Pakete lügen nicht - Wireshark

Protokoll Analyse mit Wireshark

Rolf Leutert, Leutert NetServices
Stefan Rüeger, Studerus AG

TE FO 11 STUDERUS TECHNOLOGY FORUM

Vorstellung

Rolf Leutert, Network Consultant
Leutert NetServices
8058 Zürich-Flughafen

- Netzwerk Analyse & Troubleshooting
- Protokoll Schulungen TCP/IP, WLAN, VoIP, IPv6
- Wireshark® Certified Network Analyst 2010
- Wireshark® Instructor seit 2006
- Sniffer® certified Instructor seit 1990

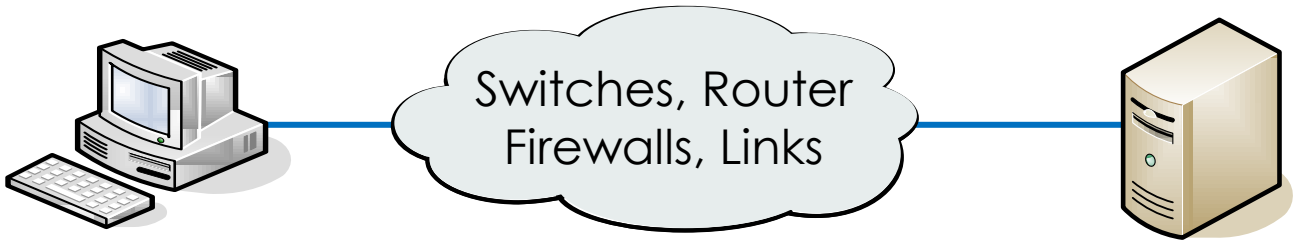
leutert@wireshark.ch
www.wireshark.ch

Agenda

- Einführung in die Fehlersuche
- Wireshark Packet Analyser
- Einführung in die TCP Analyse
- Fehlersuche Fall 1 : Session Hang-Up
- Fehlersuche Fall 2 : Slow Printing
- Fehlersuche Fall 3 : Bad WAN Throughput
- Kurshinweise

Einführung in die Fehlersuche

Eingrenzung der Fehlerquellen



Überlast (CPU/RAM)
Fehlkonfiguration
Software (OS/Applik.)
Interner Firewall
Interne Security SW (AV)
Bediener Fehler

Überlast (CPU/RAM)
Fehlkonfiguration
Software (FW/OS)
Bandbreiten

LAN, WLAN, WAN, ISP

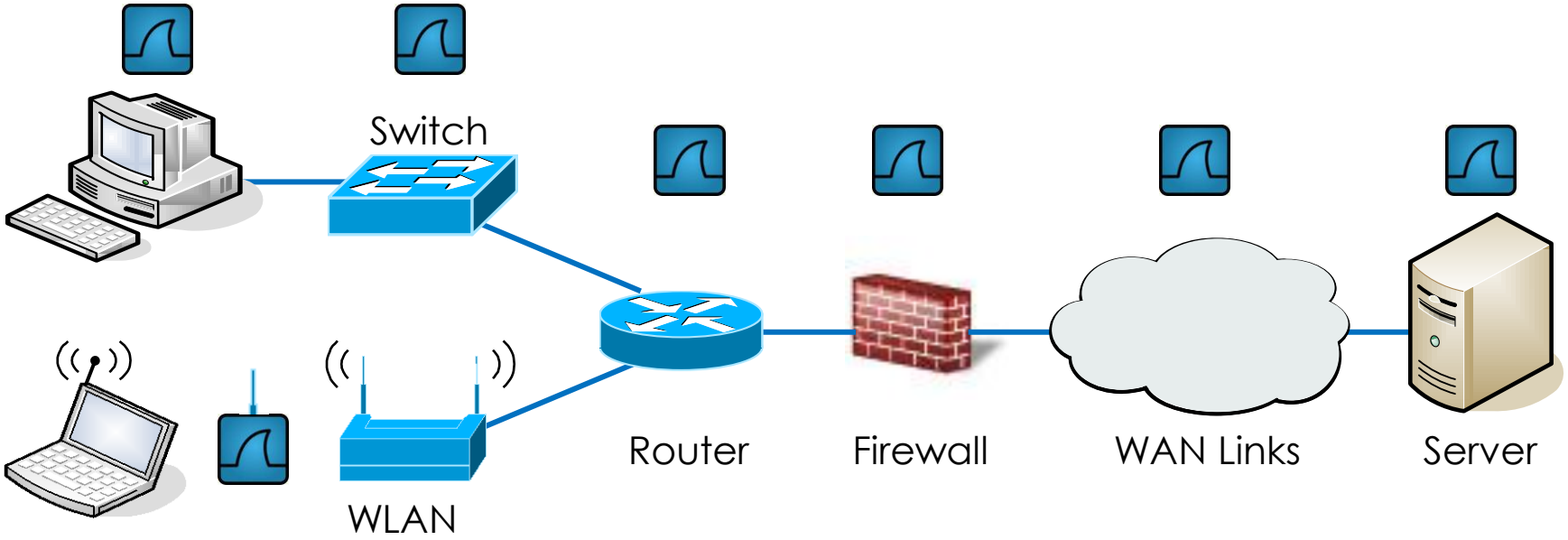
Lange Laufzeit
Paketverlust
Session Abbruch

Überlast (CPU/RAM)
Fehlkonfiguration
Software (OS/Applik.)
Interner Firewall
Interne Security SW (AV)
Services DNS/DHCP usw.

