May I analyze your network?

Planning and preparing packet captures.

Matthias Kaiser – ExperTeach GmbH
Germany

WhoamI

- Matthias Kaiser
- Senior Trainer and Consultant at ExperTeach GmbH in Germany
  - Wireshark Training on packet analysis and troubleshooting
  - Consulting Services for Packet Analysis
    - Mainly network analysis, application performance analysis and VoIP
- Formerly
  - Sniffer University Instructor at Network General / NAI
  - Freelancer with own network analysis courses
- WCA-101

Why I chose this topic

- Packet analysis skills are important
  - Know and handle key Wireshark functions and features
  - Learn about network protocols and related processes
  - Learn about troubleshooting methodology
  - Know TCP/IP inside out – especially TCP
- Next level
  - Differentiate between good and bad behavior
  - Learn about typical problems and how to identify them using Wireshark
    - Slow network, Long delays, High process times
    - Security issues
- BUT
  - **How can we get all the packets for the analysis?**

Packet Analysis requirements

- Having clear objectives
- Having a network map
- Capturing the right packet data
  - … at the right place
  - … at the right time
  - … for the desired applications
  - … and the selected users
- Capturing **ALL** packets
  - … nothing lost?
- Identifying the user traffic in the trace files
- And then start the analysis

Packet Capture AGENDA

- Planning is everything
- What are your goals, objectives, tasks?
- Organizational stuff
- Legal and financial stuff
- Getting on site
- Start your business

Objectives and problem description

Objectives

- Objectives can vary
  - **Troubleshooting**
  - Baselining
  - Second opinion – third opinion – playing the referee
  - Setting up analysis methodology and workflow at customer site
- Hidden agendas
  - What is the ambition of the point of contact hiring you?
  - Proving something or someone right or wrong?
- Do not get into any blame games!
- Do not judge people!
- Solve problems

First contact – to customer

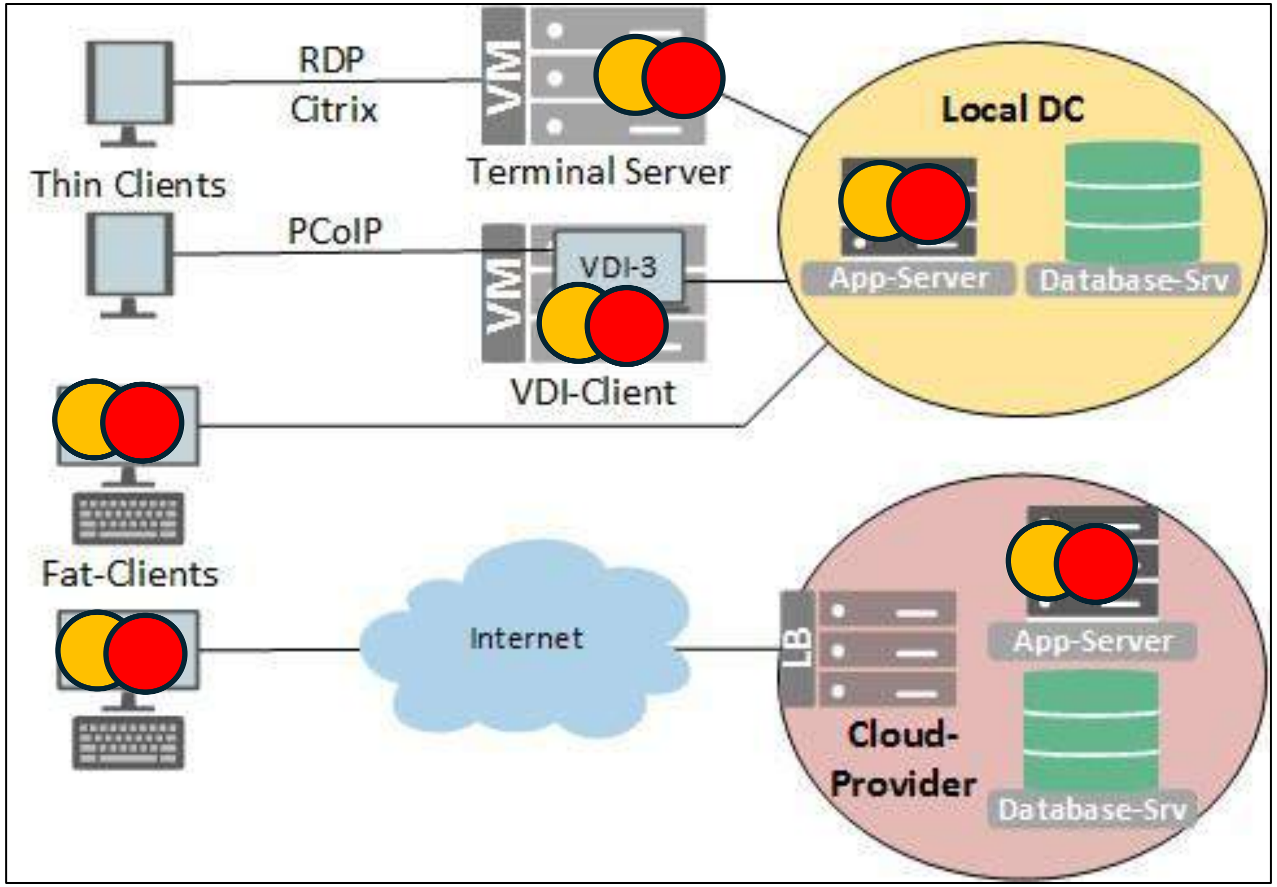
- Who is your Point of Contact?
  - Department, responsibilities, skills
- Problem description
- Actions already taken
  - First captures taken?
  - Baselines?
  - Interviews?
- Earlier tests
  - What has already been checked and can be eliminated
  - What needs to be checked, that has not been eliminated
- Result
  - Know your contact, his/her/their ambitions, and internal standing
  - Know his skills regarding packet analysis

