CompTIA Network+ Certification Exam Objectives

EXAM NUMBER: N10-010 V10

CompTIA Network+ N10-010 V10 Certification Exam
Exam Objectives Document Version 1.0

CompTIA

About the Exam

The CompTIA Network+ N10-010 V1 certification exam will certify the successful candidate has the knowledge and skills required to:

- Explain basic data center, automation, cloud, virtual networking, and AI concepts.
- Maintain network documentation and adhere to network policies.
- Establish network connectivity by deploying wired and wireless devices.
- Configure and troubleshoot common network services.
- Monitor network activity and troubleshoot performance and availability issues.
- Implement network security hardening techniques.
- Understand basic network security, protocols, and compliance concepts.
- Manage, configure, and troubleshoot network infrastructure.

The target audience consists of professionals with the equivalent of 9–12 months of hands-on experience in the IT networking field or overall approximately 2 years of experience in the IT field.

These content examples are meant to clarify the exam 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 ANSI National Accreditation Board (ANAB) 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 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 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	Network+ N10-010 V1
Number of questions	[TBD]
Types of questions	Multiple-choice and performance-based
Length of test	[TBD]
Recommended experience	Professionals with CompTIA A+ certification or equivalent knowledge. 9–12 months of hands-on IT networking field experience or overall approximately 2 years of experience in the IT field.
Passing score	720 (on a scale of 100–900)

EXAM OBJECTIVES (DOMAINS)

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

DOMAIN		PERCENTAGE OF EXAMINATION
1.0	Networking Concepts	TBD
2.0	Network Implementation	TBD
3.0	Network Operations	TBD
4.0	Network Security	TBD
5.0	Network Troubleshooting	TBD
Total		**100%**

1.0 Networking Concepts

1.1 Compare and contrast networking appliances and functions.

- Appliances
  - Router
  - Switch
  - Firewalls
    - Traditional
    - Next generation
  - Load balancer
  - Wireless
    - Controllers
    - Access point
  - Intrusion prevention system (IPS)
  - Intrusion detection system (IDS)
  - Proxy
  - Servers
- Functions
  - Virtual private network (VPN)
  - Network access control (NAC)

1.2 Explain cloud virtualization concepts.

- Virtualization
  - Containerization
    - Microservices
  - Hypervisor
  - Network function virtualization (NFV)
- Cloud models
  - Private
    - On premises
  - Public
  - Community
  - Hybrid
- Service models
  - Infrastructure as a service (IaaS)
  - Software as a service (SaaS)
  - Platform as a service (PaaS)
- Cloud connectivity options
  - VPN
  - Peering
    - Non-transitive
  - Cloud interconnect services
- Cloud fundamentals
  - Multitenancy
  - Scalability
  - Elasticity

1.3 Explain networking protocols, models, and traffic types.

- Common protocols
  - Domain Name System (DNS)
  - Dynamic Host Configuration Protocol (DHCP)
  - Remote Desktop Protocol (RDP)
  - Network Time Protocol (NTP)
  - Secure Shell (SSH)
  - Server Message Block (SMB)
  - Session Initiation Protocol (SIP)
  - Address Resolution Protocol (ARP)
  - Hypertext Transfer Protocol (HTTP)
  - Transmission Control Protocol (TCP)
  - User Datagram Protocol (UDP)
  - Internet Control Message Protocol (ICMP)
- Ports
  - Well-known
  - Dynamic
- Internet Protocol Security (IPSec)
  - Internet Key Exchange (IKE)
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)
- Generic routing encapsulation (GRE)
- Reference models
  - Open Systems Interconnection (OSI) seven-layer model
  - Transmission Control Protocol /Internet Protocol (TCP/IP) four-layer model
- Protocol data units (PDU)
  - Encapsulation
  - Decapsulation
- Traffic types
  - Unicast
  - Multicast
  - Anycast
  - Broadcast

