CompTIA Network+ Certification Exam Objectives

EXAM NUMBER: N10-006
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 contact CompTIA at examsecurity@comptia.org to confirm.

PLEASE NOTE

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

<table>
<thead>
<tr>
<th>DOMAIN</th>
<th>PERCENTAGE 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 Industrial Standards, Practices and Network Theory</td>
<td>16%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>
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
- NAT
  - PAT
  - SNAT
  - DNAT
  - Port forwarding

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
- Fiber connectors
  - RJ-11
  - RJ-45
  - RJ-48C
  - DB-9/RS-232
  - DB-25
  - UTP coupler
  - BNC coupler
  - BNC
  - F-connector
  - 110 block
  - 66 block
- 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

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

Differentiate between common network topologies.

Differentiate between network infrastructure implementations.
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

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

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
- Spanning tree (802.1d)/rapid spanning tree (802.1w)
  - Flooding
  - Forwarding/blocking
  - Filtering
  - Interface configuration
- Trunking/802.1q
- Tag vs. untag VLANs
- 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
  - Ad hoc
  - 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 choking
    - 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
- Vulnerabilities
  - Zero-day attacks
  - 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/TLSSL
- MAC filtering
- User authentication
  - CHAP/MSCHAP
  - PAP
  - EAP
  - Kerberos
  - Multifactor authentication
  - Two-factor authentication
  - Single sign-on
- Hashes
  - MD5
  - SHA

CompTIA Network+ Certification Exam Objectives Version 2.0 (Exam Number: N10-006)
3.0 Network Security

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
  - ipconfig
  - netstat
  - 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
4.0 Troubleshooting

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
4.0 Troubleshooting

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/TCP ports
- Domain/local group configurations
- Jamming

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 rates
- 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
  - 1000BaseFX
  - 10GBaseT
  - 100BaseFX
- 10GBaseSR
- 10GBaseER
- 10GBaseSW
- IEEE 1905.1-2013
- Ethernet over HDMI
- Ethernet over power line
- Wiring standards
  - EIA/TIA 568A/568B
- Broadband standards
  - DOCSIS
5.0 Industry Standards, Practices, and Network Theory

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
  - Place
  - 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.

