SHARKFEST '13

Wireshark Developer and User Conference

Capture Limitations of a Laptop

Chris Greer – Network Analyst
Packet Pioneer

Presenter

- Chris Greer
  - Packet Pioneer LLC (2010)
  - Focused on Network and Application Performance Analysis
  - Pre-deployment Network Assessments
  - Deliver training on Wireshark, Fluke Networks, other vendors.

Agenda

- Why do I care?
- At what point does the laptop start dropping traffic?
- How can I tell in a trace file?
- Optimizing Wireshark
- Considering a hardware based capture device
- Laptop shootout
- Lab 1: Laptop shootout – default settings of Wireshark
- Lab 2: dumpcap or tshark results
- Lab 3: Optimized Wireshark capture

Why do I care?

- When analyzing complex problems, every packet counts

Why do I care?

Wireshark Downloads

- Estimated at 500,000 per month – Wireshark Network Analysis Study Guide
- How many of these downloads are to laptops?
- How many of these users leave the optimization settings at the default rate?

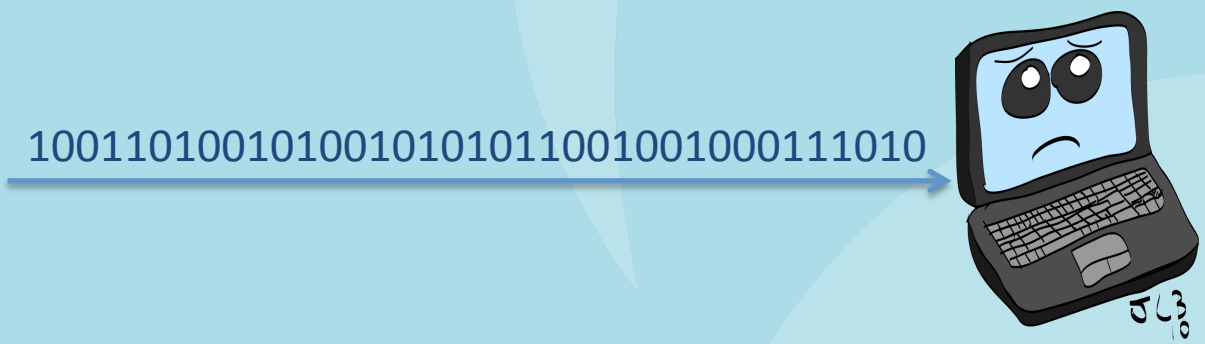
- Very likely – MOST!

Laptops have a purpose

- Email, Web, Work Applications, Music Players, etc…
- Make their owners mostly happy
- Network Analysis is not the purpose of most laptops

Is 1Gig really capturing at 1Gig?

- A laptop likely has a 1Gig interface. Does that mean that it can capture traffic at that rate?
- Most of us agree – no.
- So, when does it start dropping packets?
- At what utilization point do we really need to consider a hardware-based appliance?



Lab 1 – Capture limitation on default settings

Aggregation Switch

This is not emulated traffic – it is an easily configurable packet generator.

How about command line?

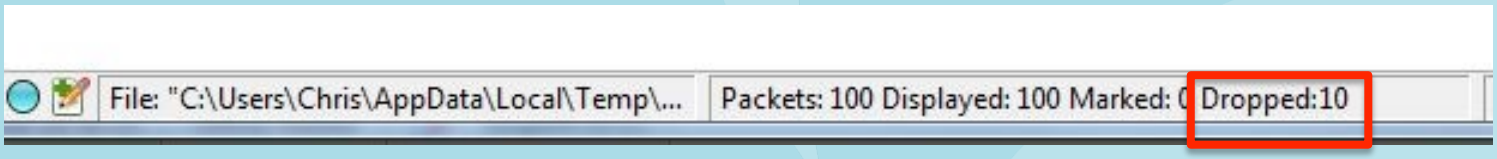
- Tshark, dumpcap? Similar result?
- Lab 2 – Capturing with dumpcap

What do dropped packets look like?

- Expert Info:
  - Previous Segment Lost
  - ACKed Lost Packet
  - Out of Order

102	○	0.705892	192.168.1.2	192.168.1.1	TCP	170	msg-icp > 65469 [PSH, ACK] Seq=2601 Ack=2133 Win=8256 Len=104 TSval=17356922 TSecr=16586
103	○	0.705892	192.168.1.1	192.168.1.2	TCP	66	65469 > msg-icp [ACK] Seq=2133 Ack=2705 Win=17416 Len=0 TSval=16586 TSecr=17356921
104	○	0.705892	192.168.1.2	192.168.1.1	TCP	170	msg-auth > 65523 [PSH, ACK] Seq=2601 Ack=2133 Win=8256 Len=104 TSval=17356923 TSecr=343424
105	○	0.775881	192.168.1.1	192.168.1.2	TCP	230	[TCP ACKed unseen segment] [TCP Previous segment not captured] 65523 > msg-auth [PSH, ACK]
106	▪	0.776881	192.168.1.1	192.168.1.2	TCP	230	[TCP ACKed unseen segment] [TCP Previous segment not captured] 65469 > msg-icp [PSH, ACK] S

