



# CompTIA Network+ Certification Exam Objectives

**EXAM NUMBER: N10-009**



# About the Exam

The CompTIA Network+ certification exam will certify the successful candidate has the knowledge and skills required to:

- Establish network connectivity by deploying wired and wireless devices.
- Explain the purpose of documentation and maintain network documentation.
- Configure common network services.
- Explain basic data-center, cloud, and virtual-networking concepts.
- Monitor network activity and troubleshoot performance and availability issues.
- Implement network security hardening techniques.
- Manage, configure, and troubleshoot network infrastructure.

## **EXAM DEVELOPMENT**

CompTIA exams result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an 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”), they should contact CompTIA at [examsecurity@comptia.org](mailto: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	N10-009
Number of questions	Maximum of 90
Types of questions	Multiple-choice and performance-based
Length of test	90 minutes
Recommended experience	A minimum of 9–12 months of experience in the IT networking field

## EXAM OBJECTIVES (DOMAINS)

The table below lists the domains measured by this examination and the extent to which they are represented.

DOMAIN	PERCENTAGE OF EXAMINATION
1.0 Networking Concepts	23%
2.0 Network Implementation	20%
3.0 Network Operations	19%
4.0 Network Security	14%
5.0 Network Troubleshooting	24%
<b>Total</b>	<b>100%</b>



## 1.0 Networking Concepts

**1.1** Explain concepts related to the Open Systems Interconnection (OSI) reference model.

**EASY**

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

**1.2** Compare and contrast networking appliances, applications, and functions.

**EASY**

- **Physical and virtual appliances**
  - Router
  - Switch
  - Firewall
  - Intrusion detection system (IDS)/intrusion prevention system (IPS)
  - Load balancer
  - Proxy
  - Network-attached storage (NAS)
- **Applications**
  - Storage area network (SAN)
  - Wireless
    - Access point (AP)
    - Controller
- **Functions**
  - Content delivery network (CDN)
  - Virtual private network (VPN)
  - Quality of service (QoS)
  - Time to live (TTL)

**1.3** Summarize cloud concepts and connectivity options.

**EASY**

**COM**

- Network functions virtualization (NFV)
- Virtual private cloud (VPC)
- Network security groups
- Network security lists
- Cloud gateways
  - Internet gateway
  - Network address translation (NAT) gateway
- Cloud connectivity options
  - VPN
  - Direct Connect
- Deployment models
  - Public
  - Private
  - Hybrid
- Service models
  - Software as a service (SaaS)
  - Infrastructure as a service (IaaS)
  - Platform as a service (PaaS)
- Scalability
- Elasticity
- Multitenancy



## 1.4 Explain common networking ports, protocols, services, and traffic types.

EASY TO UNDERSTAND  
BUT NEED TO MUG UP

### Protocols

File Transfer Protocol (FTP)	
Secure File Transfer Protocol (SFTP)	
Secure Shell (SSH)	
Telnet	
Simple Mail Transfer Protocol (SMTP)	
Domain Name System (DNS)	
Dynamic Host Configuration Protocol (DHCP)	
Trivial File Transfer Protocol (TFTP)	
Hypertext Transfer Protocol (HTTP)	
Network Time Protocol (NTP)	
Simple Network Management Protocol (SNMP)	
Lightweight Directory Access Protocol (LDAP)	
Hypertext Transfer Protocol Secure (HTTPS)	
Server Message Block (SMB)	
Syslog	
Simple Mail Transfer Protocol Secure (SMTPLS)	
Lightweight Directory Access Protocol over SSL (LDAPS)	
Structured Query Language (SQL) Server	
Remote Desktop Protocol (RDP)	
Session Initiation Protocol (SIP)	

### Ports

20/21
22
22
23
25
53
67/68
69
80
123
161/162
389
443
445
514
587
636
1433
3389
5060/5061

- Internet Protocol (IP) types
  - Internet Control Message Protocol (ICMP)
  - Transmission Control Protocol (TCP)
  - User Datagram Protocol (UDP)
  - Generic Routing Encapsulation (GRE)
  - Internet Protocol Security (IPSec)
    - Authentication Header (AH)
    - Encapsulating Security Payload (ESP)
    - Internet Key Exchange (IKE)
- Traffic types
  - Unicast
  - Multicast
  - Anycast
  - Broadcast



