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.

Test Purpose: 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; and 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, although CompTIA A+ certification is not required
- At least 9 to 12 months of work experience in IT networking

EXAM ACCREDITATION

The CompTIA Network+ exam is accredited by the American National Standards Institute (ANSI) to show compliance with the International Organization for Standardization (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: CompTIA Network+ 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 9 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:

<table>
<thead>
<tr>
<th>DOMAIN</th>
<th>PERCENTAGE OF EXAMINATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 Networking Concepts</td>
<td>23%</td>
</tr>
<tr>
<td>2.0 Infrastructure</td>
<td>18%</td>
</tr>
<tr>
<td>3.0 Network Operations</td>
<td>17%</td>
</tr>
<tr>
<td>4.0 Network Security</td>
<td>20%</td>
</tr>
<tr>
<td>5.0 Network Troubleshooting and Tools</td>
<td>22%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>
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
- 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

CompTIA Network+ Certification Exam Objectives Version 1.0 (Exam Number: N10-007)
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

CompTIA Network+ Certification Exam Objectives Version 1.0 (Exam Number: N10-007)
Summarize cloud concepts and their purposes.

- Types of services
  - SaaS
  - PaaS
  - IaaS
- Cloud delivery models
  - Private
  - Public
  - Hybrid

Explain the functions of network services.

- DNS service
  - Record types
    - A, AAA
    - 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
- **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.

<table>
<thead>
<tr>
<th>Virtual networking components</th>
<th>Network storage types</th>
<th>Jumbo frame</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Virtual switch</td>
<td>- NAS</td>
<td></td>
</tr>
<tr>
<td>- Virtual firewall</td>
<td>- SAN</td>
<td></td>
</tr>
<tr>
<td>- Virtual NIC</td>
<td>- FCoE</td>
<td></td>
</tr>
<tr>
<td>- Virtual router</td>
<td>- Fibre Channel</td>
<td></td>
</tr>
<tr>
<td>- Hypervisor</td>
<td>- iSCSI</td>
<td></td>
</tr>
<tr>
<td>- Hypervisor</td>
<td>- InfiniBand</td>
<td></td>
</tr>
</tbody>
</table>

### 2.5 Compare and contrast WAN technologies.

<table>
<thead>
<tr>
<th>Service type</th>
<th>Characteristics of service</th>
<th>Termination</th>
</tr>
</thead>
<tbody>
<tr>
<td>- ISDN</td>
<td>- MPLS</td>
<td>- Demarcation point</td>
</tr>
<tr>
<td>- T1/T3</td>
<td>- ATM</td>
<td></td>
</tr>
<tr>
<td>- E1/E3</td>
<td>- Frame relay</td>
<td>- CSU/DSU</td>
</tr>
<tr>
<td>- OC-3 – OC-192</td>
<td>- PPPoE</td>
<td>- Smart jack</td>
</tr>
<tr>
<td>- DSL</td>
<td>- PPP</td>
<td></td>
</tr>
<tr>
<td>- Metropolitan Ethernet</td>
<td>- DMVPN</td>
<td></td>
</tr>
<tr>
<td>- Cable broadband</td>
<td>- SIP trunk</td>
<td></td>
</tr>
<tr>
<td>- Dial-up</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>- PRI</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Transmission mediums</td>
<td>- ISDN</td>
<td></td>
</tr>
<tr>
<td>- Satellite</td>
<td>- ATM</td>
<td></td>
</tr>
<tr>
<td>- Copper</td>
<td>- Frame relay</td>
<td></td>
</tr>
<tr>
<td>- Fiber</td>
<td>- PPPoE</td>
<td></td>
</tr>
<tr>
<td>- Wireless</td>
<td>- DMVPN</td>
<td></td>
</tr>
</tbody>
</table>
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
3.0 Network Operations

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
- Changing native VLAN
- Switch port protection
  - Spanning tree
  - Flood guard
  - BPDU guard
  - Root guard
  - DHCP snooping
- 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
- Network segmentation
  - DMZ
  - VLAN
- Privileged user account
- File integrity monitoring
- Role separation
- Restricting access via ACLs
- Honeypot/honeynet
- Penetration testing
- Disabling unused ports
  - IP ports
  - Device ports (physical and virtual)
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
5.0 Network Troubleshooting and Tools

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
Network+ Acronym List

The following is a list of acronyms that appear on the CompTIA Network+ exam. Candidates are encouraged to review the complete list and attain a working knowledge of all listed acronyms as a part of a comprehensive exam preparation program.

