CompTIA Network+ Certification Exam Objectives

EXAM NUMBER: N10-007

About the Exam

The CompTIA Network+ certification is an internationally recognized validation of the technical knowledge required of foundation-level IT network practitioners.

This exam will certify the successful candidate has the knowledge and skills required to:

- **Troubleshoot, configure and manage common network devices**
- **Establish basic network connectivity**
- **Understand and maintain network documentation**
- **Identify network limitations and weaknesses**
- **Implement network security, standards, and protocols**

The candidate will have a basic understanding of enterprise technologies, including cloud and virtualization technologies.

CompTIA Network+ is accredited by ANSI to show compliance with the ISO 17024 Standard and, as such, the exam objectives undergo regular reviews and updates.

CompTIA Network+ candidates are recommended to have the following:

- **CompTIA A+ certification or equivalent knowledge**
- **At least 9 to 12 months of work experience in IT networking**

EXAM ACCREDITATION

The CompTIA Network+ exam is accredited by ANSI to show compliance with the ISO 17024 standard

and, as such, undergoes regular reviews and updates to the exam objectives.

EXAM DEVELOPMENT

CompTIA exams result from subject-matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an entry-level IT professional.

CompTIA AUTHORIZED MATERIALS USE POLICY

CompTIA Certifications, LLC is not affiliated with and does not authorize, endorse or condone utilizing any content provided by unauthorized third-party training sites (aka "brain dumps"). Individuals who utilize such materials in preparation for any CompTIA examination will have their certifications revoked and be suspended from future testing in accordance with the CompTIA Candidate Agreement. In an effort to more clearly communicate CompTIA's exam policies on use of unauthorized study materials, CompTIA directs all certification candidates to the **CompTIA Certification Exam Policies**. Please review all CompTIA policies before beginning the study process for any CompTIA exam. Candidates will be required to abide by the **CompTIA Candidate Agreement**. If a candidate has a question as to whether study materials are considered unauthorized (aka "brain dumps"), he/she should contact CompTIA at examsecurity@comptia.org to confirm.

PLEASE NOTE

The lists of examples provided in bulleted format are not exhaustive lists. Other examples of technologies, processes or tasks pertaining to each objective may also be included on the exam although not listed or covered in this objectives document. CompTIA is constantly reviewing the content of our exams and updating test questions to be sure our exams are current and the security of the questions is protected. When necessary, we will publish updated exams based on existing exam objectives. Please know that all related exam preparation materials will still be valid.

TEST DETAILS

Required exam	N10-007
Number of questions	Maximum of 90
Types of questions	Multiple choice and performance-based
Length of test	90 minutes
Recommended experience	• CompTIA A+ certified, or equivalent • Minimum of nine months of experience in network support or administration; or academic training
Passing score	720 (on a scale of 100—900)

EXAM OBJECTIVES (DOMAINS)

The table below lists the domains measured by this examination and the extent to which they are represented:

DOMAIN	PERCENTAGE OF EXAMINATION
1.0 Networking Concepts	23%
2.0 Infrastructure	18%
3.0 Network Operations	17%
4.0 Network Security	20%
5.0 Network Troubleshooting and Tools	22%
Total	**100%**

1.0 Networking Concepts

1.1 Explain the purposes and uses of ports and protocols.

- **Protocols and ports**
  - SSH 22
  - DNS 53
  - SMTP 25
  - SFTP 22
  - FTP 20, 21
  - TFTP 69
  - TELNET 23
  - DHCP 67, 68
  - HTTP 80
  - HTTPS 443
  - SNMP 161
  - RDP 3389
  - NTP 123
  - SIP 5060, 5061
  - SMB 445
  - POP 110
  - IMAP 143
  - LDAP 389
  - LDAPS 636
  - H.323 1720
- **Protocol types**
  - ICMP
  - UDP
  - TCP
  - IP
- **Connection-oriented vs. connectionless**

1.2 Explain devices, applications, protocols and services at their appropriate OSI layers.

- **Layer 1 – Physical**
- **Layer 2 – Data link**
- **Layer 3 – Network**
- **Layer 4 – Transport**
- **Layer 5 – Session**
- **Layer 6 – Presentation**
- **Layer 7 – Application**

