

# Wireshark用於識別Catalyst交換機上的突發流量

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[故障排除方法](#)

## 簡介

本檔案介紹如何識別Cisco Catalyst交換器交換器連線埠上的突發流量。

## 必要條件

### 需求

本文件沒有特定需求。

### 採用元件

本檔案中的資訊是根據Cisco Catalyst交換器系列。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保在執行指令之前您已瞭解任何指令可能造成的影響。

## 背景資訊

即使介面輸出速率明顯低於最大介面容量，流量突發也會導致輸出丟棄。預設情況下，**show interface**命令的輸出速率在5分鐘內平均化，不足以捕獲任何短暫的猝發。最好是平均超過三十秒。在這種情況下，您可以使用Wireshark以使用交換連線埠分析器(SPAN)擷取輸出流量，該分析器會分析識別突發。

## 故障排除方法

1. 確定具有增量輸出丟棄的介面。例如，您注意到100Mb鏈路上的輸出丟棄，而鏈路的平均利用率僅為55Mb。以下是命令的輸出：

```
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
```

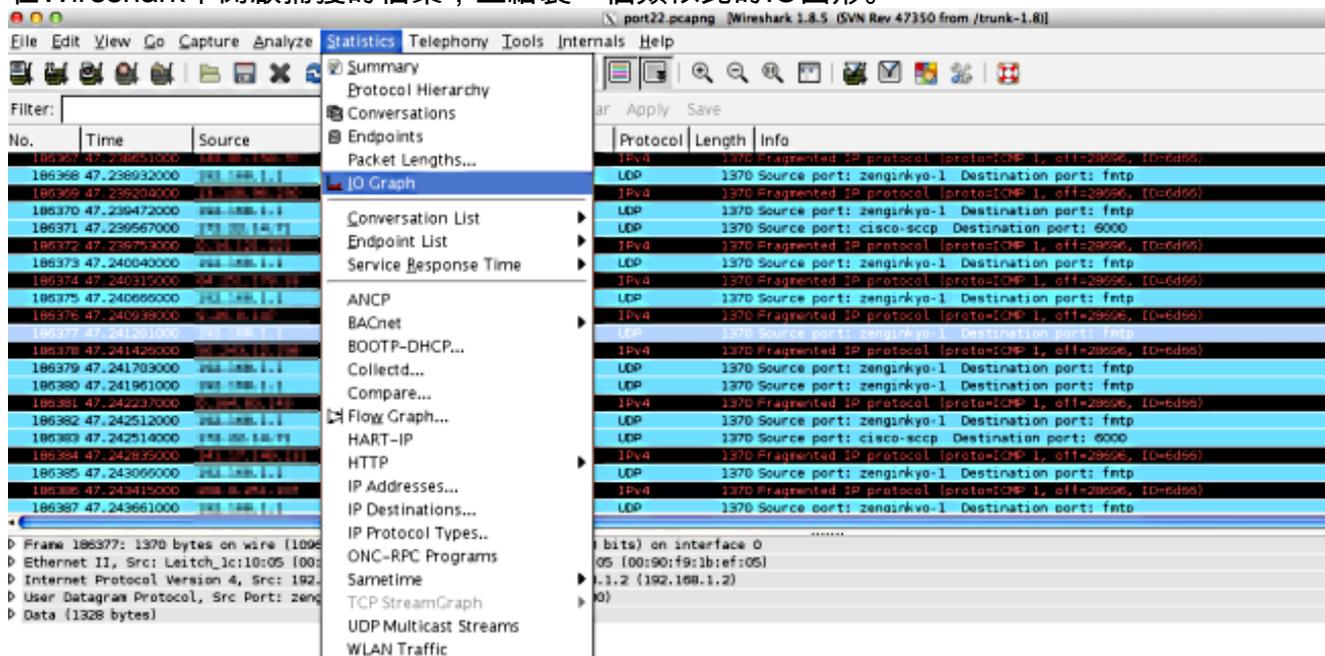
2. 在交換器上設定SPAN，以擷取傳輸的(TX)流量。為了擷取此流量，請連線執行Wireshark的PC，並在SPAN目的地連線埠上擷取封包。

```
Switch#config t
```

