Wireshark gebruik om stormachtig verkeer op Catalyst Switches te identificeren

Inhoud

Inleiding

Dit document beschrijft hoe u burst verkeer op de poorten van Cisco Catalyst switches kunt identificeren.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de Cisco Catalyst Switch Series.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de potentiële impact van om het even welke opdracht begrijpt alvorens de opdracht uit te voeren.

Achtergrondinformatie

Traffic bursts kunnen uitvoerdruppels veroorzaken, zelfs wanneer de interface-uitvoersnelheid aanzienlijk lager is dan de maximale interfacecapaciteit. Standaard zijn de uitvoersnelheden in de opdracht van de **showinterface** gemiddeld over vijf minuten, wat niet geschikt is om kortstondige barsten op te vangen. Het is het beste om deze over een periode van 30 seconden te gemiddelde. In dit geval kunt u Wireshark gebruiken om bovengemiddeld verkeer met de Switched Port Analyzer (SPAN) vast te leggen, die wordt geanalyseerd om de uitbarstingen te identificeren.

Methode voor probleemoplossing

1. Identificeer een interface die stijgende output druppels heeft. U ziet bijvoorbeeld dat uitvoer

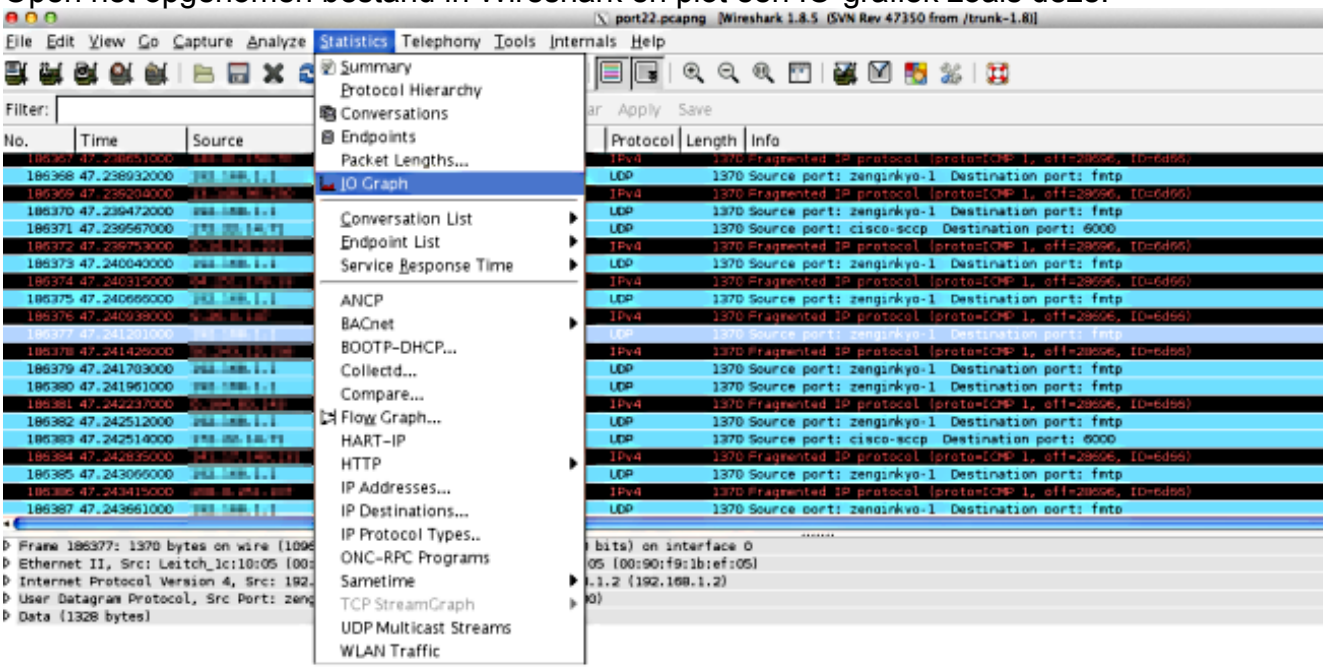
zakt op een 100MB-link terwijl het gemiddelde gebruik van de link slechts 55Mb is. Dit is de uitvoer van de opdracht:

```
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
```

