CompTIA

Network+

CompTIA Network+ Certification Exam Objectives

EXAM NUMBER: N10-006

CompTIA

About the Exam

Candidates are encouraged to use this document to help prepare for the CompTIA Network+ N10-006 exam. This exam will certify that the successful candidate has the knowledge and skills required to troubleshoot, configure and manage common network wireless and wired devices.

Knowledge and skills include:

- **Establishing basic network design and connectivity**
- **Understanding and maintaining network documentation**
- **Identifying network limitations and weaknesses**
- **Implementing network security, standards and protocols**

The successful candidate will have a basic understanding of emerging technologies including unified communications, mobile, cloud and virtualization technologies.

These content examples are meant to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination.

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 perform a search using CertGuard's engine, found **here**.

PLEASE NOTE

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

TEST DETAILS

Required exam	N10-006 JK0-023 (for CompTIA Academy Partners only)
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 Network Architecture	22%
2.0 Network Operations	20%
3.0 Network Security	18%
4.0 Troubleshooting	24%
5.0 Industrial Standards, Practices and Network Theory	16%
Total	**100%**

1.0 Network Architecture

1.1 Explain the functions and applications of various network devices.

- Router
- Switch
- Multilayer switch
- Firewall
- HIDS
- IDS/IPS
- Access point (wireless/wired)
- Content filter
- Load balancer
- Hub
- Analog modem
- Packet shaper
- VPN concentrator

1.2 Compare and contrast the use of networking services and applications.

- VPN
    - Site-to-site/host-to-site/host-to-host
    - Protocols
        - IPsec
        - GRE
        - SSL VPN
        - PTP/PPTP
- TACACS/RADIUS
- RAS
- Web services
- Unified voice services
- Network controllers

1.3 Install and configure the following networking services/applications.

- DHCP
    - Static vs. dynamic IP addressing
    - Reservations
    - Scopes
    - Leases
    - Options (DNS servers, suffixes)
    - IP helper/DHCP relay
- DNS
    - DNS servers
    - DNS records (A, MX, AAAA, CNAME, PTR)
    - Dynamic DNS
- Proxy/reverse proxy
- NAT
    - PAT
    - SNAT
    - DNAT
- Port forwarding

1.4 Explain the characteristics and benefits of various WAN technologies.

- Fiber
    - SONET
    - DWDM
    - CWDM
- Frame relay
- Satellite
- Broadband cable
- DSL/ADSL
- ISDN
- ATM
- PPP/multilink PPP
- MPLS
- GSM/CDMA
    - LTE/4G
    - HSPA+
    - 3G
    - Edge
- Dialup
- WiMAX
- MetroEthernet
- Leased lines
    - T-1
    - T-3
    - E-1
    - E-3
    - OC3
    - OC12
- Circuit switch vs. packet switch

1.5 Install and properly terminate various cable types and connectors using appropriate tools.

- **Copper connectors**
  - RJ-11
  - RJ-45
  - RJ-48C
  - DB-9/RS-232
  - DB-25
  - UTP coupler
  - BNC coupler
  - BNC
  - F-connector
  - 110 block
  - 66 block
- **Copper cables**
  - Shielded vs. unshielded
  - CAT3, CAT5, CAT5e, CAT6, CAT6a
  - PVC vs. plenum
  - RG-59
  - RG-6
  - Straight-through vs. crossover vs. rollover
- **Fiber connectors**
  - ST
  - SC
  - LC
  - MTRJ
  - FC
  - Fiber coupler
- **Fiber cables**
  - Single-mode
  - Multimode
  - APC vs. UPC
- **Media converters**
  - Single-mode fiber to Ethernet
  - Multimode fiber to Ethernet
  - Fiber to coaxial
  - Single-mode to multimode fiber
- **Tools**
  - Cable crimpers
  - Punchdown tool
  - Wire strippers
  - Snips
  - OTDR
  - Cable certifier

1.6 Differentiate between common network topologies.

- **Mesh**
  - Partial
  - Full
- **Bus**
- **Ring**
- **Star**
- **Hybrid**
- **Point-to-point**
- **Point-to-multipoint**
- **Client-server**
- **Peer-to-peer**

