COURSE SYLLABUS

CompTIA Network+ Exam Preparation Course (Self-Paced)

Build the vendor-neutral networking skills the CompTIA Network+ exam covers so you can sit it and apply them on the job.

> Group classes in Live Online and onsite training is available for this course. For more information, email onsite@graduateschool.edu or visit: https://www.graduateschool.edu/courses/network-plus-exam-prep-course-self-paced

support@graduateschool.edu •
(888) 744-4723

Course Outline

Module 1: The OSI Model, Networking Appliances, and Functions

- Lessons:
  - The OSI Reference Model: Seven Layers
  - Physical and Virtual Network Appliances
  - Applications and Functions: CDN, VPN, QoS, and TTL
  - Putting Appliances and Layers Together
- Applied activity: Learners review a short, described small office network and identify which appliance handles a stated function, then identify the OSI layer at which that appliance primarily operates.

Module 2: Cloud Concepts and Evolving Network Use Cases

- Lessons:
  - Cloud Service and Deployment Models
  - Cloud Networking Components: NFV, VPC, Security Groups, and Gateways
  - Software-Defined Networking and SD-WAN
  - Zero Trust Architecture, SASE, and Infrastructure as Code
  - VXLAN and IPv6 Adoption Challenges
- Applied activity: Learners review a short scenario describing an organization adopting cloud services and modernizing its network management and identify which of the concepts covered, cloud service model, SDN, zero trust, SASE, or IaC, addresses each described need.

Module 3: Ports, Protocols, Traffic Types, and IPv4 Addressing

- Lessons:
  - Well-Known Ports and the Protocols Behind Them
  - IP Protocol Types and Traffic Types
  - IPv4 Address Classes and Public versus Private Addressing

- Subnetting with VLSM and CIDR
- Special Addresses: APIPA and Loopback

- Applied activity: Learners review a short scenario describing a small organization's network traffic and addressing plan, identify the protocol and traffic type for several described exchanges, then subnet a provided address block using VLSM to meet the organization's departmental host requirements.

Module 4: Transmission Media, Transceivers, and Network Topologies

- Lessons:
  - Wired and Wireless Transmission Media
  - Transceivers, Form Factors, and Connector Types
  - Network Topologies and Architectures
  - Traffic Flows: North-South and East-West
- Applied activity: Learners review a short scenario describing a data center redesign and select an appropriate topology, explaining how traffic would flow between the described tiers.

Module 5: Routing Technologies

- Lessons:
  - Static versus Dynamic Routing
  - Dynamic Routing Protocols: BGP, EIGRP, and OSPF
  - Route Selection: Administrative Distance, Prefix Length, and Metric
  - Address Translation, FHRP, and Subinterfaces
- Applied activity: Learners review a short scenario describing a router with two possible routes to the same destination and determine which route it selects, based on stated administrative distance and prefix length.

Module 6: Switching Technologies, Features, and Physical Installations

- Lessons:
  - VLANs, Interface Configuration, and 802.1Q Tagging
  - Spanning Tree, Link Aggregation, and MTU
  - Rack and Location Considerations: IDF and MDF
  - Cabling Infrastructure and Power Considerations
  - Environmental Factors and a Combined Implementation Scenario
- Applied activity: Learners review a short scenario describing a new office buildout and design both the VLAN and tagging scheme for its switched network and the rack, cabling, and power provisions its equipment room needs.

Module 7: Wireless Devices and Technologies

- Lessons:
  - Wireless Channels, Frequency Bands, and Regulatory Impacts
  - SSID, BSSID, and ESSID
  - Wireless Network Types and Antennas
  - Encryption, Authentication, and Guest Networks
  - Autonomous versus Lightweight Access Points
- Applied activity: Learners review a short scenario describing a small business wireless deployment and select an appropriate frequency band, encryption standard, and authentication method, explaining the reasoning.

Module 8: Organizational Processes and Procedures

- Lessons:

- Network Documentation: Diagrams, Asset Inventory, and IPAM
- Life-Cycle Management: EOL, EOS, and Decommissioning
- Change Management
- Configuration Management: Production, Backup, and Golden Configurations

- Applied activity: Learners review a short scenario describing an undocumented network and identify which documentation types would most help the next administrator, and why.

