



Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Sie erreichen uns hier

Freistädterstraße 236, A-4040 Linz

Email: education.ecs.at@arrow.com

Phone: +43 1 370 94 40 - 34



TCP/IP Analysis with Wireshark

CODE:	LÄNGE:	PREIS:
WIS_NAW-ENG	24 Hours (3 Tage)	€2,170.00

Description

The TCP/IP family is the most widely used group of protocols used in today's communication systems. Detailed knowledge and understanding of the different elements, functions and terms is essential for troubleshooting network problems and optimizing performance.

This practical training provides you with all the relevant information. During hands-on exercises using trace files with popular errors you learn how to use Wireshark to isolate network problems and bottlenecks. All the most valuable Wireshark features like filters, graphs and TCP expert system etc. will be covered and will help you to find network issues faster.

Inhalt

Introduction

- Course objectives
- History of Ethereal and name change to Wireshark
- General technical information about Wireshark (WinPcap driver etc.)

Installation and Configuration of Wireshark

- Installation of Wireshark Software and WinPcap Drivers
- Creating Wireshark Profiles
- Configuration of 'Preferences'
- Configuration of 'Display Layout'
- Configuration of 'Coloring Rules'
- Configuration of 'Printing'
- Configuration of 'Name Resolution'
- Configuration of 'Protocols'

Techniques of Troubleshooting

- Systematic procedure for troubleshooting
- Where to place the analyzer
- Capturing data in switched and routed network environments
- Analyzing 'Broadcast Frames'

Capturing and saving data with Wireshark

- Capture Interfaces
- Capture Options

Applying the Numerous Filtering Options of Wireshark

- Simple Display/Capture Filters
- Combined Display/Capture Filters
- Complex Display/Capture Filters
- Application of 'Right Click' Filters
- Application of 'Follow TCP Stream'

Frame Analysis and Troubleshooting with Wireshark Expert System

- Fragmented & Reassembled Frames
- TCP Zero Window, Window Full, Window Size Exceeded
- TCP Lost Packet, Retransmissions, Duplicate Packets
- TCP Duplicate Acknowledges, Fast Retransmissions, low TTL etc.
- Response time analysis of TCP connections
- Using the 'Wireshark Expert System' for assistance

- Examples of analysing complex network problems

Statistical Evaluation with Wireshark

- Application and interpretation of ,IO Graphs'
- Application and interpretation of ,Conversation List'
- Application and interpretation of ,Endpoint List'
- Application and interpretation of ,Service Response Time'
- Application and interpretation of ,TCP Flow Graph'
- Application and interpretation of ,TCP Stream Graph'
- Application and interpretation of ,Round Trip Graph'
- Application and interpretation of ,Throughput Graph'

Different Wireshark Topics

- Performance limitations of Wireshark (impact of packet loss)
- Optimizing the Wireshark performance

TCP/IP Protocol Family

- Introduction to the TCP/IP Family

Layer 2 Protocols (Ethernet)

- Explanation of Ethernet Addresses Unicast, Anycast, Multicast, Broadcast
- Explanation of Autonegotiation, Duplex settings and mismatch
- Explanation of ARP, gratuitous ARP, proxy ARP
- Explanation DHCP Protocol & Process
- Microsoft Network Load Balancing Protocol (NLB used in MS server clusters)

Layer 3 Protocols

- Explanation of IP addressing
- Explanation of IP Headers Identification, TTL, Fragmentation, TOS/DiffServ
- Explanation of Chimney offloading (Checksum errors in Wireshark)
- Explanation of all ICMP messages Redirect, Destination unreachable etc.
- Analyzing MTU Problems with ,Black Hole Router'
- Explanation of MTU Discovery

Layer 4 Protocols

- Overview of TCP functions
- Explanation of TCP Session Setup and Release
- Explanation of TCP options Segment Size, Selective Acknowledgment, Time Stamp and Window Scaling
- Long Fat Pipe (LFN) impact on TCP throughput
- Tuning data throughput by activation of TCP options on servers/clients
- Explanation of TCP functions Flow Control, Sliding Window, Error Correction
- Explanation of TCP flags CWR, ECN-Echo, and Push
- Explanation of TCP Offloading large volumes (Frame size exceeded errors)
- Explanation of UDP functions

Kurstermine

Auf Anfrage. Bitte [kontaktieren Sie uns](#)

Zusätzliche Information

Diese Schulung ist auch als Vor-Ort-Schulung verfügbar. Bitte kontaktieren Sie uns, um mehr zu erfahren.