CONCEPT

Computer Networking Fundamentals: TCP/IP, Routing, Switching and Troubleshooting

Computer Networking Fundamentals: TCP/IP, Routing, Switching and Troubleshooting

Introduction:

Computer networking fundamentals are often learnt piecemeal, so helpdesk tickets bounce between teams, VLANs and subnets are added without a plan and outages last hours because nobody can read a packet capture. This Core Concept course gives support and junior network staff a working grasp of TCP/IP, IPv4 and IPv6 addressing, switching, routing, core network services and basic security controls, practised in labs every day. Participants finish by producing a Campus Network Build and Troubleshooting Runbook for a routed, multi-VLAN network.

Course Objectives:

- Explain how data moves through the OSI and TCP/IP layers and identify which layer a reported fault belongs to
- Design an IPv4 and IPv6 addressing plan with subnets, private ranges and NAT for a multi-department site
- Configure switches with VLANs, trunks and inter-VLAN routing, and routers with static routes and single-area OSPF
- Set up and verify DHCP, DNS and NAT services so that end devices obtain addresses and resolve names reliably
- Apply ACLs, firewall zones, VPN tunnels and wireless access settings that separate and protect campus traffic
- Diagnose connectivity and performance faults with Wireshark captures and a layered troubleshooting method, and record them in a runbook

Target Audience:

- IT support and helpdesk staff who resolve user connectivity, addressing and name resolution tickets
- Junior network administrators who configure and maintain switches, routers and wireless access points
- OT and automation engineers who connect plant systems to enterprise IP networks
- Systems administrators responsible for servers that depend on DHCP, DNS and routed network access
- Infrastructure technicians who install, patch and document LAN equipment across sites

Course Outline:

Day 1: Network Models, Protocols and Current-State Mapping

- OSI Seven-Layer Model and Protocol Data Units at Each Layer
- RFC 1122 TCP/IP Four-Layer Model and Its Mapping to OSI
- TCP Three-Way Handshake, UDP Datagrams and Port Numbers
- Ethernet Frames, MAC Addresses and ARP Resolution
- Current-State Network Inventory: Topology Diagram, Device List and IP Plan Audit

Day 2: IPv4 and IPv6 Addressing, Subnetting and VLAN Architecture

- RFC 791 IPv4 Header Fields and CIDR Prefix Notation
- Subnetting Worksheet: VLSM Allocation for Departments and Point-to-Point Links
- RFC 1918 Private Blocks and RFC 2663 NAT and PAT Translation
- RFC 8200 IPv6 Addressing with Global Unicast, Link-Local and RFC 4193 Unique Local Prefixes
- IEEE 802.1Q VLAN Tagging, Access and Trunk Ports and the Native VLAN

Day 3: Switching, Routing and Core Network Services Lab

- Lab: Switch Configuration with VLANs, Trunks and Inter-VLAN Routing
- Static and Default Route Configuration with Routing Table Verification
- RFC 2328 OSPFv2 Single-Area Setup: Neighbours, DR and BDR Election and SPF Cost
- DHCP Scopes, Reservations and Relay Agents Across Subnets
- DNS Resolution Path: Resolvers, Record Types and Name Lookup Testing

Day 4: Security Controls, Wireless Access and Campus Design

- IEEE 802.11 Wireless LAN Basics: SSIDs, Channel Planning and Controller-Managed Access Points
- Standard and Extended ACL Design for Inter-VLAN Traffic Filtering
- Stateful Firewall Zones and Site-to-Site and Remote-Access VPN Tunnels
- OSPF Multi-Area Concepts: Backbone Area 0, LSA Types and RFC 5340 OSPFv3 for IPv6
- Three-Tier Campus Hierarchy: Access, Distribution and Core Layer Design

Day 5: Packet Capture Troubleshooting Lab and Runbook

- Wireshark Capture and Display Filters for ARP, DHCP, DNS and TCP Sessions
- Layered Troubleshooting Method with Ping, Traceroute and Interface Counter Checks
- Lab: Fault-Injection Scenario on a Multi-VLAN Routed Campus Network
- Monitoring Baseline Worksheet: Device Logs, Interface Utilisation and Alert Thresholds
- Campus Network Build and Troubleshooting Runbook Presentation and Peer Review

Skills You Will Gain:

- Protocol Layer Fault Isolation
- IP Subnetting and Address Planning
- VLAN and Trunk Configuration
- Static and OSPF Routing
- DHCP and DNS Service Verification
- Access Control List Design
- Packet Capture Analysis
- Network Documentation

Why Attend This Course:

- Leave with a Campus Network Build and Troubleshooting Runbook you can adapt to your own site
- Spend part of every day configuring and testing switches, routers and services instead of only reading about them
- Resolve tickets faster by reading Wireshark captures and knowing which layer to check first
- Compare networking practice with support staff and engineers from offices, plants, hospitals and utilities

Conclusion:

Reliable enterprise networks depend on staff who understand how packets are addressed, switched, routed and filtered, and who can prove where a fault sits. The course moves from the OSI and TCP/IP models, through IPv4 and IPv6 addressing and VLANs, to switching, static and OSPF routing and DHCP and DNS, then wireless, ACLs, firewalls, VPNs and campus design. The final day applies packet capture and a layered method in a fault-injection lab and produces a runbook ready for daily use.