1.7 Differentiate between network infrastructure implementations.

- **WAN**
- **MAN**
- **LAN**
- **WLAN**
  - Hotspot
- **PAN**
  - Bluetooth
  - IR
  - NFC
- **SCADA/ICS**
  - ICS server
  - DCS/closed network
  - Remote terminal unit
  - Programmable logic controller
- **Medianets**
  - VTC
    - ISDN
    - IP/SIP

1.8 Given a scenario, implement and configure the appropriate addressing schema.

- **IPv6**
  - Auto-configuration
    - EUI 64
  - DHCP6
  - Link local
  - Address structure
  - Address compression
  - Tunneling 6to4, 4to6
    - Teredo, miredo
- **IPv4**
  - Address structure
  - Subnetting
  - APIPA
  - Classful A, B, C, D
  - Classless
- **Private vs. public**
- **NAT/PAT**
- **MAC addressing**
- **Multicast**
- **Unicast**
- **Broadcast**
- **Broadcast domains vs. collision domains**

1.9 Explain the basics of routing concepts and protocols.

- **Loopback interface**
- **Routing loops**
- **Routing tables**
- **Static vs. dynamic routes**
- **Default route**
- **Distance vector routing protocols**
  - RIPv2
- **Hybrid routing protocols**
  - BGP
- **Link state routing protocols**
  - OSPF
  - IS-IS
- **Interior vs. exterior gateway routing protocols**
- **Autonomous system numbers**
- **Route redistribution**
- **High availability**
  - VRRP
  - Virtual IP
  - HSRP
- **Route aggregation**
- **Routing metrics**
  - Hop counts
  - MTU, bandwidth
  - Costs
  - Latency
  - Administrative distance
  - SPB

1.10 Identify the basics elements of unified communication technologies.

- **VoIP**
- **Video**
- **Real-time services**
  - Presence
  - Multicast vs. unicast
- **QoS**
  - DSCP
  - COS
- **Devices**
  - UC servers
  - UC devices
  - UC gateways

1.11 Compare and contrast technologies that support cloud and virtualization.

- Virtualization
  - Virtual switches
  - Virtual routers
  - Virtual firewall
  - Virtual vs. physical NICs
  - Software-defined networking
- Storage area network
  - iSCSI
  - Jumbo frame
  - Fibre Channel
  - Network attached storage
- Cloud concepts
  - Public IaaS, SaaS, PaaS
  - Private IaaS, SaaS, PaaS
  - Hybrid IaaS, SaaS, PaaS
  - Community IaaS, SaaS, PaaS

1.12 Given a set of requirements, implement a basic network.

- List of requirements
- Device types/requirements
- Environment limitations
- Equipment limitations
- Compatibility requirements
- Wired/wireless considerations
- Security considerations

2.0 Network Operations

2.1 Given a scenario, use appropriate monitoring tools.

- **Packet/network analyzer**
- **Interface monitoring tools**
- **Port scanner**
- **Top talkers/listeners**
- **SNMP management software**
    - Trap
    - Get
    - Walk
    - MIBS
- **Alerts**
    - Email
    - SMS
- **Packet flow monitoring**
- **SYSLOG**
- **SIEM**
- **Environmental monitoring tools**
    - Temperature
    - Humidity
- **Power monitoring tools**
- **Wireless survey tools**
- **Wireless analyzers**

2.2 Given a scenario, analyze metrics and reports from monitoring and tracking performance tools.

- **Baseline**
- **Bottleneck**
- **Log management**
- **Graphing**
- **Utilization**
    - Bandwidth
    - Storage
    - Network device CPU
    - Network device memory
    - Wireless channel utilization
- **Link status**
- **Interface monitoring**
    - Errors
    - Utilization
    - Discards
    - Packet drops
    - Interface resets
    - Speed and duplex

2.3 Given a scenario, use appropriate resources to support configuration management.

- **Archives/backups**
- **Baselines**
- **On-boarding and off-boarding of mobile devices**
- **NAC**
- **Documentation**
    - Network diagrams (logical/physical)
    - Asset management
    - IP address utilization
    - Vendor documentation
    - Internal operating procedures/policies/standards