Wireshark Packet Analyser

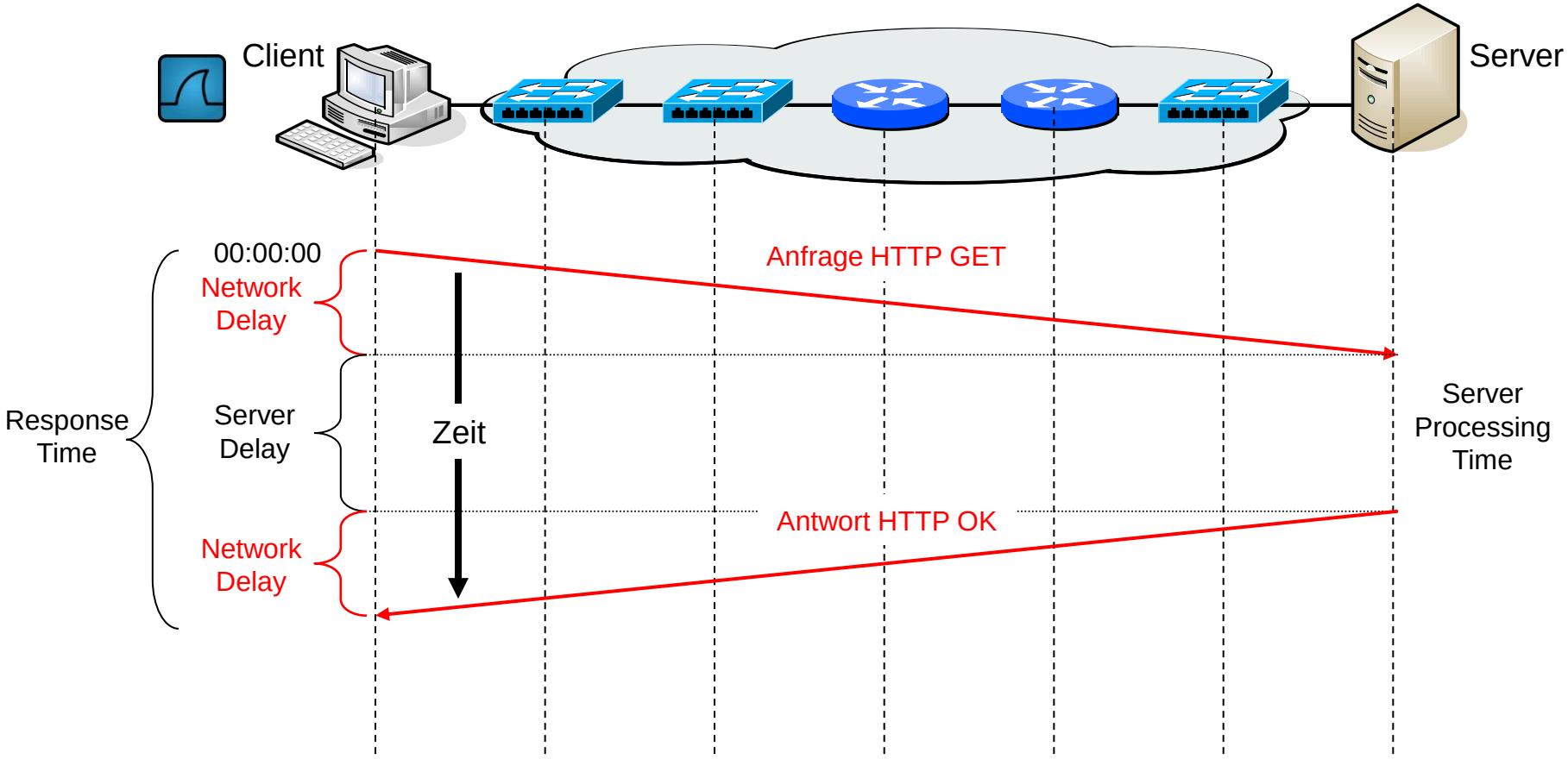
- Der am meisten eingesetzte Protocol Analyzer weltweit
- Open-Source Software, d.h. kostenlos einsetzbar, privat oder kommerziell
- Decodiert gegen 1‘000 verschiedene Netzwerk-Protokolle
- Unterstützt von allen gängigen Betriebssystem: Windows, Unix, Linux, MAC…
- Download von www.wireshark.org
- In 5 Minuten installiert, runterladen und installieren mit default Einstellungen
- Kann Tracefiles öffnen, welche mit TCPdump aufgezeichnet wurden