Problem description and isolation - Detailed

- Problem description
  - What is the problem?
  - What is the effect?
  - Who is affected? One, many, sites, location, whole company
  - Which apps? (single, all, new, old)
  - How serious is it?
  - **Function** broken or **performance** bad?
  - When does it happen? - **permanent** or **intermittend**?
- What is the network structure?
  - Network map
- What is the Client-Server architecture
  - -> Identify the ideal capture location, network, servers, middle boxes

Applications and application flows

- Client-Server Architecture
  - Fat Clients
  - Terminal Server
  - Virtual Clients (VDI)
  - Cloud environment
- Traffic flows
  - Client – Servers – DB
- 🟡 Application
  - Encrypted vs. Unencrypted
- 🔴 Capture location
  - Application
  - Client Session



Sample Trace File

- Sample trace file
  - Selecting one single, typical (user) task.
  - Start at client as capture location.
  - Create one trace file per activity.
  - Repeat at least twice
- Is there good traffic on the wire?
  - Is there data that reflects user activities -> right capture location
  - IP addresses and ports
  - Estimate of amount of data
  - Good sample or bad sample? -> checking function vs. performance
  - Encrypted or not? -> Encrypted: OSI Layers 2-4
    Not encrypted -> Include application data

Organizational stuff

Organizational stuff

- Scope of Work
  - What needs to be done
  - Estimate number of days on-site, days to analyze and write report
  - Options to extend
- Time and date
- Capture equipment
  - Depends on number of capture locations
  - Physical: Taps, Probes, Laptops
  - Virtual: Virtual client with Wireshark plus SPAN on vSwitch
  - On demand: renting equipment (taps, probes, capture devices)

Capture Equipment

External devices

- Native Wireshark
  - Notebooks or Servers with Wireshark or tshark
  - Requires span port or tap
  - OK, up to 1 Gbps
- Professional Capture Devices
  - Taps
  - Probes
  - Traffic Directors
  - With large trace buffers or not

Internal devices

- Servers
  - tcpdump for Linux based servers or services
  - Tshark/dumpcap on Windows machines
- Clients
  - Wireshark or tshark
- Middleboxes
  - Proxies, Firewalls, Load Balancers, Switches, Routers
  - Limited capacities on CPU
  - Limited capture space
  - Tendency to lose packets

Legal and financial stuff

Legal and financial stuff

- Legal
  - You need a „License to capture“ from the customers security dep.
  - Typical: Non-disclosure agreement
  - Procedures to store the data securely – external encrypted drive
  - Data hand-over and deletion policies
- Financial
  - Quotation, based upon scope of work
  - Estimated number of days on-site plus analysis plus documentation
  - Daily rate, documented by tasks and hours spent
  - Agreement, how and when to extend the # of days
  - ➔ Contract or order

Starting On-Site

Starting On-site

- Kick-off meeting
  - Objectives, action plan, focus
  - PoC with keys to every location
  - Users, who will be involved
- Capture setup at first location(s)
  - Set up capture devices
  - Synchronize clocks -> physical clocks vs. virtual clocks
  - Sample capture on-site
- Check that **ALL** packets were captured!
- Check that there are not **duplicate** packets!
- Make sure packet timing is OK.

Where to take a sample capture

- Depends on type of problem
  - Best place = local to frontend server
  - Easiest place may be on client side
- Strategy for sample capture on client side:
  - Use a tap!
  - Capture wide open and use filters afterwards
  - Isolate single transaction
  - Use markers/pings
- All depends on the application AND the client-server architecture
  - LB, Proxy outbound, proxy inbound
  - encryption

Getting a first idea

- First Look
  - Identify IP addresses and ports
  - Display filter on IP addresses and ports -> export
- Excluding network problems
  - Checking the typical stuff
  - Typical methodology: Divide and conquer -> L4, then L3, then L2
  - Check Bandwidth, Latencies, Packet Loss, Jitter, Response times
- Fix network problems first
- If network is OK, then one capture location may be OK.

But WAIT!

What is evidence, when we haven‘t captured all packets?

And what can we do, if that happens?