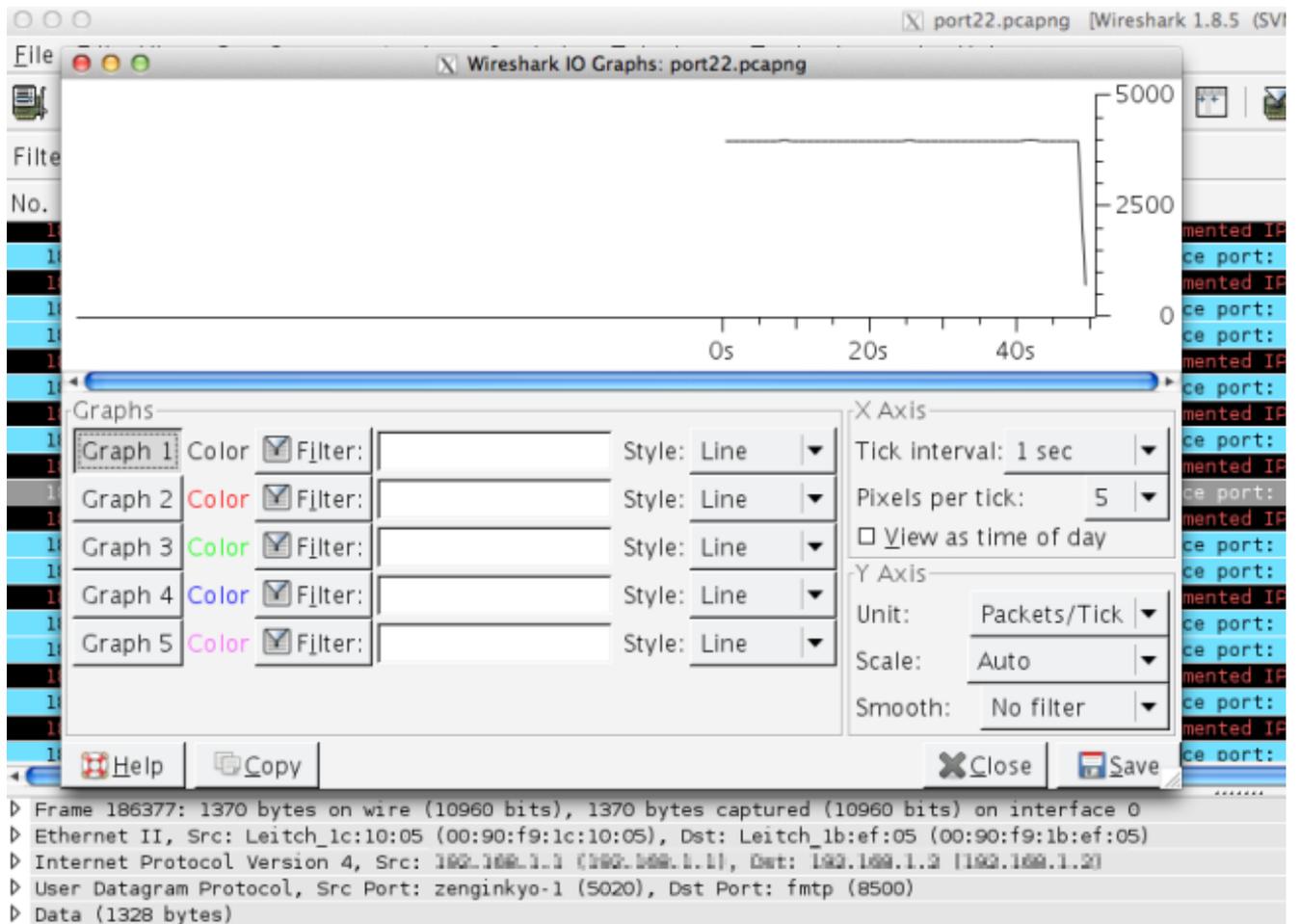
```
Switch(conf)#monitor session 1 source interface fa1/1 tx
```

```
Switch(conf)#monitor session 1 destination interface fa1/2
```