Wireshark Packet Analyser



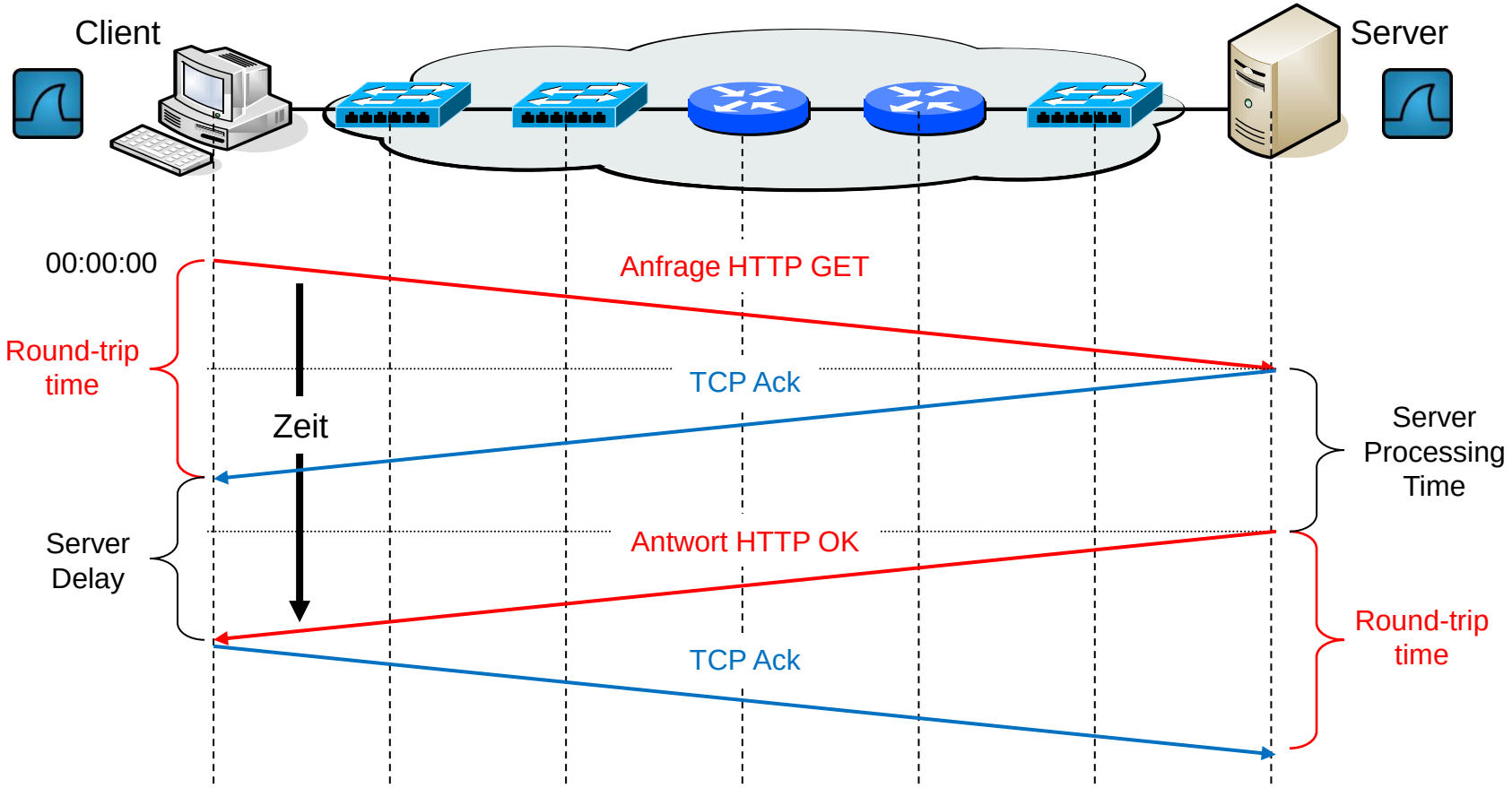
- Wireshark kann Daten an zahlreichen Messpunkten aufzeichnen
- Einige Netzwerkkomponenten haben TCPdump bereits integriert
- Der Aufzeichnungsort kann für die Analyse wichtig sein
- TCP Felder sind end-to end und können somit auf dem ganzen Datenpfad analysiert werden (good news)

