CT-Network+

CompTIA Network+

5 Days Course • Instructor Led Training

Course Objectives

CompTIA Network+ validates the technical skills needed to securely establish, maintain and troubleshoot the essential networks that businesses rely on. Unlike other vendor-specific networking certifications, CompTIA Network+ prepares candidates to support networks on any platform. CompTIA Network+ is the only certification that covers the specific skills that network professionals need. Other certifications are so broad, they don't cover the hands-on skills and precise knowledge needed in today's networking environments. CompTIA Network+ features flexible training options including self-paced learning, live online training, custom training and labs to advance the career development of IT professionals in network administration.

1.0 Networking Fundamentals

1.1 Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.

- **OSI model**
  - Layer 1 – Physical
  - Layer 2 – Data link
  - Layer 3 – Network
  - Layer 4 – Transport
  - Layer 5 – Session
  - Layer 6 – Presentation
  - Layer 7 – Application
- **Data encapsulation and decapsulation within the OSI model context**
  - Ethernet header
  - Internet Protocol (IP) header
  - Transmission Control Protocol (TCP)/ User Datagram Protocol (UDP) headers
  - TCP flags
  - Payload
  - Maximum transmission unit (MTU)

1.2 Explain the characteristics of network topologies and network types.

- **Mesh**
- **Star/hub-and-spoke**
- **Bus**
- **Ring**
- **Hybrid**
- **Network types and characteristics**
  - Peer-to-peer
  - Client-server
  - Local area network (LAN)
  - Metropolitan area network (MAN)
  - Wide area network (WAN)
  - Wireless local area network (WLAN)
  - Personal area network (PAN)
  - Campus area network (CAN)
  - Storage area network (SAN)
  - Software-defined wide area network (SDWAN)
  - Multiprotocol label switching (MPLS)
  - Multipoint generic routing encapsulation (mGRE)
- **Service-related entry point**
  - Demarcation point
  - Smartjack
- **Virtual network concepts**
  - vSwitch
  - Virtual network interface card (vNIC)
  - Network function virtualization (NFV)
  - Hypervisor
- **Provider links**
  - Satellite
  - Digital subscriber line (DSL)
  - Cable
  - Leased line
  - Metro-optical

1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution.

- **Copper**
  - Twisted pair
    - Cat 5
    - Cat 5e
    - Cat 6
    - Cat 6a
    - Cat 7
    - Cat 8
  - Coaxial/RG-6
  - Twinaxial
  - Termination standards
    - TIA/EIA-568A
    - TIA/EIA-568B
- **Fiber**
  - Single-mode
  - Multimode
- **Connector types**
  - Local connector (LC), straight tip (ST), subscriber connector (SC), mechanical transfer (MT), registered jack (RJ)
    - Angled physical contact (APC)
    - Ultra-physical contact (UPC)
  - RJ11
  - RJ45
  - F-type connector
  - Transceivers/media converters
  - Transceiver type
    - Small form-factor pluggable (SFP)
    - Enhanced form-factor pluggable (SFP+)
    - Quad small form-factor pluggable (QSFP)
    - Enhanced quad small form-factor pluggable (QSFP+)
- **Cable management**
  - Patch panel/patch bay
  - Fiber distribution panel
  - Punchdown block
    - 66
    - 110
    - Krone
    - Bix
- **Ethernet standards**
  - Copper
    - 10BASE-T
    - 100BASE-TX
    - 1000BASE-T
    - 10GBASE-T
    - 40GBASE-T
  - Fiber
    - 100BASE-FX
    - 100BASE-SX
    - 1000BASE-SX
    - 1000BASE-LX
    - 10GBASE-SR
    - 10GBASE-LR
    - Coarse wavelength division multiplexing (CWDM)
    - Dense wavelength division multiplexing (DWDM)
    - Bidirectional wavelength division multiplexing (WDM)

1.4 Given a scenario, configure a subnet and use appropriate IP addressing schemes.

- **Public vs. private**
  - RFC1918
  - Network address translation (NAT)
  - Port address translation (PAT)
- **IPv4 vs. IPv6**
  - Automatic Private IP Addressing (APIPA)
  - Extended unique identifier (EUI-64)
  - Multicast
  - Unicast
  - Anycast
  - Broadcast
  - Link local
  - Loopback
  - Default gateway
- **IPv4 subnetting**
  - Classless (variable-length subnet mask)
  - Classful
    - A
    - B
    - C
    - D
    - E
  - Classless Inter-Domain Routing (CIDR) notation
- **IPv6 concepts**
  - Tunneling
  - Dual stack
  - Shorthand notation
  - Router advertisement
  - Stateless address autoconfiguration (SLAAC)
- **Virtual IP (VIP)**
- **Subinterfaces**

