Network Protocols and Advanced Data Communication Training Course



26 - 30 Oct 2026

Cairo

3700 € (Per Person)

Ref: #TEL8108_285115

Course Introduction / Overview:

In today's interconnected world, the efficiency and security of data communication networks are paramount to organizational success. This course provides a comprehensive exploration of the principles, protocols, and technologies that form the backbone of modern networking. We delve deep into the intricate layers of the TCP/IP and OSI models, moving beyond theoretical knowledge to practical application and analysis. Participants will gain a robust understanding of how data is encapsulated, transmitted, and received across diverse network infrastructures. Drawing upon foundational concepts established by pioneers like Vint Cerf and detailed in seminal works such as "Computer Networking: A Top-Down Approach" by Kurose and Ross, this program equips professionals with the skills to design, manage, and troubleshoot complex networks. At BIG BEN Training Center, we focus on empowering attendees with the ability to perform in-depth protocol analysis, identify performance bottlenecks, and secure data in transit. This training is meticulously designed to transform your understanding of network communications, enabling you to master the tools and techniques essential for maintaining high-performing and resilient network environments in an era of ever-increasing data demands.

Target Audience / This training course is suitable for:

- Network Engineers and Administrators.
- IT Managers and Team Leaders.
- Systems Engineers.
- Cybersecurity Analysts and Professionals.
- Telecommunications Specialists.
- Network Architects and Designers.
- Technical Support Personnel involved in networking.
- IT professionals seeking to deepen their networking knowledge.

Target Sectors and Industries:

- Information Technology and Services.
- Telecommunications Providers.
- Financial Services and Banking.
- Healthcare and Medical Institutions.
- Governmental and Public Sector Agencies.
- Education and Research Institutions.
- Manufacturing and Industrial Automation.
- Retail and E-commerce.

Target Organizations Departments:

- Information Technology (IT) Department.
- Network Operations Center (NOC).
- Cybersecurity and Information Security.
- Research and Development (R&D).
- Technical Support and Help Desk.
- Infrastructure and Operations.
- Telecommunications Management.

Course Offerings:

By the end of this course, the participants will have able to:

- Analyze the complete TCP/IP protocol suite and the OSI reference model.
- Capture and interpret network traffic using protocol analysis tools like Wireshark.
- Troubleshoot complex network connectivity and performance issues effectively.
- Differentiate between the functions of various routing and switching protocols.
- Understand the intricacies of IPv4 and IPv6 addressing, subnetting, and migration.
- Secure network communications using protocols like IPsec and SSL/TLS.
- Analyze application layer protocols such as HTTP, DNS, and DHCP for anomalies.
- Evaluate network performance and identify potential bottlenecks.
- Implement best practices for designing and managing robust data networks.

Course Methodology:

The training methodology at BIG BEN Training Center is designed to be highly interactive, immersive, and practical, ensuring that participants gain tangible skills they can apply immediately in their professional roles. We move beyond traditional lecture-based formats by integrating a blended learning approach that combines expert-led instruction with extensive hands-on labs. Each theoretical concept is followed by practical exercises where participants will use industry-standard tools to capture, decode, and analyze real-world network traffic. The course heavily emphasizes collaborative learning through group discussions and team-based problem-solving activities, allowing participants to share insights and tackle complex scenarios together. Case studies of major network outages and security breaches will be dissected to understand root causes and preventative measures. Our instructors facilitate a dynamic learning environment, providing continuous feedback and personalized guidance to ensure every participant masters the course objectives. This hands-on, problem-centric approach guarantees a deeper understanding of advanced data communication and protocol analysis, fostering both competence and confidence.

Course Agenda (Course Units):

Unit One: Foundations of Data Communication and Networking

- Introduction to Data Communication and Network Models.
- The OSI Reference Model: A Layer-by-Layer Breakdown.
- The TCP/IP Protocol Suite and its Architecture.
- Physical Layer Concepts: Media, Signals, and Data Encoding.
- Data Link Layer: Framing, Error Detection, and Flow Control.
- Introduction to Protocol Analysis and Packet Sniffing.
- Setting Up and Using Wireshark for Basic Traffic Capture.

Unit Two: Network Layer and Routing Protocols

- Deep Dive into the Internet Protocol (IP): IPv4 and IPv6.
- Understanding IP Addressing, Subnetting, and Super netting.
- Address Resolution Protocol (ARP) and Neighbor Discovery Protocol (NDP).
- Internet Control Message Protocol (ICMP) for Diagnostics.
- Fundamentals of Network Routing: Static vs. Dynamic Routing.
- Analyzing Interior Gateway Protocols: OSPF and EIGRP.
- Exploring the Exterior Gateway Protocol: BGP Fundamentals.

Unit Three: Transport and Application Layer Protocols

- The Role of the Transport Layer: TCP and UDP.
- TCP Three-Way Handshake, Flow Control, and Congestion Avoidance.
- Analyzing TCP Segments and UDP Datagrams.
- Domain Name System (DNS) Operation and Troubleshooting.
- Dynamic Host Configuration Protocol (DHCP) Analysis.
- File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP).
- Hypertext Transfer Protocol (HTTP) and Secure HTTP (HTTPS).

Unit Four: Advanced Networking and Security Protocols

- Voice over IP (VoIP) Technologies: SIP, RTP, and RTCP.
- Wireless LAN (WLAN) Protocols: IEEE 802.11 Standards and Security.
- Wide Area Network (WAN) Technologies and Protocols.
- Introduction to Network Security Concepts.
- Analyzing Security Protocols: SSL/TLS Handshakes.
- IPsec for Virtual Private Networks (VPNs).
- Common Network Attacks and How to Detect Them via Protocol Analysis.

Unit Five: Network Troubleshooting and Performance Analysis

- A Systematic Approach to Network Troubleshooting.
- Using Protocol Analyzers to Isolate Problems.
- Analyzing Real-World Packet Captures for Fault Diagnosis.
- Identifying and Resolving Latency and Throughput Issues.
- Baseline Network Performance and Anomaly Detection.
- Advanced Wireshark Features: Filters, Statistics, and IO Graphs.
- Capstone Project: Analyzing and Troubleshooting a Complex Network Scenario.

FAQ:

Qualifications required for registering to this course?

There are no requirements.

How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

Something to think about:

As network protocols evolve towards greater encryption and privacy (e.g., DNS over HTTPS), how will traditional packet analysis and troubleshooting techniques need to adapt to maintain network visibility and security?

What unique qualities does this course offer compared to other courses?

This course distinguishes itself by moving beyond mere theoretical recitation of protocol standards to a deeply practical, hands-on mastery of network analysis and troubleshooting. While many courses focus on what protocols are, we emphasize why they behave the way they do in real-world, imperfect network environments. Our curriculum is built around a problem-solving ethos, using extensive hands-on labs with industry-standard tools like Wireshark to deconstruct complex network interactions and diagnose challenging issues. Participants do not just learn about the TCP three-way handshake; they analyze captures of failed handshakes to pinpoint the exact cause of a connection failure. The course uniquely integrates performance analysis and security threat detection into every module, teaching attendees to view network traffic through a dual lens of efficiency and resilience. Rather than simply presenting a collection of facts, we cultivate an analytical mindset, empowering professionals to systematically investigate and resolve any network issue, from subtle latency problems to sophisticated security anomalies, making them invaluable assets to their organizations.