Einführung in die TCP Analyse

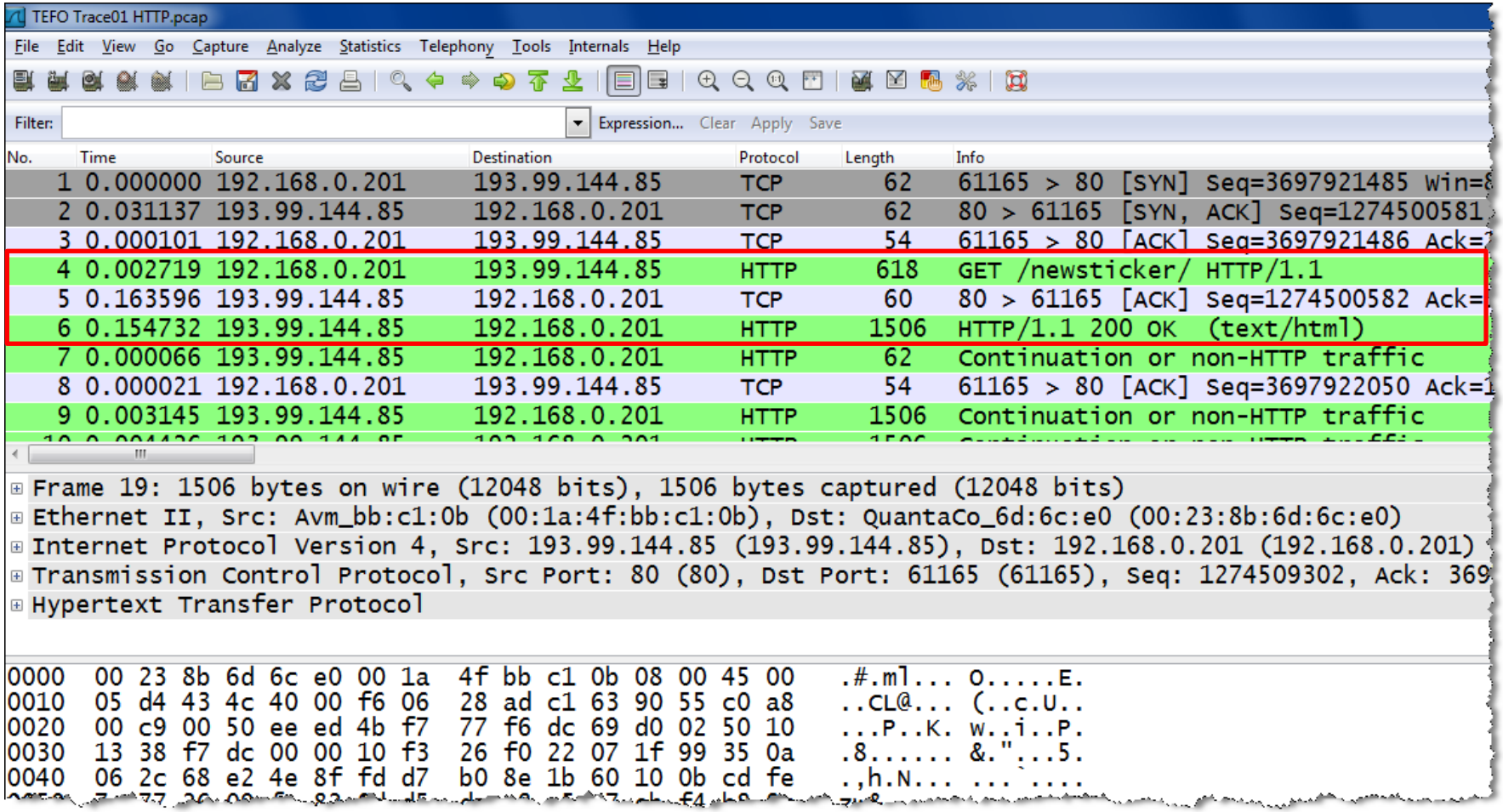


Response Time = 2 x Network Propagation Delay + Server Processing Time

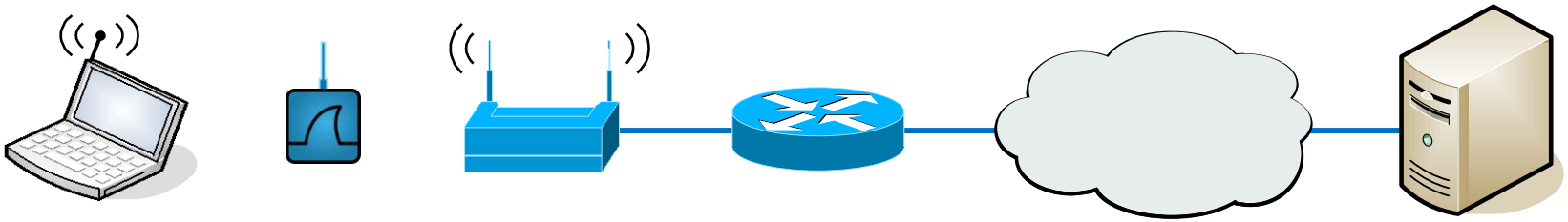
Einführung in die TCP Analyse



Einführung in die TCP Analyse



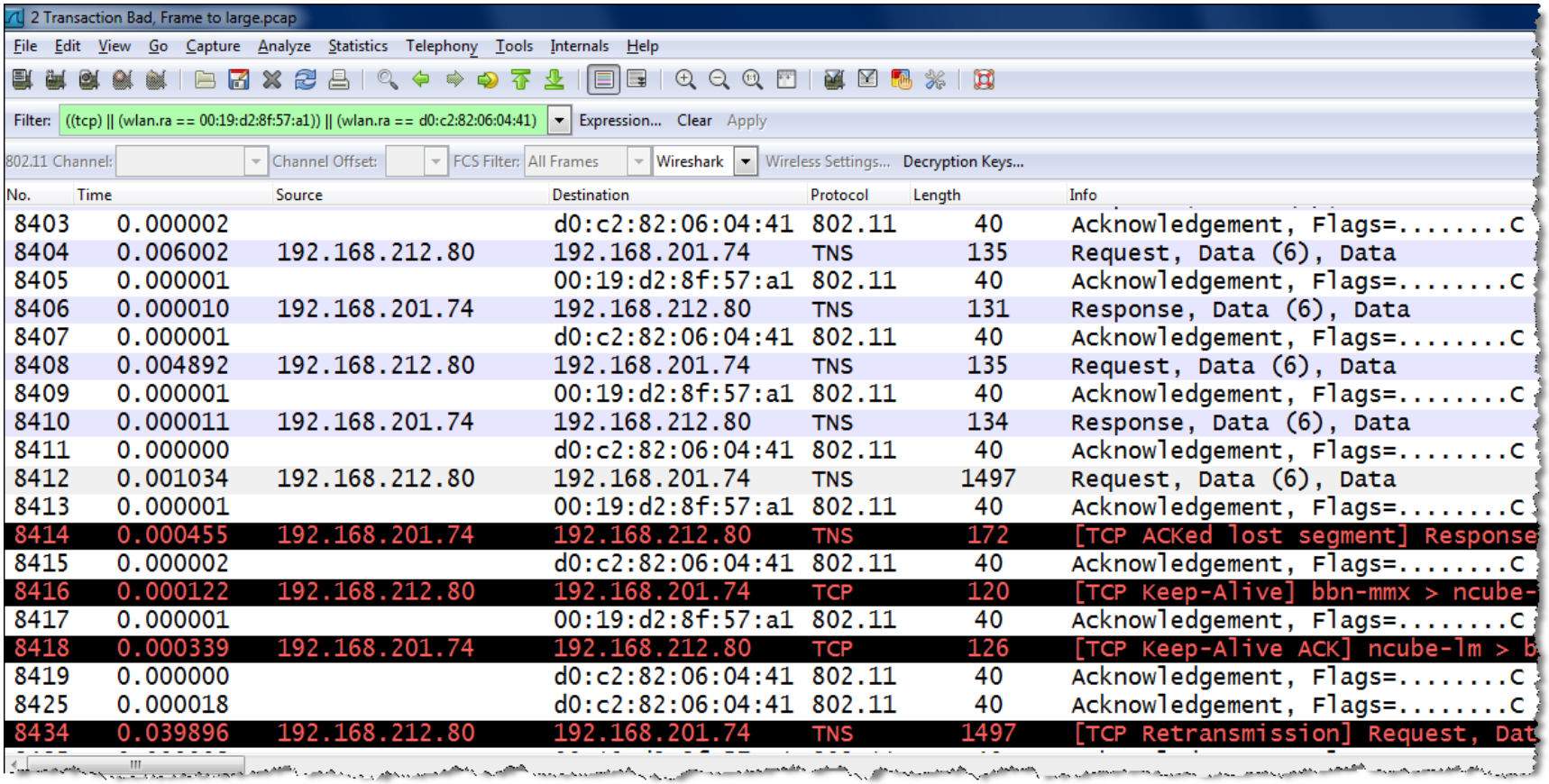
Fehlersuche Fall 1 : Session Hang-Up



Betriebswichtige Anwendung zur Personalplanung in einem Spital:

- Der Bildschirm blockiert mitten in der Anwendung
- Probleme nur im WLAN, Clients am Ethernet funktionieren einwandfrei
- Alle anderen Anwendungen funktionieren einwandfrei über WLAN
- Dadurch fühlt sich der Lieferant des WLAN nicht zuständig