- Dropped Counter



Optimizing Wireshark

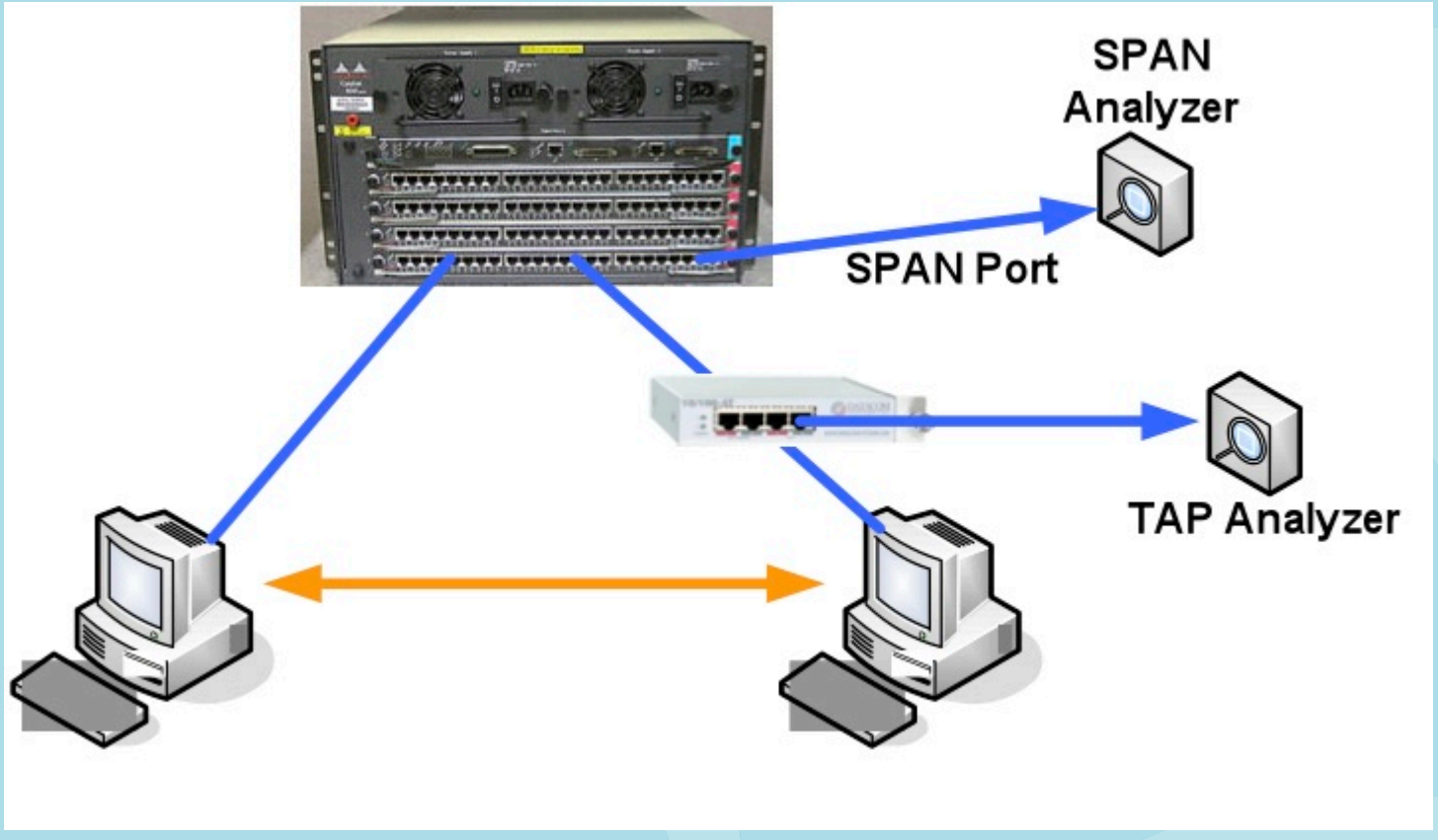
- Don't use *Update list of packets in real time* in the capture options dialog, to remove system load
- Increase the *Buffer size* in the capture options dialog (set it to a reasonable value e.g. 10MB, depending on your systems memory size)
- Don't use *capture filters*

Lab 3: Capturing with Optimized Wireshark

This doesn’t only affect laptops

- Capture methods are affected too.
- A SPAN or Mirror port can be overprovisioned
- Especially when spanning a full VLAN or several gigabit ports at one time

SPAN/Mirror Example



SPAN vs. Tap Results

- Tap Capture Results
- Packets captured: 133,126
  Delta Time at TCP Setup: 243uSec
- SPAN Capture Results
- Packets captured: 125,221
  Delta time of TCP connection setup: 221 uSec

Hardware Based Capture

- Designed to capture at full line rate up to 10Gbps
- Stream to disk with no gaps or drops

- TurboCap NIC from Riverbed

- Cascade Appliance from Riverbed

Questions?

- Thanks for Attending!