1.3 Explain the concepts and characteristics of routing and switching.

- **Properties of network traffic**
  - Broadcast domains
  - CSMA/CD
  - CSMA/CA
  - Collision domains
  - Protocol data units
  - MTU
  - Broadcast
  - Multicast
  - Unicast
- **Segmentation and interface properties**
  - VLANs
  - Trunking (802.1q)
  - Tagging and untagging ports
  - Port mirroring
  - Switching loops/spanning tree
  - PoE and PoE+ (802.3af, 802.3at)
  - DMZ
  - MAC address table
  - ARP table
- **Routing**
  - Routing protocols (IPv4 and IPv6)
    - Distance-vector routing protocols
      - RIP
      - EIGRP
    - Link-state routing protocols
      - OSPF
    - Hybrid
      - BGP
  - Routing types
    - Static
    - Dynamic
    - Default
- **IPv6 concepts**
  - Addressing
  - Tunneling
  - Dual stack
  - Router advertisement
  - Neighbor discovery
- **Performance concepts**
  - Traffic shaping
  - QoS
  - Diffserv
  - CoS
- **NAT/PAT**
- **Port forwarding**
- **Access control list**
- **Distributed switching**
- **Packet-switched vs. circuit-switched network**
- **Software-defined networking**

1.4 Given a scenario, configure the appropriate IP addressing components.

- Private vs. public
- Loopback and reserved
- Default gateway
- Virtual IP
- Subnet mask
- Subnetting
  - Classful
    - Classes A, B, C, D, and E
  - Classless
    - VLSM
    - CIDR notation (IPv4 vs. IPv6)
- Address assignments
  - DHCP
  - DHCPv6
  - Static
  - APIPA
  - EUI64
  - IP reservations

1.5 Compare and contrast the characteristics of network topologies, types and technologies.

- Wired topologies
  - Logical vs. physical
  - Star
  - Ring
  - Mesh
  - Bus
- Wireless topologies
  - Mesh
  - Ad hoc
  - Infrastructure
- Types
  - LAN
  - WLAN
  - MAN
  - WAN
  - CAN
  - SAN
  - PAN
- Technologies that facilitate the Internet of Things (IoT)
  - Z-Wave
  - Ant+
  - Bluetooth
  - NFC
  - IR
  - RFID
  - 802.11

1.6 Given a scenario, implement the appropriate wireless technologies and configurations.

- 802.11 standards
  - a
  - b
  - g
  - n
  - ac
- Cellular
  - GSM
  - TDMA
  - CDMA
- Frequencies
  - 2.4GHz
  - 5.0GHz
- Speed and distance requirements
- Channel bandwidth
- Channel bonding
- MIMO/MU-MIMO
- Unidirectional/omnidirectional
- Site surveys

1.7 Summarize cloud concepts and their purposes.

- **Types of services**
  - SaaS
  - PaaS
  - IaaS
- **Cloud delivery models**
  - Private
  - Public
  - Hybrid
- **Connectivity methods**
- **Security implications/considerations**
- **Relationship between local and cloud resources**

1.8 Explain the functions of network services.

- **DNS service**
  - Record types
    - A, AAAA
    - TXT (SPF, DKIM)
    - SRV
    - MX
    - CNAME
    - NS
    - PTR
  - Internal vs. external DNS
  - Third-party/cloud-hosted DNS
  - Hierarchy
  - Forward vs. reverse zone
- **DHCP service**
  - MAC reservations
  - Pools
  - IP exclusions
  - Scope options
  - Lease time
  - TTL
  - DHCP relay/IP helper
- **NTP**
- **IPAM**

2.0 Infrastructure

2.1 Given a scenario, deploy the appropriate cabling solution.

- **Media types**
  - Copper
    - UTP
    - STP
    - Coaxial
  - Fiber
    - Single-mode
    - Multimode
- **Plenum vs. PVC**
- **Connector types**
  - Copper
    - RJ-45
    - RJ-11
    - BNC
    - DB-9
    - DB-25
    - F-type
  - Fiber
    - LC
    - ST
    - SC
      - APC
      - UPC
    - MTRJ
- **Transceivers**
  - SFP
  - GBIC
  - SFP+
  - QSFP
  - Characteristics of fiber transceivers
    - Bidirectional
    - Duplex
- **Termination points**
  - 66 block
  - 110 block
  - Patch panel
  - Fiber distribution panel
- **Copper cable standards**
  - Cat 3
  - Cat 5
  - Cat 5e
  - Cat 6
  - Cat 6a
  - Cat 7
  - RG-6
  - RG-59
- **Copper termination standards**
  - TIA/EIA 568a
  - TIA/EIA 568b
  - Crossover
  - Straight-through
- **Ethernet deployment standards**
  - 100BaseT
  - 1000BaseT
  - 1000BaseLX
  - 1000BaseSX
  - 10GBaseT