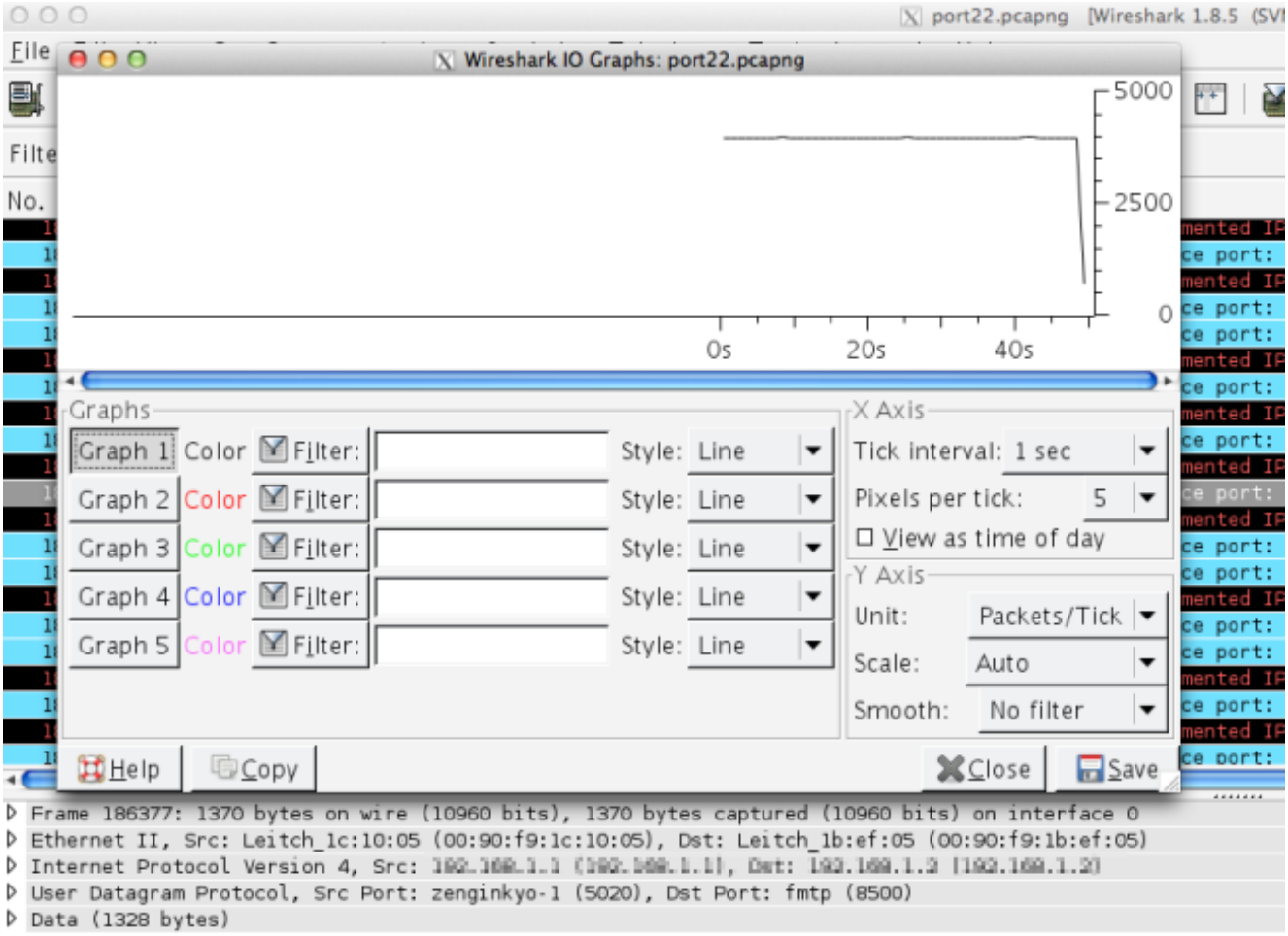
2. Configureer de SPAN in de switch om het overgedragen (TX) verkeer op te nemen. Om dit verkeer op te nemen sluit u een PC aan die Wireless-shark draait en pakketten opneemt in de SPAN bestemmingshaven.

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

3. Open het opgenomen bestand in Wireshark en plot een IO-grafiek zoals deze.



4. Op de standaardschaal lijkt er geen last van het verkeer te zijn. Echter, één seconde is een zeer groot interval wanneer je nadenkt over de snelheid waarmee het bufferen en pakketswitching plaatsvinden. In een periode van één seconde kan een link van 100 Mb/s 100 Mb van verkeer over de interface in een pasvormig profiel combineren met een minimum behoefte om een pakje te bufferen.