1.5 Explain common ports and protocols, their application, and encrypted alternatives.

Protocols	Ports
File Transfer Protocol (FTP)	20/21
Secure Shell (SSH)	22
Secure File Transfer Protocol (SFTP)	22
Telnet	23
Simple Mail Transfer Protocol (SMTP)	25
Domain Name System (DNS)	53
Dynamic Host Configuration Protocol (DHCP)	67/68
Trivial File Transfer Protocol (TFTP)	69
Hypertext Transfer Protocol (HTTP)	80
Post Office Protocol v3 (POP3)	110
Network Time Protocol (NTP)	123
Internet Message Access Protocol (IMAP)	143
Simple Network Management Protocol (SNMP)	161/162
Lightweight Directory Access Protocol (LDAP)	389
Hypertext Transfer Protocol Secure (HTTPS) [Secure Sockets Layer (SSL)]	443
HTTPS [Transport Layer Security (TLS)]	443
Server Message Block (SMB)	445
Syslog	514
SMTP TLS	587
Lightweight Directory Access Protocol (over SSL) (LDAPS)	636
IMAP over SSL	993
POP3 over SSL	995
Structured Query Language (SQL) Server	1433
SQLnet	1521
MySQL	3306
Remote Desktop Protocol (RDP)	3389
Session Initiation Protocol (SIP)	5060/5061
IP protocol types	
- Internet Control Message Protocol (ICMP)	
- TCP	
- UDP	
- Generic Routing Encapsulation (GRE)	
- Internet Protocol Security (IPSec)	
- Authentication Header (AH)/Encapsulating Security Payload (ESP)	
Connectionless vs. connection-oriented	

1.6 Explain the use and purpose of network services.

- **DHCP**
  - Scope
  - Exclusion ranges
  - Reservation
  - Dynamic assignment
  - Static assignment
  - Lease time
  - Scope options
  - Available leases
  - DHCP relay
  - IP helper/UDP forwarding
- **DNS**
  - Record types
    - Address (A vs. AAAA)
    - Canonical name (CNAME)
    - Mail exchange (MX)
    - Start of authority (SOA)
    - Pointer (PTR)
    - Text (TXT)
    - Service (SRV)
    - Name server (NS)
  - Global hierarchy
    - Root DNS servers
  - Internal vs. external
  - Zone transfers
  - Authoritative name servers
  - Time to live (TTL)
  - DNS caching
  - Reverse DNS/reverse lookup/forward lookup
  - Recursive lookup/iterative lookup
- **NTP**
  - Stratum
  - Clients
  - Servers

1.7 Explain basic corporate and datacenter network architecture.

- **Three-tiered**
  - Core
  - Distribution/aggregation layer
  - Access/edge
- **Software-defined networking**
  - Application layer
  - Control layer
  - Infrastructure layer
  - Management plane
- **Spine and leaf**
  - Software-defined network
  - Top-of-rack switching
  - Backbone
- **Traffic flows**
  - North-South
  - East-West
- **Branch office vs. on-premises datacenter vs. colocation**
- **Storage area networks**
  - Connection types
    - Fibre Channel over Ethernet (FCoE)
    - Fibre Channel
    - Internet Small Computer Systems Interface (iSCSI)

1.8 Summarize cloud concepts and connectivity options.

- **Deployment models**
  - Public
  - Private
  - Hybrid
  - Community
- **Service models**
  - Software as a service (SaaS)
  - Infrastructure as a service (IaaS)
  - Platform as a service (PaaS)
  - Desktop as a service (DaaS)
- **Infrastructure as code**
  - Automation/orchestration
- **Connectivity options**
  - Virtual private network (VPN)
  - Private-direct connection to cloud provider
- **Multitenancy**
- **Elasticity**
- **Scalability**
- **Security implications**

2.0 Network Implementations

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.