3. 在Wireshark中開啟捕獲的檔案，並繪製一個類似此的IO圖形。



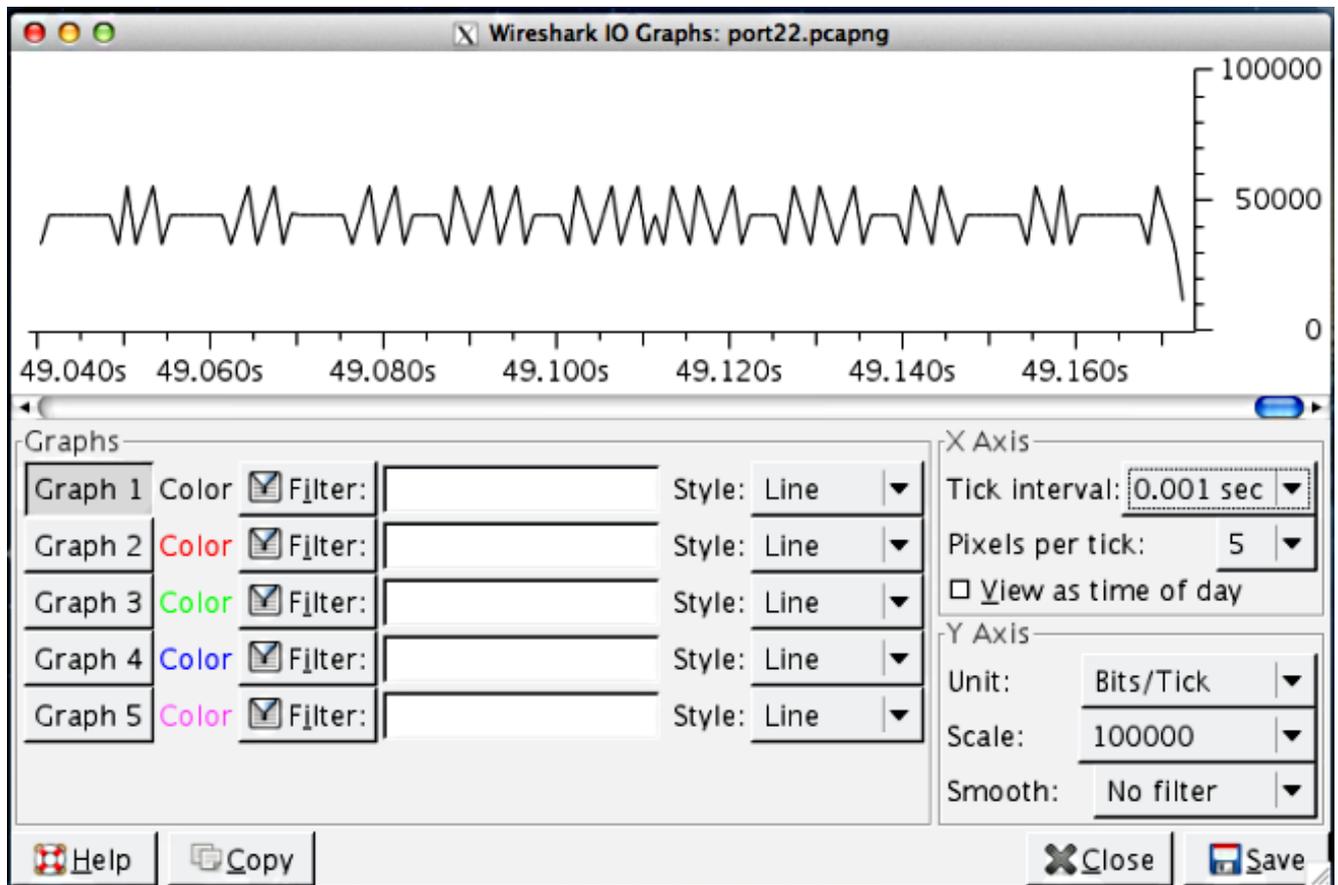
4. 在預設情況下，似乎沒有突發流量。但是，當您考慮發生緩衝和資料包交換的速率時，一秒是一個非常大的間隔。在一秒鐘的時間內，100 Mb/s的鏈路可以容納經過介面的100 Mb流量，且外形整齊，對緩衝任何資料包的最低需求。



但是，如果此流量的主要部分試圖在幾分之一秒內離開介面，則交換機需要大量緩衝資料包，並在緩衝區已滿時將其丟棄。如果使比例更精確，您就會看到更精確的實際流量分佈圖。將Y軸更改為位/勾選，因為介面以位/秒為單位顯示輸出速率。

鏈路速度為100 Mb/s  
 = 100,000,000位/秒  
 = 100,000位/0.001秒

重新計算X軸和Y軸上的比例。將刻度間距更改為X Axis=0.001 sec，並將刻度更改為Y axis=00,000 ( 位/刻度 )。



5. 在圖形中滾動以識別突發。在此示例中，您可以看到在0.001秒範圍內存在超過100,000位的突發流量。這確認流量在次秒級突發，且預期會在緩衝區滿時由交換器捨棄，以容納這些突發。
6. 按一下圖形上的流量峰值，檢視Wireshark捕獲中的資料包。捕獲分析是發現構成突發流量的有用方法。

