

CompTIA Network+

Duration: 5 Days

Course Description:

CompTIA Network+ is the premier certification for validating your knowledge of essential networking tools and concepts. You will be assessed on your abilities in network connectivity, documentation, service configuration, data centers, cloud, virtual networking, monitoring, troubleshooting, and security hardening. This certification prepares you for jobs in technical support, network operation, and system administration.

Target Audience:

If you are beginning or advancing your career in networking, Network+ is valuable for roles such as network administrator, network field technician, help desk technician, and IT consultant.

Prerequisites:

CompTIA A+ certification, with 9 to 12 months of hands-on experience in a junior network administrator or network support technician role.

Course Objectives:

Build skills with CompTIA learning and validate them with Network+ certification.

- Deploy wired and wireless devices, covering IP addressing, ports, protocols, and network architecture for network deployment.
- Understand documentation, life-cycle, change, and configuration management processes and procedures.
- Grasp virtualization, cloud service models, elasticity, and scalability to apply cloud concepts.
- Monitor networks for high availability and resolve connectivity issues to maintain network performance.
- Establish secure networks and mitigate vulnerabilities to strengthen security.
- Diagnose and resolve network issues using appropriate tools for effective troubleshooting.

Course Outlines:

Networking concepts

- **OSI model layers:** physical, data link, network, transport, session, presentation, application.
- **Networking appliances:** routers, switches, firewalls, IDS/IPS, load balancers, proxies, NAS, SAN, and wireless devices.
- **Cloud concepts:** NFV, VPC, network security groups, cloud gateways, deployment models (public, private, hybrid), service models (SaaS, IaaS, PaaS).
- **Ports and protocols:** FTP, SFTP, SSH, Telnet, SMTP, DNS, DHCP, HTTP, HTTPS, SNMP, LDAP, RDP, SIP.
- **Traffic types:** unicast, multicast, anycast, broadcast.
- **Transmission media:** wireless (802.11, cellular, satellite), wired (fiber, coaxial, DAC).
- **Transceivers and connectors:** SC, LC, ST, MPO, RJ11, RJ45, F-type, BNC.
- **Network topologies:** mesh, hybrid, star/hub and spoke, spine and leaf, point-to-point, three-tier, and collapsed core.
- **IPv4 addressing:** public vs. private, APIPA, RFC1918, loopback, subnetting (VLSM, CIDR), and address classes (A, B, C, D, E).

Network implementation

- **Routing technologies:** static and dynamic routing (BGP, EIGRP, OSPF), route selection, NAT, PAT, FHRP, VIP, and subinterfaces.
- **Switching technologies:** VLANs, interface configuration, spanning tree, MTU, and jumbo frames.
- **Wireless devices:** channels, frequency options, SSID, network types, encryption, guest networks, authentication, antennas, and access points.
- **Physical installations:** installation implications, power considerations, and environmental factors.

Network operations

- **Documentation:** physical vs. logical diagrams, rack diagrams, cable maps, network diagrams, asset inventory, IPAM, SLA, and wireless surveys.
- **Life-cycle management:** EOL, EOS, software management, and decommissioning.
- **Change management:** request process tracking.
- **Configuration management:** production, backup, baseline configurations.
- **Network monitoring:** SNMP, flow data, packet capture, baseline metrics, log aggregation, API integration, and port mirroring.
- **Disaster recovery:** RPO, RTO, MTTR, MTBF, cold/warm/hot sites, active-active/passive, and testing.
- **Network services:** DHCP, SLAAC, DNS, NTP, PTP, and NTS.
- **Access and management:** VPNs, SSH, GUI, API, and console.

Network security

- **Logical security:** encryption (data in transit/rest), PKI, IAM, MFA, SSO, RADIUS, LDAP, SAML, TACACS+, time-based authentication, authorization, least privilege, role-based access control, and geofencing.
- **Physical security:** cameras and locks.
- **Deception technologies:** honeypot and honeynet.
- **Security terminology:** risk, vulnerability, exploit, threat, and CIA triad.
- **Audits and compliance:** data locality, PCI DSS, and GDPR.
- **Network segmentation:** IoT, IIoT, SCADA, ICS, OT, guest, and BYOD.
- **Types of attacks:** DoS/DDoS, VLAN hopping, MAC flooding, ARP poisoning/spoofing, DNS poisoning/spoofing, rogue devices/services, evil twin, on-path attack, and social engineering (phishing, dumpster diving, shoulder surfing, tailgating).
- **Security features and defense:** device hardening, NAC, key management, ACL, URL/content filtering, trusted vs. untrusted zones, and screened subnet.

Network troubleshooting

- **Troubleshooting methodology:** identifying the problem, establishing a theory, testing, planning, and implementing a solution, verifying functionality, and documenting findings.
- **Cabling and physical interface issues:** cable issues (incorrect type, signal degradation, improper termination, TX/RX transposed), interface issues (increasing counters, port status), and hardware issues (PoE, transceiver mismatch, signal strength).
- **Network services issues:** switching issues (STP, VLAN assignment, ACLs), routing issues (routing table and default routes), address pool exhaustion, and incorrect gateway/IP/subnet mask.
- **Performance issues:** congestion, latency, packet loss, and wireless interference.
- **Tools and protocols:** protocol analyzers, command line tools, cable testers, and Wi-Fi analyzers.

REGISTER NOW!

training@trends.com.ph
 (+632) 8863-2123
 www.trendssacademy.com.ph