Dropping packets when capturing

Overloaded Wireshark PC

- Packet timestamps are ODD
  - Many packets with 0.000000 seconds in Delta Time
  - High Delta Time
  - Many packets with 0.000000 seconds in Delta Time
  - Constantly repeats
- Dropped packets within Wireshark
  - Statistics -> Capture File Properties -> Dropped Packets
  - Requires pcap-ng on capture
- Indication in trace file
  - "TCP ACKed unseen segment„ message in expert analysis
  - „We saw an ACK, but we did not see the original packet.“
  - The packet was on the network, but it did not make it into the trace file.

- Resolution - I
  - More RAM for capture
  - Faster hard drive
  - Capture Filter
  - And no name resolution
- Resolution – II
  - Command line tools
  - Tshark or dumpcap
- Resolution – III
  - Get some good hardware

Dropping packets when capturing

Problems with capture setup

- Overloaded switch with active SPAN port
- Overloaded proxy, firewall, router with embedded capture

How to identify?

- Indication in trace file
  - "TCP ACKed unseen segment„ message in expert analysis

Start your analysis

Permanent or intermittend

- Permanent
  - Repeatable process
  - Select typical (user) actions
  - Capture three samples per action in separate trace files
  - Document everything!
  - Automate filtering process with tshark
- Intermittend
  - Long term capture
  - Need to find packets that show the problem.
  - Often required: user reports or application logs for timestamps
  - Needle in the haystack.

Function broken or bad performance

Do the analysis

- Function broken
  - DNS resolution
  - Authentication
  - TCP Setup failures
  - Firewalls, Proxies or NAT
  - Check ICMP, when available

- Performance problems
  - High RTT
  - Packet Loss and TCP retransmissions
  - High Server response times (SRT)
  - Long Client think times
- Caution
  - VoIP needs different measures

Things that went well

Things that worked.

- Starting the on-site event with a start meeting
  - Clear objectives, good communication and focus
  - Identifying priorities
  - Discussing outcomes from today and make plans for next day.
- Doing one thing at a time, not many.
- Start gathering data and evidence from the trace files without thinking
  - When the data is complete it may speak to you automatically.
- Do it the Sherlock way
  - "Eliminate the impossible" and see, what is left.
- When fixing things, fix one thing at a time
- Question yourself.
- Also helpful: Customer with lots of experience, time and humor

Things that did not go well!

Case 1:

- Case No. 1: The notebook
  - POC insisted taking his own notebook for capture
  - Did not capture all packets.
  - Indication: TCP Acked lost segment
- Case No. 2: The switch (same customer, same case)
  - Access Layer Switch with one “monitor session”
  - SPAN session dropped packets (10-15%)
- Trace Files were not useable
- Resolution:
  - Get me a TAP!
  - And a new notebook
  - SPAN session at distribution layer switch

Case 3:

- Case No. 3: Yet another switch
  - Client-Server application
  - SPAN-Ports at client switch and at server switch
    - Wireshark PC at server switch showed 100% packets
    - Wireshark PC at client switch showed 60-70% packets
  - Swapping Wireshark PCs did not change the results.
  - Same story: SPAN session overloaded the access layer switch.
  - Trace Files were not usable!

Case No. 4

Chasing 15 seconds

- Capturing at customer site
  - Wireshark clocks were synchronized to my external wrist watch.
  - Actions were always started on the full minute
  - First captures on Fat Clients showed good results
- Next day -> Virtual client (Vmware Horizon VDI)
  - Captures were taken on virtual client
  - Action again synced on external watch and started on full minute.
  - ➔ All client actions started with a 15 second delay!
- Where is the problem?
  - Client performance or what?
- Result: Clock in the virtual world had a 15 seconds offset to the clients in the physical world.
- ➔ We had to do all the captures again!

More Cases

- Problem, what kind of problem?
  - When packet analysis leads to a clear result
  - And the resolution is only four lines of configuration away.
  - BUT: The customer refuses to take on responsibility.
  - He fears consequences
- Problem description:
  - Performance drops on SMB2 access across customer sites
  - Problem: Path-MTU discovery failed (ICMP Fragmentation needed)
  - Recommended action: MSS adjustment a.k.a. MSS clamping
  - PoC claimed that they could not reproduce the problem.

Many more ….

- When security is being sacrificed!

1. File upload of a portal for application had a 30 second “timeout”.
   - Wireshark showed TCP Zero Window.
   - Caused by malware checker
   - => Was disabled to avoid the timeout
2. Firewall caused 8 seconds of transaction time for one screen
   - Wireshark showed no TCP problems
   - Caused by 9000+ application turns
   - => Firewall was removed

Lessons I learnt

General lessons

- Do not pretend that you already know the answer.
  - Problems may look very much alike any older problems
  - Frequently they are different.
- Do not just look at packets.
  - Check what is really going on, on your network.
  - Check network sources, logs and servers, too.
- Know your capture devices and know, when they break.
- Document your captured data
- Know your capture location.
- Validate your results

Questions?

Feedback for this presentation

https://conference.wireshark.org/sharkfest-25-europe-2025/talk/NZZFEB/feedback/

#sf25eu