## 1.5 Compare and contrast transmission media and transceivers.

- **Wireless**
    - 802.11 standards
    - Cellular
    - Satellite
  - **Wired**
    - 802.3 standards
    - Single-mode vs. multimode fiber
    - Direct attach copper (DAC) cable
      - Twinaxial cable
    - Coaxial cable
    - Cable speeds
    - Plenum vs. non-plenum cable
  - **Transceivers**
    - Protocol
- |  |  |   |
|--|--|---|
| <ul style="list-style-type: none"> <li>▫ Ethernet</li> <li>▫ Fibre Channel (FC)</li> <li>- Form factors           <ul style="list-style-type: none"> <li>▫ Small form-factor pluggable (SFP)</li> <li>▫ Quad small form-factor pluggable (QSFP)</li> </ul> </li> </ul> | <ul style="list-style-type: none"> <li>▫ Ethernet</li> <li>▫ Fibre Channel (FC)</li> <li>- Form factors           <ul style="list-style-type: none"> <li>▫ Small form-factor pluggable (SFP)</li> <li>▫ Quad small form-factor pluggable (QSFP)</li> </ul> </li> </ul> | <ul style="list-style-type: none"> <li>- Bayonet Neill-Concelman (BNC)</li> </ul> <p><b>EASY TO UNDERSTAND<br/>BUT NEED TO MUG UP</b></p> |
|--|--|---|
- **Connector types**
    - Subscriber connector (SC)
    - Local connector (LC)
    - Straight tip (ST)
    - Multi-fiber push on (MPO)
    - Registered jack (RJ)11
    - RJ45
    - F-type

## 1.6 Compare and contrast network topologies, architectures, and types.

EASY

COM

- Mesh
- Hybrid
- Star/hub and spoke
- Spine and leaf
- Point to point
- Three-tier hierarchical model
  - Core
  - Distribution
  - Access

- Collapsed core
- Traffic flows
  - North-south
  - East-west

## 1.7 Given a scenario, use appropriate IPv4 network addressing.

MEDIUM

- **Public vs. private**
  - Automatic Private IP Addressing (APIPA)
  - RFC1918
  - Loopback/localhost
- **Subnetting**
  - Variable Length Subnet Mask (VLSM)
  - Classless Inter-domain Routing (CIDR)
- **IPv4 address classes**
  - Class A
  - Class B
  - Class C
  - Class D
  - Class E



## 1.8 Summarize evolving use cases for modern network environments.

- Software-defined network (SDN) and software-defined wide area network (SD-WAN)
  - Application aware
  - Zero-touch provisioning
  - Transport agnostic
  - Central policy management
- Virtual Extensible Local Area Network (VXLAN)
  - Data center interconnect (DCI)
  - Layer 2 encapsulation
- Zero trust architecture (ZTA)
  - Policy-based authentication
  - Authorization
  - Least privilege access
- Secure Access Secure Edge (SASE)/Security Service Edge (SSE)
- Infrastructure as code (IaC)
  - Automation
    - Playbooks/templates/reusable tasks
    - Configuration drift/compliance
    - Upgrades
    - Dynamic inventories
  - Source control
    - Version control
    - Central repository
    - Conflict identification
    - Branching
- IPv6 addressing
  - Mitigating address exhaustion
  - Compatibility requirements
    - Tunneling
    - Dual stack
    - NAT64



## 2.0 Network Implementation

### 2.1 Explain characteristics of routing technologies.

- Static routing
- Dynamic routing
  - Border Gateway Protocol (BGP)
  - Enhanced Interior Gateway Routing Protocol (EIGRP)
  - Open Shortest Path First (OSPF)
- Route selection
  - Administrative distance
  - Prefix length
  - Metric
- Address translation
  - NAT
  - Port address translation (PAT)
- First Hop Redundancy Protocol (FHRP)
- Virtual IP (VIP)
- Subinterfaces

### 2.2 Given a scenario, configure switching technologies and features.

EASY

- Virtual Local Area Network (VLAN)
  - VLAN database
  - Switch Virtual Interface (SVI)
- Interface configuration
  - Native VLAN
  - Voice VLAN
- 802.1Q tagging
- Link aggregation
- Speed
- Duplex
- Spanning tree
- Maximum transmission unit (MTU)
  - Jumbo frames