2.2 Given a scenario, determine the appropriate placement of networking devices on a network and install/configure them.

- **Firewall**
- **Router**
- **Switch**
- **Hub**
- **Bridge**
- **Modems**
- **Wireless access point**
- **Media converter**
- **Wireless range extender**
- **VoIP endpoint**

2.3 Explain the purposes and use cases for advanced networking devices.

- **Multilayer switch**
- **Wireless controller**
- **Load balancer**
- **IDS/IPS**
- **Proxy server**
- **VPN concentrator**
- **AAA/RADIUS server**
- **UTM appliance**
- **NGFW/Layer 7 firewall**
- **VoIP PBX**
- **VoIP gateway**
- **Content filter**

2.4 Explain the purposes of virtualization and network storage technologies.

- **Virtual networking components**
  - Virtual switch
  - Virtual firewall
  - Virtual NIC
  - Virtual router
  - Hypervisor
- **Network storage types**
  - NAS
  - SAN
- **Connection type**
  - FCoE
  - Fibre Channel
  - iSCSI
  - InfiniBand
- **Jumbo frame**

2.5 Compare and contrast WAN technologies.

- **Service type**
  - ISDN
  - T1/T3
  - E1/E3
  - OC-3 – OC-192
  - DSL
  - Metropolitan Ethernet
  - Cable broadband
  - Dial-up
  - PRI
- **Transmission mediums**
  - Satellite
  - Copper
  - Fiber
  - Wireless
- **Characteristics of service**
  - MPLS
  - ATM
  - Frame relay
  - PPPoE
  - PPP
  - DMVPN
  - SIP trunk
- **Termination**
  - Demarcation point
  - CSU/DSU
  - Smart jack

3.0 Network Operations

3.1 Given a scenario, use appropriate documentation and diagrams to manage the network.

- **Diagram symbols**
- **Standard operating procedures/ work instructions**
- **Logical vs. physical diagrams**
- **Rack diagrams**
- **Change management documentation**
- **Wiring and port locations**
- **IDF/MDF documentation**
- **Labeling**
- **Network configuration and performance baselines**
- **Inventory management**

3.2 Compare and contrast business continuity and disaster recovery concepts.

- **Availability concepts**
  - Fault tolerance
  - High availability
  - Load balancing
  - NIC teaming
  - Port aggregation
  - Clustering
  - Power management
    - Battery backups/UPS
    - Power generators
    - Dual power supplies
    - Redundant circuits
- **Recovery**
  - Cold sites
  - Warm sites
  - Hot sites
  - Backups
    - Full
    - Differential
    - Incremental
  - Snapshots
- **MTTR**
- **MTBF**
- **SLA requirements**

3.3 Explain common scanning, monitoring and patching processes and summarize their expected outputs.

- **Processes**
  - Log reviewing
  - Port scanning
  - Vulnerability scanning
  - Patch management
    - Rollback
  - Reviewing baselines
  - Packet/traffic analysis
- **Event management**
  - Notifications
  - Alerts
  - SIEM
- **SNMP monitors**
  - MIB
- **Metrics**
  - Error rate
  - Utilization
  - Packet drops
  - Bandwidth/throughput

3.4 Given a scenario, use remote access methods.

- **VPN**
  - IPSec
  - SSL/TLS/DTLS
  - Site-to-site
  - Client-to-site
- **RDP**
- **SSH**
- **VNC**
- **Telnet**
- **HTTPS/management URL**
- **Remote file access**
  - FTP/FTPS
  - SFTP
  - TFTP
- **Out-of-band management**
  - Modem
  - Console router

3.5 Identify policies and best practices.

- **Privileged user agreement**
- **Password policy**
- **On-boarding/off-boarding procedures**
- **Licensing restrictions**
- **International export controls**
- **Data loss prevention**
- **Remote access policies**
- **Incident response policies**
- **BYOD**
- **AUP**
- **NDA**
- **System life cycle**
  - Asset disposal
- **Safety procedures and policies**

4.0 Network Security

4.1 Summarize the purposes of physical security devices.

- **Detection**
  - Motion detection
  - Video surveillance
  - Asset tracking tags
  - Tamper detection
- **Prevention**
  - Badges
  - Biometrics
  - Smart cards
  - Key fob
  - Locks