- Der Lieferant der Anwendung bietet keine Unterstützung, die Software sei ‚nicht WLAN fähig'

Fehlersuche Fall 1 : Session Hang-Up



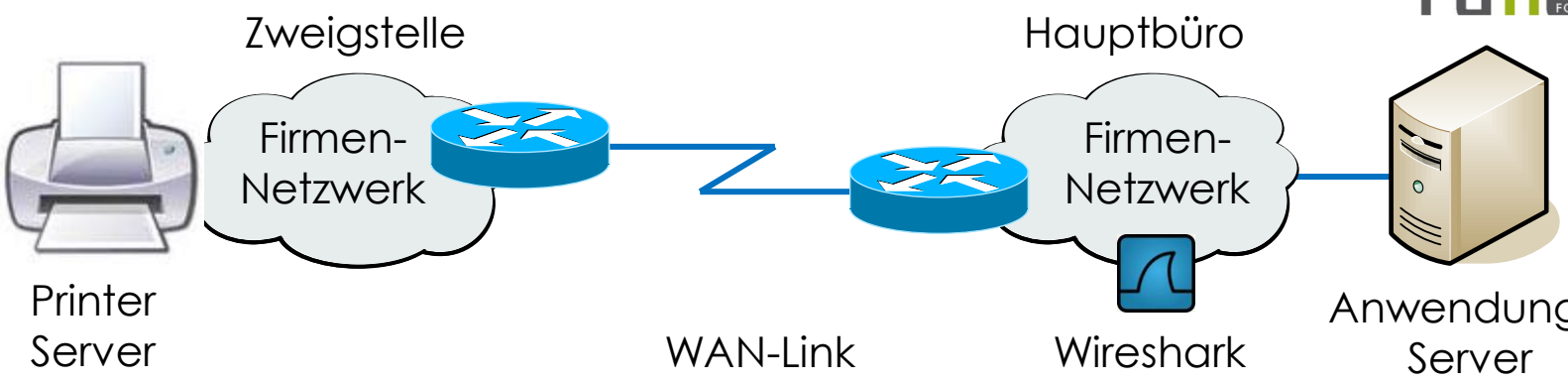
Fehlersuche Fall 1 : Session Hang-Up

Eingrenzung der Fehlerquellen

Workstation	Netzwerk	Server
Überlast (CPU/RAM)	Überlast (CPU/RAM)	Überlast (CPU/RAM)
Fehlkonfiguration	Fehlkonfiguration	Fehlkonfiguration
Software (OS/Applik.)	Software (FW/OS)	Software (OS/Applik.)
Interner Firewall	Bandbreiten	Interner Firewall
Interne Security SW (AV)	---	Interne Security SW (AV)
Bediener Fehler	LAN, WLAN, WAN, ISP	Services DNS/DHCP usw.

