INTRODUCTION

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 that the successful candidate has the knowledge and skills required to troubleshoot, configure, and manage common network wireless and wired devices, establish basic network design and 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 emerging technologies including unified communications, mobile, cloud, and virtualization technologies.

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

It is recommended for CompTIA Network+ candidates to have the following:

- CompTIA A+ certification or equivalent knowledge, though CompTIA A+ certification is not required.
- Have at least 9 to 12 months of work experience in IT networking.

The table below lists the domains measured by this examination and the extent to which they are represented. CompTIA Network+ exams are based on these objectives.

<table>
<thead>
<tr>
<th>Domain</th>
<th>% of Examination</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 Network architecture</td>
<td>22%</td>
</tr>
<tr>
<td>2.0 Network operations</td>
<td>20%</td>
</tr>
<tr>
<td>3.0 Network security</td>
<td>18%</td>
</tr>
<tr>
<td>4.0 Troubleshooting</td>
<td>24%</td>
</tr>
<tr>
<td>5.0 Industry standards, practices, and network theory</td>
<td>16%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>
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 webpage:
http://certification.comptia.org/Training/testingcenters/policies.aspx

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 (http://certification.comptia.org/Training/testingcenters/policies/agreement.aspx) at the time of exam delivery.

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:
http://www.certguard.com/search.asp

Or verify against this list:

**Note: The lists of examples provided in bulleted format below each objective 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.

(A list of acronyms used in these objectives appears at the end of this document.)
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
- Metro-Ethernet
- 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
  - Punch down 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
  • DHCPv6
  • 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
  o RIP v2
• Hybrid routing protocols
  o BGP
• Link state routing protocols
  o OSPF
  o IS-IS
• Interior vs exterior gateway routing protocols
• Autonomous system numbers
• Route redistribution
• High availability
  o VRRP
  o Virtual IP
  o HSRP
• Route aggregation
• Routing metrics
  o Hop counts
  o MTU, bandwidth
  o Costs
  o Latency
  o Administrative distance
  o SPB

1.10 Identify the basics elements of unified communication technologies
• VoIP
• Video
• Real time services
  o Presence
  o Multicast vs unicast
• QoS
  o DSCP
  o COS
• Devices
  o UC servers
CompTIA Network+ Certification Exam Objectives

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
  o Configuration backup

2.6 Given a scenario, configure a switch using proper features
• VLAN
  o Native VLAN/Default VLAN
  o VTP
• Spanning tree (802.1d)/rapid spanning tree (802.1w)
  o Flooding
  o Forwarding/blocking
  o Filtering
• Interface configuration
  o Trunking/802.1q
  o Tag vs untag VLANs
  o Port bonding (LACP)
  o Port mirroring (local vs remote)
  o Speed and duplexing
  o IP address assignment
  o VLAN assignment
• Default gateway
• PoE and PoE+ (802.3af, 802.3at)
• Switch management
  o User/passwords
  o AAA configuration
  o Console
  o Virtual terminals
  o 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/MUMIMO
- 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
  o Critical nodes
  o Critical assets
  o Redundancy
• Adherence to standards and policies
• Vulnerability scanning
• Penetration testing