Module 9: Network Monitoring Technologies

- Lessons:
  - SNMP: Traps, MIBs, and Versions
  - Flow Data, Packet Capture, and Baseline Metrics
  - Log Aggregation: Syslog and SIEM
  - Monitoring Solutions: Discovery, Traffic Analysis, and Availability
- Applied activity: Learners review a short, described set of monitoring data from multiple sources and identify which monitoring approach, SNMP, flow data, or packet capture, would best confirm a suspected problem.

Module 10: Disaster Recovery Concepts and Network Access and Management Methods

- Lessons:
  - DR Metrics: RPO, RTO, MTTR, and MTBF
  - DR Sites and High-Availability Approaches
  - DR Testing: Tabletop Exercises and Validation
  - VPN Types and Remote Management Methods
  - Jump Boxes and In-Band versus Out-of-Band Management
- Applied activity: Learners review a short scenario describing an organization's recovery requirements and select an appropriate DR site type and VPN approach for its remote offices.

Module 11: IPv4 and IPv6 Network Services: DHCP, DNS, and Time Protocols

- Lessons:
  - DHCP: Scope, Reservations, Lease Time, and Relay
  - DNS Record Types and Zone Concepts
  - DNS Security: DNSSEC, DoH, and DoT
  - Time Protocols: NTP, PTP, and NTS
  - SLAAC for IPv6 Addressing
- Applied activity: Learners review a short scenario describing a new subnet that needs both DHCP and DNS configured and identify the settings each service needs.

Module 12: Basic Network Security Concepts

- Lessons:
  - Logical Security: Encryption, Certificates, and PKI
  - Identity and Access Management: Authentication and Authorization
  - Physical Security and Deception Technologies
  - Common Security Terminology and the CIA Triad
  - Compliance and Network Segmentation for IoT, OT, and BYOD
- Applied activity: Learners review a short scenario describing a network with IoT devices, guest users, and BYOD laptops and design a segmentation approach that isolates each from the production network.

Module 13: Common Network Attacks and Defense Techniques

- Lessons:
  - Denial-of-Service and Layer 2 Attacks: VLAN Hopping and MAC Flooding
  - ARP and DNS Poisoning, Rogue Devices, and Evil Twin
  - On-Path Attacks, Social Engineering, and Malware
  - Device Hardening and Network Access Control
  - Access Control Lists, Content Filtering, and Key Management
  - Security Zones and Building a Defensible Network Design
- Applied activity: Learners review a short, described network design relying on a single perimeter firewall that recently experienced a described attack, identify the attack type, and propose at least two additional defense layers that would have reduced its impact.

Module 14: The Troubleshooting Methodology and Tools

- Lessons:
  - Identifying the Problem and Establishing a Theory
  - Testing the Theory, Planning, and Implementing the Solution
  - Verifying, Documenting, and Following Up
  - Command-Line Tools: ping, traceroute, nslookup, and dig
  - Additional Software and Hardware Tools
  - Basic Device Commands
- Applied activity: Learners are given a short, described network problem and walk through the full troubleshooting methodology, selecting the correct command-line tool, software tool, or device command at each step to gather the information needed.

Module 15: Troubleshooting Cabling and Physical Interface Issues

- Lessons:
  - Common Cable Issues: Incorrect Cable and Signal Degradation
  - Interface Issues: CRC Errors, Runts, Giants, and Port Status
  - Hardware Issues: PoE and Transceiver Mismatches
  - A Guided Walkthrough: Diagnosing a Physical Layer Problem
- Applied activity: Learners review a short, described set of interface counters and port status indicators and identify the most likely physical layer problem.

Module 16: Troubleshooting Network Services and Performance Issues

- Lessons:
  - Switching Issues: STP Loops and Incorrect VLAN Assignment
  - Routing and Addressing Issues
  - A Guided Walkthrough: Diagnosing a Connectivity Problem
  - Congestion, Bottlenecking, and Bandwidth
  - Latency, Packet Loss, Jitter, and Wireless Performance Issues
- Applied activity: Learners review a short, described connectivity and performance complaint along with basic diagnostic details and identify whether the cause is a switching, routing, addressing, or performance issue.