<table>
<thead>
<tr>
<th>ACRONYM</th>
<th>SPELLED OUT</th>
<th>ACRONYM</th>
<th>SPELLED OUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Address</td>
<td>CAM</td>
<td>Channel Access Method</td>
</tr>
<tr>
<td>AAA</td>
<td>Authentication, Authorization and Accounting</td>
<td>CAN</td>
<td>Campus Area Network</td>
</tr>
<tr>
<td>AAAA</td>
<td>Authentication, Authorization, Accounting and Address</td>
<td>CARP</td>
<td>Common Address Redundancy Protocol</td>
</tr>
<tr>
<td>ABR</td>
<td>Area Border Router</td>
<td>CAT</td>
<td>Computer And Telephone</td>
</tr>
<tr>
<td>ACL</td>
<td>Access Control List</td>
<td>CCTV</td>
<td>Closed Circuit TV</td>
</tr>
<tr>
<td>AD</td>
<td>Active Directory</td>
<td>CDMA</td>
<td>Code Division Multiple Access</td>
</tr>
<tr>
<td>ADSL</td>
<td>Asymmetric Digital Subscriber Line</td>
<td>CDMA/CD</td>
<td>Carrier Sense Multiple Access/Collision Detection</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
<td>CHAP</td>
<td>Challenge Handshake Authentication Protocol</td>
</tr>
<tr>
<td>AH</td>
<td>Authentication Header</td>
<td>CIDR</td>
<td>Classless Inter-Domain Routing</td>
</tr>
<tr>
<td>AP</td>
<td>Access Point</td>
<td>CIFS</td>
<td>Common Internet File System/Services</td>
</tr>
<tr>
<td>APC</td>
<td>Angle Polished Connector</td>
<td>CLI</td>
<td>Command Line Interface</td>
</tr>
<tr>
<td>APIPA</td>
<td>Automatic Private Internet Protocol Addressing</td>
<td>CNAME</td>
<td>Canonical Name</td>
</tr>
<tr>
<td>APT</td>
<td>Advanced Persistent Protocol</td>
<td>COOP</td>
<td>Concurrent Object-Oriented Programming</td>
</tr>
<tr>
<td>ARIN</td>
<td>American Registry for Internet Numbers</td>
<td>COS</td>
<td>Class Of Service</td>
</tr>
<tr>
<td>ARP</td>
<td>Address Resolution Protocol</td>
<td>CRAM</td>
<td>Challenge-Response Authentication Mechanism–Message Digest 5</td>
</tr>
<tr>
<td>AS</td>
<td>Autonomous System</td>
<td>CRC</td>
<td>Cyclic Redundancy Checking</td>
</tr>
<tr>
<td>ASIC</td>
<td>Application Specific Integrated Circuit</td>
<td>CSMA/CA</td>
<td>Carrier Sense Multiple Access/Collision Avoidance</td>
</tr>
<tr>
<td>ASP</td>
<td>Application Service Provider</td>
<td>CSU</td>
<td>Channel Service Unit</td>
</tr>
<tr>
<td>ATM</td>
<td>Asynchronous Transfer Mode</td>
<td>CWDM</td>
<td>Course Wave Division Multiplexing</td>
</tr>
<tr>
<td>AUI</td>
<td>Attachment Unit Interface</td>
<td>dB</td>
<td>Decibels</td>
</tr>
<tr>
<td>AUP</td>
<td>Acceptable Use Policy</td>
<td>DCS</td>
<td>Distributed Computer System</td>
</tr>
<tr>
<td>BCP</td>
<td>Business Continuity Plan</td>
<td>DDoS</td>
<td>Distributed Denial of Service</td>
</tr>
<tr>
<td>BCS</td>
<td>Business Connectivity Services</td>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>BDR</td>
<td>Backup Designated Router</td>
<td>DLC</td>
<td>Data Link Control</td>
</tr>
<tr>
<td>BERT</td>
<td>Bit Error Rate Test</td>
<td>DLP</td>
<td>Data Leak Prevention</td>
</tr>
<tr>
<td>BGP</td>
<td>Border Gateway Protocol</td>
<td>DLR</td>
<td>Device Level Ring</td>
</tr>
<tr>
<td>BLE</td>
<td>Bluetooth Low Energy</td>
<td>DMZ</td>
<td>Demilitarized Zone</td>
</tr>
<tr>
<td>BNC</td>
<td>British Naval Connector</td>
<td>DNAT</td>
<td>Destination Network Address Translation</td>
</tr>
<tr>
<td>or Bayonet Neill-Concelman</td>
<td></td>
<td>DNS</td>
<td>Domain Name Service or Domain Name Server or Domain Name System</td>
</tr>
<tr>
<td>BootP</td>
<td>Boot Protocol or Bootstrap Protocol</td>
<td>DOC/</td>
<td>Data-Over-Cable Service Interface Specification</td>
</tr>
<tr>
<td>BPDU</td>
<td>Bridge Protocol Data Unit</td>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>BRI</td>
<td>Basic Rate Interface</td>
<td>DR</td>
<td>Designated Router</td>
</tr>
<tr>
<td>BSSID</td>
<td>Basic Service Set Identifier</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BYOD</td>
<td>Bring Your Own Device</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACRONYM</td>
<td>SPELLED OUT</td>
<td>ACRONYM</td>
<td>SPELLED OUT</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------</td>
<td>------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>DSCP</td>
<td>Differentiated Services Code Point</td>
<td>IaaS</td>
<td>Infrastructure as a Service</td>
</tr>
<tr>
<td>DSL</td>
<td>Digital Subscriber Line</td>
<td>IANA</td>
<td>Internet Assigned Numbers Authority</td>
</tr>
<tr>
<td>DSSS</td>
<td>Direct Sequence Spread Spectrum</td>
<td>ICA</td>
<td>Independent Computer Architecture</td>
</tr>
<tr>
<td>DSU</td>
<td>Data Service Unit</td>
<td>ICANN</td>
<td>Internet Corporation for Assigned Names and Numbers</td>
</tr>
<tr>
<td>DWDM</td>
<td>Dense Wavelength Division Multiplexing</td>
<td>ICMP</td>
<td>Internet Control Message Protocol</td>
</tr>
<tr>
<td>E1</td>
<td>E-Carrier Level 1</td>
<td>ICS</td>
<td>Internet Connection Sharing or Industrial Control System</td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
<td>IDF</td>
<td>Intermediate Distribution Frame</td>
</tr>
<tr>
<td>EDNS</td>
<td>Extension Mechanisms for DNS</td>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>EGP</td>
<td>Exterior Gateway Protocol</td>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>EIA/TIA</td>
<td>Electronic Industries Alliance/Telecommunication Industries Association</td>
<td>IGMP</td>
<td>Internet Group Multicast Protocol</td>
</tr>
<tr>
<td>EIGRP</td>
<td>Enhanced Interior Gateway Routing Protocol</td>
<td>IGP</td>
<td>Interior Gateway Protocol</td>
</tr>
<tr>
<td>EMI</td>
<td>Electromagnetic Interference</td>
<td>IGRP</td>