- **Networking devices**
  - Layer 2 switch
  - Layer 3 capable switch
  - Router
  - Hub
  - Access point
  - Bridge
  - Wireless LAN controller
  - Load balancer
  - Proxy server
  - Cable modem
  - DSL modem
  - Repeater
  - Voice gateway
  - Media converter
  - Intrusion prevention system (IPS)/intrusion detection system (IDS) device
  - Firewall
  - VPN headend
- **Networked devices**
  - Voice over Internet Protocol (VoIP) phone
  - Printer
  - Physical access control devices
  - Cameras
  - Heating, ventilation, and air conditioning (HVAC) sensors
  - Internet of Things (IoT)
    - Refrigerator
    - Smart speakers
    - Smart thermostats
    - Smart doorbells
  - Industrial control systems/ supervisory control and data acquisition (SCADA)

2.2 Compare and contrast routing technologies and bandwidth management concepts.

- **Routing**
  - Dynamic routing
    - Protocols [Routing Internet Protocol (RIP), Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Border Gateway Protocol (BGP)]
    - Link state vs. distance vector vs. hybrid
  - Static routing
  - Default route
  - Administrative distance
  - Exterior vs. interior
  - Time to live
- **Bandwidth management**
  - Traffic shaping
  - Quality of service (QoS)

2.3 Given a scenario, configure and deploy common Ethernet switching features.

- Data virtual local area network (VLAN)
- Voice VLAN
- Port configurations
  - Port tagging/802.1Q
  - Port aggregation
    - Link Aggregation Control Protocol (LACP)
  - Duplex
  - Speed
  - Flow control
  - Port mirroring
  - Port security
  - Jumbo frames
  - Auto-medium-dependent interface crossover (MDI-X)
- Media access control (MAC) address tables
- Power over Ethernet (PoE)/ Power over Ethernet plus (PoE+)
- Spanning Tree Protocol
- Carrier-sense multiple access with collision detection (CSMA/CD)
- **Address Resolution Protocol (ARP)**
- **Neighbor Discovery Protocol**

2.4 Given a scenario, install and configure the appropriate wireless standards and technologies.

- **802.11 standards**
  - a
  - b
  - g
  - n (WiFi 4)
  - ac (WiFi 5)
  - ax (WiFi 6)
- **Frequencies and range**
  - 2.4GHz
  - 5GHz
- **Channels**
  - Regulatory impacts
- **Channel bonding**
- **Service set identifier (SSID)**
  - Basic service set
  - Extended service set
  - Independent basic service set (Ad-hoc)
  - Roaming
- **Antenna types**
  - Omni
  - Directional
- **Encryption standards**
  - WiFi Protected Access (WPA)/ WPA2 Personal [Advanced Encryption Standard (AES)/ Temporal Key Integrity Protocol (TKIP)]
  - WPA/WPA2 Enterprise (AES/TKIP)
- **Cellular technologies**
  - Code-division multiple access (CDMA)
  - Global System for Mobile Communications (GSM)
  - Long-Term Evolution (LTE)
  - 3G, 4G, 5G
- **Multiple input, multiple output (MIMO) and multi-user MIMO (MU-MIMO)**

3.0 Network Operations

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.

- **Performance metrics/sensors**
  - Device/chassis
    - Temperature
    - Central processing unit (CPU) usage
    - Memory
  - Network metrics
    - Bandwidth
    - Latency
    - Jitter
- **SNMP**
  - Traps
  - Object identifiers (OIDs)
  - Management information bases (MIBs)
- **Network device logs**
  - Log reviews
    - Traffic logs
    - Audit logs
    - Syslog
  - Logging levels/severity levels
- **Interface statistics/status**
  - Link state (up/down)
  - Speed/duplex
  - Send/receive traffic
  - Cyclic redundancy checks (CRCs)
  - Protocol packet and byte counts
- **Interface errors or alerts**
  - CRC errors
  - Giants
  - Runts
  - Encapsulation errors
- **Environmental factors and sensors**
  - Temperature
  - Humidity
  - Electrical
  - Flooding
- **Baselines**
- **NetFlow data**
- **Uptime/downtime**

3.2 Explain the purpose of organizational documents and policies.

- **Plans and procedures**
  - Change management
  - Incident response plan
  - Disaster recovery plan
  - Business continuity plan
  - System life cycle
  - Standard operating procedures
- **Hardening and security policies**
  - Password policy
  - Acceptable use policy
  - Bring your own device (BYOD) policy
  - Remote access policy
  - Onboarding and offboarding policy
  - Security policy
  - Data loss prevention
- **Common documentation**
  - Physical network diagram
    - Floor plan
    - Rack diagram
    - Intermediate distribution frame (IDF)/main distribution frame (MDF) documentation
  - Logical network diagram
  - Wiring diagram
  - Site survey report
  - Audit and assessment report
  - Baseline configurations
- **Common agreements**
  - Non-disclosure agreement (NDA)
  - Service-level agreement (SLA)
  - Memorandum of understanding (MOU)

3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.