2.4 Explain the importance of implementing network segmentation.

- **SCADA systems/industrial control systems**
- **Legacy systems**
- **Separate private/public networks**
- **Honeypot/honeynet**
- **Testing lab**
- **Load balancing**
- **Performance optimization**
- **Security**
- **Compliance**

2.5 Given a scenario, install and apply patches and updates.

- **OS updates**
- **Firmware updates**
- **Driver updates**
- **Feature changes/updates**
- **Major vs. minor updates**
- **Vulnerability patches**
- **Upgrading vs. downgrading**
  - Configuration backup

2.6 Given a scenario, configure a switch using proper features.

- **VLAN**
  - Native VLAN/default VLAN
  - VTP
  - Trunking/802.1q
  - Tag vs. untag VLANs
- **Spanning tree (802.1d)/rapid spanning tree (802.1w)**
  - Flooding
  - Forwarding/blocking
  - Filtering
- **Interface configuration**
  - Port bonding (LACP)
  - Port mirroring (local vs. remote)
  - Speed and duplexing
  - IP address assignment
  - VLAN assignment
- **Default gateway**
- **PoE and PoE+ (802.3af, 802.3at)**
- **Switch management**
  - User/passwords
  - AAA configuration
  - Console
  - Virtual terminals
  - In-band/out-of-band management
- **Managed vs. unmanaged**

2.7 Install and configure wireless LAN infrastructure and implement the appropriate technologies in support of wireless capable devices.

- **Small office, home office wireless router**
- **Wireless access points**
  - Device density
  - Roaming
  - Wireless controllers
    - VLAN pooling
    - LWAPP
- **Wireless bridge**
- **Site surveys**
  - Heat maps
- **Frequencies**
  - 2.4 Ghz
  - 5.0 Ghz
- **Channels**
- **Goodput**
- **Connection types**
  - 802.11a-ht
  - 802.11g-ht
- **Antenna placement**
- **Antenna types**
  - Omnidirectional
  - Unidirectional
- **MIMO/MU-MIMO**
- **Signal strength**
  - Coverage
  - Differences between device antennas
- **SSID broadcast**
- **Topologies**
  - Adhoc
  - Mesh
  - Infrastructure
- **Mobile devices**
  - Cell phones
  - Laptops
  - Tablets
  - Gaming devices
  - Media devices

3.0 Network Security

3.1 Compare and contrast risk related concepts.

- **Disaster recovery**
- **Business continuity**
- **Battery backups/UPS**
- **First responders**
- **Data breach**
- **End user awareness and training**
- **Single point of failure**
  - Critical nodes
  - Critical assets
  - Redundancy
- **Adherence to standards and policies**
- **Vulnerability scanning**
- **Penetration testing**

3.2 Compare and contrast common network vulnerabilities and threats.

- **Attacks/threats**
  - DoS
    - Distributed DoS
      - Botnet
      - Traffic spike
      - Coordinated attack
    - Reflective/amplified
      - DNS
      - NTP
      - Smurfing
    - Friendly/unintentional DoS
    - Physical attack
      - Permanent DoS
  - ARP cache poisoning
  - Packet/protocol abuse
  - Spoofing
  - Wireless
    - Evil twin
    - Rogue AP
    - War driving
    - War chalking
    - Bluejacking
    - Bluesnarfing
    - WPA/WEP/WPS attacks
  - Brute force
  - Session hijacking
  - Social engineering
  - Man-in-the-middle
  - VLAN hopping
  - Compromised system
  - Effect of malware on the network
  - Insider threat/malicious employee
  - Zero-day attacks
- **Vulnerabilities**
  - Unnecessary running services
  - Open ports
  - Unpatched/legacy systems
  - Unencrypted channels
  - Clear text credentials
  - Unsecure protocols
    - TELNET
    - HTTP
    - SLIP
    - FTP
    - TFTP
    - SNMPv1 and SNMPv2
  - TEMPEST/RF emanation

