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
- 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:

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

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.

ACRONYM	SPELLED OUT
AAA	Authentication Authorization and Accounting
AAAA	Authentication, Authorization, Accounting and Auditing
ACL	Access Control List
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
AH	Authentication Header
AP	Access Point
APC	Angle Polished Connector
APIPA	Automatic Private Internet Protocol Addressing
APT	Advanced Persistent Tool
ARIN	American Registry for Internet Numbers
ARP	Address Resolution Protocol
AS	Autonomous System
ASCII	American Standard Code for Information Exchange
ASIC	Application Specific Integrated Circuit
ASP	Application Service Provider
ATM	Asynchronous Transfer Mode
AUP	Acceptable Use Policy
Auto-MDX	Automatic Medium-Dependent Interface Crossover
BCP	Business Continuity Plan
BERT	Bit-Error Rate Test
BGP	Border Gateway Protocol
BLE	Bluetooth Low Energy
BNC	British Naval Connector/Bayonet Niell-Concelman
BootP	Boot Protocol/Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
BSSID	Basic Service Set Identifier
BYOD	Bring Your Own Device
CaaS	Communication as a Service
CAM	Content Addressable Memory
CAN	Campus Area Network

ACRONYM	SPELLED OUT
CARP	Common Address Redundancy Protocol
CASB	Cloud Access Security Broker
CAT	Category
CCMP	Counter-mode Cipher Block Chaining Message Authentication Code Protocol
CCTV	Closed Circuit TV
CDMA	Code Division Multiple Access
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Inter-Domain Routing
CIFS	Common Internet File System
CNAME	Canonical Name
CoS	Class of Service
CPU	Central Processing Unit
CRAM-MD5	Challenge-Response Authentication Mechanism–Message Digest 5
CRC	Cyclic Redundancy Checking
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CSU	Channel Service Unit
CVE	Common Vulnerabilities and Exposures
CVW	Collaborative Virtual Workspace
CWDM	Coarse Wave Division Multiplexing
Daas	Desktop as a Service
dB	Decibel
DCS	Distributed Computer System
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DLC	Data Link Control
DLP	Data Loss Prevention
DLR	Device Level Ring
DMVPN	Dynamic Multipoint Virtual Private Network
DMZ	Demilitarized Zone
DNAT	Destination Network Address Translation
DNS	Domain Name Service/Domain Name Server/ Domain Name System

ACRONYM	SPELLED OUT
DOCSIS	Data-Over-Cable Service Interface Specification
DoS	Denial of Service
DPI	Deep Packet Inspection
DR	Designated Router
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
DSSS	Direct Sequence Spread Spectrum
DSU	Data Service Unit
DTLS	Datagram Transport Layer Security
DWDM	Dense Wavelength Division Multiplexing
E1	E-Carrier Level 1
EAP	Extensible Authentication Protocol
EBCDIC	Extended Binary Coded Decimal Interchange Code
EDNS	Extension Mechanisms for DNS
EGP	Exterior Gateway Protocol
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 Security
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

ACRONYM	SPELLED OUT
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
IPAM	IP Address Management
IPS	Intrusion Prevention System
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
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

ACRONYM	SPELLED OUT
LWAPP	Light Weight Access Point Protocol
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
MFA	Multifactor Authentication
MGCP	Media Gateway Control Protocol
MIB	Management Information Base
MIMO	Multiple Input, Multiple Output
MLA	Master License Agreement/ Multilateral Agreement
MMF	Multimode Fiber
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MPLS	Multiprotocol Label Switching
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
MSA	Master Service Agreement
MSDS	Material Safety Data Sheet
MT-RJ	Mechanical Transfer-Registered Jack
MTU	Maximum Transmission Unit
MTTR	Mean Time To Recovery
MTBF	Mean Time Between Failures
MU-MIMO	Multiuser Multiple Input, Multiple Output
MX	Mail Exchanger
NAC	Network Access Control
NAS	Network Attached Storage
NAT	Network Address Translation
NCP	Network Control Protocol
NDR	Non-Delivery Receipt
NetBEUI	Network Basic Input/Output Extended User Interface
NetBIOS	Network Basic Input/Output System
NFC	Near Field Communication
NFS	Network File Service
NGFW	Next-Generation Firewall
NIC	Network Interface Card
NIDS	Network Intrusion Detection System
NIPS	Network Intrusion Prevention System
NIU	Network Interface Unit
nm	Nanometer
NNTP	Network News Transport Protocol

