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 implement a defined network architecture with basic network security. Furthermore, a successful candidate will be able to configure, maintain, and troubleshoot network devices using appropriate network tools and understand the features and purpose of network technologies. Candidates will be able to make basic solution recommendations, analyze network traffic, and be familiar with common protocols and media types.

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 Concepts</td>
<td>21%</td>
</tr>
<tr>
<td>2.0 Network Installation and Configuration</td>
<td>23%</td>
</tr>
<tr>
<td>3.0 Network Media and Topologies</td>
<td>17%</td>
</tr>
<tr>
<td>4.0 Network Management</td>
<td>20%</td>
</tr>
<tr>
<td>5.0 Network Security</td>
<td>19%</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: http://certification.comptia.org/Training/testingcenters/policies/unauthorized.aspx

**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.)
Networking Concepts

1.1 Compare the layers of the OSI and TCP/IP models.

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

- **TCP/IP model:**
  - Network Interface Layer
  - Internet Layer
  - Transport Layer
  - Application Layer

  (Also described as: Link Layer, Internet Layer, Transport Layer, Application Layer)

1.2 Classify how applications, devices, and protocols relate to the OSI model layers.

- MAC address
- IP address
- EUI-64
- Frames
- Packets
- Switch
- Router
- Multilayer switch
- Hub
- Encryption devices
- Cable
- NIC
- Bridge

1.3 Explain the purpose and properties of IP addressing.

- Classes of addresses
  - A, B, C and D
  - Public vs. Private
- Classless (CIDR)
- IPv4 vs. IPv6 (formatting)
• MAC address format
• Subnetting
• Multicast vs. unicast vs. broadcast
• APIPA

1.4 Explain the purpose and properties of routing and switching.
• EIGRP
• OSPF
• RIP
• Link state vs. distance vector vs. hybrid
• Static vs. dynamic
• Routing metrics
  o Hop counts
  o MTU, bandwidth
  o Costs
  o Latency
• Next hop
• Spanning Tree Protocol
• VLAN (802.1q)
• Port mirroring
• Broadcast domain vs. collision domain
• IGP vs. EGP
• Routing tables
• Convergence (steady state)

1.5 Identify common TCP and UDP default ports.
• SMTP – 25
• HTTP – 80
• HTTPS – 443
• FTP – 20, 21
• TELNET – 23
• IMAP – 143
• RDP – 3389
• SSH – 22
• DNS – 53
• DHCP – 67, 68
• POP3-110

1.6 Explain the function of common networking protocols.
• TCP
• FTP
• UDP
• TCP/IP suite
• DHCP
• TFTP
• DNS
• HTTPS
• HTTP
• ARP
• SIP (VoIP)
• RTP (VoIP)
• SSH
• POP3
• NTP
• IMAP4
• Telnet
• SMTP
• SNMP2/3
• ICMP
• IGMP
• TLS

1.7 Summarize DNS concepts and its components.
   • DNS servers
   • DNS records (A, MX, AAAA, CNAME, PTR)
   • Dynamic DNS

1.8 Given a scenario, implement the following network troubleshooting methodology:
   • Identify the problem:
     o Information gathering
     o Identify symptoms
     o Question users
     o Determine if anything has changed
   • Establish a theory of probable cause
     o Question the obvious
   • Test the theory to determine cause:
     o Once theory is confirmed determine next steps to resolve problem.
     o 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

1.9 Identify virtual network components.
• Virtual switches
• Virtual desktops
• Virtual servers
• Virtual PBX
• Onsite vs. offsite
• Network as a Service (NaaS)

2.0 Network Installation and Configuration

2.1 Given a scenario, install and configure routers and switches.
• Routing tables
• NAT
• PAT
• VLAN (trunking)
• Managed vs. unmanaged
• Interface configurations
  o Full duplex
  o Half duplex
  o Port speeds
  o IP addressing
  o MAC filtering
• PoE
• Traffic filtering
• Diagnostics
• VTP configuration
• QoS
• Port mirroring

2.2 Given a scenario, install and configure a wireless network.
• WAP placement
• Antenna types
• Interference
• Frequencies
• Channels
• Wireless standards
• SSID (enable/disable)
• Compatibility (802.11 a/b/g/n)