1.4 Given a scenario, install transmission and media receivers.

- Media types
  - Fiber
    - Single-mode
    - Multimode
  - Copper
    - Shielded
    - Unshielded
    - Plenum
  - Wireless
  - Media converters
- Transceivers
  - Small Form-factor Pluggable (SFP)
  - Quad Small Form-factor Pluggable (QSFP)
- Connector types
  - Local connector (LC)
  - Subscriber connector (SC)
  - Straight tip (ST)
  - Registered Jack Function 11 (RJ11)
  - Registered Jack Function 45 (RJ45)
- Installation considerations
  - Noise
  - Distance
  - Attenuation
  - Interference
  - Weather/climate
  - Budget
  - Bandwidth

1.5 Explain the importance of network topologies, architectures, and types.

- Architectures
  - Two-tier
  - Three-tier
- Topologies
  - Spine-and-leaf
  - Mesh
  - Star/hub-and-spoke
- Types
  - Internet of Things (IoT)
  - Operational technology (OT)
    - Supervisory control and data acquisition (SCADA)
  - Intranet
  - Extranet
  - Demilitarized zone (DMZ)
  - Air-gapped
  - Wireless bridge
- Traffic flow
  - North–south
  - East–west

1.6 Given a scenario, use appropriate Internet Protocol version 4 (IPv4) network addressing.

- Classful addresses
- Classless addresses
  - Variable length subnet mask (VLSM)
- Classless Inter-Domain Routing (CIDR) notation
- Public vs. private IP addresses
  - Request for Comments (RFC) 1918
  - Loopback
  - Automatic Private Internet Protocol Addressing (APIPA)

1.7 Summarize appropriate use cases for modern network environments.

- Zero Trust architecture
  - Policy-based authentication
  - Authorization
  - Least privileged network access
    - Microtunneling
  - Context-aware policies
  - Integrated solutions
- Internet Protocol version 6 (IPv6) addressing
  - Mitigating address exhaustion
    - Stateless address autoconfiguration (SLAAC)
  - Compatibility requirements
    - Tunneling
    - Dual stack
    - Network address translation 64 (NAT64)
- Network automation and programmability
  - Application programming interface (API)
    - Representational State Transfer (REST)
    - Graph Query Language (GraphQL)
    - Simple Object Access Protocol (SOAP)
    - Infrastructure as code (IaC)
    - Automation
      - Playbooks/templates/reusable tasks
      - Configuration drift/compliance
      - Upgrades
      - Dynamic inventories
    - Source control
      - Version control
      - Central repository
      - Conflict identification
      - Branching
- Virtual eXtensible LAN [local area network] (VXLAN)
  - Data center interconnect (DCI)
  - Layer 2 encapsulation
- Software-defined network (SDN) and software-defined wide area network (SD-WAN)
  - Application aware
  - Zero-touch provisioning
  - Transport agnostic
  - Central policy management
- Content delivery network (CDN)

2.0 Network Implementation

2.1 Explain concepts and characteristics of routing technologies.

- Routes
  - Default
  - Dynamic
  - Static
- Route announcement
- IP route table
- Inter-virtual local area network (Inter-VLAN) routing
  - 802.1Q
  - Sub-interface
- Route selection
  - Metrics
  - Attributes
  - Administrative distance
  - Prefix length
- Address translation
  - Network address translation (NAT)
  - Port address translation (PAT)
- First Hop Redundancy Protocol (FHRP)
- Routing protocols
  - Open Shortest Path First (OSPF)
  - Border Gateway Protocol (BGP)
  - Enhanced Interior Gateway Routing Protocol (EIGRP)

2.2 Given a scenario, apply the appropriate configurations on switching technologies.

- Virtual local area network (VLAN)
- Native
- Management
- Default
- Access vs. trunk ports
- Tagged vs. untagged
- Spanning Tree Protocol
  - Bridge selection
  - Port types
  - Port states
  - Modes
- Media access control (MAC) address table
- Link aggregation
  - Link Aggregation Control Protocol (LACP)
  - Multi-chassis Link Aggregation Group (MLAG)
- Port mirroring
- Switch virtual interface (SVI)
- Half duplex
- Full duplex
- Error disable detection
- Power over Ethernet (PoE)
- Cisco Discovery Protocol (CDP)
- Link Layer Discovery Protocol (LLDP)