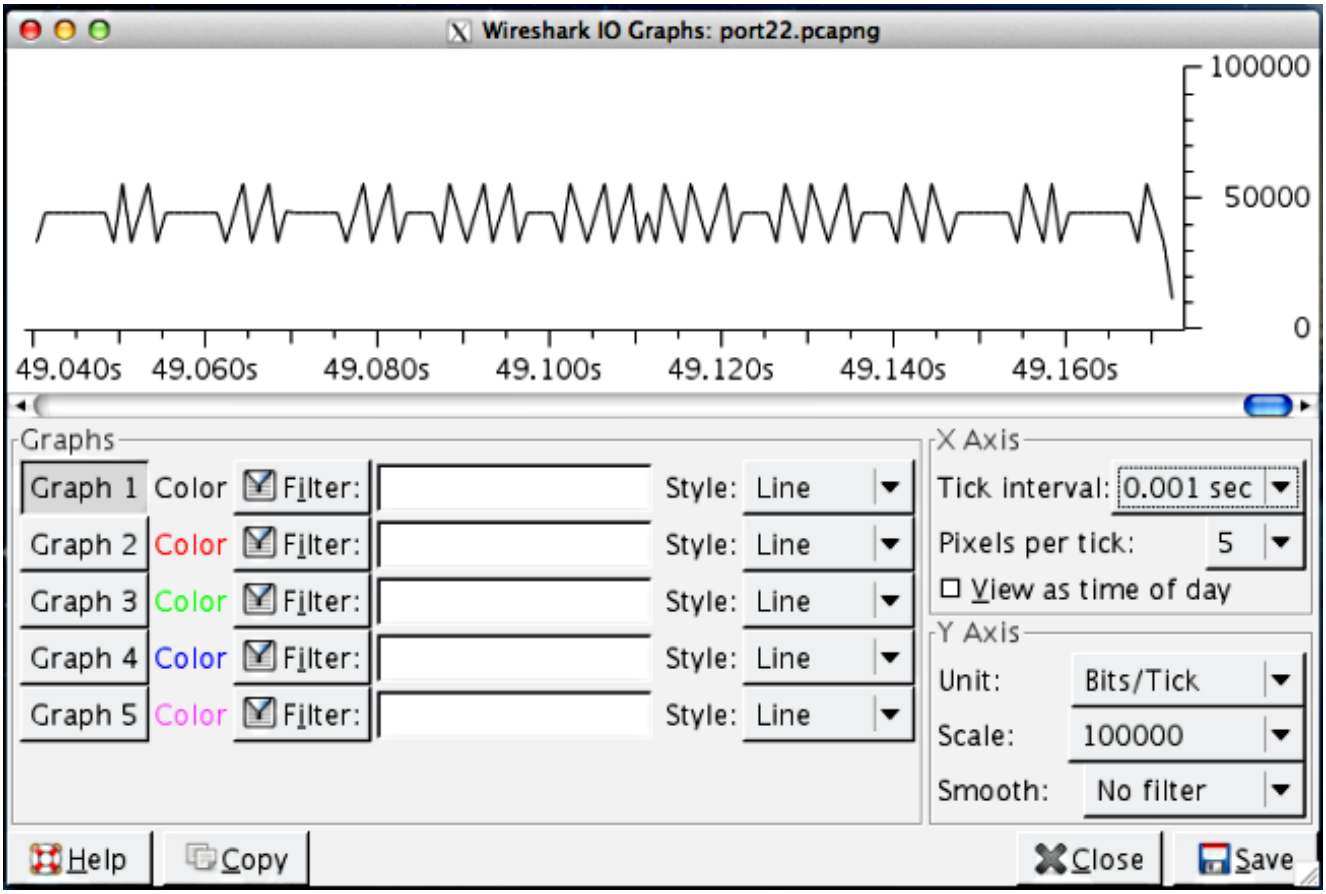
Als echter een groot deel van dit verkeer de interface in een fractie van een seconde probeert te verlaten, moet de switch pakketten uitgebreid bufferen en laten vallen als de buffers vol zijn. Als je de schaal korter maakt, zie je een nauwkeuriger beeld van het echte verkeersprofiel. Verander de **Y**-as in bits/tick omdat interfaces uitvoersnelheden in bits/sec tonen.

Link-snelheid is 100 MB/s

= 100.000.000 bits/s

= 100.000 bits/0,001 s

Bereken de schalen op de **X**-en **Y**-assen opnieuw. Verander het aanvinkinterval in **X Axis=0,001 sec** en de schaal in **Y as=00,000 (bits/aanvinken)**.



5. Scrolt door de grafiek om bursten te identificeren. In dit voorbeeld, kun je zien dat er een uitbarsting van verkeer is die 100.000 bits op een tweede schaal van 0.001 overtrof. Dit bevestigt dat het verkeer op het subtweede niveau zwaar is en naar verwachting door de switch zal vallen als de buffers vol zijn om deze uitbarstingen op te vangen.
6. Klik op de verkeersplein in de grafiek om dat pakket in de WirelessShark-opname te bekijken. De vangsanalyse is een bruikbare manier om te ontdekken wat het verkeer vormt.