3.2 Compare and contrast common network vulnerabilities and threats
• Attacks/threats
  o Denial of service
    ▪ Distributed DoS
      • Botnet
      • Traffic spike
      • Coordinated attack
    ▪ Reflective/amplified
      • DNS
      • NTP
      • Smurfing
    ▪ Friendly/unintentional DoS
    ▪ Physical attack
      • Permanent DoS
  o ARP cache poisoning
  o Packet/protocol abuse
  o Spoofing
  o Wireless
    ▪ Evil twin
    ▪ Rogue AP
    ▪ War driving
    ▪ War chalking
    ▪ Bluejacking
    ▪ Bluesnarfing
    ▪ WPA/WEP/WPS attacks
  o Brute force
  o Session hijacking
  o Social engineering
  o Man-in-the-middle
  o VLAN hopping
  o Compromised system
  o Effect of malware on the network
  o 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
     o ipconfig
     o netstat
     o ifconfig
     o ping/ping6/ping -6
     o tracert/tracert -6/traceroute6/traceroute -6
     o nbtstat
     o nslookup
     o arp
     o mac address lookup table
     o 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
     o Mismatched channels
   • Signal-to-noise ratio
   • Device saturation
   • Bandwidth saturation
   • Untested updates
   • Wrong SSID
   • Power levels
   • Open networks
   • Rogue access point
   • Incompatibilities
   • Wrong encryption
   • Bounce
   • MIMO
   • AP placement
   • AP configurations
     o LWAPP
     o Thin vs thick
• Environmental factors
  o Concrete walls
  o Window film
  o Metal studs
• Wireless standard related issues
  o Throughput
  o Frequency
  o Distance
  o Channels

4.4 Given a scenario, troubleshoot and resolve common copper cable issues
• Shorts
• Opens
• Incorrect termination (mismatched standards)
  o Straight-through
  o Crossover
• Cross-talk
  o Near end
  o 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
  o Active-active vs active-passive
  o Multicast vs broadcast

4.7 Given a scenario, troubleshoot and resolve common security issues
• Misconfigured firewall
• Misconfigured ACLs/applications
• Malware
• Denial of service
• Open/closed ports
• ICMP related issues
  o Ping of death
  o Unreachable default gateway
• Unpatched firmware/OSs
• Malicious users
  o Trusted
  o Untrusted users
  o Packet sniffing
• Authentication issues
  o TACACS/RADIUS misconfigurations
  o 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
  o Smart jack/NIU
  o Demarc
  o Loopback
  o CSU/DSU
  o Copper line drivers/repeaters
• Company security policy
  o Throttling
  o Blocking
  o Fair access policy/utilization limits
• Satellite issues
  o 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
    o Multiplexing
    o De-multiplexing
    o Analog and digital techniques
    o TDM
  • Numbering systems
    o Binary
    o Hexadecimal
    o Octal
  • Broadband/base band
  • Bit rates vs baud rate
  • Sampling size
  • CDMA
  • CSMA/CD and CSMA/CA
  • Carrier detect/sense
• Wavelength
• TCP/IP suite
  o ICMP
  o UDP
  o 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
  o 10BaseT
  o 100BaseT
  o 1000BaseT
  o 1000BaseTX
  o 10GBaseT
  o 100BaseFX
  o 10Base2
  o 10GBaseSR
  o 10GBaseER
  o 10GBaseSW
  o IEEE 1905.1-2013
    ▪ Ethernet over HDMI
    ▪ Ethernet over power line
• Wiring standards
  o EIA/TIA 568A/568B
• Broadband standards
  o DOCSIS

5.5 Given a scenario, implement the appropriate policies or procedures
• Security policies
  o Consent to monitoring
• Network policies
• Acceptable use policy
• Standard business documents
  o SLA
  o MOU
  o MSA
  o SOW

5.6 Summarize safety practices
• Electrical safety
  o Grounding
• ESD
  o Static
• Installation safety
  o Lifting equipment
  o Rack installation
  o Placement
  o Tool safety
• MSDS
• Emergency procedures
  o Building layout
  o Fire escape plan
  o Safety/emergency exits
  o Fail open/fail close
  o 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
  o Patch panels
• Power management
  o Power converters
  o Circuits
  o UPS
  o Inverters
  o Power redundancy
• Device placement
• Air flow
• Cable trays
• Rack systems
  o Server rail racks
  o Two-post racks
  o Four-post racks
  o Free-standing racks
• Labeling
  o Port labeling
  o System labeling
  o Circuit labeling
  o Naming conventions
  o Patch panel labeling
• Rack monitoring
• Rack security