2.3 Explain the purpose and properties of DHCP.
  • Static vs. dynamic IP addressing
  • Reservations
  • Scopes
  • Leases
  • Options (DNS servers, suffixes)

2.4 Given a scenario, troubleshoot common wireless problems.
  • Interference
  • Signal strength
  • Configurations
  • Incompatibilities
  • Incorrect channel
  • Latency
  • Encryption type
  • Bounce
  • SSID mismatch
  • Incorrect switch placement

2.5 Given a scenario, troubleshoot common router and switch problems.
  • Switching loop
  • Bad cables/improper cable types
  • Port configuration
  • VLAN assignment
  • Mismatched MTU/MUT black hole
  • Power failure
  • Bad/missing routes
  • Bad modules (SFPs, GBICs)
  • Wrong subnet mask
  • Wrong gateway
  • Duplicate IP address
  • Wrong DNS

2.6 Given a set of requirements, plan and implement a basic SOHO network.
  • List of requirements
  • Cable length
  • Device types/requirements
  • Environment limitations
  • Equipment limitations
  • Compatibility requirements
3.0 Network Media and Topologies

3.1 Categorize standard media types and associated properties.

- Fiber:
  - Multimode
  - Singlemode
- Copper:
  - UTP
  - STP
  - CAT3
  - CAT5
  - CAT5e
  - CAT6
  - CAT6a
  - Coaxial
  - Crossover
  - T1 Crossover
  - Straight-through
- Plenum vs. non-plenum
- Media converters:
  - Singlemode fiber to Ethernet
  - Multimode fiber to Ethernet
  - Fiber to Coaxial
  - Singlemode to multimode fiber
- Distance limitations and speed limitations
- Broadband over powerline

3.2 Categorize standard connector types based on network media.

- Fiber:
  - ST
  - SC
  - LC
  - MTRJ
- Copper:
  - RJ-45
  - RJ-11
  - BNC
  - F-connector
  - DB-9 (RS-232)
o Patch panel
o 110 block (T568A, T568B)

3.3 Compare and contrast different wireless standards.
- 802.11 a/b/g/n standards
  - Distance
  - Speed
  - Latency
  - Frequency
  - Channels
  - MIMO
  - Channel bonding

3.4 Categorize WAN technology types and properties.
- Types:
  - T1/E1
  - T3/E3
  - DS3
  - OCx
  - SONET
  - SDH
  - DWDM
  - Satellite
  - ISDN
  - Cable
  - DSL
  - Cellular
  - WiMAX
  - LTE
  - HSPA+
  - Fiber
  - Dialup
  - PON
  - Frame relay
  - ATMs
- Properties:
  - Circuit switch
  - Packet switch
  - Speed
  - Transmission media
  - Distance

3.5 Describe different network topologies.
• MPLS
• Point-to-point
• Point-to-multipoint
• Ring
• Star
• Mesh
• Bus
• Peer-to-peer
• Client-server
• Hybrid

3.6 Given a scenario, troubleshoot common physical connectivity problems.
• Cable problems:
  o Bad connectors
  o Bad wiring
  o Open, short
  o Split cables
  o dB loss
  o TXRX reversed
  o Cable placement
  o EMI/Interference
  o Distance
  o Cross-talk

3.7 Compare and contrast different LAN technologies.
• Types:
  o Ethernet
  o 10BaseT
  o 100BaseT
  o 1000BaseT
  o 100BaseTX
  o 100BaseFX
  o 1000BaseX
  o 10GBaseSR
  o 10GBaseLR
  o 10GBaseER
  o 10GBaseSW
  o 10GBaseLW
  o 10GBaseEW
  o 10GBaseT

• Properties:
  o CSMA/CD
3.8 Identify components of wiring distribution.
   - IDF
   - MDF
   - Demarc
   - Demarc extension
   - Smart jack
   - CSU/DSU

4.0 Network Management

4.1 Explain the purpose and features of various network appliances.
   - Load balancer
   - Proxy server
   - Content filter
   - VPN concentrator