<table>
<thead>
<tr>
<th>ACRONYM</th>
<th>SPELLED OUT</th>
<th>ACRONYM</th>
<th>SPELLED OUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Authentication Authorization and Accounting</td>
<td>CDMA</td>
<td>Code Division Multiple Access</td>
</tr>
<tr>
<td>AAAA</td>
<td>Authentication, Authorization, Accounting and Auditing</td>
<td>CSMA/CD</td>
<td>Carrier Sense Multiple Access/Collision Detection</td>
</tr>
<tr>
<td>ACL</td>
<td>Access Control List</td>
<td>CHAP</td>
<td>Challenge Handshake Authentication Protocol</td>
</tr>
<tr>
<td>ADSL</td>
<td>Asymmetric Digital Subscriber Line</td>
<td>CIDR</td>
<td>Classless Inter-Domain Routing</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
<td>CNAME</td>
<td>Canonical Name</td>
</tr>
<tr>
<td>AH</td>
<td>Authentication Header</td>
<td>CoS</td>
<td>Class of Service</td>
</tr>
<tr>
<td>AP</td>
<td>Access Point</td>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>APC</td>
<td>Angle Polished Connector</td>
<td>CRAM-MD5</td>
<td>Challenge-Response Authentication</td>
</tr>
<tr>
<td>APIPA</td>
<td>Automatic Private Internet Protocol Addressing</td>
<td>CRC</td>
<td>Cyclic Redundancy Checking</td>
</tr>
<tr>
<td>APT</td>
<td>Advanced Persistent Tool</td>
<td>CSMA/CA</td>
<td>Carrier Sense Multiple Access/Collision Avoidance</td>
</tr>
<tr>
<td>ARIN</td>
<td>American Registry for Internet Numbers</td>
<td>CSU</td>
<td>Channel Service Unit</td>
</tr>
<tr>
<td>ARP</td>
<td>Address Resolution Protocol</td>
<td>CVW</td>
<td>Collaborative Virtual Workspace</td>
</tr>
<tr>
<td>AS</td>
<td>Autonomous System</td>
<td>CWDM</td>
<td>Course Wave Division Multiplexing</td>
</tr>
<tr>
<td>ASIC</td>
<td>Application Specific Integrated Circuit</td>
<td>Daas</td>
<td>Desktop as a Service</td>
</tr>
<tr>
<td>ASP</td>
<td>Application Service Provider</td>
<td>dB</td>
<td>Decibel</td>
</tr>
<tr>
<td>ATM</td>
<td>Asynchronous Transfer Mode</td>
<td>DCS</td>
<td>Distributed Computer System</td>
</tr>
<tr>
<td>AUP</td>
<td>Acceptable Use Policy</td>
<td>DDoS</td>
<td>Distributed Denial of Service</td>
</tr>
<tr>
<td>BCP</td>
<td>Business Continuity Plan</td>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>BERT</td>
<td>Bit-Error Rate Test</td>
<td>DLC</td>
<td>Data Link Control</td>
</tr>
<tr>
<td>BGP</td>
<td>Border Gateway Protocol</td>
<td>DLP</td>
<td>Data Loss Prevention</td>
</tr>
<tr>
<td>BLE</td>
<td>Bluetooth Low Energy</td>
<td>DLR</td>
<td>Device Level Ring</td>
</tr>
<tr>
<td>BNC</td>
<td>British Naval Connector/Bayonet Niell-Concelman</td>
<td>DMZ</td>
<td>Demilitarized Zone</td>
</tr>
<tr>
<td>BootP</td>
<td>Boot Protocol/Bootstrap Protocol</td>
<td>DNAT</td>
<td>Destination Network Address Translation</td>
</tr>
<tr>
<td>BPDU</td>
<td>Bridge Protocol Data Unit</td>
<td>DNS</td>
<td>Domain Name Service</td>
</tr>
<tr>
<td>BRI</td>
<td>Basic Rate Interface</td>
<td>DOC/SIS</td>
<td>Data-Over-Cable Service Interface Specification</td>
</tr>
<tr>
<td>BSSID</td>
<td>Basic Service Set Identifier</td>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>BYOD</td>
<td>Bring Your Own Device</td>
<td>DR</td>
<td>Designated Router</td>
</tr>
<tr>
<td>CaaS</td>
<td>Communication as a Service</td>
<td>DSCP</td>
<td>Differentiated Services Code Point</td>
</tr>
<tr>
<td>CAM</td>
<td>Content Addressable Memory</td>
<td>DSL</td>
<td>Digital Subscriber Line</td>
</tr>
<tr>
<td>CAN</td>
<td>Campus Area Network</td>
<td>DSSS</td>
<td>Direct Sequence Spread Spectrum</td>
</tr>
<tr>
<td>CARP</td>
<td>Common Address Redundancy Protocol</td>
<td>DSU</td>
<td>Data Service Unit</td>
</tr>
<tr>
<td>CASB</td>
<td>Cloud Access Security Broker</td>
<td>DWDM</td>
<td>Dense Wavelength Division Multiplexing</td>
</tr>
<tr>
<td>CAT</td>
<td>Category</td>
<td>E1</td>
<td>E-Carrier Level 1</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed Circuit TV</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