5.8 Explain the basics of change management procedures
• Document reason for a change
• Change request
  o Configuration procedures
  o Rollback process
  o Potential impact
  o Notification
• Approval process
• Maintenance window
  o Authorized downtime
• Notification of change
• Documentation
  o Network configurations
  o Additions to network
  o 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
  o Connection-oriented
• UDP
  o 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
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Address</td>
</tr>
<tr>
<td>AAA</td>
<td>Authentication Authorization and Accounting</td>
</tr>
<tr>
<td>AAAA</td>
<td>Authentication, Authorization, Accounting and Address</td>
</tr>
<tr>
<td>ACL</td>
<td>Access Control List</td>
</tr>
<tr>
<td>ADSL</td>
<td>Asymmetric Digital Subscriber Line</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>AH</td>
<td>Authentication Header</td>
</tr>
<tr>
<td>AP</td>
<td>Access Point</td>
</tr>
<tr>
<td>APC</td>
<td>Angle Polished Connector</td>
</tr>
<tr>
<td>APIPA</td>
<td>Automatic Private Internet Protocol Addressing</td>
</tr>
<tr>
<td>APT</td>
<td>Advanced Persistent Protocol</td>
</tr>
<tr>
<td>ARIN</td>
<td>American Registry for Internet Numbers</td>
</tr>
<tr>
<td>ARP</td>
<td>Address Resolution Protocol</td>
</tr>
<tr>
<td>AS</td>
<td>Autonomous System</td>
</tr>
<tr>
<td>ASIC</td>
<td>Application Specific Integrated Circuit</td>
</tr>
<tr>
<td>ASP</td>
<td>Application Service Provider</td>
</tr>
<tr>
<td>ATM</td>
<td>Asynchronous Transfer Mode</td>
</tr>
<tr>
<td>AUP</td>
<td>Acceptable Use Policy</td>
</tr>
<tr>
<td>BERT</td>
<td>Bit-Error Rate Test</td>
</tr>
<tr>
<td>BGP</td>
<td>Border Gateway Protocol</td>
</tr>
<tr>
<td>BLE</td>
<td>Bluetooth Low Energy</td>
</tr>
<tr>
<td>BNC</td>
<td>British Naval Connector/Bayonet Niell-Concelman</td>
</tr>
<tr>
<td>BootP</td>
<td>Boot Protocol/Bootstrap Protocol</td>
</tr>
<tr>
<td>BPDU</td>
<td>Bridge Protocol Data Unit</td>
</tr>
<tr>
<td>BRI</td>
<td>Basic Rate Interface</td>
</tr>
<tr>
<td>BSSID</td>
<td>Basic Service Set Identifier</td>
</tr>
<tr>
<td>CAM</td>
<td>Channel Access Method</td>
</tr>
<tr>
<td>CAN</td>
<td>Campus Area Network</td>
</tr>
<tr>
<td>CARP</td>
<td>Common Address Redundancy Protocol</td>
</tr>
<tr>
<td>CAT</td>
<td>Computer and Telephone</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed Circuit TV</td>
</tr>
<tr>
<td>CDMA</td>
<td>Code Division Multiple Access</td>
</tr>
<tr>
<td>CDMA/CD</td>
<td>Carrier Sense Multiple Access/Collision Detection</td>
</tr>
<tr>
<td>CHAP</td>
<td>Challenge Handshake Authentication Protocol</td>
</tr>
<tr>
<td>CIDR</td>
<td>Classless Inter Domain Routing</td>
</tr>
<tr>
<td>CNAME</td>
<td>Canonical Name</td>
</tr>
<tr>
<td>COS</td>
<td>Class of Service</td>
</tr>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>CRAM</td>
<td>Challenge-Response Authentication Mechanism–Message Digest 5</td>
</tr>
</tbody>
</table>
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/Domain Name Server/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
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
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GSM</td>
<td>Global System for Mobile Communications</td>
</tr>
<tr>
<td>HDLC</td>
<td>High-Level Data Link Control</td>
</tr>
<tr>
