Workflow-based Analysis of Wireshark Traces

Now we can all be experts

Paul Offord
Project Leader, TribeLab
Agenda

- Recurring Gray Problems
- Principles and objectives of our approach
- Performance problem scenarios
- Performance analysis concepts
- Analysis strategy
- Worked example – get into some packets
- Q&A
The Issue

Recurring

It keeps happening

Gray

The causing technology is unknown

Problem

Performance Error Incorrect output

“It must be the network”
The Challenge

Ongoing Problem
- Static cause
- Recreate
- Short capture
- Easy analysis

Recurring Gray Problem
- Transient cause
- Can’t recreate
- Long-term capture
- Challenging analysis
Analysis Principles

We look at **one symptom** at a time

We study a **specific instance** of that symptom

We capture **live** problems

Produce **irrefutable evidence** of the cause
User experiences 15s response time

Packet capture units (dumpcap, NetShark, etc.)

The problem is here
**Process-to-Process Communication**

<table>
<thead>
<tr>
<th>Browser</th>
<th>Network</th>
<th>Web Server</th>
</tr>
</thead>
</table>

**NB:** Application messages (APDUs) not packets

APDU Response Time → Application Request ➔ Application Response ➔ Service Time

Increasing Time of Day

SharkFest’17 US • Carnegie Mellon University • June 19-22, 2017
Slow Response - Scenario 1

Browser

Network

Web Server

Database

Mouse Click

APDU Req

APDU Rsp

APDU Req

APDU Rsp

Page Rendered

0.1 s

9.9 s

9.8 s

9.3 s

0.1 s

10 s

9.4 s

0.1 s
Slow Response - Scenario 2

Browser

0.1 s

Web Server

9.6 s

Database

0.2 s

Network

0.1 s

Mouse Click

APDU Req

APDU Rsp

APDU Req

APDU Rsp

10 s

9.9 s

9.8 s

0.1 s

0.1 s

Page Rendered

Page Rendered

0.1 s

SharkFest’17 US • Carnegie Mellon University • June 19-22, 2017
Slow Response - Scenario 2b

Browser

Network

Web Server

Web Svc

Database

Mouse Click

APDU Req

APDU Req

APDU Req

APDU Req

APDU Rsp

APDU Rsp

APDU Rsp

APDU Rsp

Page Rendered

0.1 s

0.1 s

0.4 s

9.2 s

0.2 s

9.8 s

9.9 s

10 s

0.4 s

SharkFest’17 US • Carnegie Mellon University • June 19-22, 2017
Slow Response - Scenario 3

Browser 0.7 s 9.3 s

Web Server 0.6 s

Database 0.2 s 0.4 s

Mouse Click

Page Rendered

Network

APDU Req

APDU Rsp

APDU Req

APDU Rsp

APDU Rsp
Slow Response - Scenario 4

Mouse Click

0.1 s
Browser

9.3 s
Network

0.2 s
Web Server

0.4 s
Database

9.9 s
APDU Req

Retransmissions

10 s
APDU Rsp

0.6 s
APDU Req

0.4 s
APDU Rsp

0.1 s
APDU Rsp

0.1 s
APDU Rsp

Mouse Click

Page Rendered

SharkFest’17 US • Carnegie Mellon University • June 19-22, 2017
Multi-tier Trace Correlation

Paul Offord
CTO, Advance7

Network Trace Analysis Guide

You've got a basic understanding of networking and you can drive Wireshark to a reasonable level (capture, display and filter). You can mimic the tips and tricks that you've seen demonstrated on YouTube and you are keen to get the most out of Wireshark. Your boss has asked you to take a look at a response time problem with an important business system. You've successfully captured trace data from multiple points in the end-to-end system but you are struggling to analyze it. Where do you start? Which tips and tricks are applicable? If this sounds familiar you've come to the right place.

The Network Trace Analysis Guide describes a systematic way to analyze traces captured from a multi-tier system, and the other resources on this page provide further help and guidance.

Resources

The Network Trace Analysis Guide electronic book in this course details a systematic way to carry out network trace analysis. The guide refers to a number of techniques that are described in the book RPR: A Problem Diagnosis Method for IT Professionals, a copy of which we include here for completeness.

Discussion Forum

Post questions, feedback and general comments relating to the the Network Trace Analysis Guide on this forum.

Network Trace Analysis Guide

This guide is for anyone looking for a systematic way to analyze network trace data. We focus on the analysis of traces gathered in enterprise IT environments, but the principles and techniques should be applicable across a broad range of scenarios.

