

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:

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

- 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

- 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
- 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)

- 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

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

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

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

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

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

- SC
 - APC
 - UPC
 - MTRI
- 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 re
- 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
- Given a scenario, determine the appropriate placement of networking devices on a network and install/configure them.
 - Firewall
 - Router
 - Switch
 - HubBridge

- Modems
- Wireless access point
- Media converter
- · Wireless range extender
- VoIP endpoint

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

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

- 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
- 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
- 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



Given a scenario, use remote access methods.

• VPN

- IPSec

- SSL/TLS/DTLS

- Site-to-site

- Client-to-site

• RDP

 $\cdot \, \mathsf{SSH}$

VNC

Telnet

• HTTPS/management URL

Remote file access

- FTP/FTPS

- SFTP

- TFTP

· Out-of-band management

- Modem

- Console router

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

- 41 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
- 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

- 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



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

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)

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

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



- Given a scenario, troubleshoot common wired connectivity and performance issues.
 - Attenuation
 - Latency
 - litter
 - 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
- 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	ACRONYM	SPELLED OUT
AAA	Authentication Authorization and Accounting	CDMA	Code Division Multiple Access
AAAA	Authentication, Authorization,	CSMA/CD	Carrier Sense Multiple Access/Collision Detection
	Accounting and Auditing	CHAP	Challenge Handshake Authentication Protocol
ACL	Access Control List	CIDR	Classless Inter-Domain Routing
ADSL	Asymmetric Digital Subscriber Line	CNAME	Canonical Name
AES	Advanced Encryption Standard	CoS	Class of Service
AH	Authentication Header	CPU	Central Processing Unit
AP	Access Point	CRAM-MD5	Challenge-Response Authentication
APC	Angle Polished Connector		Mechanism–Message Digest 5
APIPA	Automatic Private Internet Protocol Addressing	CRC	Cyclic Redundancy Checking
APT	Advanced Persistent Tool	CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
ARIN	American Registry for Internet Numbers	CSU	Channel Service Unit
ARP	Address Resolution Protocol	CVW	Collaborative Virtual Workspace
AS	Autonomous System	CWDM	Course Wave Division Multiplexing
ASIC	Application Specific Integrated Circuit	Daas	Desktop as a Service
ASP	Application Service Provider	dB	Decibel
ATM	Asynchronous Transfer Mode	DCS	Distributed Computer System
AUP	Acceptable Use Policy	DDoS	Distributed Denial of Service
BCP	Business Continuity Plan	DHCP	Dynamic Host Configuration Protocol
BERT	Bit-Error Rate Test	DLC	Data Link Control
BGP	Border Gateway Protocol	DLP	Data Loss Prevention
BLE	Bluetooth Low Energy	DLR	Device Level Ring
BNC	British Naval Connector/Bayonet Niell-Concelman	DMZ	Demilitarized Zone
BootP	Boot Protocol/Bootstrap Protocol	DNAT	Destination Network Address Translation
BPDU	Bridge Protocol Data Unit	DNS	Domain Name Service/Domain Name Server/
BRI	Basic Rate Interface		Domain Name System
BSSID	Basic Service Set Identifier	DOCSIS	Data-Over-Cable Service Interface Specification
BYOD	Bring Your Own Device	DoS	Denial of Service
CaaS	Communication as a Service	DR	Designated Router
CAM	Content Addressable Memory	DSCP	Differentiated Services Code Point
CAN	Campus Area Network	DSL	Digital Subscriber Line
CARP	Common Address Redundancy Protocol	DSSS	Direct Sequence Spread Spectrum
CASB	Cloud Access Security Broker	DSU	Data Service Unit
CAT	Category	DWDM	Dense Wavelength Division Multiplexing
CCTV	Closed Circuit TV	E1	E-Carrier Level 1



