Catalyst 스위치에서 버스트 트래픽을 식별하는 Wireshark 사용

목차

소개

이 문서에서는 Cisco Catalyst 스위치의 스위치 포트에서 버스트 트래픽을 식별하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco Catalyst 스위치 시리즈를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 명령을 실행하기 전에 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

트래픽 버스트는 인터페이스 출력 속도가 최대 인터페이스 용량보다 훨씬 낮더라도 출력을 떨어뜨릴 수 있습니다.기본적으로 **show interface** 명령의 출력 속도는 5분 동안 평균화되어 있으므로 짧은 버스트를 캡처하는 데 적합하지 않습니다.30초 이상 평균하는 것이 가장 좋습니다.이 경우 버스트를 식별하기 위해 분석되는 SPAN(Switched Port Analyzer)으로 이그레스 트래픽을 캡처하기 위해 Wireshark를 사용할 수 있습니다.

문제 해결 방법론

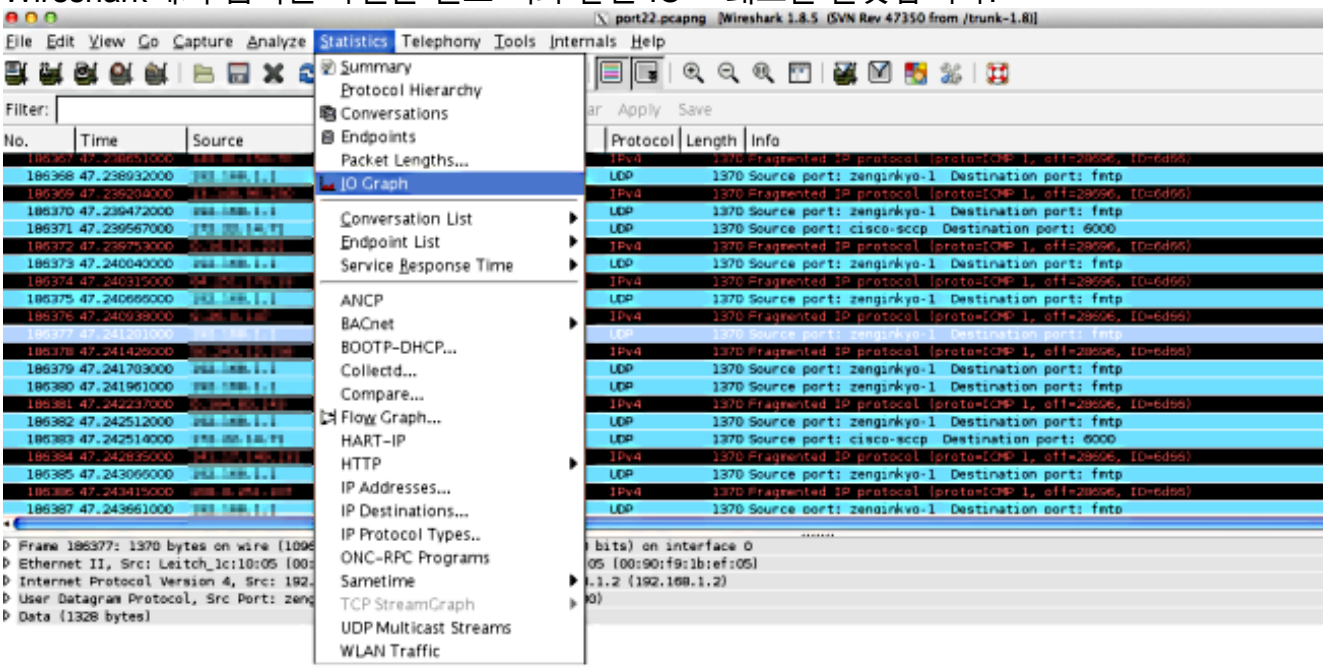
1. 증분 출력 드랍이 있는 인터페이스를 식별합니다.예를 들어, 100Mb 링크의 출력이 떨어지고 링크의 평균 사용률은 55Mb에 불과합니다.다음은 명령의 출력입니다.

```
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
```