2.3 Given a scenario, apply the appropriate configurations on wireless technologies and hardware.

- Technologies
  - Encryption
    - Methods
      - Wi-Fi Protected Access (WPA)
        - WPA2
        - WPA3
      - Advanced Encryption Standard (AES)
      - Temporal Key Integrity Protocol (TKIP)
  - Deployment modes
    - Lightweight access points
    - Autonomous access points
  - Wi-Fi standards
    - Wi-Fi 5
    - Wi-Fi 6
    - Wi-Fi 6e
    - Wi-Fi 7
    - Bands
      - 2.4GHz
      - 5GHz
      - 6GHz
    - Band steering
    - Channels
  - Cellular technologies
  - Satellite technologies
  - Basic service set
- Extended service set
- Wireless hardware
  - Controllers
  - Access points
    - Low-power
    - Standard-power
  - Extenders
  - Antennas
    - Directional
    - Omnidirectional
- Guest networks
  - Captive portals
- Network types
  - Point-to-point
  - Point-to-multipoint
  - Mesh

2.4 Explain important aspects of physical installations.

- Environmental factors
  - Power
    - Power distribution units (PDUs)
    - Power source
    - Power load
  - Regional considerations
    - Colocations
  - Heating, ventilation, and air conditioning (HVAC)
    - Humidity
    - Temperature
    - Air flow
      - Port-side exhaust/intake
    - Air cooling vs. water cooling
    - Ventilation
  - Fire suppression system
  - Device placement considerations
    - Location
    - Size
    - Clearance
    - Lockable
  - Data connection
    - Management port setup
    - Cable management
  - Backup power sources
    - Uninterruptible power supply (UPS)
    - Generator
  - Physical security
    - Access control vestibule
    - Video camera
    - Access cards
    - Biometrics
  - Asset labeling
- Telecommunication considerations
  - Intermediate distribution frame (IDF)
  - Main distribution frame (MDF)
  - Patch panel
  - Fiber distribution panel
  - Demarcation point
  - Meet-me room (MMR)
- Safety
  - Personal protective equipment (PPE)
  - Accessibility
  - Crash cart
  - Medical
  - Emergency plans and procedures

3.0 Network Operations

3.1 Given a scenario, apply organizational policies, processes, and procedures.

- Change management
- Service windows
- Network documentation
  - Service-level agreement (SLA)
  - Master service agreement (MSA)
  - Business continuity (BC)/Disaster recovery (DR)
  - Standard operating procedure (SOP)
  - Diagrams
    - Wireless heat map
    - Physical
    - Logical
  - Knowledge base
- Vendor management
  - Licensing
  - Warranty support
  - Lock-in
  - Lock-out
  - Non-disclosure agreement (NDA)
- Incident response
- Backup procedures
- Internal/external compliance
- Ticketing system
- Key risk indicators (KRIs)
- Policies
  - Acceptable use
  - Bring your own device (BYOD)
  - Password
- Asset Inventory
- Life-cycle management
  - End-of-life (EOL)
  - End-of-support (EOS)
  - Software management
    - Patches and bug fixes
    - Operating system (OS)
    - Firmware updates
  - Decommissioning

3.2 Given a scenario, use appropriate network monitoring technologies to determine common issues.

- Simple Network Management Protocol (SNMP) v2/v3
- Syslog
- Log aggregators
- Security information and event management (SIEM)
- Packet capture
- Synthetic path monitoring
- Internet Protocol Address Management (IPAM)
- Baseline metrics
- Network discovery tools
- Performance tools
- Dashboards and reporting
- Traffic analysis tools

3.3 Explain BC and DR concepts.

- BC
  - High availability
    - Active-active
    - Active-passive
  - Fault tolerance
  - Stress testing
- Site availabilities
  - Cold
  - Warm
  - Hot
  - Mobile
- Backups and restore
- DR testing
  - Bubble
  - Tabletop
  - Parallel
  - Validation
  - Vendor considerations
- DR metrics
  - Recovery time objective (RTO)
  - Recovery point objective (RPO)
  - Mean time to recover (MTTR)
  - Mean time between failures (MTBF)

