Wireshark zur Identifizierung von Burst-Datenverkehr auf Catalyst-Switches

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Burst-Datenverkehr auf den Switch-Ports der Cisco Catalyst Switches identifiziert werden kann.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco Catalyst Switch-Serie.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, vergewissern Sie sich, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie den Befehl ausführen.

Hintergrundinformationen

Datenverkehrsspitzen können zu Ausgabeverwerfungen führen, selbst wenn die Schnittstellenausgangsrate deutlich unter der maximalen Schnittstellenkapazität liegt. Standardmäßig werden die Ausgaberaten im Befehl **show interface** über fünf Minuten gemittelt, was nicht ausreicht, um kurzlebige Spitzen zu erfassen. Es ist am besten, sie über einen Zeitraum von 30 Sekunden zu durchschnittlich. In diesem Fall können Sie Wireshark verwenden, um Ausgangs-Datenverkehr mit dem Switched Port Analyzer (SPAN) zu erfassen, der analysiert wird, um die Bursts zu identifizieren.

Fehlerbehebungsmethode

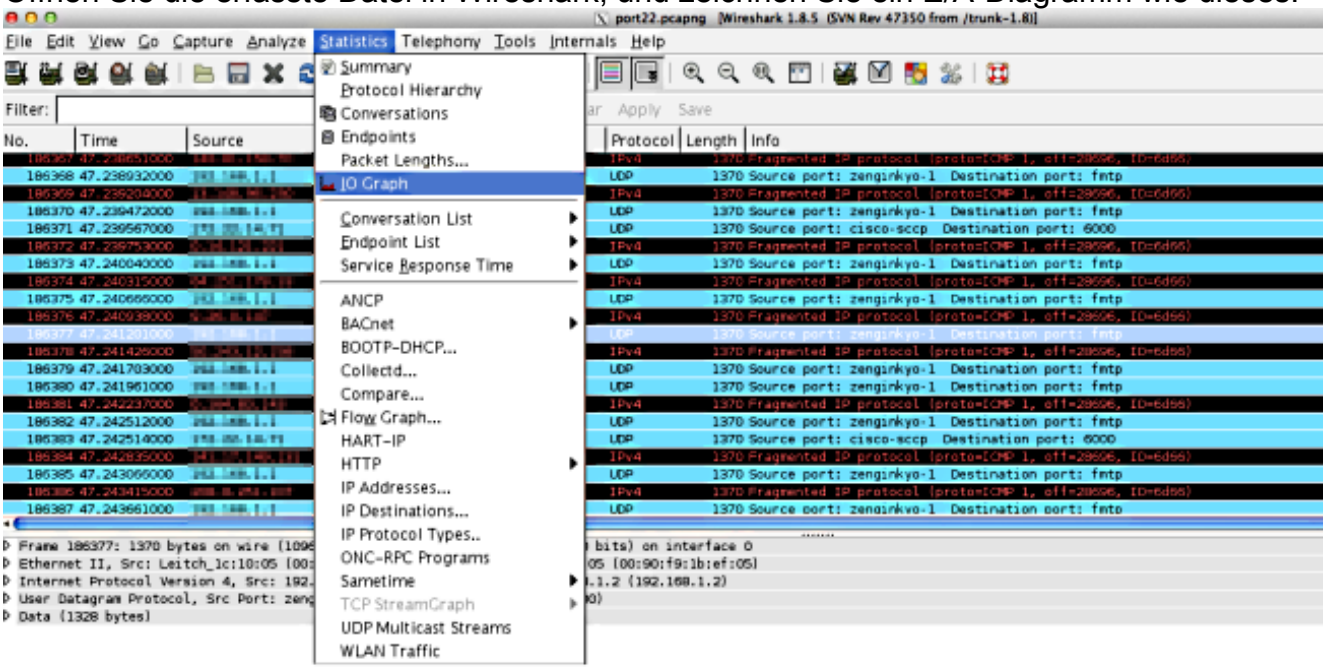
1. Identifizieren Sie eine Schnittstelle, deren Ausgabe inkrementell verworfen wird. Beispielsweise fällt die Ausgabe auf eine 100-Mbit-Verbindung ab, während die durchschnittliche Nutzung der Verbindung nur 55 Mbit/s beträgt. Hier ist die Ausgabe des Befehls:

```
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
```

