SharkFest '17 Europe

Solving Real Problems for Real People

Step-by-step case studies

8 november 2017

Kary Rogers

Director, Staff Engineering - Riverbed

Packet A-(nalysis) Team

Helping strangers on the Internet via packetbomb.com

PCAPS

http://packetbomb.com/sf17eu

Slow Tput for first 6.5 Sec

- Post on /r/networking
- Rack of 7 Dell PowerEdge servers
- 1Gbps TOR switch
- Low throughput
- Initial delay of 6.5sec
- Troubleshooting for over a month
- Show me the pcap

6.5 Sec Delay Takeaway

- Capture the 3way handshake
  - MSS tells you the MTU
  - Need wscale to calculate receive window
- Add TCP seq numbers to columns
- Big round numbers mean something- 200, 400, 800
- Set a time reference
- Learn TCP/IP basics
  - PMTUD
  - MTU probing - /proc/sys/net/ipv4/tcp_mtu_probing

Slow FTP Upload

- Replaced Fortigate firewall with new Checkpoint
- Video team complains of slow upload to London
- NetEng team doesn’t deal with many performance issues
- ~5Mbps now, was ~20Mbps
- To the pcaps!

Slow FTP Upload Takeway

- Always look at RTT
- Latency is a huge factor for some apps/protocols
- PSH bit can be an indicator of buffer size
- Bytes in flight should reach BDP

DC2DC Transfer Performance

- Poor TCP performance between two DCs in one direction
- Easily reproducible with FTP or iperf
- Problem doesn’t exist in the opposite direction

DC2DC Performance Takeaway

- Tcptrace stream graph is your friend
- Look at the angle of the line in the stream graph
- Changes in angle means something happened
- Do sequence number analysis
  - Go slow and be patient
  - Double and triple check
- Get captures from both ends

Contact

- Fill out the session survey!

- kary@packetbomb.com
- @packetbomb
- Packetbomb.com