4.2 Given a scenario, use appropriate hardware tools to troubleshoot connectivity issues.
   - Cable tester
   - Cable certifier
   - Crimper
   - Butt set
   - Toner probe
   - Punch down tool
   - Protocol analyzer
   - Loop back plug
   - TDR
   - OTDR
   - Multimeter
   - Environmental monitor

4.3 Given a scenario, use appropriate software tools to troubleshoot connectivity issues.
   - Protocol analyzer
   - Throughput testers
• Connectivity software
• Ping
• Tracert/traceroute
• Dig
• Ipconfig/ifconfig
• Nslookup
• Arp
• Nbtstat
• Netstat
• Route

4.4 Given a scenario, use the appropriate network monitoring resource to analyze traffic.
• SNMP
• SNMPv2
• SNMPv3
• Syslog
• System logs
• History logs
• General logs
• Traffic analysis
• Protocol Analyzer

4.5 Describe the purpose of configuration management documentation.
• Wire schemes
• Network maps
• Documentation
• Cable management
• Asset management
• Baselines
• Change management

4.6 Explain different methods and rationales for network performance optimization.
• Methods:
  o QoS
  o Traffic shaping
  o Load balancing
  o High availability
  o Caching engines
  o Fault tolerance
  o CARP
• Reasons:
  o Latency sensitivity
  o High bandwidth applications (VoIP, video applications, unified communications)
  o Uptime

5.0 Network Security

5.1 Given a scenario, implement appropriate wireless security measures.
  • Encryption protocols:
    o WEP
    o WPA
    o WPA2
    o WPA Enterprise
  • MAC address filtering
  • Device placement
  • Signal strength

5.2 Explain the methods of network access security.
  • ACL:
    o MAC filtering
    o IP filtering
    o Port filtering
  • Tunneling and encryption:
    o SSL VPN
    o VPN
    o L2TP
    o PPTP
    o IPSec
    o ISAKMP
    o TLS
    o TLS1.2
    o Site-to-site and client-to-site
  • Remote access:
    o RAS
    o RDP
    o PPPoE
    o PPP
    o ICA
    o SSH

5.3 Explain methods of user authentication.
5.4 Explain common threats, vulnerabilities, and mitigation techniques.

- **Wireless:**
  - War driving
  - War chalking
  - WEP cracking
  - WPA cracking
  - Evil twin
  - Rogue access point

- **Attacks:**
  - DoS
  - DDoS
  - Man in the middle
  - Social engineering
  - Virus
  - Worms
  - Buffer overflow
  - Packet sniffing
  - FTP bounce
  - Smurf

- **Mitigation techniques:**
  - Training and awareness
  - Patch management
  - Policies and procedures
  - Incident response

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

- **Types:**
  - Software and hardware firewalls

- **Port security**
- **Stateful inspection vs. packet filtering**
- **Firewall rules:**
5.6 Categorize different types of network security appliances and methods.

- **IDS and IPS:**
  - Behavior based
  - Signature based
  - Network based
  - Host based