	Lange Laufzeit	
	Paketverlust	
	Session Abbruch	

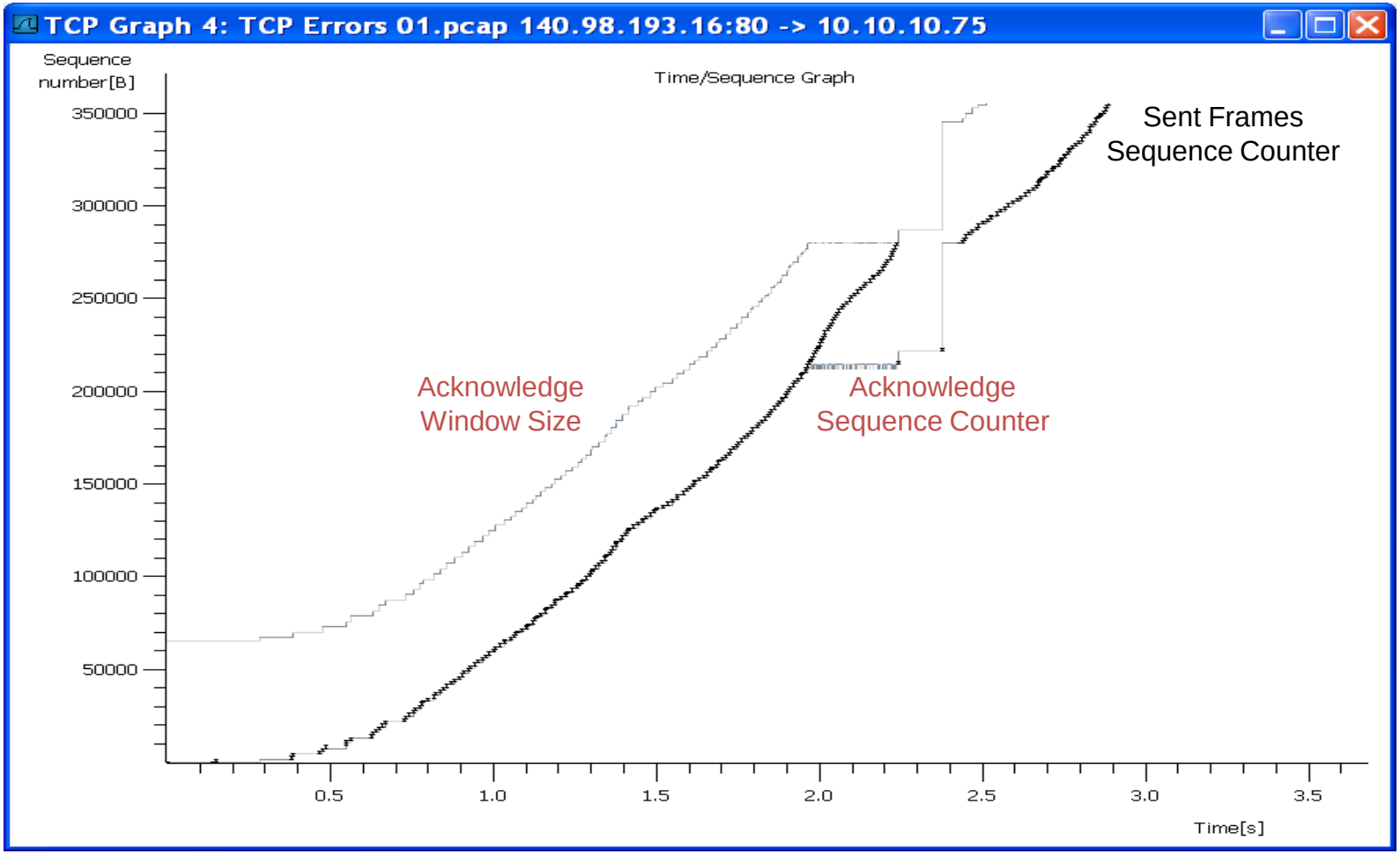
Fehlersuche Fall 2 : Slow Printing



Handelsfirma mit Hauptbüro und Zweigstellen angebunden über WAN

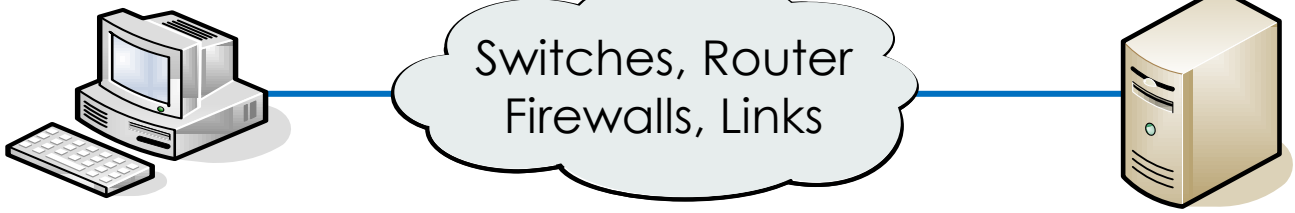
- Warenlieferungen von Zweigstellen, dezentraler Druck von Lieferscheinen
- Der Ausdruck von Lieferpapieren dauert Minuten und verzögert Abläufe
- Die Druckjobs werden vom zentralen SAP Server zur Zweigstelle geschickt
- Vermutet wird ein Bandbreite-Problem im WAN
- WAN Bandbreite wurde bereits auf 1Mbps verdoppelt, ohne Erfolg!
- Situation dauert schon Monate