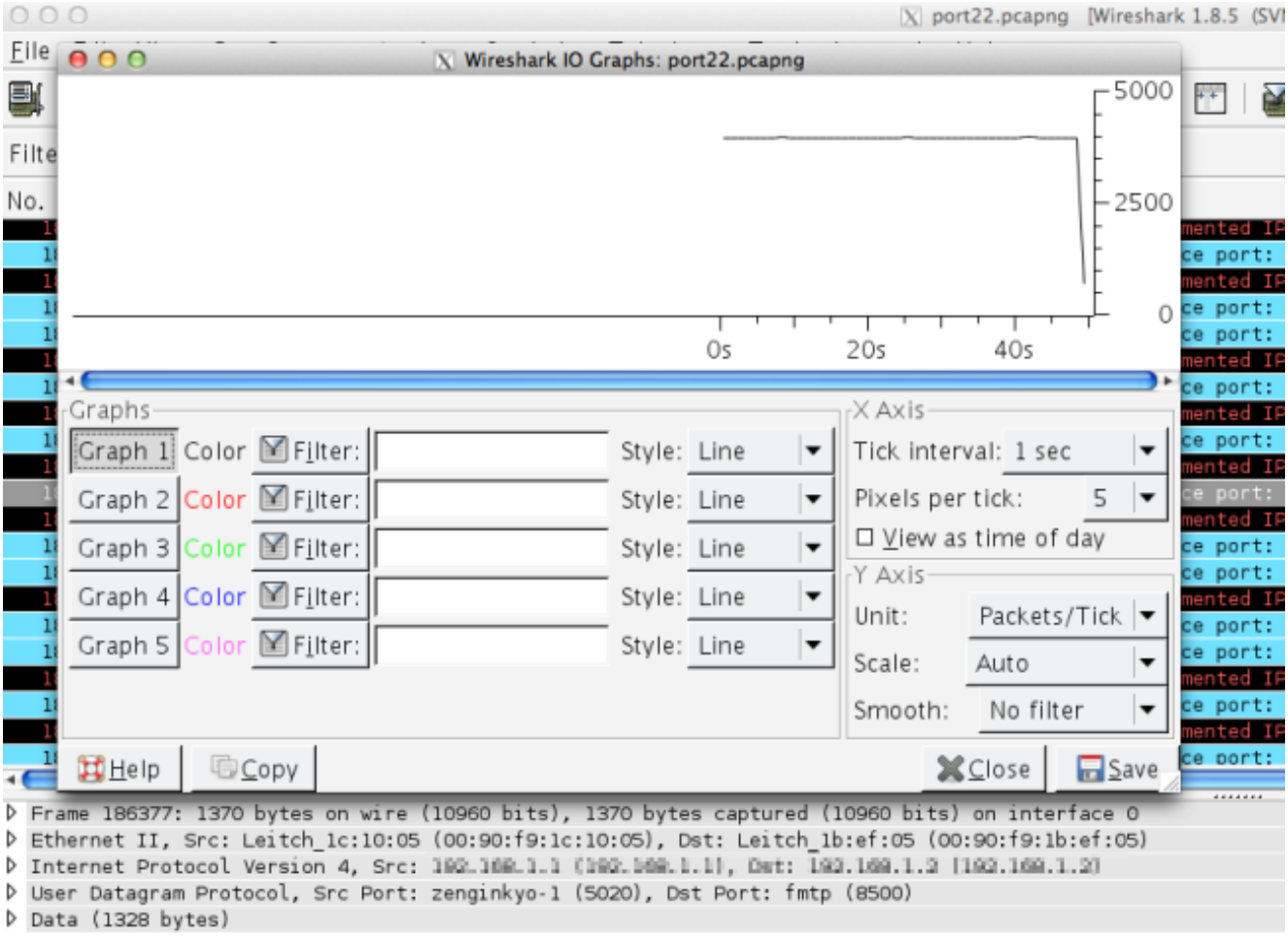
2. Konfigurieren Sie SPAN auf dem Switch, um den übertragenen (TX-)Datenverkehr zu erfassen. Um diesen Datenverkehr zu erfassen, schließen Sie einen PC an, der Wireshark ausführt und Pakete am SPAN-Zielport erfasst.

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

3. Öffnen Sie die erfasste Datei in Wireshark, und zeichnen Sie ein E/A-Diagramm wie dieses.



4. Bei der Standardskala scheint kein Datenverkehr durch Bursts zu bestehen. Eine Sekunde ist jedoch ein sehr großes Intervall, wenn man die Geschwindigkeit berücksichtigt, mit der Pufferung und Paket-Switching stattfinden. Innerhalb einer Sekunde kann eine 100-Mbit/s-Verbindung 100 Mbit/s Datenverkehr über die Schnittstelle in einem fein geformten Profil aufnehmen, wobei mindestens ein Paket gepuffert werden muss.