CompTIA Network+ Certification Exam Objectives Version 1.0 (Exam Number: N10-007)
EAP Extensible Authentication Protocol
EDNS Extension Mechanisms for DNS
EGP Exterior Gateway Protocol
EIA/TIA Electronic Industries Alliance/Telecommunication Industries Association
EMI Electromagnetic Interference
ESD Electrostatic Discharge
ESP Encapsulated Security Payload
ESSID Extended Service Set Identifier
EUI Extended Unique Identifier
FC Fibre Channel
FCoE Fibre Channel over Ethernet
FCS Frame Check Sequence
FDM Frequency Division Multiplexing
FHSS Frequency Hopping Spread Spectrum
FM Frequency Modulation
FQDN Fully Qualified Domain Name
FTP File Transfer Protocol
FTPS File Transfer Protocol Secure
GBIC Gigabit Interface Converter
Gbps Gigabits per second
GLBP Gateway Load Balancing Protocol
GPG GNU Privacy Guard
GRE Generic Routing Encapsulation
GSM Global System for Mobile Communications
HA High Availability
HDLC High-Level Data Link Control
HDMI High-Definition Multimedia Interface
HIDS Host Intrusion Detection System
HIPS Host Intrusion Prevention System
HSPA High-Speed Packet Access
HSRP Hot Standby Router Protocol
HT High Throughput
HTTP Hypertext Transfer Protocol
HTTPS Hypertext Transfer Protocol Secure
HVAC Heating, Ventilation and Air Conditioning
Hz Hertz
IaaS Infrastructure as a Service
IANA Internet Assigned Numbers Authority
ICA Independent Computer Architecture
ICANN Internet Corporation for Assigned Names and Numbers
ICMP Internet Control Message Protocol
ICS Internet Connection Sharing/Industrial Control System
IDF Intermediate Distribution Frame
IDS Intrusion Detection System
IEEE Institute of Electrical and Electronics Engineers
IGMP Internet Group Message Protocol
IGP Interior Gateway Protocol
IGRP Interior Gateway Routing Protocol
IKE Internet Key Exchange
IMAP4 Internet Message Access Protocol version 4
InterNIC Internet Network Information Center
IoT Internet of Things
IP Internet Protocol
IPSec Internet Protocol Security
IPv4 Internet Protocol version 4
IPv6 Internet Protocol version 6
ISAKMP Internet Security Association and Key Management Protocol
ISDN Integrated Services Digital Network
IS-IS Intermediate System to Intermediate System
ISP Internet Service Provider
IT Information Technology
ITS Intelligent Transportation System
IV Initialization Vector
Kbps Kilobits per second
KVM Keyboard Video Mouse
L2TP Layer 2 Tunneling Protocol
LACP Link Aggregation Control Protocol
LAN Local Area Network
LC Local Connector
LDAP Lightweight Directory Access Protocol
LDA Local Exchange Carrier
LEC Local Exchange Carrier
LED Light Emitting Diode
LLC Logical Link Control
LLDP Link Layer Discovery Protocol
LSA Link State Advertisements
LTE Long Term Evolution
MaaS Mobility as a Service
MAC Media Access Control/Medium Access Control
MAN Metropolitan Area Network
Mbps Megabits per second
MBps Megabytes per second
MDF Main Distribution Frame
MDI Media Dependent Interface
MDIX Media Dependent Interface Crossover
MGCP Media Gateway Control Protocol
MIB Management Information Base
<table>
<thead>
<tr>
<th>ACRONYM</th>
<th>SPELLED OUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIMO</td>
<td>Multiple Input, Multiple Output</td>
</tr>
<tr>
<td>MLA</td>
<td>Master License Agreement/Multilateral Agreement</td>
</tr>
<tr>
<td>MMF</td>
<td>Multimode Fiber</td>
</tr>
<tr>
<td>MOA</td>
<td>Memorandum of Agreement</td>
</tr>
<tr>
<td>MOU</td>
<td>Memorandum of Understanding</td>
</tr>
<tr>
<td>MPLS</td>
<td>Multiprotocol Label Switching</td>
</tr>
<tr>
<td>MS-CHAP</td>
<td>Microsoft Challenge Handshake Authentication Protocol</td>
</tr>
<tr>
<td>MSA</td>
<td>Master Service Agreement</td>
</tr>
<tr>
<td>MSDS</td>
<td>Material Safety Data Sheet</td>
</tr>
<tr>
<td>MT-RJ</td>