- **Load balancing**
- **Multipathing**
- **Network interface card (NIC) teaming**
- **Redundant hardware/clusters**
  - Switches
  - Routers
  - Firewalls
- **Facilities and infrastructure support**
  - Uninterruptible power supply (UPS)
  - Power distribution units (PDUs)
  - Generator
  - HVAC
  - Fire suppression
- **Redundancy and high availability (HA) concepts**
  - Cold site
  - Warm site
  - Hot site
  - Cloud site
  - Active-active vs. active-passive
    - Multiple Internet service providers (ISPs)/diverse paths
    - Virtual Router Redundancy Protocol (VRRP)/First Hop Redundancy Protocol (FHRP)
  - Mean time to repair (MTTR)
  - Mean time between failure (MTBF)
  - Recovery time objective (RTO)
  - Recovery point objective (RPO)
- **Network device backup/restore**
  - State
  - Configuration

4.0 Network Security

4.1 Explain common security concepts.

- **Confidentiality, integrity, availability (CIA)**
- **Threats**
  - Internal
  - External
- **Vulnerabilities**
  - Common vulnerabilities and exposures (CVE)
  - Zero-day
- **Exploits**
- **Least privilege**
- **Role-based access**
- **Zero Trust**
- **Defense in depth**
  - Network segmentation enforcement
  - Screened subnet [previously known as demilitarized zone (DMZ)]
  - Separation of duties
  - Network access control
  - Honeypot
- **Authentication methods**
  - Multifactor
  - Terminal Access Controller Access-Control System Plus (TACACS+)
  - Single sign-on (SSO)
  - Remote Authentication Dial-in User Service (RADIUS)
  - LDAP
  - Kerberos
  - Local authentication
  - 802.1X
  - Extensible Authentication Protocol (EAP)
- **Risk Management**
  - Security risk assessments
    - Threat assessment
    - Vulnerability assessment
    - Penetration testing
    - Posture assessment
  - Business risk assessments
    - Process assessment
    - Vendor assessment
- **Security information and event management (SIEM)**

4.2 Compare and contrast common types of attacks.

- **Technology-based**
  - Denial-of-service (DoS)/ distributed denial-of-service (DDoS)
    - Botnet/command and control
  - On-path attack (previously known as man-in-the-middle attack)
  - DNS poisoning
  - VLAN hopping
  - ARP spoofing
  - Rogue DHCP
  - Rogue access point (AP)
  - Evil twin
  - Ransomware
  - Password attacks
    - Brute-force
    - Dictionary
  - MAC spoofing
  - IP spoofing
  - Deauthentication
  - Malware
- **Human and environmental**
  - Social engineering
    - Phishing
    - Tailgating
    - Piggybacking
    - Shoulder surfing

4.3 Given a scenario, apply network hardening techniques.

- **Best practices**
  - Secure SNMP
  - Router Advertisement (RA) Guard
  - Port security
  - Dynamic ARP inspection
  - Control plane policing
  - Private VLANs
  - Disable unneeded switchports
  - Disable unneeded network services
  - Change default passwords
  - Password complexity/length
  - Enable DHCP snooping
  - Change default VLAN
  - Patch and firmware management
  - Access control list
  - Role-based access
  - Firewall rules
    - Explicit deny
    - Implicit deny
- **Wireless security**
  - MAC filtering
  - Antenna placement
  - Power levels
  - Wireless client isolation
  - Guest network isolation
  - Preshared keys (PSKs)
  - EAP
  - Geofencing
  - Captive portal
- **IoT access considerations**

4.4 Compare and contrast remote access methods and security implications.

- **Site-to-site VPN**
- **Client-to-site VPN**
  - Clientless VPN
  - Split tunnel vs. full tunnel
- **Remote desktop connection**
- **Remote desktop gateway**
- **SSH**
- **Virtual network computing (VNC)**
- **Virtual desktop**
- **Authentication and authorization considerations**
- **In-band vs. out-of-band management**