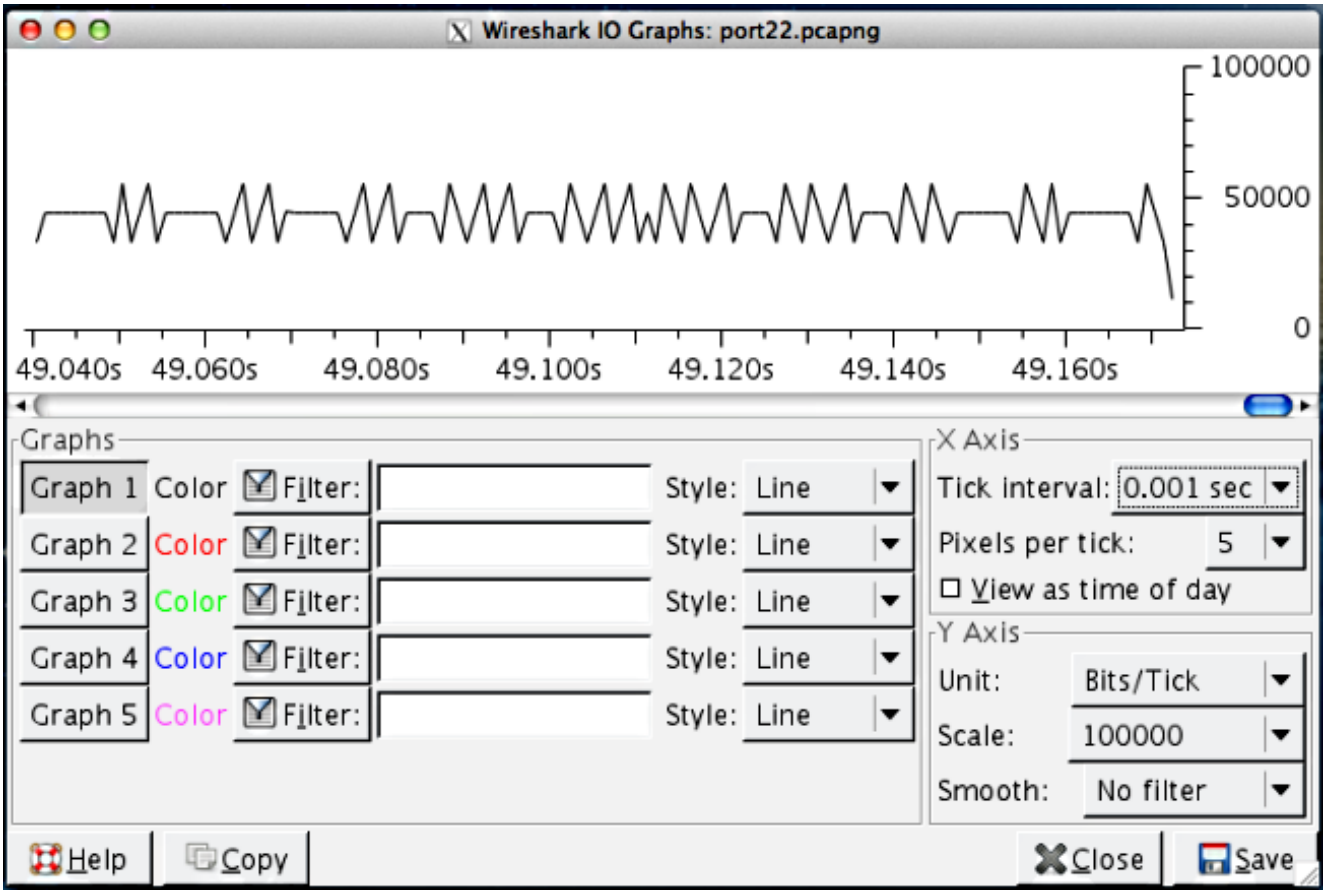
Wenn jedoch ein Großteil dieses Datenverkehrs versucht, die Schnittstelle innerhalb einer Bruchteile von Sekunden zu verlassen, muss der Switch Pakete umfassend puffern und verwerfen, wenn die Puffer voll sind. Wenn Sie die Skalierung detaillierter gestalten, erhalten Sie ein genaueres Bild des tatsächlichen Datenverkehrsprofils. Ändern Sie die **Y**-Achse in Bit/Tick, da Schnittstellen die Ausgaberaten in Bit/Sek. anzeigen.