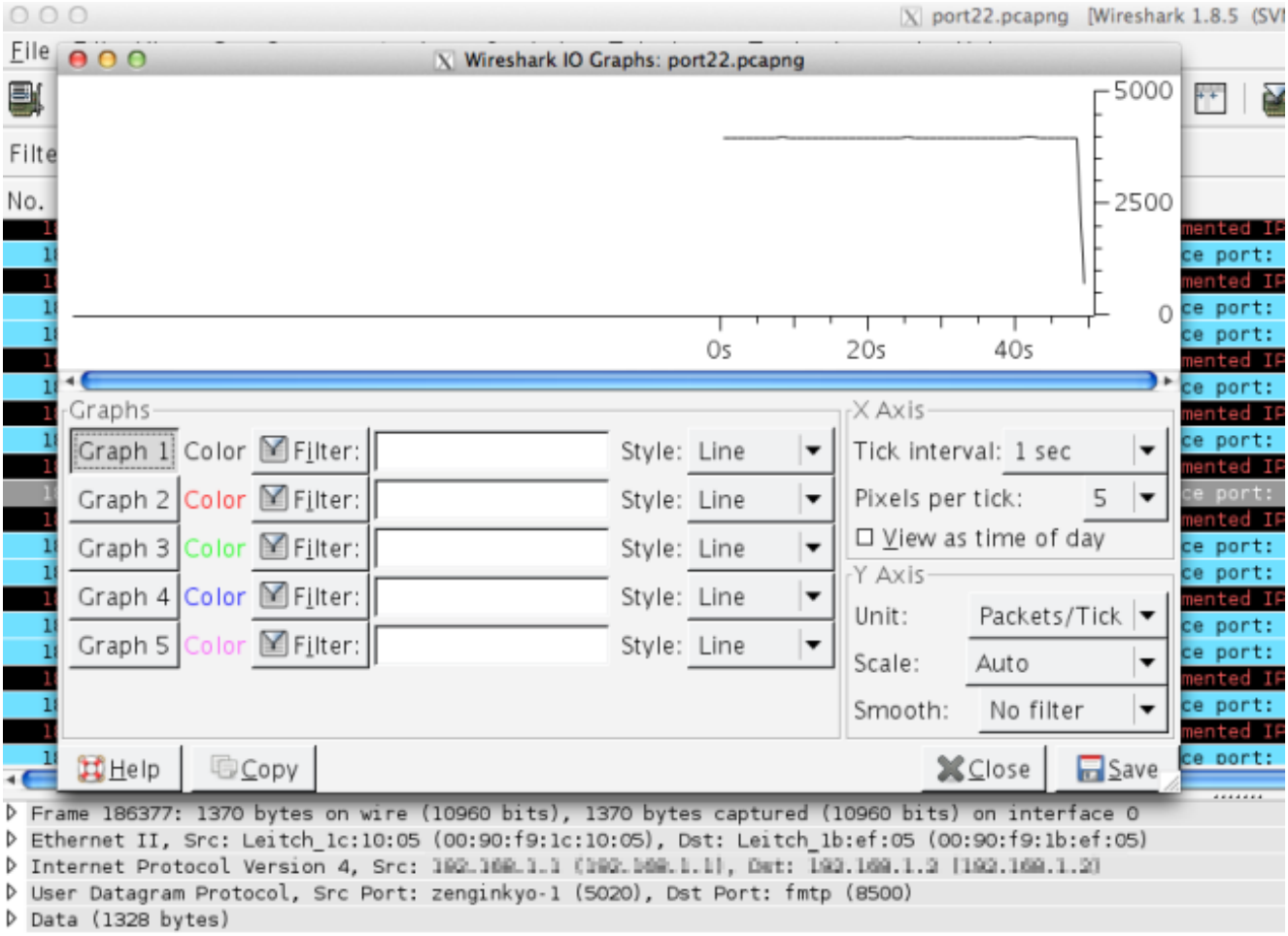
2. TX(Transmitted) 트래픽을 캡처하기 위해 스위치에서 SPAN을 구성합니다.이 트래픽을 캡처하려면 Wireshark를 실행하는 PC를 연결하고 SPAN 대상 포트에서 패킷을 캡처합니다.

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

3. Wireshark에서 캡처된 파일을 열고 이와 같은 IO 그래프를 플롯합니다.



4. 기본 규모에서는 버스트 트래픽이 없는 것으로 나타납니다.그러나 버퍼링 및 패킷 스위칭이 발생하는 속도를 고려할 때 1초는 매우 큰 간격입니다.1초 이내에 100Mb/s 링크는 인터페이스 전체에서 100Mb의 트래픽을 깔끔하게 형성하며, 최소한의 경우 패킷을 버퍼링할 필요가 있습니다.