3.4 Given a scenario, use the appropriate network access and device management methods.

- In-band vs. out-of-band management
- VPN
  - Site-to-site
  - Client-to-site
    - Split tunneling
    - Full tunneling
- Connection types
  - Console
  - Management interface
- Remote access
  - Command-line interface (CLI)
  - Graphical User Interface (GUI)
    - Management
      - Standalone
      - Centralized
  - Protocols
    - SSH
    - RDP
    - Hypertext Transfer Protocol Secure (HTTPS)
  - Jump box/bastion host
- Local access
- Identity and authentication
- API calls

3.5 Summarize important concepts related to artificial intelligence (AI) usage.

- AI types
  - Generative AI
    - Skill augmentation
  - Non-generative AI
  - Agentic AI
    - Network infrastructure for AI
  - Large language models (LLMs)
  - Machine learning
- Common uses
  - Research
  - Knowledge base/repository
  - Anomaly detection
  - Data analysis
    - Documentation summary
    - Output analysis
  - Trend detection
  - Process improvement
- Public vs. private system
- Acceptable use policy (AUP)
- Proper tool use
  - Results verification
    - Bias
    - Hallucinations
    - Ethics
  - Avoiding overreliance
- Security considerations
  - Data poisoning
  - Prompt injection
  - Social engineering
  - Access control (AC)

4.0 Network Security

4.1 Explain basic network security and compliance concepts.

- Common security terminology
  - Risk
  - Threat
  - Vulnerability
    - Zero-day
    - Common Vulnerabilities and Exposures (CVE)
  - Attack surface
  - Attack vector
  - Confidentiality, integrity, and availability (CIA)
- Encryption
  - Data in transit
  - Data at rest
  - Data in use
- Public key infrastructure (PKI)
  - Certificates
    - Self-signed
  - Trust authority
- Identity and access management
  - Single sign-on (SSO)
    - Security Assertions Markup Language (SAML)
  - Multifactor authentication (MFA)
  - Privileged access management (PAM)
  - Authentication, authorization, and accounting (AAA)
  - Remote Authentication Dial-in User Service (RADIUS)
  - Terminal Access Controller Access-control System Plus (TACACS+)
  - Geofencing
- Security baselining
- Secure vs. non-secure protocols
- Host-based intrusion detection system (HIDS)
- Host-based intrusion prevention system (HIPS)
- Hardening
- Compliance considerations
  - Data locality
  - BYOD
  - Regulations
  - Audits
- Frameworks
- Risk management strategies
  - Acceptance
  - Avoidance
  - Mitigation
  - Transference
    - Insurance

4.2 Explain types of attacks and their impact on the network.

- Attacks
  - Social engineering
  - Denial of service (DoS)
  - Distributed denial of service (DDoS)
  - Spoofing
  - VLAN hopping
  - Poisoning
  - Exploits
    - Unpatched firmware
    - Unpatched software
  - On-path attack (formerly man-in-the-middle)
  - Overflow
  - Ping sweeping
  - Rubber duck
  - Password sniffing
  - Evil twin
  - Malicious code
  - Vandalism
  - Hijacking
- Impacts
  - Data exfiltration
  - Compromised credentials
  - Reputation
  - Privilege escalation
  - Service degradation
  - Financial impact
  - Network performance
  - Regulatory consequences
  - Legal
  - Insurance
  - Competitive advantage
  - BC

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

- AC
  - Role-based access control (RBAC)
  - Least privilege
- Access control list (ACL)
  - Allow
  - Deny
- Patch management
- Honeypot
- Honeynet
- Vulnerability scanning
- Segmentation
- Hardening techniques
  - Changing default password
  - Disabling unused services and ports
  - Securing version of protocols
  - ARP inspection
  - Port security
  - DHCP snooping
  - 802.1X
- Key management

