SHARKFEST '13

Wireshark Developer and User Conference

PA-7 Troubleshooting from the field

Herbert Grabmayer

Technical Sales Consultant

PA-7 Troubleshooting from the field

- Introduction about me
- SMB in the unoptimized environment
- SMB in the optimized environment
- Customer reports that open a file is not so fast as copy the file

About me

- Around 5 Years IT Datacenter Operations and Help desk
- Around 15 Years network administration, network design, Troubleshooting different problems that are not seen in the network configuration, first contact with network analyzer (Sniffer, Network General)

About me

- Around 13 Years Network Analyst, working with different products to analyze and monitor performance problems. (change to Wireshark and Cacetech)
- Working as Technical Sales Consultant with Riverbed Performance Optimization Products
  - Steelhead (WAN Optimization)
  - Granite (Branch Office Consolidation)
  - Stingray (Application Delivery Controller)
  - Cascade (Performance Monitoring)

LAB Config

- Virtual Network in an ESX Environment
  - Fileserver
  - Datacenter Steelhead
  - WAN Emulator (WANEm)
  - Office Steelhead
  - Two PCs
  - WAN Simulation with 4 Mbit/s and 40 ms RTT

Unoptimized SMB

- what commands we see
- what errors we see
- what timing we see
- what bandwidth we see
- investigate a trace from the Client and Server Side with Wireshark and Pilot Console

Unoptimized SMB

- The client trace shows that SMB_READ_AND_X have the most transaction time.
- All the others reflect mainly the roundtrip time
- in this case we see no errors

optimized SMB technic behind

- Compression and deduplication on bit level
- TCP optimization
- Latency optimization with read ahead and write behind

optimized SMB File Copy

- what commands we see
- what errors we see
- what timing we see
- what bandwidth we see
- investigate a trace from the Client and Server Side with Wireshark and Pilot Console

optimized SMB File Copy

- The client trace shows that SMB_READ_AND_X have the much better transaction time.
- All the others reflect mainly the roundtrip time
- no errors
- Blocksize is mainly 64K
- bandwidth thats much more as the available 2 Mbit line

optimized SMB Open File

- Customer reports that the file is slower opened then copied.
- what commands we see
- what errors we see
- what timing we see
- what bandwidth we see
- investigate a trace from the Client with Wireshark and Pilot Console

optimized SMB Open File

- a lot of object path and name not found
  - that cannot be optimized
- a lot of reads with small block size
  - will be optimized as good as possible but with this blocksize we get also in the LAN slow troughput

How optimization works

- optimization is transparent
  - so cannot work as a proxy
  - for a example must ask each time a file is opened if it is there on the server
  - transport of the file can be optimized in volume and roundtrip time with different mechanism of the optimization vendor
  - best result can be reached when the application reads the file sequential.

optimized SMB Open File

- with this knowledge customer exported a project in a transfer directory.
- when he then opened the project it opens much faster
- when we investigate in the trace we se no more path not found or name not found in the trace.

WAN Optimization Configuration Problem

- How is the Optimization Device placed in the network
- Two Faces Device between Layer 2 and Layer 3
- Customer Reports that Application is sometimes slower with optimization enabled