3.3 Given a scenario, implement network hardening techniques.

- **Anti-malware software**
  - Host-based
  - Cloud/server-based
  - Network-based
- **Switch port security**
  - DHCP snooping
  - ARP inspection
  - MAC address filtering
  - VLAN assignments
    - Network segmentation
- **Security policies**
- **Disable unneeded network services**
- **Use secure protocols**
  - SSH
  - SNMPv3
  - TLS/SSL
  - SFTP
  - HTTPS
  - IPsec
- **Access lists**
  - Web/content filtering
  - Port filtering
  - IP filtering
  - Implicit deny
- **Wireless security**
  - WEP
  - WPA/WPA2
    - Enterprise
    - Personal
  - TKIP/AES
  - 802.1x
  - TLS/TTLS
  - MAC filtering
- **User authentication**
  - CHAP/MSCHAP
  - PAP
  - EAP
  - Kerberos
  - Multifactor authentication
  - Two-factor authentication
  - Single sign-on
- **Hashes**
  - MD5
  - SHA

3.4 Compare and contrast physical security controls.

- Mantraps
- Network closets
- Video monitoring
  - IP cameras/CCTVs
- Door access controls
- Proximity readers/key fob
- Biometrics
- Keypad/cipher locks
- Security guard

3.5 Given a scenario, install and configure a basic firewall.

- Types of firewalls
  - Host-based
  - Network-based
  - Software vs. hardware
  - Application aware/context aware
  - Small office, home office firewall
  - Stateful vs. stateless inspection
  - UTM
- Settings/techniques
  - ACL
  - Virtual wire vs. routed
  - DMZ
  - Implicit deny
  - Block/allow
    - Outbound traffic
    - Inbound traffic
  - Firewall placement
    - Internal/external

3.6 Explain the purpose of various network access control models.

- 802.1x
- Posture assessment
- Guest network
- Persistent vs. non-persistent agents
- Quarantine network
- Edge vs. access control

3.7 Summarize basic forensic concepts.

- First responder
- Secure the area
  - Escalate when necessary
- Document the scene
- eDiscovery
- Evidence/data collection
- Chain of custody
- Data transport
- Forensics report
- Legal hold

4.0 Troubleshooting

4.1 Given a scenario, implement the following 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 cause**
  - Once theory is confirmed, determine next steps to resolve problem
  - If theory is not confirmed, re-establish 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 preventative measures**
- **Document findings, actions and outcomes**

4.2 Given a scenario, analyze and interpret the output of troubleshooting tools.

- **Command line tools**
  - ipconfignetstat
  - ifconfig
  - ping/ping6/ping -6
  - tracert/tracert -6/ traceroute6/traceroute -6
  - nbtstat
  - nslookup
  - arp
  - mac address lookup table
  - pathping
- **Line testers**
- **Certifiers**
- **Multimeter**
- **Cable tester**
- **Light meter**
- **Toner probe**
- **Speed test sites**
- **Looking glass sites**
- **WiFi analyzer**
- **Protocol analyzer**

4.3 Given a scenario, troubleshoot and resolve common wireless issues.

- **Signal loss**
- **Interference**
- **Overlapping channels**
  - Mismatched channels
- **Signal-to-noise ratio**
- **Device saturation**
- **Bandwidth saturation**
- **Untested updates**
- **Wrong SSID**
- **Power levels**
- **Open networks**
- **Rogue access point**
- **Wrong antenna type**
- **Incompatibilities**
- **Wrong encryption**
- **Bounce**
- **MIMO**
- **AP placement**
- **AP configurations**
  - LWAPP
  - Thin vs. thick
- **Environmental factors**
  - Concrete walls
  - Window film
  - Metal studs
- **Wireless standard related issues**
  - Throughput
  - Frequency
  - Distance
  - Channels

4.4 Given a scenario, troubleshoot and resolve common copper cable issues.

- Shorts
- Opens
- Incorrect termination (mismatched standards)
  - Straight-through
  - Crossover
- Cross-talk
  - Near end
  - Far end
- EMI/RFI
- Distance limitations
- Attenuation/Db loss
- Bad connector
- Bad wiring
- Split pairs
- Tx/Rx reverse
- Cable placement
- Bad SFP/GBIC - cable or transceiver

4.5 Given a scenario, troubleshoot and resolve common fiber cable issues.

- Attenuation/Db loss
- SFP/GBIC - cable mismatch
- Bad SFP/GBIC - cable or transceiver
- Wavelength mismatch
- Fiber type mismatch
- Dirty connectors
- Connector mismatch
- Bend radius limitations
- Distance limitations