ACRONYM	SPELLED OUT	ACRONYM	SPELLED OUT
EAP	Extensible Authentication Protocol	IDS	Intrusion Detection System
EDNS	Extension Mechanisms for DNS	IEEE	Institute of Electrical and Electronics Engineers
EGP	Exterior Gateway Protocol	IGMP	Internet Group Message Protocol
EIA/TIA	Electronic Industries Alliance/	IGP	Interior Gateway Protocol
	Telecommunication Industries Association	IGRP	Interior Gateway Routing Protocol
EMI	Electromagnetic Interference	IKE	Internet Key Exchange
ESD	Electrostatic Discharge	IMAP4	Internet Message Access Protocol version 4
ESP	Encapsulated Security Payload	InterNIC	Internet Network Information Center
ESSID	Extended Service Set Identifier	IoT	Internet of Things
EUI	Extended Unique Identifier	IP	Internet Protocol
FC	Fibre Channel	IPS	Intrusion Prevention System
FCoE	Fibre Channel over Ethernet	IPSec	Internet Protocol Security
FCS	Frame Check Sequence	IPv4	Internet Protocol version 4
FDM	Frequency Division Multiplexing	IPv6	Internet Protocol version 6
FHSS	Frequency Hopping Spread Spectrum	ISAKMP	Internet Security Association and
FM	Frequency Modulation		Key Management Protocol
FQDN	Fully Qualified Domain Name	ISDN	Integrated Services Digital Network
FTP	File Transfer Protocol	IS-IS	Intermediate System to Intermediate System
FTPS	File Transfer Protocol Security	ISP	Internet Service Provider
GBIC	Gigabit Interface Converter	IT	Information Technology
Gbps	Gigabits per second	ITS	Intelligent Transportation System
GLBP	Gateway Load Balancing Protocol	IV	Initialization Vector
GPG	GNU Privacy Guard	Kbps	Kilobits per second
GRE	Generic Routing Encapsulation	KVM	Keyboard Video Mouse
GSM	Global System for Mobile Communications	L2TP	Layer 2 Tunneling Protocol
HA	High Availability	LACP	Link Aggregation Control Protocol
HDLC	High-Level Data Link Control	LAN	Local Area Network
HDMI	High-Definition Multimedia Interface	LC	Local Connector
HIDS	Host Intrusion Detection System	LDAP	Lightweight Directory Access Protocol
HIPS	Host Intrusion Prevention System	LEC	Local Exchange Carrier
HSPA	High-Speed Packet Access	LED	Light Emitting Diode
HSRP	Hot Standby Router Protocol	LLC	Logical Link Control
HT	High Throughput	LLDP	Link Layer Discovery Protocol
HTTP	Hypertext Transfer Protocol	LSA	Link State Advertisements
HTTPS	Hypertext Transfer Protocol Secure	LTE	Long Term Evolution
HVAC	Heating, Ventilation and Air Conditioning	LWAPP	Light Weight Access Point Protocol
Hz	Hertz	MaaS	Mobility as a Service
IaaS	Infrastructure as a Service	MAC	Media Access Control/Medium Access Control
IANA	Internet Assigned Numbers Authority	MAN	Metropolitan Area Network
ICA	Independent Computer Architecture	Mbps	Megabits per second
ICANN	Internet Corporation for	MBps	Megabytes per second
	Assigned Names and Numbers	MDF	Main Distribution Frame
ICMP	Internet Control Message Protocol	MDI	Media Dependent Interface
ICS	Internet Connection Sharing/Industrial	MDIX	Media Dependent Interface Crossover
	Control System	MGCP	Media Gateway Control Protocol
IDF	Intermediate Distribution Frame	MIB	Management Information Base



ACRONYM	SPELLED OUT	ACRONYM	SPELLED OUT
MIMO	Multiple Input, Multiple Output	PC	Personal Computer
MLA	Master License Agreement/	PCM	Phase-Change Memory
	Multilateral Agreement	PDoS	Permanent Denial of Service
MMF	Multimode Fiber	PDU	Protocol Data Unit
MOA	Memorandum of Agreement	PGP	Pretty Good Privacy
MOU	Memorandum of Understanding	PKI	Public Key Infrastructure
MPLS	Multiprotocol Label Switching	PoE	Power over Ethernet
MS-CHAP	Microsoft Challenge Handshake	POP	Post Office Protocol
WIS CITA	Authentication Protocol	POP3	Post Office Protocol version 3
MSA	Master Service Agreement	POTS	Plain Old Telephone Service
MSDS	Material Safety Data Sheet	PPP	Point-to-Point Protocol
MT-RJ	Mechanical Transfer-Registered Jack	PPPoE	Point-to-Point Protocol over Ethernet
MTU	Maximum Transmission Unit	PPTP	Point-to-Point Tunneling Protocol
MTTR	Mean Time To Recovery	PRI	Primary Rate Interface
MTBF	Mean Time Between Failures	PSK	Pre-Shared Key
MU-MIMO		PSTN	Public Switched Telephone Network
	Multiuser Multiple Input, Multiple Output		•
MX	Mail Exchanger	PTP	Point-to-Point
NAC	Network Access Control	PTR	Pointer
NAS	Network Attached Storage	PUA	Privileged User Agreement
NAT	Network Address Translation	PVC	Permanent Virtual Circuit
NCP	Network Control Protocol	QoS	Quality of Service
NDR	Non-Delivery Receipt	QSFP	Quad Small Form-Factor Pluggable
NetBEUI	Network Basic Input/Output	RADIUS	Remote Authentication Dial-In User Service
	Extended User Interface	RARP	Reverse Address Resolution Protocol
NetBIOS	Network Basic Input/Output System	RAS	Remote Access Service
NFC	Near Field Communication	RDP	Remote Desktop Protocol
NFS	Network File Service	RF	Radio Frequency
NGFW	Next-Generation Firewall	RFI	Radio Frequency Interference
NIC	Network Interface Card	RFP	Request for Proposal
NIDS	Network Intrusion Detection System	RG	Radio Guide
NIPS	Network Intrusion Prevention System	RIP	Routing Internet Protocol
NIU	Network Interface Unit	RJ	Registered Jack
nm	Nanometer	RPO	Recovery Point Objective
NNTP	Network News Transport Protocol	RSA	Rivest, Shamir, Adelman
NTP	Network Time Protocol	RSH	Remote Shell
OCSP	Online Certificate Status Protocol	RSTP	Rapid Spanning Tree Protocol
OCx	Optical Carrier	RTO	Recovery Time Objective
OS	Operating System	RTP	Real-Time Protocol
OSI	Open Systems Interconnect	RTSP	Real-Time Streaming Protocol
OSPF	Open Shortest Path First	RTT	Round Trip Time or Real Transfer Time
OTDR	Optical Time Domain Reflectometer	SA	Security Association
OUI	Organizationally Unique Identifier	SaaS	Software as a Service
PaaS	Platform as a Service	SC	Standard Connector/Subscriber Connector
PAN	Personal Area Network	SCADA	Supervisory Control and Data Acquisition
PAP	Password Authentication Protocol	SCP	Secure Copy Protocol
PAT	Port Address Translation	SDLC	Software Development Life Cycle