<td>HDMI</td>
<td>High Definition Multimedia Interface</td>
</tr>
<tr>
<td>HIDS</td>
<td>Host Intrusion Detection System</td>
</tr>
<tr>
<td>HIPS</td>
<td>Host Intrusion Prevention System</td>
</tr>
<tr>
<td>HSPA</td>
<td>High-Speed Packet Access</td>
</tr>
<tr>
<td>HSRP</td>
<td>Hot Standby Router Protocol</td>
</tr>
<tr>
<td>HT</td>
<td>High Throughput</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol Secure</td>
</tr>
<tr>
<td>HVAC</td>
<td>Heating, Ventilation and Air Conditioning</td>
</tr>
<tr>
<td>Hz</td>
<td>Hertz</td>
</tr>
<tr>
<td>IaaS</td>
<td>Infrastructure as a Service</td>
</tr>
<tr>
<td>IANA</td>
<td>Internet Assigned Numbers Authority</td>
</tr>
<tr>
<td>ICA</td>
<td>Independent Computer Architecture</td>
</tr>
<tr>
<td>ICANN</td>
<td>Internet Corporation for Assigned Names and Numbers</td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Message Protocol</td>
</tr>
<tr>
<td>ICS</td>
<td>Internet Connection Sharing/Industrial Control System</td>
</tr>
<tr>
<td>IDF</td>
<td>Intermediate Distribution Frame</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IGMP</td>
<td>Internet Group Multicast Protocol</td>
</tr>
<tr>
<td>IGP</td>
<td>Interior Gateway Protocol</td>
</tr>
<tr>
<td>IKE</td>
<td>Internet Key Exchange</td>
</tr>
<tr>
<td>IMAP4</td>
<td>Internet Message Access Protocol version 4</td>
</tr>
<tr>
<td>InterNIC</td>
<td>Internet Network Information Center</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPS</td>
<td>Intrusion Prevention System</td>
</tr>
<tr>
<td>IPsec</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>IPv4</td>
<td>Internet Protocol version 4</td>
</tr>
<tr>
<td>IPv6</td>
<td>Internet Protocol version 6</td>
</tr>
<tr>
<td>ISAKMP</td>
<td>Internet Security Association and Key Management Protocol</td>
</tr>
<tr>
<td>ISDN</td>
<td>Integrated Services Digital Network</td>
</tr>
<tr>
<td>IS-IS</td>
<td>Intermediate System to Intermediate System</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>ITS</td>
<td>Intelligent Transportation System</td>
</tr>
<tr>
<td>IV</td>
<td>Initialization Vector</td>
</tr>
<tr>
<td>Kbps</td>
<td>Kilobits per second</td>
</tr>
<tr>
<td>KVM</td>
<td>Keyboard Video Mouse</td>
</tr>
<tr>
<td>L2F</td>
<td>Layer 2 Forwarding</td>
</tr>
</tbody>
</table>
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/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
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
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIDS</td>
<td>Network Intrusion Detection System</td>
</tr>
<tr>
<td>NIPS</td>
<td>Network Intrusion Prevention System</td>
</tr>
<tr>
<td>NIU</td>
<td>Network Interface Unit</td>
</tr>
<tr>
<td>nm</td>
<td>Nanometer</td>
</tr>
<tr>
<td>NNTP</td>
<td>Network News Transport Protocol</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>OCx</td>
<td>Optical Carrier</td>
</tr>
<tr>
<td>OS</td>
<td>Operating Systems</td>
</tr>
<tr>
<td>OSI</td>
<td>Open Systems Interconnect</td>
</tr>
<tr>
<td>OSPF</td>
<td>Open Shortest Path First</td>
</tr>
<tr>
<td>OTDR</td>
<td>Optical Time Domain Reflectometer</td>
</tr>
<tr>
<td>OUI</td>
<td>Organizationally Unique Identifier</td>
</tr>
<tr>
<td>PaaS</td>
<td>Platform as a Service</td>
</tr>
<tr>
<td>PAN</td>
<td>Personal Area Network</td>
</tr>
<tr>
<td>PAP</td>
<td>Password Authentication Protocol</td>
