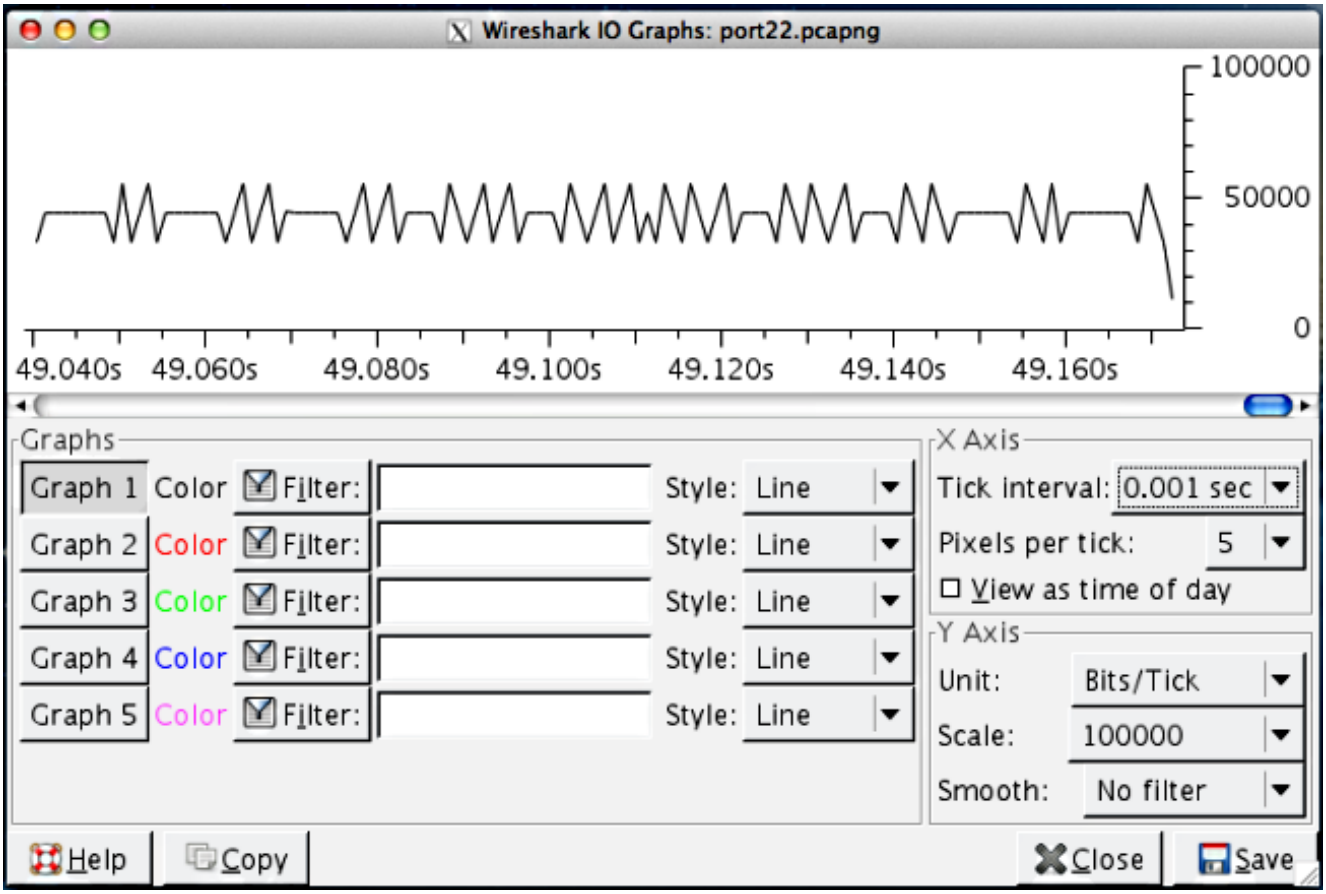
但是，如果此流量的主要部分尝试以一秒的几分之一离开接口，交换机需要大量缓冲数据包并在缓冲区已满时丢弃这些数据包。如果您使扩展更加精细，您会看到实际流量量变曲线的更准确图片。将Y轴**更改**为位/刻度，因为接口以位/秒为单位显示输出速率。

链路速度为100 Mb/s

= 100,000,000位/秒

= 100,000位/0.001秒

重新计算X轴**和Y轴上的**比例。将刻度间隔更**改为X Axis=0.001**秒，将刻度**改为Y axis=00,000（位/刻度）**。



5. 滚动浏览图形以识别突发。在本例中，您可以看到流量突发，在0.001秒的比例尺中超过100,000位。这确认了流量在次秒级突发，当缓冲区已满时，交换机会丢弃流量，以适应这些突发。
6. 单击图形上的流量尖峰，以在Wireshark捕获中查看该数据包。捕获分析是发现构成突发流量的有用方法。