Wireless Training

SHARK300: Advanced Network Analysis and Troubleshooting with Wireshark

Wireshark is an essential network analysis tool for network professionals. It is the tool of choice for acquiring an in-depth understanding of network protocols, performing in-depth network examination, determining traffic patterns, planning capacity and expansion, and conducting network security reviews. Wireshark is a powerful and complex tool, but it is not intuitive and requires advanced training to master. This live class is available virtually with RemoteLive™ or locally at our Phoenix, AZ location.

$3,695.00

- 4 Days
- Replay recordings not included due to content licensing

Upcoming Dates

Course Description

This 4-day instructor-led training course shows learners how to use Wireshark to view, capture, analyze, and troubleshoot network traffic. Emphasis is placed on a hands-on lab-based approach where learners use Wireshark on a live network. The course is vendor-agnostic and is not specific to any single model or brand of networking gear like Cisco, Juniper, Intel, or HP. The course covers protocol analysis and troubleshooting across all vendors and types of network infrastructure.

This course is taught by instructor and author Dr. Avril Salter, CCNP-W, CCNA-S. Dr. Salter has extensive experience in packet-level network analysis and frequently lectures on this topic. She is a guest instructor at numerous telecommunications and network companies, teaching their internal staff to perform network analysis on the equipment that they design and manufacture. This experience gives Dr. Salter the unique, industry-wide perspective that she brings to the classroom.

Course Outline

Module 1: Wireshark Fundamentals

- Introduction to Wireshark
- When to use Wireshark
- Where to physically connect
- Wireshark Graphical User Interface
- Capturing network traffic

Labs:

- Install Wireshark
- Explore Wireshark installation
- Capture and save network traffic
- Understanding the packet details pane

Module 2: Viewing network protocols with Wireshark

- Capture filters
- Display filters
- Preferences
- Time stamps
- Mark and ignore packets
- Import and export packet captures

Labs:

- Capture filters
- Display filters

Module 3: Analyzing tools and troubleshooting techniques

- Troubleshooting methodology
- Configuration profiles
- Preferences
- Creating coloring rules
- Establishing a baseline
- Leveraging Wireshark statistical reports and graphs

Labs:

- Custom profile
- Coloring rules
- Traffic baselines

Module 4: Analyze and troubleshoot Layer 2 protocols

- Ethernet frames
- MAC addresses
- ARP request/response procedure
- STP
- BPDU format
- Bridge selection
- Port states
- VLANs
- 802.1Q frame encapsulation

Labs:

- Ethernet
- ARP
- STP
- 802.1Q

Module 5: Analyze and troubleshoot wireless protocols

- How to sniff wireless networks
- 802.11 WLAN traffic
- Radiotap information
- Beacons and network capabilities
- ZigBee and ZigBee Pro

Labs:

- RadioTap
- IEEE 802.11
- ZigBee

Module 6: Analyze and troubleshoot /P

- IPv4 header
- IPv4 address
- IP packet fragmentation
- ICMP messaging
- RPL and 6LoWPAN to support the IoT

Labs:

- IP
- ICMP
- RPL / 6LoWPAN (OPTIONAL)

Module 7: Analyze and troubleshoot TCP

- Establishing a TCP connection
- TCP header
- Port numbers and sockets
- Selective acknowledgements
- Sliding window
- Contention and advertised receiving windows
- Congestion control

Labs:

- TCP 3-Way Handshake
- TCP fields
- TCP traffic

Module 8: Analyze and troubleshoot UDP and higher level protocols

- Compare and contrast TCP and UDP
- UDP header
- DHCP communications
- DNS process
- HTTP/HTTPS

Labs:

- UDP, DNS and DHCP
- HTTP

Module 9: Course wrap up and best practices

- Checklists
- Managing trace files

- Course wrap up

Audience

This course is designed for advanced IT networking professionals who work on wired and wireless networks and need to perform network assessment, traffic analysis, and enterprise-wide network troubleshooting.

Prerequisites

Students must be experienced with deploying, managing, and operating enterprise-level networks. Learners must also have a full understanding of the TCP/IP protocol stack and IP routing. No prior experience with Wireshark is required.

Before attending this class, students must hold a Cisco CCNA Routing and Switching Certification, Net+ or equivalent network certification.

What You Will Learn

In this class, you will learn how to:

- Understand key network protocols in today's enterprise wired and wireless networks. Analyzed protocols include: HTTP, TCP, UDP, IP, DHCP, DNS, ICMP, Ethernet, IEEE 802.11, Bluetooth, ZigBee, and ZigBee IP.
- View and analyze network traffic.
- Capture and filter network traffic.
- Analyze previously captured network traffic.
- Develop reusable profiles for analyzing and troubleshooting network traffic.
- Interpret the Wireshark graphs and statistical reports.
- Identify and troubleshoot common network problems, including:

  Latency.
  Packet errors.
  Bandwidth performance issues.