WAN Optimization Configuration Problem

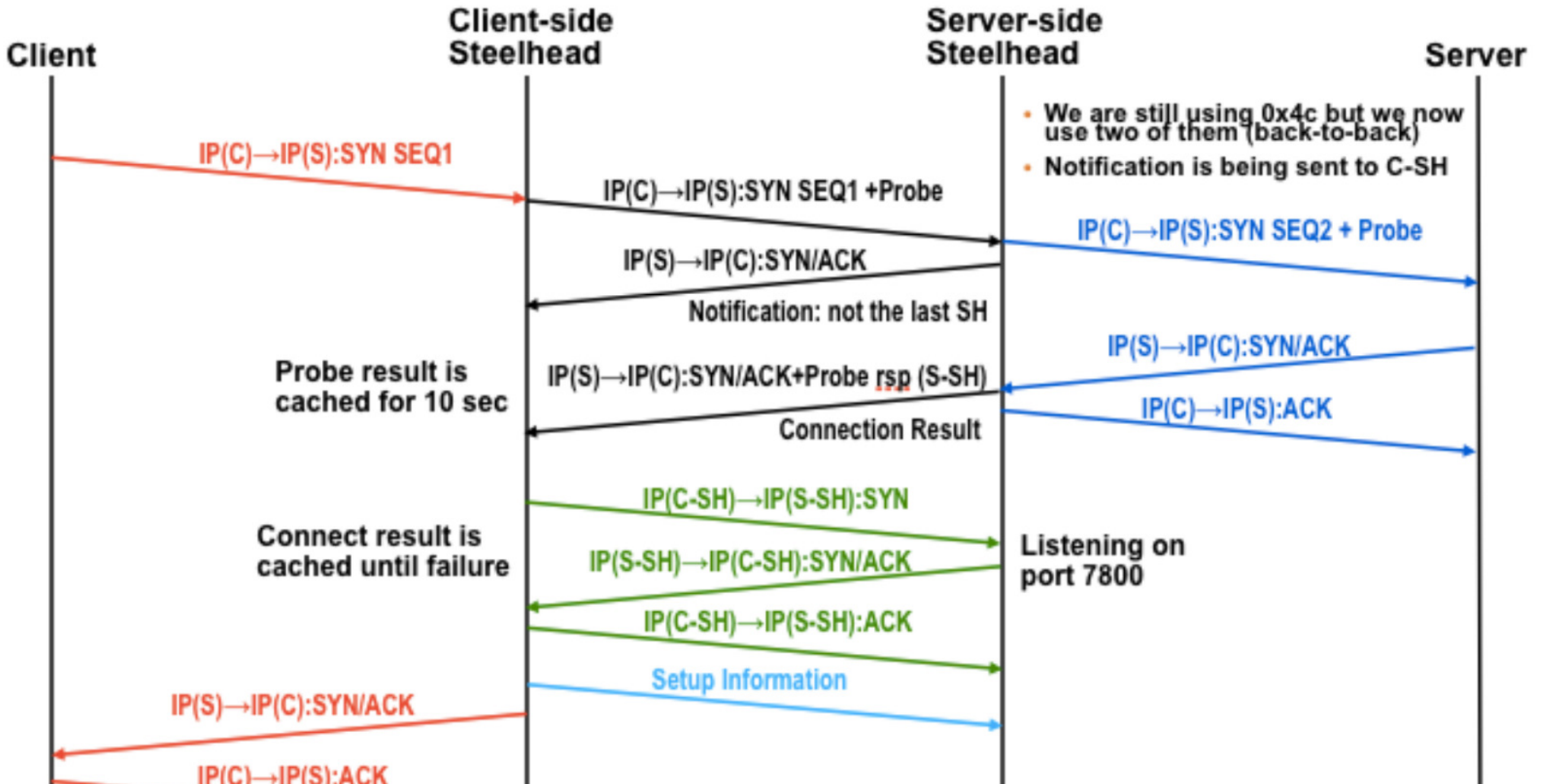
- Lets investigate the connections of the client
- There are a lot of different connections
- we had to investigate what sessions are part of the application
- Then I checked this connections with my knowledge of the tests before if optimization works

WAN Optimization Configuration Problem

- as i found no hints i go in a more general view of TCP behavior
- I found that sometimes the max. Roundtriptime was 9 seconds.
- Investigate with Wireshark whats going on.
- Investigate on Client LAN side
- Investigate on Client WAN side
- Investigate on Server WAN side

Session Setup Optimization by Riverbed

In-path Enhanced Auto-discovery First Connection Packet Flow



WAN Optimization Configuration Problem

- Customer reported a wrong subnet mask for the inpath interface
- because of this Serverside Steelhead does a ARP as he thinks the Server is on the same network.
- after the second SYN he knows that someone is going wrong and switch to bridge mode for this connection
- now the packet is no more inspected and will be bridged to the router
- Steelhead turns off optimization for a connection before

PA-7 Troubleshooting from the field

- Thank you
- h.grabmayer@arrowecs.at