SHARKFEST '12

Wireshark Developer and User Conference

Hansang Bae
A-1: Deep Dive Packet Analysis

Director, Citi (f.k.a Citigroup)

hansang@gmail.com

This session came about due to feedback from 2011

Trace file (deepdive.zip)

https://www.box.com/s/24c25c3109ec54777c2e

A-1: Deep Dive Packet Analysis

- Develop a methodical system!
  - Review all the trace files the same way
  - Over time, you'll train your brain to pick up patterns
  - My favorite technique?
    - Use relative sequence numbers
    - Must add a delta column
    - Use "tcp.analysis.flags"
    - Add Cumulative Bytes, and use Time Reference markers
    - Use multiple profiles to convenience (real/relative seq, etc.)
    - Always sort by delta column

A-1: Deep Dive Packet Analysis

- Packet loss is a fact of life!
  - Where there's packet loss, there is slow ……?
    - Easy to spot because it happens after…..?
    - But what is the catch?
    - Look at packet 12776 for a classic example

A-1: Deep Dive Packet Analysis

- Not all retransmissions are the same
  - What causes retransmissions vs. fast retransmissions?
  - In a modern TCP stack, why would you encounter “normal” retransmission?
    - Analogy: Sergeant York and any Western/Indian movie
  - What recourse do you have?
    - Knowing what we know, what are our options to mitigate this behavior?

A-1: Deep Dive Packet Analysis

- Not all delays are the same.
  - When you can find author’s mistake, you really know your stuff.
  - Become familiar with TCP stack behavior and you can spot odd behaviors quickly.
    - Use deductive reasoning to nail down what may be wrong
  - What recourse do you have?
    - Knowing what we know, what are our options to mitigate this behavior?

A-1: Deep Dive Packet Analysis

- Mystery deepens!
  - Sometimes the performance was fine for day or more.
  - Suddenly, performance dropped off considerably.
  - How can you nail it down?
    - Try to recreate the problem.
    - Must have continuous capture so you can surgically zoom in when the problem occurs
    - Use all tricks at your disposal
    - Having a network background can *really* help you (what happens on the switch side when the server reboots?)
  - In the end, the problems were identified as….(next page)

A-1: Deep Dive Packet Analysis

- By using Shark appliance and Pilot, we were able to zoom in when performance suffered.
- When we tested using READ and WRITE scripts, performance was better. Why was that?
- We found that when Window Scaling is used, the mystery delays happened.
- We turned off the QoS features to make packet loss more randome
- We filed a bug with the vendor to fix the stack