### 2.3 Given a scenario, select and configure wireless devices and technologies.

MEDIUM

- Channels
  - Channel width
  - Non-overlapping channels
  - Regulatory impacts
    - 802.11h
- Frequency options
  - 2.4GHz
  - 5GHz
  - 6GHz
  - Band steering
- Service set identifier (SSID)
  - Basic service set identifier (BSSID)
- Extended service set identifier (ESSID)
- Network types
  - Mesh networks
  - Ad hoc
  - Point to point
  - Infrastructure
- Encryption
  - Wi-Fi Protected Access 2 (WPA2)
  - WPA3
- Authentication
  - Pre-shared key (PSK) vs. Enterprise
- Antennas
  - Omnidirectional vs. directional
- Autonomous vs. lightweight access point
- Guest networks
  - Captive portals



## 2.4 Explain important factors of physical installations.

**EASY**

- Important installation implications

**COM**

- Locations
  - Intermediate distribution frame (IDF)
  - Main distribution frame (MDF)
- Rack size
- Port-side exhaust/intake
- Cabling
  - Patch panel
  - Fiber distribution panel
- Lockable

- Power

- Uninterruptible power supply (UPS)
- Power distribution unit (PDU)
- Power load
- Voltage

- Environmental factors

- Humidity
- Fire suppression
- Temperature



EASY

## 3.0 Network Operations

### 3.1 Explain the purpose of organizational processes and EASY procedures.

- Documentation
  - Physical vs. logical diagrams
  - Rack diagrams
  - Cable maps and diagrams
  - Network diagrams
    - Layer 1
    - Layer 2
    - Layer 3
  - Asset inventory
    - Hardware
    - Software
    - Licensing
    - Warranty support
  - IP address management (IPAM)
  - Service-level agreement (SLA)
  - Wireless survey/heat map
- Life-cycle management
  - End-of-life (EOL)
  - End-of-support (EOS)
  - Software management
    - Patches and bug fixes
    - Operating system (OS)
    - Firmware
  - Decommissioning
- Change management
  - Request process tracking/  
service request
- Configuration management
  - Production configuration
  - Backup configuration
  - Baseline/golden configuration

### 3.2 Given a scenario, use network monitoring technologies.

EASY TO  
MEDIUM

- Methods
  - SNMP
    - Traps
    - Management information base (MIB)
    - Versions
      - o v2c
      - o v3
    - Community strings
    - Authentication
- Solutions
  - Flow data
  - Packet capture
  - Baseline metrics
    - Anomaly alerting/notification
  - Log aggregation
    - Syslog collector
    - Security information and event management (SIEM)
  - Application programming interface (API) integration
  - Port mirroring



### 3.3 Explain disaster recovery (DR) concepts.

EASY

- DR metrics
  - Recovery point objective (RPO)
  - Recovery time objective (RTO)
  - Mean time to repair (MTTR)
  - Mean time between failures (MTBF)
- DR sites
  - Cold site
  - Warm site
  - Hot site
- High-availability approaches
  - Active-active
  - Active-passive
- Testing
  - Tabletop exercises
  - Validation tests

### 3.4 Given a scenario, implement IPv4 and IPv6 network services.

EASY

- Dynamic addressing
  - DHCP
    - Reservations
    - Scope
    - Lease time
    - Options
    - Relay/IP helper
    - Exclusions
  - Stateless address autoconfiguration (SLAAC)
- Name resolution
  - DNS
    - Domain Name Security Extensions (DNSSEC)
    - DNS over HTTPS (DoH) and DNS over TLS (DoT)
  - Record types
    - o Address (A)
    - o AAAA
    - o Canonical name (CNAME)
    - o Mail exchange (MX)
    - o Text (TXT)
    - o Nameserver (NS)
    - o Pointer (PTR)
  - Zone types
    - o Forward
    - o Reverse
  - Authoritative vs. non-authoritative
  - Primary vs. secondary
  - Recursive
  - Hosts file
- Time protocols
  - NTP
  - Precision Time Protocol (PTP)
  - Network Time Security (NTS)

### 3.5 Compare and contrast network access and management methods.

EASY

- Site-to-site VPN
- Client-to-site VPN
  - Clientless
  - Split tunnel vs. full tunnel
- Connection methods
  - SSH
  - Graphical user interface (GUI)
  - API
  - Console
- Jump box/host
- In-band vs. out-of-band management