4.5 Explain the importance of physical security.

- **Detection methods**
  - Camera
  - Motion detection
  - Asset tags
  - Tamper detection
- **Prevention methods**
  - Employee training
  - Access control hardware
    - Badge readers
    - Biometrics
  - Locking racks
  - Locking cabinets
  - Access control vestibule (previously known as a mantrap)
  - Smart lockers
- **Asset disposal**
  - Factory reset/wipe configuration
  - Sanitize devices for disposal

5.0 Network Troubleshooting

5.1 Explain the network troubleshooting methodology.

- **Identify the problem**
  - Gather information
  - Question users
  - Identify symptoms
  - Determine if anything has changed
  - Duplicate the problem, if possible
  - Approach multiple problems individually
- **Establish a theory of probable cause**
  - Question the obvious
  - Consider multiple approaches
    - Top-to-bottom/ bottom-to-top OSI model
    - Divide and conquer
- **Test the theory to determine the cause**
  - If the theory is confirmed, determine the next steps to resolve the problem
  - If the theory is not confirmed, reestablish a new theory or escalate
- **Establish a plan of action to resolve the problem and identify potential effects**
- **Implement the solution or escalate as necessary**
- **Verify full system functionality and, if applicable, implement preventive measures**
- **Document findings, actions, outcomes, and lessons learned**

5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

- **Specifications and limitations**
  - Throughput
  - Speed
  - Distance
- **Cable considerations**
  - Shielded and unshielded
  - Plenum and riser-rated
- **Cable application**
  - Rollover cable/console cable
  - Crossover cable
  - Power over Ethernet
- **Common issues**
  - Attenuation
  - Interference
  - Decibel (dB) loss
  - Incorrect pinout
  - Bad ports
  - Open/short
  - Light-emitting diode (LED) status indicators
  - Incorrect transceivers
  - Duplexing issues
  - Transmit and receive (TX/RX) reversed
  - Dirty optical cables
- **Common tools**
  - Cable crimper
  - Punchdown tool
  - Tone generator
  - Loopback adapter
  - Optical time-domain reflectometer (OTDR)
  - Multimeter
  - Cable tester
  - Wire map
  - Tap
  - Fusion splicers
  - Spectrum analyzers
  - Snips/cutters
  - Cable stripper
  - Fiber light meter

5.3 Given a scenario, use the appropriate network software tools and commands.

- **Software tools**
  - WiFi analyzer
  - Protocol analyzer/packet capture
  - Bandwidth speed tester
  - Port scanner
  - iperf
  - NetFlow analyzers
  - Trivial File Transfer Protocol (TFTP) server
  - Terminal emulator
  - IP scanner
- **Command line tool**
  - ping
  - ipconfig/ifconfig/ip
  - nslookup/dig
  - traceroute/tracert
  - arp
  - netstat
  - hostname
  - route
  - telnet
  - tcpdump
  - nmap
- **Basic network platform commands**
  - show interface
  - show config
  - show route

5.4 Given a scenario, troubleshoot common wireless connectivity issues.

- **Specifications and limitations**
  - Throughput
  - Speed
  - Distance
  - Received signal strength indication (RSSI) signal strength
  - Effective isotropic radiated power (EIRP)/power settings
- **Considerations**
  - Antennas
    - Placement
    - Type
    - Polarization
  - Channel utilization
  - AP association time
  - Site survey
- **Common issues**
  - Interference
    - Channel overlap
  - Antenna cable attenuation/signal loss
  - RF attenuation/signal loss
  - Wrong SSID
  - Incorrect passphrase
  - Encryption protocol mismatch
  - Insufficient wireless coverage
  - Captive portal issues
  - Client disassociation issues

5.5 Given a scenario, troubleshoot general networking issues.

- **Considerations**
  - Device configuration review
  - Routing tables
  - Interface status
  - VLAN assignment
  - Network performance baselines
- **Common issues**
  - Collisions
  - Broadcast storm
  - Duplicate MAC address
  - Duplicate IP address
  - Multicast flooding
  - Asymmetrical routing
  - Switching loops
  - Routing loops
  - Rogue DHCP server
  - DHCP scope exhaustion
  - IP setting issues
    - Incorrect gateway
    - Incorrect subnet mask
    - Incorrect IP address
    - Incorrect DNS
  - Missing route
  - Low optical link budget
  - Certificate issues
  - Hardware failure
  - Host-based/network-based firewall settings
  - Blocked services, ports, or addresses
  - Incorrect VLAN
  - DNS issues
  - NTP issues
  - BYOD challenges
  - Licensed feature issues
  - Network performance issues