</tr>
<tr>
<td>PAT</td>
<td>Port Address Translation</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>PDU</td>
<td>Protocol Data Unit</td>
</tr>
<tr>
<td>PGP</td>
<td>Pretty Good Privacy</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>PoE</td>
<td>Power over Ethernet</td>
</tr>
<tr>
<td>POP</td>
<td>Post Office Protocol</td>
</tr>
<tr>
<td>POP3</td>
<td>Post Office Protocol version 3</td>
</tr>
<tr>
<td>POTS</td>
<td>Plain Old Telephone System</td>
</tr>
<tr>
<td>PPP</td>
<td>Point-to-Point Protocol</td>
</tr>
<tr>
<td>PPPoE</td>
<td>Point-to-Point Protocol over Ethernet</td>
</tr>
<tr>
<td>PPTP</td>
<td>Point-to-Point Tunneling Protocol</td>
</tr>
<tr>
<td>PRI</td>
<td>Primary Rate Interface</td>
</tr>
<tr>
<td>PSK</td>
<td>Pre-Shared Key</td>
</tr>
<tr>
<td>PSTN</td>
<td>Public Switched Telephone Network</td>
</tr>
<tr>
<td>PTP</td>
<td>Point-to-Point</td>
</tr>
<tr>
<td>PTR</td>
<td>Pointer</td>
</tr>
<tr>
<td>PVC</td>
<td>Permanent Virtual Circuit</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial-In User Service</td>
</tr>
<tr>
<td>RARP</td>
<td>Reverse Address Resolution Protocol</td>
</tr>
<tr>
<td>RAS</td>
<td>Remote Access Service</td>
</tr>
<tr>
<td>RDP</td>
<td>Remote Desktop Protocol</td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency</td>
</tr>
<tr>
<td>RFI</td>
<td>Radio Frequency Interference</td>
</tr>
<tr>
<td>RG</td>
<td>Radio Guide</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>RIP</td>
<td>Routing Internet Protocol</td>
</tr>
<tr>
<td>RJ</td>
<td>Registered Jack</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest, Shamir, Adelman</td>
</tr>
<tr>
<td>RSH</td>
<td>Remote Shell</td>
</tr>
<tr>
<td>RTP</td>
<td>Real Time Protocol</td>
</tr>
<tr>
<td>RTSP</td>
<td>Real Time Streaming Protocol</td>
</tr>
<tr>
<td>RTT</td>
<td>Round Trip Time or Real Transfer Time</td>
</tr>
<tr>
<td>SA</td>
<td>Security Association</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as a Service</td>
</tr>
<tr>
<td>SC</td>
<td>Standard Connector/Subscriber Connector</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition</td>
</tr>
<tr>
<td>SCP</td>
<td>Secure Copy Protocol</td>
</tr>
<tr>
<td>SDLC</td>
<td>Software Development Life Cycle</td>
</tr>
<tr>
<td>SDP</td>
<td>Session Description Protocol</td>
</tr>
<tr>
<td>SDSL</td>
<td>Symmetrical Digital Subscriber Line</td>
</tr>
<tr>
<td>SFP</td>
<td>Small Form-factor Pluggable</td>
</tr>
<tr>
<td>SFTP</td>
<td>Secure File Transfer Protocol</td>
</tr>
<tr>
<td>SGCP</td>
<td>Simple Gateway Control Protocol</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hash Algorithm</td>
</tr>
<tr>
<td>SIEM</td>
<td>Security Information and Event Management</td>
</tr>
<tr>
<td>SIP</td>
<td>Session Initiation Protocol</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>SLIP</td>
<td>Serial Line Internet Protocol</td>
</tr>
<tr>
<td>SM</td>
<td>Single Mode Fiber</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Message Service</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
</tr>
<tr>
<td>SNAT</td>
<td>Static Network Address Translation/Source Network Address</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SNTP</td>
<td>Simple Network Time Protocol</td>
</tr>
<tr>
<td>SOA</td>
<td>Start of Authority</td>
</tr>
<tr>
<td>SOHO</td>
<td>Small Office/Home Office</td>
</tr>
<tr>
