Case Study: Wireshark in the Large Enterprise

June 15th, 2011

Hansang Bae
Senior VP| Citi (f.k.a. Citigroup)
hansang@gmail.com

(Which format should I use? Hit-n-run or more in depth?)

SHARKFEST **'11**
Stanford University
June 13-16, 2011

Case Study: Wireshark in the Large Enterprise

June 15th, 2011

The video/audio recording made during the session will be made available on YouTube and www.lovemytool.com by the end of June.

On Youtube, just search for "hansangb wireshark"

Also, as I mentioned during the presentation, please provide me with some feedback about what level of detail these presentations should be. Should there be more hit-n-run/quick analysis sessions or should I present less number of cases with in depth analysis? Thank you!

Internet is slow…now what?

- Problem: User complains that "Internet is not working".
- Toughest part is getting an accurate description of the problem.
  - In this case, the user reported that the web site "just locked up around 11:15 or so.."
  - Sometimes you have to work with half a capture. But based on what you know, you can "devine" the information that you need.

- You have to understand how other technologies work and be able to tie it all together.
- What is the purpose of the proxy? And how does it work with DNS queries?

Application is timing out?

- Problem: Application throughput is not very good.
- If you have the luxury, capture with a liberal filter.

- Use the application logging to pinpoint the time of the problem.
- Talk to the developers to see how the application is supposed to work.
- What would cause the server to RST the connection?
- Application log showed an error at 17:31hrs.
- It's always easy once you know what to look for!

NFS is slow!

- Problem: NFS is slow….(expected behavior?)
- What are the usual suspects?
- Does TCP Window come into play for NFS v3 over TCP?
- FACT:
  - MSS is 1448 (why isn't it 1460?)
  - TCP Offload engine is using 10 X MSS = 14,480
  - NFS Server's receive window size is 26,280
- Do we have a problem? What is the throughput, can we calculate it?
- We don't even have to have a packet trace to realize we have a problem!

Citrix users are locking up!

- Problem: Overseas Citrix users are experiencing session lock ups and disconnects.
- There is an external carrier involved. Usual suspect?
- Is it just routine packet loss?
- Let's examine the evidence…

- Sometimes, you have to work with one way view of TCP. You'd be surprised how much information you can "devine" from a one way packet capture.
- Sometimes, you have to look at the IP layer to ferret out the answer.

TCP and Real-time doesn't mix!

- Problem: A trading application log shows there are delays that cannot be accounted for.
- Rule out the usual suspects.
- Could it be the network? Let's examine the evidence…
- Lessons Learned:
  - In general TCP is not great at handling real-time requirements.
  - Recovery from packet loss may not be worth the efforts.
  - Some applications suffer horribly from packet loss.

TCP and Real-time doesn't mix!

- Fruits of our labor…after some angina!!