Fehlersuche Fall 2 : Slow Printing



Fehlersuche Fall 2 : Slow Printing

Eingrenzung der Fehlerquellen

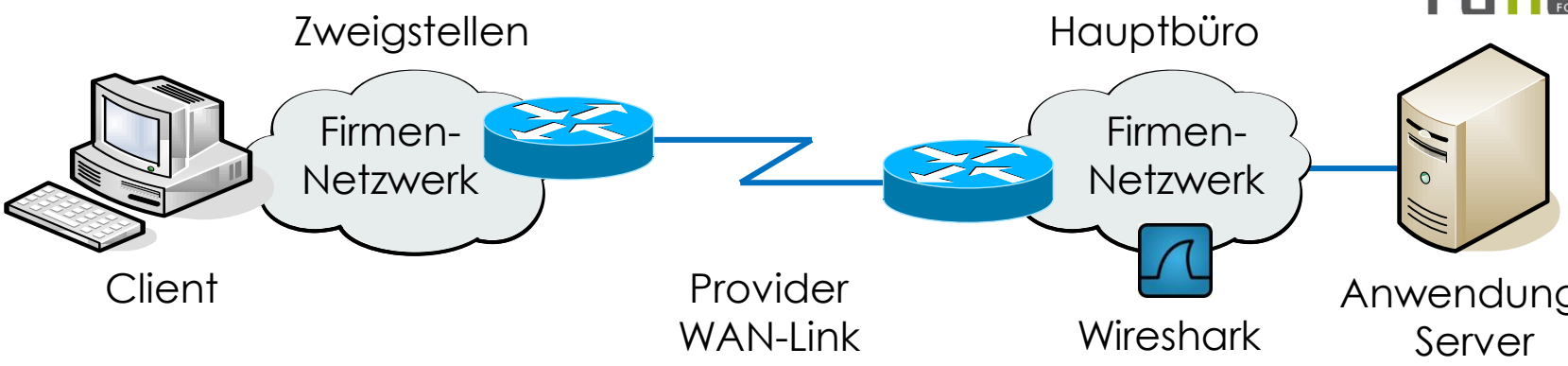


Workstation	Netzwerk	Server
Überlast (CPU/RAM)	Überlast (CPU/RAM)	Überlast (CPU/RAM)
Fehlkonfiguration	Fehlkonfiguration	Fehlkonfiguration
Software (OS/Applik.)	Software (FW/OS)	Software (OS/Applik.)
Interner Firewall	Bandbreiten	Interner Firewall
Interne Security SW (AV)	---	Interne Security SW (AV)
Bediener Fehler	LAN, WLAN, WAN, ISP	Services DNS/DHCP usw.