- **Vulnerability scanners:**
  - Nessus
  - Nmap

- **Methods:**
  - Honeypots
  - Honeynets
## Network+ Acronym List

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Authentication Authorization and Accounting</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>AM</td>
<td>Amplitude Modulation</td>
</tr>
<tr>
<td>APIPA</td>
<td>Automatic Private Internet Protocol Addressing</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>ASP</td>
<td>Application Service Provider</td>
</tr>
<tr>
<td>ATM</td>
<td>Asynchronous Transfer Mode</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>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>CARP</td>
<td>Common Address Redundancy Protocol</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed Capkon TV</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>CRAM-MD5</td>
<td>Challenge-Response Authentication Mechanism – Message Digest 5</td>
</tr>
<tr>
<td>CSMA / CA</td>
<td>Carrier Sense Multiple Access / Collision Avoidance</td>
</tr>
<tr>
<td>CSMA / CD</td>
<td>Carrier Sense Multiple Access / Collision Detection</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>CSU</td>
<td>Channel Service Unit</td>
</tr>
<tr>
<td>dB</td>
<td>decibels</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DLC</td>
<td>Data Link Control</td>
</tr>
<tr>
<td>DMZ</td>
<td>Demilitarized Zone</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name Service / Domain Name Server / Domain Name System</td>
</tr>
<tr>
<td>DOCSIS</td>
<td>Data-Over-Cable Service Interface Specification</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>DDoS</td>
<td>Distributed Denial of Service</td>
</tr>
<tr>
<td>DSL</td>
<td>Digital Subscriber Line</td>
</tr>
<tr>
<td>DSSS</td>
<td>Direct Sequence Spread Spectrum</td>
</tr>
<tr>
<td>DSU</td>
<td>Data Service Unit</td>
</tr>
<tr>
<td>DWDM</td>
<td>Dense Wavelength Division Multiplexing</td>
</tr>
<tr>
<td>E1</td>
<td>E-Carrier Level 1</td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
</tr>
<tr>
<td>EDNS</td>
<td>Extension Mechanisms for DNS</td>
</tr>
<tr>
<td>EGP</td>
<td>Exterior Gateway Protocol</td>
</tr>
<tr>
<td>EIGRP</td>
<td>Enhanced Interior Gateway Routing Protocol</td>
</tr>
<tr>
<td>EMI</td>
<td>Electromagnetic Interference</td>
</tr>
<tr>
<td>ESD</td>
<td>Electrostatic Discharge</td>
</tr>
<tr>
<td>ESSID</td>
<td>Extended Service Set Identifier</td>
</tr>
<tr>
<td>ESP</td>
<td>Encapsulated security packets</td>
</tr>
<tr>
<td>FDDI</td>
<td>Fiber Distributed Data Interface</td>
</tr>
<tr>
<td>FDM</td>
<td>Frequency Division Multiplexing</td>
</tr>
<tr>
<td>FHSS</td>
<td>Frequency Hopping Spread Spectrum</td>
</tr>
<tr>
<td>FM</td>
<td>Frequency Modulation</td>
</tr>
<tr>
<td>FQDN</td>
<td>Fully Qualified Domain Name / Fully Qualified Distinguished Name</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>FTPS</td>
<td>File Transfer Protocol Security</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>GBIC</td>
<td>Gigabit Interface Converter</td>
</tr>
<tr>
<td>Gbps</td>
<td>Giga bits per second</td>
</tr>
<tr>
<td>GPG</td>
<td>GNU Privacy Guard</td>
</tr>
<tr>
<td>HDLC</td>
<td>High-Level Data Link Control</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>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol Secure</td>
</tr>
<tr>
<td>Hz</td>
<td>Hertz</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</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>IIS</td>
<td>Internet Information Services</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>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</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>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>IV</td>
<td>Initialization Vector</td>
</tr>
<tr>
<td>Kbps</td>
<td>Kilobits per second</td>
</tr>
<tr>
<td>L2F</td>
<td>Layer 2 Forwarding</td>
</tr>
<tr>
<td>L2TP</td>
<td>Layer 2 Tunneling Protocol</td>
</tr>
<tr>
<td>LACP</td>
<td>Link aggregation control protocol</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LC</td>
<td>Local Connector</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>LEC</td>
<td>Local Exchange Carrier</td>
</tr>
<tr>
<td>LED</td>
<td>Light Emitting Diode</td>
</tr>
<tr>
<td>LLC</td>