<td>Interior Gateway Routing Protocol</td>
</tr>
<tr>
<td>ESD</td>
<td>Electrostatic Discharge</td>
<td>IKE</td>
<td>Internet Key Exchange</td>
</tr>
<tr>
<td>ESP</td>
<td>Encapsulated Security Packets</td>
<td>IMAP4</td>
<td>Internet Message Access Protocol version 4</td>
</tr>
<tr>
<td>ESSID</td>
<td>Extended Service Set Identifier</td>
<td>InterNIC</td>
<td>Internet Network Information Center</td>
</tr>
<tr>
<td>EUI</td>
<td>Extended Unique Identifier</td>
<td>IO</td>
<td>Input/Output</td>
</tr>
<tr>
<td>FC</td>
<td>Fibre Channel</td>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>FCS</td>
<td>Frame Check Sequence</td>
<td>IPS</td>
<td>Intrusion Prevention System</td>
</tr>
<tr>
<td>FDDI</td>
<td>Fiber Distributed Data Interface</td>
<td>IPSec</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>FDM</td>
<td>Frequency Division Multiplexing</td>
<td>IPv4</td>
<td>Internet Protocol version 4</td>
</tr>
<tr>
<td>FHSS</td>
<td>Frequency Hopping Spread Spectrum</td>
<td>IPv6</td>
<td>Internet Protocol version 6</td>
</tr>
<tr>
<td>FIPS</td>
<td>Federal Information Processing Standard</td>
<td>IR</td>
<td>Infrared</td>
</tr>
<tr>
<td>FM</td>
<td>Frequency Modulation</td>
<td>ISAKMP</td>
<td>Internet Security Association and Key Management Protocol</td>
</tr>
<tr>
<td>FQDN</td>
<td>Fully Qualified Domain Name</td>
<td>iSCSI</td>
<td>Internet Small Computer System</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
<td>ISDN</td>
<td>Integrated Services Digital Network</td>
</tr>
<tr>
<td>GBIC</td>
<td>Gigabit Interface Converter</td>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>Gbps</td>
<td>Gigabits per second</td>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>GLBP</td>
<td>Gateway Load Balancing Protocol</td>
<td>ITS</td>
<td>Intelligent Transportation System</td>
</tr>
<tr>
<td>GPG</td>
<td>GNU Privacy Guard</td>
<td>IV</td>
<td>Initialization Vector</td>
</tr>
<tr>
<td>GPRS</td>
<td>General Packet Radio Service</td>
<td>Kbps</td>
<td>Kilobits per second</td>
</tr>
<tr>
<td>GRE</td>
<td>Generic Routing Encapsulation</td>
<td>KVM</td>
<td>Keyboard Video Mouse</td>
</tr>
<tr>
<td>GSM</td>
<td>Global System for Mobile communications</td>
<td>L2F</td>
<td>Layer 2 Forwarding</td>
</tr>
<tr>
<td>HBA</td>
<td>Host Bus Adapter</td>
<td>L2TP</td>
<td>Layer 2 Tunneling Protocol</td>
</tr>
<tr>
<td>HDLC</td>
<td>High-level Data Link Control</td>
<td>LACP</td>
<td>Link Aggregation Control Protocol</td>
</tr>
<tr>
<td>HDMI</td>
<td>High Definition Multimedia Interface</td>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>HIDS</td>
<td>Host Intrusion Detection System</td>
<td>LC</td>
<td>Local Connector</td>
</tr>
<tr>
<td>HIPS</td>
<td>Host Intrusion Prevention System</td>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>HSPA</td>
<td>High-Speed Packet Access</td>
<td>LEC</td>
<td>Local Exchange Carrier</td>
</tr>
<tr>
<td>HSRP</td>
<td>Hot Standby Router Protocol</td>
<td>LED</td>
<td>Light Emitting Diode</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
<td>LLC</td>
<td>Logical Link Control</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol Secure</td>
<td>LSA</td>
<td>Link State Advertisement</td>
</tr>
<tr>
<td>HVAC</td>
<td>Heating, Ventilation and Air Conditioning</td>
<td>LTE</td>
<td>Long Term Evolution</td>
</tr>
<tr>
<td>Hz</td>
<td>Hertz</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACRONYM</td>
<td>SPELLED OUT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LWAPP</td>
<td>Light Weight Access Point Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control or Medium Access Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAN</td>
<td>Metropolitan Area Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mbps</td>
<td>Megabits per second</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MBps</td>
<td>Megabytes per second</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MDF</td>
<td>Main Distribution Frame</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MDI</td>
<td>Media Dependent Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MDIX</td>
<td>Media Dependent Interface Crossover</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MGCP</td>
<td>Media Gateway Control Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MIB</td>
<td>Management Information Base</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MIBS</td>
<td>Management Information Bases</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MIMO</td>
<td>Multiple Input, Multiple Output</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MLA</td>
<td>Master License Agreement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MLA</td>
<td>Multilateral Agreement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MMF</td>
<td>Multimode Fiber</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MOA</td>
<td>Memorandum Of Agreement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MOU</td>
<td>Memorandum Of Understanding</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPLS</td>
<td>Multi-Protocol Label Switching</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MS-CHAP</td>
<td>Microsoft Challenge Handshake Authentication Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MSA</td>
<td>Master Service Agreement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MSDS</td>
<td>Material Safety Data Sheet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MT-RJ</td>
<td>Mechanical Transfer-Registered Jack</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum Transmission Unit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MUMIMO</td>