4.6 Given a scenario, troubleshoot and resolve common network issues.

- Incorrect IP configuration/default gateway
- Broadcast storms/switching loop
- Duplicate IP
- Speed and duplex mismatch
- End-to-end connectivity
- Incorrect VLAN assignment
- Hardware failure
- Misconfigured DHCP
- Misconfigured DNS
- Incorrect interface/interface misconfiguration
- Cable placement
- Interface errors
- Simultaneous wired/wireless connections
- Discovering neighboring devices/nodes
- Power failure/power anomalies
- MTU/MTU black hole
- Missing IP routes
- NIC teaming misconfiguration
  - Active-active vs. active-passive
  - Multicast vs. broadcast

4.7 Given a scenario, troubleshoot and resolve common security issues.

- **Misconfigured firewall**
- **Misconfigured ACLs/applications**
- **Malware**
- **DoS**
- **Open/closed ports**
- **ICMP related issues**
    - Ping of death
    - Unreachable default gateway
- **Unpatched firmware/OSs**
- **Malicious users**
    - Trusted
    - Untrusted users
    - Packet sniffing
- **Authentication issues**
    - TACACS/RADIUS misconfigurations
    - Default passwords/settings
- **Improper access/backdoor access**
- **ARP issues**
- **Banner grabbing/OUI**
- **Domain/local group configurations**
- **Jamming**

4.8 Given a scenario, troubleshoot and resolve common WAN issues.

- **Loss of Internet connectivity**
- **Interface errors**
- **Split horizon**
- **DNS issues**
- **Interference**
- **Router configurations**
- **Customer premise equipment**
    - Smart jack/NIU
    - Demarc
    - Loopback
    - CSU/DSU
    - Copper line drivers/repeaters
- **Company security policy**
    - Throttling
    - Blocking
    - Fair access policy/utilization limits
- **Satellite issues**
    - Latency

5.0 Industry Standards, Practices and Network Theory

5.1 Analyze a scenario and determine the corresponding OSI layer.

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

5.2 Explain the basics of network theory and concepts.

- **Encapsulation/de-encapsulation**
- **Modulation techniques**
  - Multiplexing
  - De-multiplexing
  - Analog and digital techniques
  - TDM
- **Numbering systems**
  - Binary
  - Hexadecimal
  - Octal
- **Broadband/baseband**
- **Bit rates vs. baud rate**
- **Sampling size**
- **CDMA**
- **CSMA/CD and CSMA/CA**
- **Carrier detect/sense**
- **Wavelength**
- **TCP/IP suite**
  - ICMP
  - UDP
  - TCP
- **Collision**

5.3 Given a scenario, deploy the appropriate wireless standard.

- **802.11a**
- **802.11b**
- **802.11g**
- **802.11n**
- **802.11ac**

5.4 Given a scenario, deploy the appropriate wired connectivity standard.

- **Ethernet standards**
  - 10BaseT
  - 100BaseT
  - 1000BaseT
  - 1000BaseTX
  - 10GBaseT
  - 100BaseFX
  - 10Base2
  - 10GBaseSR
  - 10GBaseER
  - 10GBaseSW
  - IEEE 1905.1-2013
    - Ethernet over HDMI
    - Ethernet over power line
- **Wiring standards**
  - EIA/TIA 568A/568B
- **Broadband standards**
  - DOCSIS

5.5 Given a scenario, implement the appropriate policies or procedures.

- **Security policies**
  - Consent to monitoring
- **Network policies**
- **Acceptable use policy**
- **Standard business documents**
  - SLA
  - MOU
  - MSA
  - SOW

5.6 Summarize safety practices.

- **Electrical safety**
  - Grounding
- **ESD**
  - Static
- **Installation safety**
  - Lifting equipment
  - Rack installation
  - Placement
  - Tool safety
- **MSDS**
- **Emergency procedures**
  - Building layout
  - Fire escape plan
  - Safety/emergency exits
  - Fail open/fail close
  - Emergency alert system
- **Fire suppression systems**
- **HVAC**