<td>SONET</td>
<td>Synchronous Optical Network</td>
</tr>
<tr>
<td>SOW</td>
<td>Statement of Work</td>
</tr>
<tr>
<td>SPB</td>
<td>Shortest Path Bridging</td>
</tr>
<tr>
<td>SPI</td>
<td>Stateful Packet Inspection</td>
</tr>
<tr>
<td>SPS</td>
<td>Standby Power Supply</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>SSID</td>
<td>Service Set Identifier</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>ST</td>
<td>Straight Tip or Snap Twist</td>
</tr>
<tr>
<td>STP</td>
<td>Spanning Tree Protocol / Shielded Twisted Pair</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>SVC</td>
<td>Switched Virtual Circuit</td>
</tr>
<tr>
<td>SYSLOG</td>
<td>System Log</td>
</tr>
<tr>
<td>T1</td>
<td>Terrestrial Carrier Level 1</td>
</tr>
<tr>
<td>TA</td>
<td>Terminal Adaptor</td>
</tr>
<tr>
<td>TACACS</td>
<td>Terminal Access Control Access Control System</td>
</tr>
<tr>
<td>TACACS+</td>
<td>Terminal Access Control Access Control System+</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TCP / IP</td>
<td>Transmission Control Protocol/Internet Protocol</td>
</tr>
<tr>
<td>TDM</td>
<td>Time Division Multiplexing</td>
</tr>
<tr>
<td>TDR</td>
<td>Time Domain Reflectometer</td>
</tr>
<tr>
<td>Telco</td>
<td>Telephone Company</td>
</tr>
<tr>
<td>TFTP</td>
<td>Trivial File Transfer Protocol</td>
</tr>
<tr>
<td>TKIP</td>
<td>Temporal Key Integrity Protocol</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TMS</td>
<td>Transportation Management System</td>
</tr>
<tr>
<td>TOS</td>
<td>Type of Service</td>
</tr>
<tr>
<td>TTL</td>
<td>Time to Live</td>
</tr>
<tr>
<td>TTLS</td>
<td>Tunneled Transport Layer Security</td>
</tr>
<tr>
<td>UC</td>
<td>Unified Communications</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>UNC</td>
<td>Universal Naming Convention</td>
</tr>
<tr>
<td>UPC</td>
<td>Ultra Polished Connector</td>
</tr>
<tr>
<td>UPS</td>
<td>Uninterruptible Power Supply</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
<tr>
<td>USB</td>
<td>Universal Serial Bus</td>
</tr>
<tr>
<td>UTM</td>
<td>Unified Threat Management</td>
</tr>
<tr>
<td>UTP</td>
<td>Unshielded Twisted Pair</td>
</tr>
<tr>
<td>VDSL</td>
<td>Variable Digital Subscriber Line</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
<tr>
<td>VNC</td>
<td>Virtual Network Connection</td>
</tr>
<tr>
<td>VoIP</td>
<td>Voice over IP</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>VRRP</td>
<td>Virtual Router Redundancy Protocol</td>
</tr>
<tr>
<td>VTC</td>
<td>Video Teleconference</td>
</tr>
<tr>
<td>VTP</td>
<td>VLAN Trunk Protocol</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>WAP</td>
<td>Wireless Application Protocol/Wireless Access Point</td>
</tr>
<tr>
<td>WEP</td>
<td>Wired Equivalent Privacy</td>
</tr>
<tr>
<td>WINS</td>
<td>Window Internet Name Service</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
<tr>
<td>WMS</td>
<td>Warehouse Management System</td>
</tr>
</tbody>
</table>
Network+ Proposed Hardware and Software List

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

Equipment

- Optical and copper patch panels
- Punch downs 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
- Punch down tool
- Cable stripper
- 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
• Antimalware software
• Network monitoring software

Other

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