Troubleshooting Networks with Wireshark

Duration: 3 Days Course Code: GK9880 Version: 2.1

Overview:

This hands-on based Wireshark training gets you familiar with the most popular network analyzer today, Wireshark®, and provides hands-on experience in troubleshooting the most common network-errors using Wireshark®.

Target Audience:

Anyone that in their daily operations encounter TCP/IP based networks or networking equipment and needs to be able to understand or troubleshoot the communication between endpoints.

Objectives:

- Understand the troubleshooting process
- Make use of available tools
- Get familiar with the workings of a protocol analyzer
- Get familiar with using Wireshark®
- Learn how to customize Wireshark® to your needs
- Learn how to use filters
- Learn how to use statistics
- Learn how to make baseline
- Learn how to observe normal and abnormal protocol behavior
- Understand the difference in application needs
- Get an insight into the most common networking issues

Prerequisites:

Testing and Certification

Content:

1. Troubleshooting methodology

a. Before you start

b. Guidelines

c. Troubleshooting tools

d. Intercepting traffic

e. Network characteristics

- Delay

- Jitter

- Packet loss

f. Application types

- Batch

- Streaming

- Interactive

g. Creating a baseline

2. Wireshark® Fundamentals

a. Background

b. GUI vs CLI

c. How to customize Wireshark®

d. Using capture- and display-filters

e. Using statistics for troubleshooting

3. Troubleshooting an Ethernet LAN

a. How to intercept traffic in a switched environment

b. Troubleshooting cabling issues

c. Troubleshooting speed/duplex-settings

d. Troubleshooting Spanning-Tree issues

e. Troubleshooting Link Aggregation

4. Troubleshooting IPv4- and IPv6-based communications

a. Determining path through the network

b. Troubleshooting endpoints

c. Troubleshooting Address Resolution/Neighbor Discovery

d. Troubleshooting DHCP issues

e. Troubleshooting DNS issues

5. Using ICMP for diagnostics

a. Using PING effectively

b. Using traceroute effectively

c. Interpreting ICMP messages

6. Troubleshooting TCP/UDP sessions

a. Using Wireshark® to observe TCP

i. 3-way handshake

ii. Flow control

iii. Error messages

b. Statistics

i. Round-trip times

ii. Sessions

c. Using netstat effectively

LABS

Lab 1: Customize Wireshark® to your preferences

Lab 2: Using Wireshark® to create a baseline

Lab 3: Setting up a mirror-port to capture traffic (class-room only)

Lab 4: Creating and observing a duplex mismatch (class-room only)

Lab 5: Observing Spanning Tree operations using Wireshark®

Lab 6: Observing LACP operations using Wireshark®

Lab 7: Using Wireshark® to determine endpoint-issues

Lab 8: Using Wireshark® to observe ARP/ND operations

Lab 9: Using Wireshark® to troubleshoot DHCP-issues

Lab 10: Using Wireshark® to troubleshoot DNS-issues

Lab 11: Using Wireshark® to profile traceroute operations

Lab 12: Using Wireshark® to interpret and use ICMP-messages

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.com/en-be/