5.7 Given a scenario, install and configure equipment in the appropriate location using best practices.

- **Intermediate distribution frame**
- **Main distribution frame**
- **Cable management**
  - Patch panels
- **Power management**
  - Power converters
  - Circuits
  - UPS
  - Inverters
  - Power redundancy
- **Device placement**
- **Air flow**
- **Cable trays**
- **Rack systems**
  - Server rail racks
  - Two-post racks
  - Four-post racks
  - Free-standing racks
- **Labeling**
  - Port labeling
  - System labeling
  - Circuit labeling
  - Naming conventions
  - Patch panel labeling
- **Rack monitoring**
- **Rack security**

5.8 Explain the basics of change management procedures.

- **Document reason for a change**
- **Change request**
  - Configuration procedures
  - Rollback process
  - Potential impact
  - Notification
- **Approval process**
- **Maintenance window**
  - Authorized downtime
- **Notification of change**
- **Documentation**
  - Network configurations
  - Additions to network
  - Physical location changes

5.9 Compare and contrast the following ports and protocols.

80	HTTP
443	HTTPS
137-139	NetBIOS
110	POP
143	IMAP

25	SMTP
5060/5061	SIP
2427/2727	MGCP
5004/5005	RTP
1720	H.323

- TCP
    - Connection-oriented
- UDP
    - Connectionless

5.10 Given a scenario, configure and apply the appropriate ports and protocols.

20,21	FTP
161	SNMP
22	SSH
23	Telnet
53	DNS
67,68	DHCP
69	TFTP
445	SMB
3389	RDP

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
A	Address
AAA	Authentication, Authorization and Accounting
AAAA	Authentication, Authorization, Accounting and Address
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 Protocol
ARIN	American Registry for Internet Numbers
ARP	Address Resolution Protocol
AS	Autonomous System
ASIC	Application Specific Integrated Circuit
ASP	Application Service Provider
ATM	Asynchronous Transfer Mode
AUP	Acceptable Use Policy
BERT	Bit Error Rate Test
BGP	Border Gateway Protocol
BLE	Bluetooth Low Energy
BNC	British Naval Connector or Bayonet Neill-Concelman
BootP	Boot Protocol or Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
BSSID	Basic Service Set Identifier
CAM	Channel Access Method
CAN	Campus Area Network
CARP	Common Address Redundancy Protocol
CAT	Computer And Telephone
CCTV	Closed Circuit TV
CDMA	Code Division Multiple Access
CDMA/CD	Carrier Sense Multiple Access/Collision Detection
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Inter-Domain Routing
CNAME	Canonical Name
COS	Class Of Service
CPU	Central Processing Unit
CRAM	Challenge-Response Authentication Mechanism–Message Digest 5
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CSU	Channel Service Unit
CWDM	Course Wave Division Multiplexing
dB	Decibels
DCS	Distributed Computer System
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DLC	Data Link Control
DLP	Data Leak Prevention
DMZ	Demilitarized Zone
DNAT	Destination Network Address Translation
DNS	Domain Name Service or Domain Name Server or Domain Name System
DOCSIS	Data-Over-Cable Service Interface Specification
DoS	Denial of Service
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
DSSS	Direct Sequence Spread Spectrum
DSU	Data Service Unit
DWDM	Dense Wavelength Division Multiplexing
E1	E-Carrier Level 1
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

ACRONYM	SPELLED OUT
ESP	Encapsulated Security Packets
ESSID	Extended Service Set Identifier
EUI	Extended Unique Identifier
FC	Fibre Channel
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
GPG	GNU Privacy Guard
GRE	Generic Routing Encapsulation
GSM	Global System for Mobile communications
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 or Industrial Control System
IDF	Intermediate Distribution Frame
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Multicast Protocol
IGP	Interior Gateway Protocol
IKE	Internet Key Exchange
IMAP4	Internet Message Access Protocol version 4
InterNIC	Internet Network Information Center
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4

ACRONYM	SPELLED OUT
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
L2F	Layer 2 Forwarding
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
LTE	Long Term Evolution
LWAPP	Light Weight Access Point Protocol
MAC	Media Access Control or 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
MIBS	Management Information Bases
MIMO	Multiple Input, Multiple Output
MLA	Master License Agreement
MLA	Multilateral Agreement
MMF	Multimode Fiber
MOU	Memorandum Of Understanding
MPLS	Multi-Protocol 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
MUMIMO	Multiuser Multiple Input, Multiple Output
MX	Mail Exchanger