RPR: A Problem Diagnosis Method for IT Professionals

This is a PDF version of the RPR manual. The guide references some techniques described in this manual.
APDU vs. Packets

tcp.port==80 && tcp.len>0

Request APDU

Response APDU

SharkFest’17 US • Carnegie Mellon University • June 19-22, 2017
Response Time Element (RTE) Model

Browser  
| Network  | Web Server  | Database |

Mouse Click  
Client Time  
APDU Response Time  
APDU Req - Part a  
APDU Req - Part b  
APDU Req - Part c  
APDU Req - Part d  
APDU Rsp - Part α  
APDU Rsp - Part β  
APDU Rsp - Part γ  
Request Spread  
Service Time  
Response Spread  
Data Packets tcp.len>0  
SharkFest’17 US • Carnegie Mellon University • June 19-22, 2017
TRANSUM and RTE

- TRANSUM is a Wireshark plugin
- Standard in Wireshark 2.4 (mid-late July)
- TribeLab Plugin for Wireshark 2.2
TRANSUM adds a new decode section

**RTE Data**

- Frame 51: 561 bytes on wire (4488 bits), 561 bytes payload
- Ethernet II, Src: Vmware_90:e0:d3 (00:0c:29:90:e0:d3)
- Internet Protocol Version 4, Src: 192.168.1.100
- Transmission Control Protocol, Src Port: 60000
- Hypertext Transfer Protocol

**TRANSUM RTE Data**

- [RTE Status: OK]
- [Req First Seg: 51]
- [Req Last Seg: 51]
- [Rsp First Seg: 53]
- [Rsp Last Seg: 55]
- [APDU Rsp Time: 1.011444000 seconds]
- [Service Time: 1.011305000 seconds]
- [Req Spread: 0.000000000 seconds]
- [Rsp Spread: 0.000139000 seconds]
- [Trace clip filter: tcp.stream==3 && frame==51]
- [Calculation: Generic TCP]
RTE Summary

• APDU Response Time
  • Client perspective
  • Big number = There’s a problem

• Service Time
  • Service perspective
  • Big number = There’s a problem with the service

• Spread Time
  • Network perspective
  • Big number = There’s a problem with the network
Simple Analysis Strategy

• No high APDU Response Times
  • Problem in the client program

• High Service Time
  • Confirm with matching traces
  • Translate data into something meaningful to service owner
  • Hit the service owner with the facts

• High Spread Time
  • Focus in the problem time frame
  • Use techniques *a la* Betty, Chris, Hansang, Jasper, Kary, Laura, etc.
Questions?
Introducing Workbench
<table>
<thead>
<tr>
<th>Workbench</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Any data</td>
<td>Any tool</td>
</tr>
<tr>
<td>Any tool</td>
<td>Expert guidance</td>
</tr>
<tr>
<td>In dev - Free trial</td>
<td>FOC Community Edition</td>
</tr>
<tr>
<td>Large volume</td>
<td>Marker finder</td>
</tr>
<tr>
<td>filtering</td>
<td>Transformation</td>
</tr>
<tr>
<td></td>
<td>Packet matching</td>
</tr>
<tr>
<td></td>
<td>Side-by-side analysis</td>
</tr>
</tbody>
</table>
Main Features
• Model work practices
• Adds context
• Adapts
Sharing Workflows

- Community
- TribeLab
- 3rd Parties
  - Private
  - Private and shared with colleagues
  - Public

In Development

SharkFest’17 US • Carnegie Mellon University • June 19-22, 2017
Now for the Main Course

Use Case
The Symptom
And now ... Analyze the Data
TCP Segmentation Offload (TSO)

Without Large Receive Offload (LRO)

tcp.len = 5,120 bytes

tcp.len = 1,460 bytes

tcp.len = 1,460 bytes

tcp.len = 1,460 bytes

tcp.len = 740 bytes

SharkFest'17 US • Carnegie Mellon University • June 19-22, 2017
Summary

• Recurring gray problems – “It’s the network”
• Analyzing the packet volumes is challenging
• Markers help a lot – see Matthew York, SF16
• Most applications - Request-Response pattern
• TRANSUM allows top-down performance analysis
• Workflow approach - fast, accurate & consistent
• Workbench platform allows sharing of workflows
Contact

- Paul Offord
- P  +44 (0) 1279 211 668
- E  paul@tribelab.com
- W  www.tribelab.com
- T  @paulofforda7