4.2 Explain authentication and access controls.

- **Authorization, authentication and accounting**
  - RADIUS
  - TACACS+
  - Kerberos
  - Single sign-on
  - Local authentication
  - LDAP
  - Certificates
  - Auditing and logging
- **Multifactor authentication**
  - Something you know
  - Something you have
  - Something you are
  - Somewhere you are
  - Something you do
- **Access control**
  - 802.1X
  - NAC
  - Port security
  - MAC filtering
  - Captive portal
  - Access control lists

4.3 Given a scenario, secure a basic wireless network.

- **WPA**
- **WPA2**
- **TKIP-RC4**
- **CCMP-AES**
- **Authentication and authorization**
  - EAP
    - PEAP
    - EAP-FAST
    - EAP-TLS
  - Shared or open
  - Preshared key
  - MAC filtering
- **Geofencing**

4.4 Summarize common networking attacks.

- DoS
  - Reflective
  - Amplified
  - Distributed
- Social engineering
- Insider threat
- Logic bomb
- Rogue access point
- Evil twin
- War-driving
- Phishing
- Ransomware
- DNS poisoning
- ARP poisoning
- Spoofing
- Deauthentication
- Brute force
- VLAN hopping
- Man-in-the-middle
- Exploits vs. vulnerabilities

4.5 Given a scenario, implement network device hardening.

- Changing default credentials
- Avoiding common passwords
- Upgrading firmware
- Patching and updates
- File hashing
- Disabling unnecessary services
- Using secure protocols
- Generating new keys
- Disabling unused ports
  - IP ports
  - Device ports (physical and virtual)

4.6 Explain common mitigation techniques and their purposes.

- Signature management
- Device hardening
- Change native VLAN
- Switch port protection
  - Spanning tree
  - Flood guard
  - BPDU guard
  - Root guard
  - DHCP snooping
- Network segmentation
  - DMZ
  - VLAN
- Privileged user account
- File integrity monitoring
- Role separation
- Restricting access via ACLs
- Honeypot/honeynet
- Penetration testing

5.0 Network Troubleshooting and Tools

5.1 Explain the network troubleshooting methodology.

- **Identify the problem**
    - Gather information
    - Duplicate the problem, if possible
    - Question users
    - Identify symptoms
    - Determine if anything has changed
    - 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**
    - Once 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, and outcomes**

5.2 Given a scenario, use the appropriate tool.

- **Hardware tools**
    - Crimper
    - Cable tester
    - Punchdown tool
    - OTDR
    - Light meter
    - Tone generator
    - Loopback adapter
    - Multimeter
    - Spectrum analyzer
- **Software tools**
    - Packet sniffer
    - Port scanner
    - Protocol analyzer
    - WiFi analyzer
    - Bandwidth speed tester
    - Command line
        - ping
        - tracert, traceroute
        - nslookup
        - ipconfig
        - ifconfig
        - iptables
        - netstat
        - tcpdump
        - pathping
        - nmap
        - route
        - arp
        - dig

5.3 Given a scenario, troubleshoot common wired connectivity and performance issues.

- Attenuation
- Latency
- Jitter
- Crosstalk
- EMI
- Open/short
- Incorrect pin-out
- Incorrect cable type
- Bad port
- Transceiver mismatch
- TX/RX reverse
- Duplex/speed mismatch
- Damaged cables
- Bent pins
- Bottlenecks
- VLAN mismatch
- Network connection LED status indicators

5.4 Given a scenario, troubleshoot common wireless connectivity and performance issues.

- Reflection
- Refraction
- Absorption
- Latency
- Jitter
- Attenuation
- Incorrect antenna type
- Interference
- Incorrect antenna placement
- Channel overlap
- Overcapacity
- Distance limitations
- Frequency mismatch
- Wrong SSID
- Wrong passphrase
- Security type mismatch
- Power levels
- Signal-to-noise ratio

5.5 Given a scenario, troubleshoot common network service issues.

- Names not resolving
- Incorrect gateway
- Incorrect netmask
- Duplicate IP addresses
- Duplicate MAC addresses
- Expired IP address
- Rogue DHCP server
- Untrusted SSL certificate
- Incorrect time
- Exhausted DHCP scope
- Blocked TCP/UDP ports
- Incorrect host-based firewall settings
- Incorrect ACL settings
- Unresponsive service
- Hardware failure