ACRONYM	SPELLED OUT	ACRONYM	SPELLED OUT
SDN	Software Defined Network	TMS	Transportation Management System
SDP	Session Description Protocol	TOS	Type of Service
SDSL	Symmetrical Digital Subscriber Line	TPM	Trusted Platform Module
SFP	Small Form-factor Pluggable	TTL	Time to Live
SFTP	Secure File Transfer Protocol	TTLS	Tunneled Transport Layer Security
SGCP	Simple Gateway Control Protocol	UC	Unified Communications
SHA	Secure Hash Algorithm	UDP	User Datagram Protocol
SIEM	Security Information and Event Management	UNC	Universal Naming Convention
SIP	Session Initiation Protocol	UPC	Ultra Polished Connector
SLA	Service Level Agreement	UPS	Uninterruptible Power Supply
SLAAC	Stateless Address Auto Configuration	URL	Uniform Resource Locator
SLIP	Serial Line Internet Protocol	USB	Universal Serial Bus
SMB	Server Message Block	UTM	Unified Threat Management
SMF	Single-Mode Fiber	UTP	Unshielded Twisted Pair
SMS	Short Message Service	VDSL	Variable Digital Subscriber Line
SMTP	Simple Mail Transfer Protocol	VLAN	Virtual Local Area Network
SNAT	Static Network Address Translation/Source	VNC	Virtual Network Connection
	Network Address Translation	VoIP	Voice over IP
SNMP	Simple Network Management Protocol	VPN	Virtual Private Network
SNTP	Simple Network Time Protocol	VRF	Virtual Routing Forwarding
SOA	Start of Authority	VRRP	Virtual Router Redundancy Protocol
SOHO	Small Office Home Office	VTC	Video Teleconference
SONET	Synchronous Optical Network	VTP	VLAN Trunk Protocol
SOP	Standard Operating Procedure	WAF	Web Application Firewall
SOW	Statement of Work	WAN	Wide Area Network
SPB	Shortest Path Bridging	WAP	Wireless Application Protocol/
SPI	Stateful Packet Inspection		Wireless Access Point
SPS	Standby Power Supply	WEP	Wired Equivalent Privacy
SSH	Secure Shell	WLAN	Wireless Local Area Network
SSID	Service Set Identifier	WMS	Warehouse Management System
SSL	Secure Sockets Layer	WPA	WiFi Protected Access
ST	Straight Tip or Snap Twist	WPS	WiFi Protected Setup
STP	Spanning Tree Protocol/Shielded Twisted Pair	WWN	World Wide Name
SVC	Switched Virtual Circuit	XDSL	Extended Digital Subscriber Line
SYSLOG	System Log	XML	eXtensible Markup Language
T1	Terrestrial Carrier Level 1	Zeroconf	Zero Configuration
TA	Terminal Adaptor		<u> </u>
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		
TKIP	Temporal Key Integrity Protocol		
TLS	Transport Layer Security		



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 pointBasic 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
- RI-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