<td>Mechanical Transfer-Registered Jack</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum Transmission Unit</td>
</tr>
<tr>
<td>MTBF</td>
<td>Mean Time To Recovery</td>
</tr>
<tr>
<td>MU-MIMO</td>
<td>Multiuser Multiple Input, Multiple Output</td>
</tr>
<tr>
<td>MX</td>
<td>Mail Exchanger</td>
</tr>
<tr>
<td>NAC</td>
<td>Network Access Control</td>
</tr>
<tr>
<td>NAS</td>
<td>Network Attached Storage</td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
</tr>
<tr>
<td>NCP</td>
<td>Network Control Protocol</td>
</tr>
<tr>
<td>NDR</td>
<td>Non-Delivery Receipt</td>
</tr>
<tr>
<td>NetBEUI</td>
<td>Network Basic Input/Output Extended User Interface</td>
</tr>
<tr>
<td>NetBIOS</td>
<td>Network Basic Input/Output System</td>
</tr>
<tr>
<td>NFC</td>
<td>Near Field Communication</td>
</tr>
<tr>
<td>NFS</td>
<td>Network File Service</td>
</tr>
<tr>
<td>NGFW</td>
<td>Next-Generation Firewall</td>
</tr>
<tr>
<td>NIC</td>
<td>Network Interface Card</td>
</tr>
<tr>
<td>NIDS</td>
<td>Network Intrusion Detection System</td>
</tr>
<tr>
<td>NIPS</td>
<td>Network Intrusion Prevention System</td>
</tr>
<tr>
<td>NIU</td>
<td>Network Interface Unit</td>
</tr>
<tr>
<td>nm</td>
<td>Nanometer</td>
</tr>
<tr>
<td>NNTP</td>
<td>Network News Transport Protocol</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>OCSP</td>
<td>Online Certificate Status Protocol</td>
</tr>
<tr>
<td>OCx</td>
<td>Optical Carrier</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>OSI</td>
<td>Open Systems Interconnect</td>
</tr>
<tr>
<td>OSPF</td>
<td>Open Shortest Path First</td>
</tr>
<tr>
<td>OTDR</td>
<td>Optical Time Domain Reflectometer</td>
</tr>
<tr>
<td>OUI</td>
<td>Organizationally Unique Identifier</td>
</tr>
<tr>
<td>PaaS</td>
<td>Platform as a Service</td>
</tr>
<tr>
<td>PAN</td>
<td>Personal Area Network</td>
</tr>
<tr>
<td>PAP</td>
<td>Password Authentication Protocol</td>
</tr>
<tr>
<td>PAT</td>
<td>Port Address Translation</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>PCM</td>
<td>Phase-Change Memory</td>
</tr>
<tr>
<td>PDoS</td>
<td>Permanent Denial of Service</td>
</tr>
<tr>
<td>PDU</td>
<td>Protocol Data Unit</td>
</tr>
<tr>
<td>PGP</td>
<td>Pretty Good Privacy</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>PoE</td>
<td>Power over Ethernet</td>
</tr>
<tr>
<td>POP</td>
<td>Post Office Protocol</td>
</tr>
<tr>
<td>POP3</td>
<td>Post Office Protocol version 3</td>
</tr>
<tr>
<td>POT</td>
<td>Plain Old Telephone Service</td>
</tr>
<tr>
<td>PPP</td>
<td>Point-to-Point Protocol</td>
</tr>
<tr>
<td>PPoE</td>
<td>Point-to-Point Protocol over Ethernet</td>
</tr>
<tr>
<td>PPTP</td>
<td>Point-to-Point Tunneling Protocol</td>
</tr>
<tr>
<td>PRI</td>
<td>Primary Rate Interface</td>
</tr>
<tr>
<td>PSK</td>
<td>Pre-Shared Key</td>
</tr>
<tr>
<td>PSTN</td>
<td>Public Switched Telephone Network</td>
</tr>
<tr>
<td>PTP</td>
<td>Point-to-Point</td>
</tr>
<tr>
<td>PTR</td>
<td>Pointer</td>
</tr>
<tr>
<td>PUA</td>
<td>Privileged User Agreement</td>
</tr>
<tr>
<td>PVC</td>
<td>Permanent Virtual Circuit</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>QSFp</td>
<td>Quad Small Form-Factor Pluggable</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial-In User Service</td>
</tr>
<tr>
<td>RARP</td>
<td>Reverse Address Resolution Protocol</td>
</tr>
<tr>
<td>RAS</td>
<td>Remote Access Service</td>
</tr>
<tr>
<td>RDP</td>
<td>Remote Desktop Protocol</td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency</td>
</tr>
<tr>
<td>RFI</td>
<td>Radio Frequency Interference</td>
</tr>
<tr>
<td>RFP</td>
<td>Request for Proposal</td>
</tr>
<tr>
<td>RG</td>
<td>Radio Guide</td>
</tr>
<tr>
<td>RIP</td>
<td>Routing Internet Protocol</td>
</tr>
<tr>
<td>RJ</td>
<td>Registered Jack</td>