EASY

## 4.0 Network Security

### 4.1 Explain the importance of basic network security concepts.

EASY

- **Logical security**
    - Encryption
      - Data in transit
      - Data at rest
    - Certificates
      - Public key infrastructure (PKI)
      - Self-signed
    - Identity and access management (IAM)
      - Authentication
        - Multifactor authentication (MFA)
        - Single sign-on (SSO)
        - Remote Authentication Dial-in User Service (RADIUS)
        - LDAP
        - Security Assertion Markup Language (SAML)
        - Terminal Access Controller Access Control System Plus (TACACS+)
        - Time-based authentication
  - Authorization
    - Least privilege
    - Role-based access control
  - Geofencing
- **Physical security**
  - Camera
  - Locks
- **Deception technologies**
  - Honeypot
  - Honeynet
- **Common security terminology**
  - Risk
  - Vulnerability
  - Exploit
  - Threat
  - Confidentiality, Integrity, and Availability (CIA) triad
- **Audits and regulatory compliance**
  - Data locality
  - Payment Card Industry Data Security Standards (PCI DSS)
  - General Data Protection Regulation (GDPR)

### 4.2 Summarize various types of attacks and their impact to the network.

EASY

- Denial-of-service (DoS)/distributed denial-of-service (DDoS)
- VLAN hopping
- Media Access Control (MAC) flooding
- Address Resolution Protocol (ARP) poisoning
- ARP spoofing
- DNS poisoning
- DNS spoofing
- Rogue devices and services
  - DHCP
  - AP
- Evil twin
- On-path attack
- Social engineering
  - Phishing
  - Dumpster diving
  - Shoulder surfing
  - Tailgating
- Malware



## 4.3 Given a scenario, apply network security features, defense techniques, and solutions.

EASY TO  
MEDIUM

- Device hardening
  - Disable unused ports and services
  - Change default passwords
- Network access control (NAC)
  - Port security
  - 802.1X
  - MAC filtering
- Key management
- Security rules
  - Access control list (ACL)
  - Uniform Resource Locator (URL) filtering
  - Content filtering
- Zones
  - Trusted vs. untrusted
  - Screened subnet



EASY

## 5.0 Network Troubleshooting

### 5.1 Explain the troubleshooting methodology.

EASY

- Identify the problem
  - Gather information
  - Question users
  - Identify symptoms
  - Determine if anything has changed
  - Duplicate the problem, if possible
  - Approach multiple problems individually
- Establish a theory of probable cause
  - Question the obvious
  - Consider multiple approaches
    - Top-to-bottom/bottom-to-top OSI model
    - Divide and conquer
- Test the theory to determine the cause
  - If theory is confirmed, determine next steps to resolve problem
  - If theory is not confirmed, establish a new theory or escalate
- Establish a plan of action to resolve the problem and identify potential effects
- Implement the solution or escalate as necessary
- Verify full system functionality and implement preventive measures if applicable
- Document findings, actions, outcomes, and lessons learned throughout the process

### 5.2 Given a scenario, troubleshoot common cabling and physical interface issues.

- Cable issues
  - Incorrect cable
    - Single mode vs. multimode
    - Category 5/6/7/8
    - Shielded twisted pair (STP) vs. unshielded twisted pair (UTP)
  - Signal degradation
    - Crosstalk
    - Interference
    - Attenuation
  - Improper termination
  - Transmitter (TX)/Receiver (RX) transposed
- Interface issues
  - Increasing interface counters
    - Cyclic redundancy check (CRC)
- Hardware issues
  - Port status
    - Runts
    - Giants
    - Drops
  - Power over Ethernet (PoE)
    - Power budget exceeded
    - Incorrect standard
  - Transceivers
    - Mismatch
    - Signal strength



## 5.3 Given a scenario, troubleshoot common issues with network services.

- **Switching issues**
  - STP
    - Network loops
    - Root bridge selection
    - Port roles
    - Port states
  - Incorrect VLAN assignment
  - ACLs

- **Route selection**
  - Routing table
  - Default routes
- **Address pool exhaustion**
- **Incorrect default gateway**
- **Incorrect IP address**
  - Duplicate IP address
- **Incorrect subnet mask**

SHOULD REMEBER THE TOPICS  
THATS IT AND MOST OF THEM ARE COVERED IN BEFORE MODULES

## 5.4 Given a scenario, troubleshoot common performance issues.

**EASY**

- Congestion/contention
- Bottlenecking
- Bandwidth
  - Throughput capacity
- Latency
- Packet loss
- Jitter