ACRONYM	SPELLED OUT
NAC	Network Access Control
NAS	Network Attached Storage
NAT	Network Address Translation
NCP	Network Control Protocol
NetBEUI	Network Basic Input/Output Extended User Interface
NetBIOS	Network Basic Input/Output System
NFS	Network File Service
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
NTP	Network Time Protocol
OCx	Optical Carrier
OS	Operating Systems
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
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 System
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
PVC	Permanent Virtual Circuit
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RARP	Reverse Address Resolution Protocol
RAS	Remote Access Service

ACRONYM	SPELLED OUT
RDP	Remote Desktop Protocol
RF	Radio Frequency
RFI	Radio Frequency Interference
RG	Radio Guide
RIP	Routing Internet Protocol
RJ	Registered Jack
RSA	Rivest, Shamir, Adelman
RSH	Remote Shell
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
SC	Standard Connector or Subscriber Connector
SCADA	Supervisory Control And Data Acquisition
SCP	Secure Copy Protocol
SDLC	Software Development Life Cycle
SDP	Session Description Protocol
SDSL	Symmetrical Digital Subscriber Line
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
SLIP	Serial Line Internet Protocol
SMF	Single-Mode Fiber
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNAT	Static Network Address Translation/ Source Network Address
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SOA	Start Of Authority
SOHO	Small Office, Home Office
SONET	Synchronous Optical Network
SOW	Statement Of Work
SPB	Shortest Path Bridging
SPI	Stateful Packet Inspection
SPS	Standby Power Supply
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
ST	Straight Tip or Snap Twist
STP	Spanning Tree Protocol or Shielded Twisted Pair

ACRONYM	SPELLED OUT
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 Plus
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDM	Time Division Multiplexing
TDR	Time Domain Reflectometer
Telco	Telephone company
TFTP	Trivial File Transfer Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TMS	Transportation Management System
TOS	Type Of Service
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

ACRONYM	SPELLED OUT
UTM	Unified Threat Management
UTP	Unshielded Twisted Pair
VDSL	Variable Digital Subscriber Line
VLAN	Virtual Local Area Network
VNC	Virtual Network Connection
VoIP	Voice over IP
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
VTC	Video Teleconference
VTP	VLAN Trunk Protocol
WAN	Wide Area Network
WAP	Wireless Application Protocol or Wireless Access Point
WEP	Wired Equivalent Privacy
WINS	Window Internet Name Service
WLAN	Wireless Local Area Network
WMS	Warehouse Management System
WPA	WiFi Protected Access
WPS	WiFi Protected Setup
WWW	World Wide Web
XDSL	Extended Digital Subscriber Line
XML	Extensible Markup Language
ZEROCONF	Zero configuration

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 3 switch/router
- Layer 2 switch
- Firewall
- VPN concentrator
- DHCP server
- DNS server
- IDS/IPS
- Wireless access point
- Two basic PCs
- Media converters
- Configuration terminal (with Telnet and SSH)
- VoIP system (including a phone)
- KVM switch

SPARE HARDWARE

- NICs
- Power supplies
- GBICs
- SFPs
- Switch
- Hub
- Wireless access point
- UPS

SPARE PARTS

- Patch cables
- RJ-45 connectors, modular jacks
- RJ-11 connectors
- Cable spool
- Coaxial cable spool
- F-connectors
- Fiber connectors
- Antennas
- Bluetooth/wireless adapters
- Console cables

TOOLS

- Telco/network crimper
- Cable tester
- Punchdown tool
- Cable striper
- Coaxial crimper
- Wire cutter
- Tone generator
- Fiber termination kit
- Snips
- Butt set
- Optical power meter

SOFTWARE

- Packet sniffer
- Protocol analyzer
- Terminal emulation software
- Linux/Windows OSs
- Software firewall
- Software IDS/IPS
- Network mapper
- Virtual network environment
- WiFi analyzer
- Spectrum analyzer
- Anti-malware software
- Network monitoring software

OTHER

- Sample network documentation
- Sample logs
- Defective cables
- Sample malware/viruses

© 2015 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. 01654-Oct2015