<td>Logical Link Control</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control / Medium Access Control</td>
</tr>
<tr>
<td>Mbps</td>
<td>Megabits per second</td>
</tr>
<tr>
<td>MBps</td>
<td>Megabytes per second</td>
</tr>
<tr>
<td>MDF</td>
<td>Main Distribution Frame</td>
</tr>
<tr>
<td>MDI</td>
<td>Media Dependent Interface</td>
</tr>
<tr>
<td>MDIX</td>
<td>Media Dependent Interface Crossover</td>
</tr>
<tr>
<td>MIB</td>
<td>Management Information Base</td>
</tr>
<tr>
<td>MIMO</td>
<td>Multiple Input, Multiple Output</td>
</tr>
<tr>
<td>MMF</td>
<td>Multimode Fiber</td>
</tr>
<tr>
<td>MPLS</td>
<td>Multi-Protocol Label Switching</td>
</tr>
<tr>
<td>MS-CHAP</td>
<td>Microsoft Challenge Handshake Authentication Protocol</td>
</tr>
<tr>
<td>MT-RJ</td>
<td>Mechanical Transfer-Registered Jack</td>
</tr>
<tr>
<td>MX</td>
<td>Mail Exchanger</td>
</tr>
</tbody>
</table>
NAC  Network Access Control
NaaS  Network as a Service
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
nm  Nanometer
NNTP  Network News Transport Protocol
NTP  Network Time Protocol
NWLINK  Microsoft IPX/SPX Protocol
OCx  Optical Carrier
OS  Operating Systems
OSI  Open Systems Interconnect
OSPF  Open Shortest Path First
OTDR  Optical Time Domain Reflectometer
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
POP3  Post Office Protocol version 3
POTS  Plain Old Telephone System
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>PSTN</td>
<td>Public Switched Telephone Network</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>RFI</td>
<td>Radio Frequency Interface</td>
</tr>
<tr>
<td>RG</td>
<td>Radio Guide</td>
</tr>
<tr>
<td>RIP</td>
<td>Routing Internet Protocol</td>
</tr>
<tr>
<td>RJ</td>
<td>Registered Jack</td>
</tr>
<tr>
<td>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>SC</td>
<td>Standard Connector / Subscriber Connector</td>
</tr>
<tr>
<td>SCP</td>
<td>Secure Copy Protocol</td>
</tr>
<tr>
<td>SDSL</td>
<td>Symmetrical Digital Subscriber Line</td>
</tr>
<tr>
<td>SFTP</td>
<td>Secure File Transfer Protocol</td>
</tr>
<tr>
<td>SFP</td>
<td>Small Form-factor Pluggable</td>
</tr>
<tr>
<td>SIP</td>
<td>Session Initiation Protocol</td>
</tr>
<tr>
<td>SLIP</td>
<td>Serial Line Internet Protocol</td>
</tr>
<tr>
<td>SMF</td>
<td>Single Mode Fiber</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
</tr>
<tr>
<td>SNAT</td>
<td>Static Network Address Translation</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>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</td>
</tr>
<tr>
<td>STP</td>
<td>Shielded Twisted Pair</td>
</tr>
<tr>
<td>SVC</td>
<td>Switched Virtual Connection</td>
</tr>
<tr>
<td>T1</td>
<td>T-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>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>TTL</td>
<td>Time to Live</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>UNC</td>
<td>Universal Naming Convention</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</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>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>WPA</td>
<td>Wi-Fi Protected Access</td>
</tr>
<tr>
<td>www</td>
<td>World Wide Web</td>
</tr>
<tr>
<td>X.25</td>
<td>CCITT Packet Switching Protocol</td>
</tr>
<tr>
<td>XML</td>
<td>eXtensible Markup Language</td>
</tr>
<tr>
<td>XDSL</td>
<td>Extended Digital Subscriber Line</td>
</tr>
<tr>
<td>Zeroconf</td>
<td>Zero Configuration</td>
</tr>
</tbody>
</table>
**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**
- Patch Panels
- Punch downs blocks
- Layer 3 Switch
- Router
- Firewall
- Two basic PCs
- Access point
- Media converters
- Configuration terminal (with telnet and SSH)

**Spare hardware**
- NICs
- Power supplies
- GBICs
- SFPs

**Spare parts**
- Patch cables
- RJ-45 connectors, modular jacks
- RJ-11 connectors
- Cable spool
- Coaxial cable spool
- F-connectors

**Tools**
- Telco/network crimper
- Cable tester
- Punch down tool
- Cable stripper
- Coaxial crimper
- Wire cutter
- Tone generator

**Software**
- Packet Sniffer
- Protocol Analyzer
• Terminal Emulation Software
• Linux/Windows OSs
• Software Firewall
• Software IDS / IPS
• Network mapper
• Virtual network environment

Other

• Sample network documentation
• Sample logs
• Defective cables