- **Wireless**
  - Interference
    - Channel overlap
  - Signal degradation or loss
  - Insufficient wireless coverage
  - Client disassociation issues
  - Roaming misconfiguration

## 5.5 Given a scenario, use the appropriate tool or protocol to solve networking issues.

- **Software tools**
  - Protocol analyzer
  - Command line
    - ping
    - traceroute/tracert
    - nslookup
    - tcpdump
    - dig
    - netstat
    - ip/ifconfig/ipconfig
    - arp

- Nmap
- Link Layer Discovery Protocol (LLDP)/Cisco Discovery Protocol (CDP)
- Speed tester
- **Hardware tools**
  - Toner
  - Cable tester
  - Taps
  - Wi-Fi analyzer
  - Visual fault locator

- **Basic networking device commands**
  - show mac-address-table
  - show route
  - show interface
  - show config
  - show arp
  - show vlan
  - show power

# CompTIA Network+ N10-009 Acronym List

The following is a list of acronyms that appear on the CompTIA Network+ N10-009 exam. Candidates are encouraged to review the complete list and attain a working knowledge of all listed acronyms as part of a comprehensive exam preparation program.

<b>Acronym</b>	<b>Spelled Out</b>	<b>Acronym</b>	<b>Spelled Out</b>
A	Address	EIGRP	Enhanced Interior Gateway Routing Protocol
ACL	Access Control List	EOL	End-of-life
AH	Authentication Header	EOS	End-of-support
AP	Access Point	ESP	Encapsulating Security Payload
API	Application Programming Interface	ESSID	Extended Service Set Identifier
APIPA	Automatic Private Internet Protocol Addressing	EULA	End User License Agreement
ARP	Address Resolution Protocol	FC	Fibre Channel
AUP	Acceptable Use Policy	FHRP	First Hop Redundancy Protocol
BGP	Border Gateway Protocol	FTP	File Transfer Protocol
BNC	Bayonet Neill-Concelman	GDPR	General Data Protection Regulation
BSSID	Basic Service Set Identifier	GRE	Generic Routing Encapsulation
BYOD	Bring Your Own Device	GUI	Graphical User Interface
CAM	Content-addressable Memory	HTTP	Hypertext Transfer Protocol
CDN	Content Delivery Network	HTTPS	Hypertext Transfer Protocol Secure
CDP	Cisco Discovery Protocol	IaaS	Infrastructure as a Service
CIA	Confidentiality, Integrity, and Availability	IaC	Infrastructure as Code
CIDR	Classless Inter-domain Routing	IAM	Identity and Access Management
CLI	Command-line Interface	ICMP	Internet Control Message Protocol
CNAME	Canonical Name	ICS	Industrial Control System
CPU	Central Processing Unit	IDF	Intermediate Distribution Frame
CRC	Cyclic Redundancy Check	IDS	Intrusion Detection System
DAC	Direct Attach Copper	IoT	Internet of Things
DAS	Direct-attached Storage	IIoT	Industrial Internet of Things
DCI	Data Center Interconnect	IKE	Internet Key Exchange
DDoS	Distributed Denial-of-service	IP	Internet Protocol
DHCP	Dynamic Host Configuration Protocol	IPAM	Internet Protocol Address Management
DLP	Data Loss Prevention	IPS	Intrusion Prevention System
DNS	Domain Name System	IPSec	Internet Protocol Security
DNSSEC	Domain Name System Security Extensions	IS-IS	Intermediate System to Intermediate System
DoH	DNS over Hypertext Transfer Protocol	LACP	Link Aggregation Control Protocol
	Secure	LAN	Local Area Network
DoS	Denial-of-service	LC	Local Connector
DoT	DNS over Transport Layer Security	LDAP	Lightweight Directory Access Protocol
DR	Disaster Recovery	LDAPS	Lightweight Directory Access Protocol over SSL
EAPoL	Extensible Authentication Protocol over LAN	LLDP	Link Layer Discovery Protocol