<td>Multiplexer Multiple Input, Multiple Output</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MX</td>
<td>Mail Exchanger</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAC</td>
<td>Network Access Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAS</td>
<td>Network Attached Storage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NCP</td>
<td>Network Control Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NDR</td>
<td>Non-Delivery Receipt</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NetBEUI</td>
<td>Network Basic Input/Output</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NetBIOS</td>
<td>Network Basic Input/Output System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NFC</td>
<td>Near Field Communication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NFS</td>
<td>Network File Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NIC</td>
<td>Network Interface Card</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NIDS</td>
<td>Network Intrusion Detection System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NIPS</td>
<td>Network Intrusion Prevention System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NIST</td>
<td>Network Information Security &amp; Technology</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NIU</td>
<td>Network Interface Unit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>nm</td>
<td>Nanometer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NMS</td>
<td>Network Management System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NNTP</td>
<td>Network News Transport Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACRONYM</th>
<th>SPELLED OUT</th>
</tr>
</thead>
<tbody>
<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>P2P</td>
<td>Peer-to-Peer</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>PBX</td>
<td>Private Branch Exchange</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>PCM</td>
<td>Phase Change Memory</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>PLC</td>
<td>Programmable Logic Controller</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>POT5</td>
<td>Plain Old Telephone System</td>
</tr>
<tr>
<td>PPP</td>
<td>Point-to-Point Protocol</td>
</tr>
<tr>
<td>PPoE</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>QAM</td>
<td>Quadrature Amplitude Modulation</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>RDS</td>
<td>Radio Data System</td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency</td>
</tr>
<tr>
<td>RFI</td>
<td>Radio Frequency Interference</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio Frequency Identification</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>RPO</td>
<td>Recovery Point Objective</td>
</tr>
<tr>
<td>ACRONYM</td>
<td>SPELLED OUT</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest, Shamir, Adelman</td>
</tr>
<tr>
<td>RSH</td>
<td>Remote Shell</td>
</tr>
<tr>
<td>RSTP</td>
<td>Rapid Spanning Tree Protocol</td>
</tr>
<tr>
<td>RTP</td>
<td>Real-Time Protocol</td>
</tr>
<tr>
<td>RTS/CTS</td>
<td>Request to Send/Clear to Send</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>SAN</td>
<td>Storage Area Network</td>
</tr>
<tr>
<td>SATA</td>
<td>Serial Advanced Technology Attachment</td>
</tr>
<tr>
<td>SC</td>
<td>Standard Connector or Subscriber Connector</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control And Data Acquisition</td>
</tr>
<tr>
<td>SCP</td>
<td>Secure File Transfer 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>SDSSL</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>SLAAC</td>
<td>Stateless Address Auto Configuration</td>
</tr>
<tr>
<td>SLIP</td>
<td>Serial Line Internet Protocol</td>
</tr>
<tr>
<td>SMB</td>
<td>Server Message Block</td>
</tr>
<tr>
<td>SMF</td>
<td>Single-Mode Fiber</td>
</tr>
<tr>
<td>S/MIME</td>
<td>Secure/Multipurpose Internet Email Extensions</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 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>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>SQL</td>
<td>Search and Query Language</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 or Shielded Twisted Pair</td>
</tr>
<tr>
<td>SVC</td>
<td>Switched Virtual Circuit</td>
</tr>
<tr>
<td>SYSLOG</td>
<td>System Log</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACRONYM</th>
<th>SPELLED OUT</th>
</tr>
</thead>
<tbody>
<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 Plus</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>VDI</td>
<td>Video Device Interface</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>VRF</td>
<td>Virtual Routing Forwarding</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 or 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>
<tr>
<td>WPA</td>
<td>WiFi Protected Access</td>
</tr>
<tr>
<td>WPS</td>
<td>WiFi Protected Setup</td>
</tr>
<tr>
<td>WWN</td>
<td>World Wide Name</td>
</tr>
<tr>
<td>WWW</td>
<td>World Wide Web</td>
</tr>
<tr>
<td>XDSL</td>
<td>Extended Digital Subscriber Line</td>
</tr>
<tr>
<td>XML</td>
<td>Extensible Markup Language</td>
</tr>
<tr>
<td>ZEROCONF</td>
<td>Zero configuration</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
- 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 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
- Anti-malware software
- Network monitoring software

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

© 2016 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 Jan 2016