Hands-On

Introduction to Troubleshooting IP Services

with WireShark

Course Description

This Hands-On course is geared toward troubleshooting faults in IP services using protocol analyzers on their own for the first time. Its aim is to make them comfortable with using the key functions of a protocol analyzer and then to learn how to systematically locate and find faults.

It will then teach the fundamentals of how IP and Internet Protocol works by using practical analysis of classroom using and Internet simulator to demonstrate the impact of packet loss, delay variation and miss ordering of traffic. Students will then apply their skills to analyze real Internet service traffic over Wireless links.

Attendees will also analyze the protocol exchanges and experiment to identify how failures impact the service, fix the faults and confirm their success by retesting services.

This class can also be customized to add additioanl Hands-On sessions monitoring and troubleshooting live services, upon request.

Students Will Learn

- **Install Wireshark Protocol Analyzer Software**
- **Use Key Functions To Display And Analyze Traffic**
- **Measure Delay, Bandwidth, Jitter And Packet Loss**
- **Analyze Protocol Exchanges Between Different IP Systems**
- **Troubleshoot Addressing And Routing Problems**
- **Build Filters To Locate Particular Protocols And Services**
- **Record And Save Traffic Exchanges For Later Analysis**
- **Recognize Voip, Web Server And Email Traffic By Protocol**
- **Identify Protocols By TCP And UDP Ports**
- **And More...**

Target Audience

This course is aimed at Field Service technicians, Systems Engineers, Systems Specialists, Integrators, Developers, Designers, Customer Support and Systems Delivery Project Engineers who need to troubleshoot IP Internet and IP services for business and domestic users.

Course Outline

Module I: Protocol Analyzers

Functions of protocol analyzers

Selecting an analyzer

WireShark: History and evolution from Ethereal and TCP Dump

Downloading and installing the analyzer hands-on

Configuring the analyzer for field service use

Learning to Capture and save traffic hands-on

Using the analyzer to measure bandwidth and throughput

Hands-on Discovering which protocols are used

Module II: Using WireShark to Analyze Protocols

How Protocols are displayed

Expanding Headers

Arranging the display

Turning on and off functions using preferences

Color coding protocols

Hands-on Exercise configuring Wireshark Display

Hands-on Color coding Key IP Protocols

Module III: Building WireShark Filters

Why we need to filter traffic

Filtering by Protocol

Filtering by Addresses

Filtering by Protocol Fields

Learning to build complex filters for selecting particular traffic

Hands-on Filtering to select particular conversations

Module IV: Analyzing Ethernet Headers

How Ethernet LANs work

Ethernet Addressing

Ether-Type field for recognizing protocols

Recognizing ARP and IP Protocol Packet within Ethernet Frames

Address Resolution Protocol (ARP) tables

Hands-on Analysis of Ethernet LAN Traffic

Hands-on Troubleshooting ARP Tables

Tagged VLAN Traffic

Hands-on Analysis of VLANs

Module V: Analyzing IP Headers

Evolution of IP

IP version 4

IP Type of Service

Differentiated Code Points

IP Length and Fragmentation

Time To Live (TTL) and its impact or reachability

Tracing routes using TTL

Protocol Field

IP Address classes

Recognizing Unicast and Multicast Addresses

Broadcast Addresses

Hands-on Analysis of IP Exchanges

Hands-on Recognizing Packet loss using IP Header

Module VI: Analysing TCP and UDP Traffic

Transmission Control Protocol

Full Associations and Half Associations

Port Numbers and how to find out what they mean

Recognizing a conversations

Using WireShark Graphing functions

Recognizing Packet loss through retransmissions

Segment sizes and their impact

TCP Option field negotiations

TCP Window Field

Hands-on Analysis Application traffic over TCP

UDP Streams

Following UDP Streams

Reconstructing Streams for playback

Hands-on Analysis of Stream Traffic over UDP

Delivery Method

Instructor-Led with Hands-On Labs and numerous exercises.

Equipment Requirements

(This apply's to our hands-on courses only)

BTS always provides equipment to have a very successful Hands-On course. BTS also encourages all attendees to bring their own equipment to the course. This will provide attendees the opportunity to incorporate their own gear into the labs and gain valuable training using their specific equipment.

Course Length

3 Days