	Lange Laufzeit	
	Paketverlust	
	Session Abbruch	

+

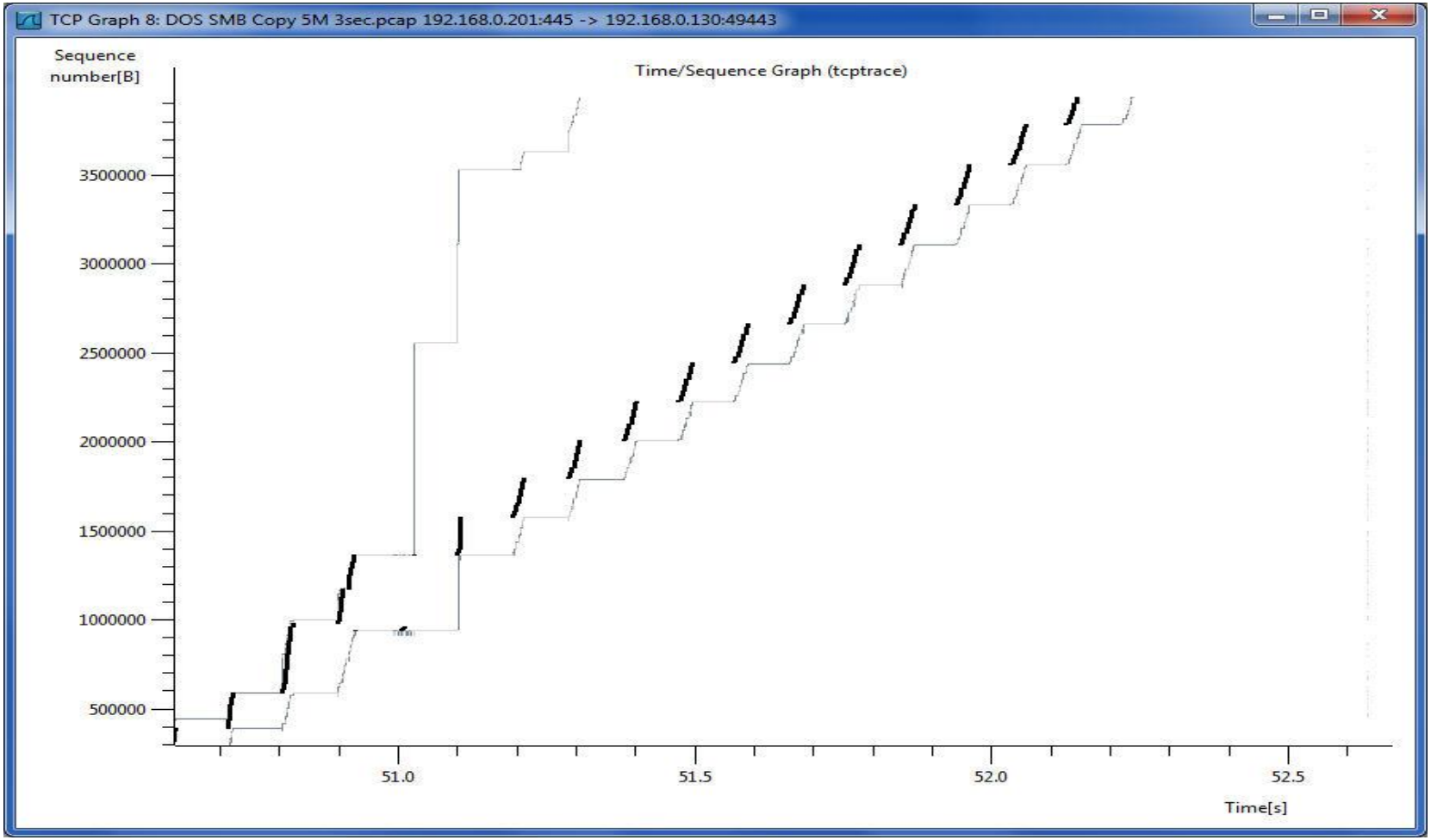
Fehlersuche Fall 3 : Bad WAN Throughput



Grosse schweizerische Herstellerfirma mit weltweiten Niederlassungen

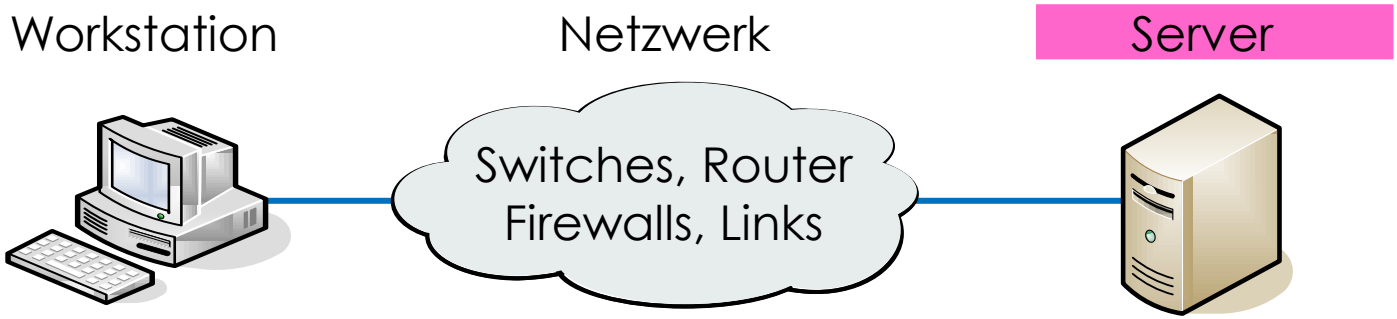
- Niederlassungen sind über WAN-Provider mit 45Mbps Links angeschlossen
- Die Links werden für regelmässige Softwareupdates der Clients verwendet.
- Die Übertragung dauert zu lange, kann über Nacht nicht beendet werden
- Grobe Berechnungen ergeben eine Durchsatz von nur 1Mbps
- Der Kunde vermutet Daten-Drosselung durch den WAN-Provider

Fehlersuche Fall 3 : Bad WAN Throughput



Fehlersuche Fall 3 : Bad WAN Throughput

Eingrenzung der Fehlerquellen



Workstation	Netzwerk	Server
Überlast (CPU/RAM)	Überlast (CPU/RAM)	Überlast (CPU/RAM)
Fehlkonfiguration	Fehlkonfiguration	Fehlkonfiguration
Software (OS/Applik.)	Software (FW/OS)	Software (OS/Applik.)
Interner Firewall	Bandbreiten	Interner Firewall
Interne Security SW (AV)	---	Interne Security SW (AV)
Bediener Fehler	LAN, WLAN, WAN, ISP	Services DNS/DHCP usw.

	Lange Laufzeit	
	Paketverlust	
	Session Abbruch	

+

Danke für Ihre Aufmerksamkeit

Gerne begrüssen wir Sie an einem Kurs von Leutert NetServices

Grundkurse bei Studerus:

- **NET-Analyse** mit Wireshark
- **IPv6-Protokoll** Einführung

LAB-Kurse bei HSR
(Hochschule Rapperswil)

- **TCP/IP Protokoll**
- **WLAN Analyse**
- **IPv6 Praxisworkshop**

Registrieren sie sich für den technischen Newsletter www.wireshark.ch