5.0 Network Troubleshooting

5.1 Given a scenario, troubleshoot common cabling and transmission issues.

- Wired
  - Interface counters
    - Cyclic redundancy check (CRC) error
    - Giants
    - Runts
    - Overrun
    - Drops
  - Crosstalk
  - Physical connection issues
    - Copper
    - Fiber
    - Modules
  - Maximum transmission unit (MTU) mismatch
    - Jumbo frames
  - Duplex mismatch
  - Speed mismatch
  - Interface states
  - Cable length
  - PoE considerations
    - Standard selection
    - Power budget
- Wireless
  - Interference
    - Rogue devices
    - Noise
    - Co-channel
  - Roaming
  - Spectrum
  - Signal strength
  - Placement
  - Antenna
    - Receiver (RX) levels
    - Transmitter (TX) levels
    - Poor gain
- Port status
  - Error disabled
  - Administratively down
  - Suspended

5.2 Given a scenario, troubleshoot common issues with network devices and services.

- DNS
  - Zone types
    - Forward
    - Reverse
  - Recursive
  - Record types
  - Authoritative vs. non-authoritative
  - Primary vs. secondary
- Host file
- DHCP
  - Address exhaustion
  - Missing options
  - IP helper
  - Lease expiration
- NTP
  - Time drift
- NAT
  - Exhaustion
- NAC
  - Posture issues
  - MAC bypass issues
  - Policy misconfiguration
  - Allow list
- Routing
  - Asymmetrical
  - Sub-optimal
  - Routing loops
  - Missing route
  - Black hole/sink hole/bit bucket
- Telephony
  - Jitter
  - VLAN assignment
  - Real-time Transport Protocol (RTP)
  - Codec mismatch
- Virtualization
  - Host configuration
  - Guest configuration
- Switching
  - Broadcast storm
  - VLAN
  - Unidirectional link
  - Spanning Tree Protocol (STP)
- Firewall
  - ACL
  - Rule order
  - Security services
    - Packet filtering
    - Inspection
    - VPN
  - Incorrect classification
- Network performance
  - Quality of service (QoS)
  - Latency
  - Service delivery
    - Intermittent connectivity
    - Misdelivery
    - Capacity issues
  - Packet loss
- IP addressing
  - Subnet masks
  - Default gateway
- Management of devices
  - Reachability
  - Versioning
  - Misconfiguration
  - Baseline
  - Remote access

5.3 Given a scenario, use the appropriate tool or protocol to diagnose networking issues.

- Toner
- Probe
- Spectrum analyzer
- Packet analyzer
- Log collector
- Packet capture
- CLI commands
  - `traceroute/tracert`
  - `ping`
  - `netstat`
  - `nmap`
  - `netcat`
  - `nslookup`
  - `dig`
  - `tcpdump`
  - `ipconfig/ip`
  - `arp`
  - `debug`
- Network taps
- NetFlow
- Display outputs
  - Tables
  - Configurations
  - Settings
  - Interfaces
  - Logs
  - Routes

CompTIA Network+ Acronym List

The following is a list of acronyms that appear on the CompTIA Network+ N10-010 V1 certification 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.

ACRONYM	DEFINITION
AAA	authentication, authorization, and accounting
AC	access control
ACL	access control list
AES	Advanced Encryption Standard
AH	Authentication Header
AI	artificial intelligence
API	application programming interface
APIPA	Automatic Private Internet Protocol Address
ARP	Address Resolution Protocol
AUP	acceptable use policy
BC	business continuity
BGP	Border Gateway Protocol
BYOD	bring your own device
CDN	content delivery network
CDP	Cisco Discovery Protocol
CIA	confidentiality, integrity, and availability
CIDR	Classless Inter-Domain Routing
CLI	command-line interface
CRC	cyclic redundancy check
CVE	Common Vulnerabilities and Exposures
DCI	data center interconnect
DDoS	distributed denial of service
DHCP	Dynamic Host Configuration Protocol
DMZ	demilitarized zone
DNS	Domain Name System
DoS	denial of service
DR	disaster recovery
EIGRP	Enhanced Interior Gateway Routing Protocol
EOL	end-of-life
EOS	end-of-service
ESP	Encapsulating Security Payload
FHRP	First Hop Redundancy Protocol
GRE	generic routing encapsulation
GUI	Graphical User Interface
HIDS	host-based intrusion detection system
HIPS	host-based intrusion prevention system