<b>Acronym</b>	<b>Spelled Out</b>	<b>Acronym</b>	<b>Spelled Out</b>
MAC	Media Access Control	SCADA	Supervisory Control and Data Acquisition
MDF	Main Distribution Frame	SDN	Software-defined Network
MDIX	Medium Dependent Interface Crossover	SD-WAN	Software-defined Wide Area Network
MFA	Multifactor Authentication	SFP	Small Form-factor Pluggable
MIB	Management Information Base	SFTP	Secure File Transfer Protocol
MPO	Multifiber Push On	SIP	Session Initiation Protocol
MTBF	Mean Time Between Failure	SIEM	Security Information and Event Management
MTTR	Mean Time To Repair	SLA	Service-level Agreement
MTU	Maximum Transmission Unit	SLAAC	Stateless Address Autoconfiguration
MX	Mail Exchange	SMB	Server Message Block
NAC	Network Access Control	SMTP	Simple Mail Transfer Protocol
NAS	Network-attached Storage	SMTPS	Simple Mail Transfer Protocol Secure
NAT	Network Address Translation	SNMP	Simple Network Management Protocol
NFV	Network Functions Virtualization	SOA	Start of Authority
NIC	Network Interface Cards	SQL	Structured Query Language
NS	Name Server	SSE	Security Service Edge
NTP	Network Time Protocol	SSH	Secure Shell
NTS	Network Time Security	SSID	Service Set Identifier
OS	Operating System	SSL	Secure Socket Layer
OSPF	Open Shortest Path First	SSO	Single Sign-on
OSI	Open Systems Interconnection	ST	Straight Tip
OT	Operational Technology	STP	Shielded Twisted Pair
PaaS	Platform as a Service	SVI	Switch Virtual Interface
PAT	Port Address Translation	TACAS+	Terminal Access Controller Access Control
PCI DSS	Payment Card Industry Data Security Standards	TCP	Transmission Control Protocol
PDU	Power Distribution Unit	TFTP	Trivial File Transfer Protocol
PKI	Public Key Infrastructure	TTL	Time to Live
PoE	Power over Ethernet	TX	Transmitter
PSK	Pre-shared Key	TXT	Text
PTP	Precision Time Protocol	UDP	User Datagram Protocol
PTR	Pointer	UPS	Uninterruptible Power Supply
QoS	Quality of Service	URL	Uniform Resource Locator
QSFP	Quad Small Form-factor Pluggable	USB	Universal Serial Bus
RADIUS	Remote Authentication Dial-in User Service	UTM	Unified Threat Management
RDP	Remote Desktop Protocol	UTP	Unshielded Twisted Pair
RFID	Radio Frequency Identifier	VIP	Virtual IP
RIP	Routing Information Protocol	VLAN	Virtual Local Area Network
RJ	Registered Jack	VLSM	Variable Length Subnet Mask
RPO	Recovery Point Objective	VoIP	Voice over IP
RSTP	Rapid Spanning Tree Protocol	VPC	Virtual Private Cloud
RTO	Recovery Time Objective	VPN	Virtual Private Network
RX	Receiver	WAN	Wide Area Network
SaaS	Software as a Service	WPA	Wi-Fi Protected Access
SAML	Security Assertion Markup Language	WPS	Wi-Fi Protected Setup
SAN	Storage Area Network	VXLAN	Virtual Extensible LAN
SASE	Secure Access Service Edge	ZTA	Zero Trust Architecture
SC	Subscriber Connector		

# CompTIA 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
- Layer 3 switch/managed switch/PoE switch
- Router
- Firewall
- Wireless access point
- Basic laptops that support virtualization
- Voice over IP (VoIP) phone

## Spare Hardware

- Network interface card (NIC)
- Power supplies
- SFPs
- Wireless access point
- UPS
- PoE injector

## Spare Parts

- Patch cables
  - Fiber
  - Copper
- Antennas
- Bluetooth/wireless adapters
- Console cables [Universal Serial Bus (USB) to RS-232 serial adapter]
- Additional NIC/USB NIC

## Tools

- Cable tester
- Tone generator
- Optical power meter
- PoE Tester

## Software

- Protocol analyzer/packet capture
- Terminal emulation software
- Linux/Windows operating systems
- Software firewall
- Software IDS/IPS
- Network mapper
- Hypervisor software
- IaaS cloud lab/demo accounts
- Virtual network environment
- Wi-Fi analyzer
- Spectrum analyzer
- Network monitoring tools
- Flow data analyzer
- TFTP server
- Various firmware versions

## Other

- Sample network documentation
- Sample logs
- Defective cables
- Cloud network diagrams
- Sample configuration playbook/runbook