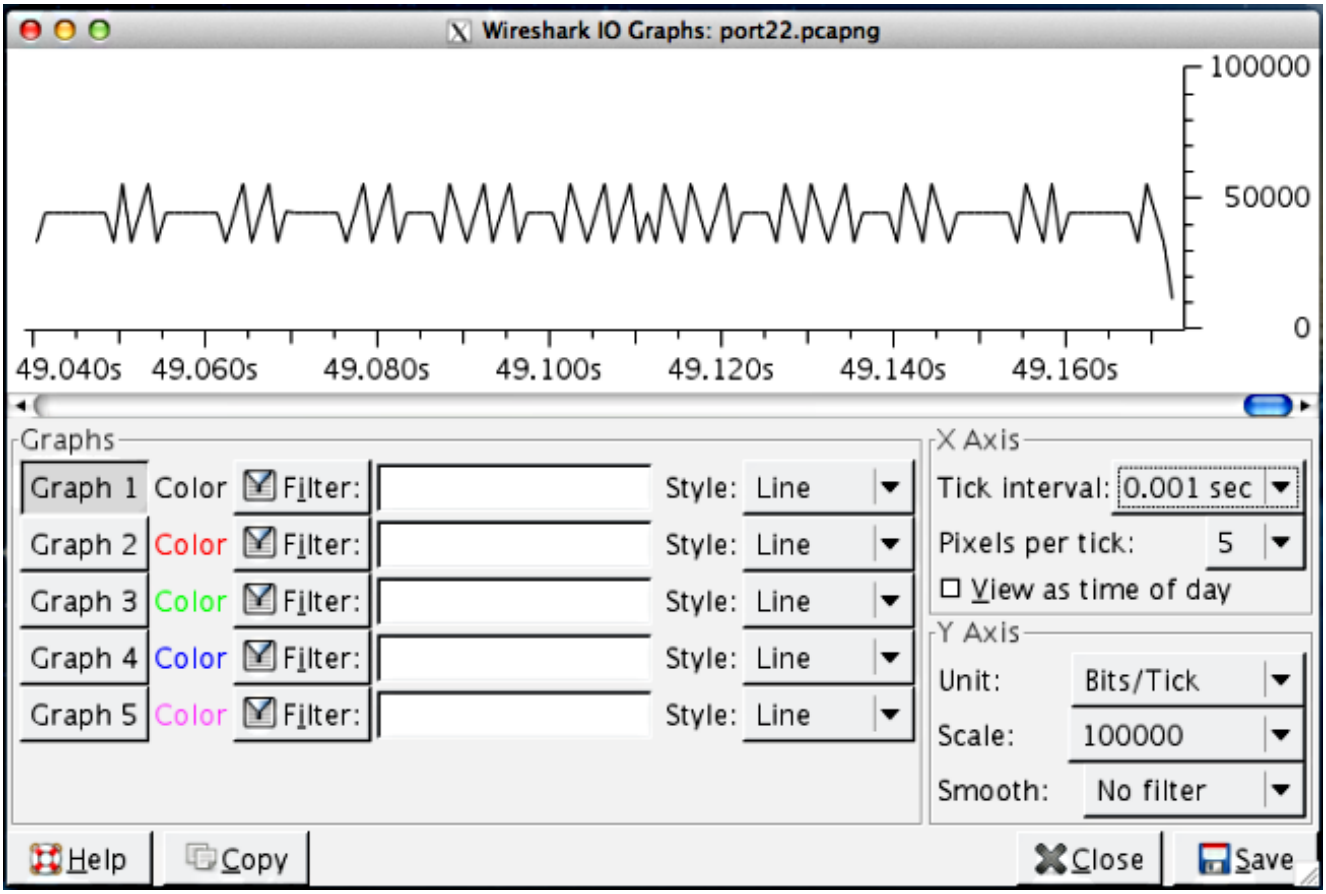
그러나 이 트래픽의 주요 부분이 몇 초 내에 인터페이스를 종료하려고 시도하면, 버퍼가 가득 차면 스위치에서 패킷을 광범위하게 버퍼링하고 삭제해야 합니다.를 더 세부적으로 확장하면 실제 트래픽 프로필에 대한 더 정확한 그림이 표시됩니다.인터페이스는 출력 속도를 비트/초 단위로 표시하므로 **Y**축을 비트/틱으로 변경합니다.

링크 속도는 100Mb/s입니다.

= 100,000,000비트/초

= 100,000비트/0.001s

X 및 **Y** 축의 배율을 다시 계산합니다.눈금 간격을 **X Axis=0.001초로** 변경하고, **Y축=00,000(비트/눈금)**으로 **변경합니다**.



5. 버스트를 식별하기 위해 그래프를 스크롤합니다.이 예에서는 0.001초 스케일에서 100,000비트를 초과하는 트래픽의 버스트가 있음을 확인할 수 있습니다.이렇게 하면 트래픽이 초 단위 이하의 속도로 버스트되고 이러한 버스트를 수용할 수 있도록 버퍼가 가득 차면 스위치에서 삭제될 것으로 예상됩니다.
6. Wireshark 캡처에서 해당 패킷을 보려면 그래프의 트래픽 스파이크를 클릭합니다.캡처 분석은 버스트를 구성하는 트래픽을 검색하는 유용한 방법입니다.