</tr>
<tr>
<td>RPO</td>
<td>Recovery Point Objective</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest, Shamir, Adelman</td>
</tr>
<tr>
<td>RSH</td>
<td>Remote Shell</td>
</tr>
<tr>
<td>RSTP</td>
<td>Rapid Spanning Tree Protocol</td>
</tr>
<tr>
<td>RTO</td>
<td>Recovery Time Objective</td>
</tr>
<tr>
<td>RTP</td>
<td>Real-Time Protocol</td>
</tr>
<tr>
<td>RTSP</td>
<td>Real-Time Streaming Protocol</td>
</tr>
<tr>
<td>RTT</td>
<td>Round Trip Time or Real Transfer Time</td>
</tr>
<tr>
<td>SA</td>
<td>Security Association</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as a Service</td>
</tr>
<tr>
<td>SC</td>
<td>Standard Connector/Subscriber Connector</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition</td>
</tr>
<tr>
<td>SCP</td>
<td>Secure Copy Protocol</td>
</tr>
<tr>
<td>SDLC</td>
<td>Software Development Life Cycle</td>
</tr>
<tr>
<td>ACRONYM</td>
<td>SPELLED OUT</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>SDN</td>
<td>Software Defined Network</td>
</tr>
<tr>
<td>SDP</td>
<td>Session Description Protocol</td>
</tr>
<tr>
<td>SDSL</td>
<td>Symmetrical Digital Subscriber Line</td>
</tr>
<tr>
<td>SFP</td>
<td>Small Form-factor Pluggable</td>
</tr>
<tr>
<td>SFTP</td>
<td>Secure File Transfer Protocol</td>
</tr>
<tr>
<td>SGCP</td>
<td>Simple Gateway Control Protocol</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hash Algorithm</td>
</tr>
<tr>
<td>SIEM</td>
<td>Security Information and Event Management</td>
</tr>
<tr>
<td>SIP</td>
<td>Session Initiation Protocol</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>SLAAC</td>
<td>Stateless Address Auto Configuration</td>
</tr>
<tr>
<td>SLIP</td>
<td>Serial Line Internet Protocol</td>
</tr>
<tr>
<td>SMB</td>
<td>Server Message Block</td>
</tr>
<tr>
<td>SMF</td>
<td>Single-Mode Fiber</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Message Service</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
</tr>
<tr>
<td>SNAT</td>
<td>Static Network Address Translation/Source</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SNTP</td>
<td>Simple Network Time Protocol</td>
</tr>
<tr>
<td>SOA</td>
<td>Start of Authority</td>
</tr>
<tr>
<td>SOHO</td>
<td>Small Office Home Office</td>
</tr>
<tr>
<td>SONET</td>
<td>Synchronous Optical Network</td>
</tr>
<tr>
<td>SOP</td>
<td>Standard Operating Procedure</td>
</tr>
<tr>
<td>SOW</td>
<td>Statement of Work</td>
</tr>
<tr>
<td>SPB</td>
<td>Shortest Path Bridging</td>
</tr>
<tr>
<td>SPI</td>
<td>Stateful Packet Inspection</td>
</tr>
<tr>
<td>SPS</td>
<td>Standby Power Supply</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>SSID</td>
<td>Service Set Identifier</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>ST</td>
<td>Straight Tip or Snap Twist</td>
</tr>
<tr>
<td>STP</td>
<td>Spanning Tree Protocol/Shielded Twisted Pair</td>
</tr>
<tr>
<td>SVC</td>
<td>Switched Virtual Circuit</td>
</tr>
<tr>
<td>SYSLOG</td>
<td>System Log</td>
</tr>
<tr>
<td>T1</td>
<td>Terrestrial Carrier Level 1</td>
</tr>
<tr>
<td>TA</td>
<td>Terminal Adaptor</td>
</tr>
<tr>
<td>TACACS</td>
<td>Terminal Access Control Access Control System</td>
</tr>
<tr>
<td>TACACS+</td>
<td>Terminal Access Control Access Control System+</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>Transmission Control Protocol/Internet Protocol</td>
</tr>
<tr>
<td>TDM</td>
<td>Time Division Multiplexing</td>
</tr>
<tr>
<td>TDR</td>
<td>Time Domain Reflectometer</td>
</tr>
<tr>
<td>Telco</td>
<td>Telecommunications Company</td>
</tr>
<tr>
<td>TFTP</td>
<td>Trivial File Transfer Protocol</td>
</tr>
<tr>
<td>TKIP</td>
<td>Temporal Key Integrity Protocol</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
</tbody>
</table>
Network+ Proposed Hardware and Software List

CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the Network+ exam. This list may also be helpful for training companies who wish to create a lab component to their training offering. The bulleted lists below each topic are a sample list and not exhaustive.

**EQUIPMENT**
- Optical and copper patch panels
- Punchdown blocks (110)
- Layer 2/3 switch
- PoE switch
- Router
- Firewall
- VPN concentrator
- Wireless access point
- Basic laptops that support virtualization
- Tablet/cell phone
- Media converters
- Configuration terminal (with Telnet and SSH)
- VoIP system (including a phone)

**SPARE HARDWARE**
- NICs
- Power supplies
- GBICs
- SFPs
- Managed switch
- Hub
- Wireless access point
- UPS

**SPARE PARTS**
- Patch cables
- RJ-45 connectors, modular jacks
- RJ-11 connectors
- Unshielded twisted pair cable spool
- Coaxial cable spool
- F-connectors
- Fiber connectors
- Antennas
- Bluetooth/wireless adapters
- Console cables (RS-232 to USB serial adapter)

**TOOLS**
- Telco/network crimper
- Cable tester
- Punchdown tool
- Cable stripper
- Coaxial crimper
- Wire cutter
- Tone generator
- Fiber termination kit
- Optical power meter

**SOFTWARE**
- Packet sniffer
- Protocol analyzer
- Terminal emulation software
- Linux/Windows OSs
- Software firewall
- Software IDS/IPS
- Network mapper
- Hypervisor software
- Virtual network environment
- WiFi analyzer
- Spectrum analyzer
- Network monitoring tools
- DHCP service
- DNS service

**OTHER**
- Sample network documentation
- Sample logs
- Defective cables

© 2017 CompTIA Properties, LLC, used under license by CompTIA Certifications, LLC. All rights reserved. All certification programs and education related to such programs are operated exclusively by CompTIA Certifications, LLC. CompTIA is a registered trademark of CompTIA Properties, LLC in the U.S. and internationally. Other brands and company names mentioned herein may be trademarks or service marks of CompTIA Properties, LLC or of their respective owners. Reproduction or dissemination prohibited without written consent of CompTIA Properties, LLC. Printed in the U.S. 03/14 Apr 2017