ACRONYM	SPELLED OUT
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OCx	Optical Carrier
OID	Object Identifier
OOB	Out of Band
OS	Operating System
OSI	Open Systems Interconnect
OSPF	Open Shortest Path First
OTDR	Optical Time Domain Reflectometer
OUI	Organizationally Unique Identifier
PaaS	Platform as a Service
PAN	Personal Area Network
PAP	Password Authentication Protocol
PAT	Port Address Translation
PC	Personal Computer
PCM	Phase-Change Memory
PDoS	Permanent Denial of Service
PDU	Protocol Data Unit
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
PoE	Power over Ethernet
POP	Post Office Protocol
POP3	Post Office Protocol version 3
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point-to-Point Tunneling Protocol
PRI	Primary Rate Interface
PSK	Pre-Shared Key
PSTN	Public Switched Telephone Network
PTP	Point-to-Point
PTR	Pointer
PUA	Privileged User Agreement
PVC	Permanent Virtual Circuit
QoS	Quality of Service
QSFP	Quad Small Form-Factor Pluggable
RADIUS	Remote Authentication Dial-In User Service
RARP	Reverse Address Resolution Protocol
RAS	Remote Access Service
RDP	Remote Desktop Protocol
RF	Radio Frequency
RFI	Radio Frequency Interference
RFP	Request for Proposal
RG	Radio Guide
RIP	Routing Internet Protocol
RJ	Registered Jack

ACRONYM	SPELLED OUT
RPO	Recovery Point Objective
RSA	Rivest, Shamir, Adelman
RSH	Remote Shell
RSTP	Rapid Spanning Tree Protocol
RTO	Recovery Time Objective
RTP	Real-Time Protocol
RTSP	Real-Time Streaming Protocol
RTT	Round Trip Time or Real Transfer Time
SA	Security Association
SaaS	Software as a Service
SAN	Storage Area Network
SC	Standard Connector/Subscriber Connector
SCADA	Supervisory Control and Data Acquisition
SCP	Secure Copy Protocol
SCSI	Small Computer System Interface
SDLC	Software Development Life Cycle
SDN	Software Defined Network
SDP	Session Description Protocol
SDSL	Symmetrical Digital Subscriber Line
SECaaS	Security as a Service
SFP	Small Form-factor Pluggable
SFTP	Secure File Transfer Protocol
SGCP	Simple Gateway Control Protocol
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLAAC	Stateless Address Auto Configuration
SLIP	Serial Line Internet Protocol
SMB	Server Message Block
SMF	Single-Mode Fiber
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNAT	Static Network Address Translation/Source Network Address Translation
SNMP	Simple Network Management Protocol
SNR	Signal-to-Noise Ratio
SNTP	Simple Network Time Protocol
SOA	Start of Authority
SOHO	Small Office Home Office
SONET	Synchronous Optical Network
SOP	Standard Operating Procedure
SOW	Statement of Work
SPB	Shortest Path Bridging
SPI	Stateful Packet Inspection
SPS	Standby Power Supply
SSH	Secure Shell

ACRONYM	SPELLED OUT
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-on
ST	Straight Tip or Snap Twist
STP	Spanning Tree Protocol/Shielded Twisted Pair
SVC	Switched Virtual Circuit
SYSLOG	System Log
T1	Terrestrial Carrier Level 1
TA	Terminal Adaptor
TACACS	Terminal Access Control Access Control System
TACACS+	Terminal Access Control Access Control System+
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDM	Time Division Multiplexing
TDR	Time Domain Reflectometer
Telco	Telecommunications Company
TFTP	Trivial File Transfer Protocol
TIA/EIA	Telecommunication Industries Association/ Electronic Industries Alliance
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TMS	Transportation Management System
TOS	Type of Service
TPM	Trusted Platform Module
TTL	Time to Live
TTLS	Tunneled Transport Layer Security
UC	Unified Communications
UDP	User Datagram Protocol
UNC	Universal Naming Convention
UPC	Ultra Polished Connector
UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTM	Unified Threat Management
UTP	Unshielded Twisted Pair
VDSL	Variable Digital Subscriber Line
VLAN	Virtual Local Area Network
VLSM	Variable Length Subnet Mask
VNC	Virtual Network Connection
VoIP	Voice over IP
VPN	Virtual Private Network
VRF	Virtual Routing Forwarding
VRRP	Virtual Router Redundancy Protocol
VTC	Video Teleconference
VTP	VLAN Trunk Protocol
WAF	Web Application Firewall
WAN	Wide Area Network

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

CompTIA.