Verbindungsgeschwindigkeit beträgt 100 Mbit/s

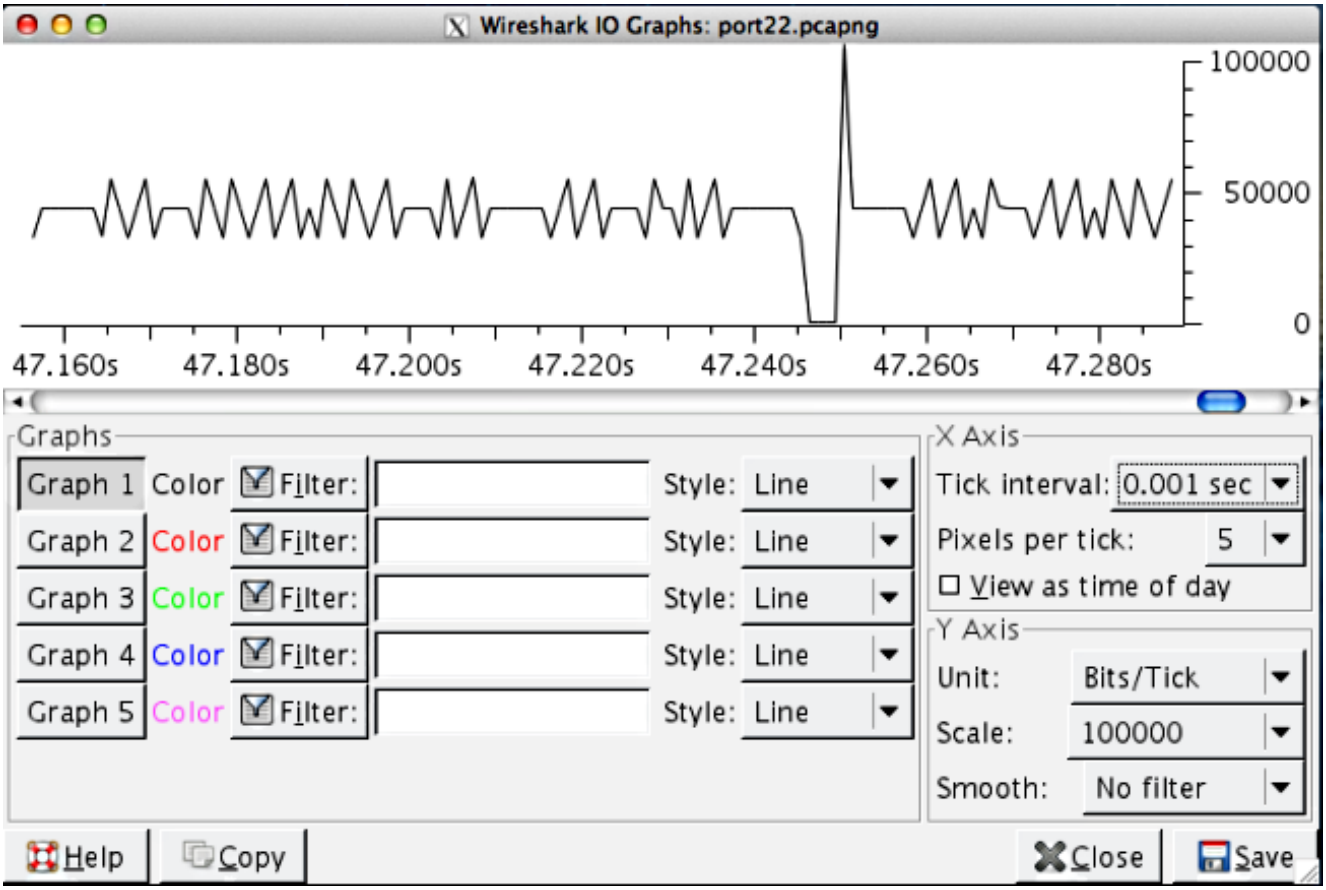
= 100.000.000 Bit/s

= 100.000 Bit/0,001 s

Die Skalierung der **X-** und **Y-**Achsen neu berechnen. Ändern Sie das Tick-Intervall auf **X Axis=0,001 sec** und die Skalierung auf **Y-Achse=00,000 (bits/tick)**.



5. Scrollen Sie durch das Diagramm, um Spitzen zu identifizieren. In diesem Beispiel sehen Sie, dass es eine Datenverkehrsexplosion von mehr als 100.000 Bit auf einer Skala von 0,001 Sekunden gibt. Dies bestätigt, dass der Datenverkehr auf der Ebene von unter einer Sekunde explodiert und vom Switch voraussichtlich verworfen wird, wenn die Puffer voll sind, um diese Spitzen zu bewältigen.
6. Klicken Sie auf den Datenverkehrsspitzen im Diagramm, um dieses Paket in der Wireshark-Erfassung anzuzeigen. Die Erfassungsanalyse ist eine nützliche Methode, um zu ermitteln, welcher Datenverkehr den Burst ausmacht.


Wireshark IO Graphs: port22.pcapng
100000
50000
0
47.160s
47.180s
47.200s
47.220s
47.240s
47.260s
47.280s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: Style: Line
Graph 3 Color Filter: Style: Line
Graph 4 Color Filter: Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 0.001 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Bits/Tick
Scale: 100000
Smooth: No filter
Help
Copy
Close
Save