Real World Case Studies

Solving Real Problems for Real People

#sf24us

Kary Rogers

Sr Director, Services Excellence @ Zscaler

#sf24us

Download pcaps: packetbomb.com/sf24us

Packet A-Team?

SharkFest'24 US
June 15-20 · Fairfax, VA

#sf24us

Real world problems from real Internet strangers

Slow Tput for First 6.5 Seconds

#sf24us

- Post on /r/networking
- Rack of 7 Dell PowerEdge servers
- 1Gbps TOR switch
- Low throughput
- Initial delay of 6.5 seconds
- Troubleshooting for over a month
- Where‘s the pcap?

6.5 Second Delay Take Aways

#sf24us

- Learn the basics of packet analysis
- Add TCP seq numbers to columns
- Have a delta column
- Set a Time reference
- Learn TCP/IP basics
  - PMTUD
  - MTU probing - /proc/sys/net/ipv4/tcp_mtu_probing

One-Way Performance Issue

#sf24us

- Transatlantic MPLS
- ~100ms
- 100Mbps bandwidth
- Wget test
- 100Mbps in one direction
- 20 to 40Mbps in the other
- Why god why?

One-Way Perf Take Aways

#sf24us

- Wireshark setup
- iRTT to determine client or server side
- Tcptrace stream graph is your friend
- Analyze from the perspective of client or server
- Know what you should see (fast retransmission)
- Play with config settings e.g. relative sequence numbers

Slow Web Page Load

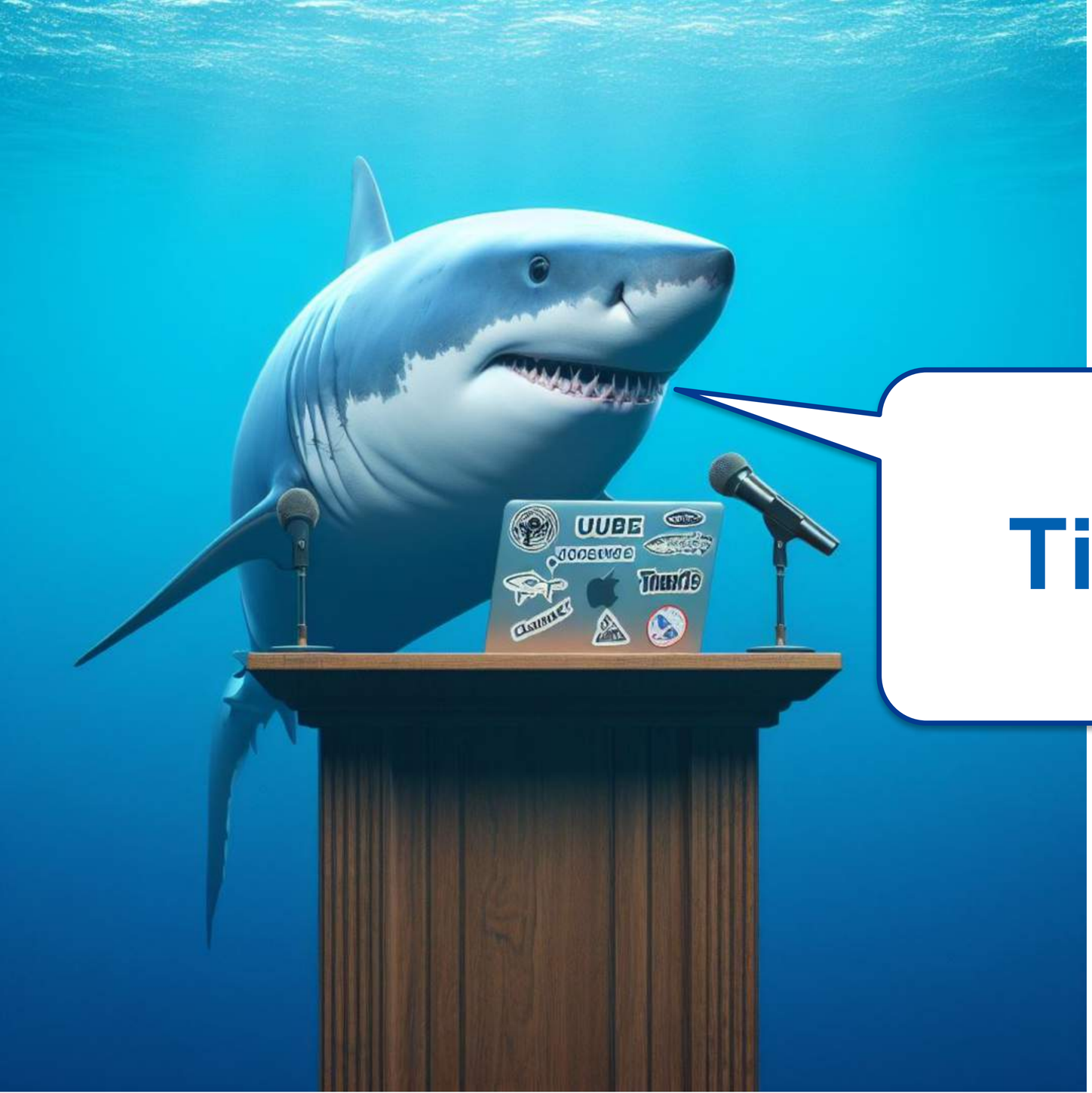
#sf24us

- Users experiencing very slow load times
- All external sites
- Checked DNS
- Asked for simple test case

Slow Web Page Load Take Aways

#sf24us

- Start with Stats > Conversations
- Ask user for simple, specific test and only capture that
- Always check the iRTT
- TCP pref – Allow subdissectors to reassemble streams
- Add TCP conversation deltas for HTTP analysis
- Troubleshoot up the stack (don‘t forget about layer 2)
- When in doubt, Google



SharkFest'24 US
June 15-20 · Fairfax, VA

#sf24us

Time for Q & A