ACRONYM	DEFINITION
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HVAC	heating, ventilation, and air conditioning
IaaS	infrastructure as a service
IaC	Infrastructure as code
ICMP	Internet Control Message Protocol
IDF	intermediate distribution frame
IDS	intrusion detection system
IKE	Internet Key Exchange
IoT	Internet of Things
IPAM	Internet Protocol Address Management
IP	Internet Protocol
IPS	intrusion prevention system
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
LACP	Link Aggregation Control Protocol
LAN	local area network
LC	local connector
LLDP	Link Layer Discovery Protocol
LLM	large language model
MAC	media access control
MDF	main distribution frame
MFA	Multifactor authentication
MLAG	Multi-chassis Link Aggregation Group
MMR	meet-me room
MSA	master service agreement
MTBF	mean time between failures
MTTR	mean time to recovery
MTU	maximum transmission unit
NAC	network access control
NAT	network access translation
NAT64	network address translation 64
NDA	non-disclosure agreement
NFV	network function virtualization
NIC	network interface card
NTP	Network Time Protocol
OS	operating system
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OT	operational technology
PaaS	platform as a service
PAM	privileged access management

ACRONYM	DEFINITION
PAT	port address translation
PDU	power distribution units
PDU	protocol data units
PKI	public key infrastructure
PoE	Power over Ethernet
PPE	personal protective equipment
QL	query language
QoS	quality of service
QSFP	Quad Small Form-factor Pluggable
RADIUS	Remote Authentication Dial-in User Service
RBAC	role-based access control
RDP	Remote Desktop Protocol
REST	Representational State Transfer
RFC	Request for Comments
RJ	Registered Jack
RPO	recovery point objective
RTO	recovery time objective
RTP	Real-time Transport Protocol
RX	receiver
SaaS	software as a service
SAML	Security Assertions Markup Language
SC	subscriber connector
SCADA	supervisory control and data acquisition
SDN	software-defined network
SD-WAN	software-defined wide area network
SFP	Small Form-factor Pluggable
SIEM	security information and event management
SIP	Session Initiation Protocol
SLA	service-level agreement
SLAAC	stateless address autoconfiguration
SMB	Server Message Block
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SOP	standard operating procedure
SSH	Secure Shell
SSO	single sign-on
ST	straight tip
STP	Spanning Tree Protocol
SVI	switch virtual interface
TACAS+	Terminal Access Controller Access-control System Plus
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TKIP	Temporal Key Integrity Protocol

ACRONYM	DEFINITION
TX	transmitter
UDP	User Datagram Protocol
UPS	uninterruptible power supply
VLAN	virtual local area network
VLSM	variable length subnet mask
VoIP	Voice over Internet Protocol
VPN	virtual private network
VXLAN	Virtual eXtensible local area network
WAP	wireless access point
WPA	Wi-Fi Protected Access

CompTIA Network+ Hardware and Software List

CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the CompTIA Network+ N10-010 V1 certification exam. This list may also be helpful for training companies that wish to create a lab component for their training offering. The Bulleted lists below each topic are sample lists and are not exhaustive.

EQUIPMENT

- Computers that support virtualization
- Optical and copper patch panels
- Layer 3 switch/managed switch/PoE switch
- Router
- Firewall
- Wireless access point (WAP)
- Voice over Internet Protocol (VoIP) phone

HARDWARE

- Network interface cards (NICs)
- Power supplies
- SFPs
- WAP
- UPS
- PoE injector

SPARE PARTS

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

SOFTWARE

- Protocol analyzer/packet capture
- Terminal emulation software
- Linux/Windows OSs
- 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
- Trivial File Transfer Protocol (TFTP) server
- Various firmware versions
- Diagramming software

TOOLS

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

OTHER

- Basic internet access
- Sample network documentation
- Sample logs
- Defective cables
- Cloud network diagrams
- Sample configuration playbook/runbook
- Sample policies, procedures, and standards