

CompTIA Network+ Certification Exam Objectives

EXAM NUMBER: N10-009 V9













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.

ANSI ACCREDITATION

The CompTIA Network+ exam is accredited by ANSI to show compliance with the 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 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%
Total		100%





-1.0 Networking Concepts

- 1.1 Explain concepts related to the Open Systems Interconnection (OSI) reference model.
 - 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.
 - · Physical and virtual appliances
 - Router
 - Switch
 - Firewall
 - Intrusion detection system (IDS)/ intrusion prevention system (IPS)
 - Load balancer
 - Proxy
 - Network-attached storage (NAS)
 - Storage area network (SAN)
 - Wireless
 - Access point (AP)
 - Controller

- Applications
- Content delivery network (CDN)
- Functions
- Virtual private network (VPN)
- Quality of service (QoS)
- Time to live (TTL)

- 1.3 Summarize cloud concepts and connectivity options.
 - 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 (laaS)
- Platform as a service (PaaS)
- Scalability
- Elasticity
- Multitenancy



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

Protocols	Ports
File Transfer Protocol (FTP)	20/21
Secure File Transfer Protocol (SFTP)	22
Secure Shell (SSH)	22
Telnet	23
Simple Mail Transfer Protocol (SMTP)	25
Domain Name System (DNS)	53
Dynamic Host Configuration Protocol (DHCP)	67/68
Trivial File Transfer Protocol (TFTP)	69
Hypertext Transfer Protocol (HTTP)	80
Network Time Protocol (NTP)	123
Simple Network Management Protocol (SNMP)	161/162
Lightweight Directory Access Protocol (LDAP)	389
Hypertext Transfer Protocol Secure (HTTPS)	443
Server Message Block (SMB)	445
Syslog	514
Simple Mail Transfer Protocol Secure (SMTPS)	587
Lightweight Directory Access Protocol over SSL (LDAPS)	636
Structured Query Language (SQL) Server	1433
Remote Desktop Protocol (RDP)	3389
Session Initiation Protocol (SIP)	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
 - Ethernet
 - Fibre Channel (FC)
- Form factors
 - Small form-factor pluggable (SFP)
 - Quad small form-factor pluggable (QSFP)
- · Connector types
- Subscriber connector (SC)
- Local connector (LC)
- Straight tip (ST)
- Multi-fiber push on (MPO)
- Registered jack (RJ)11
- RJ45
- F-type
- Bayonet Neill-Concelman (BNC)
- 1.6 Compare and contrast network topologies, architectures, and types.
 - Mesh
 - Hvbrid
 - 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.
 - 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 softwaredefined 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.
 - 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.

- 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
- · Guest networks
- Captive portals
- Authentication
- Pre-shared key (PSK) vs. Enterprise

- Antennas
- Omnidirectional vs. directional
- Autonomous vs. lightweight access point

2.4 Explain important factors of physical installations.

- · Important installation implications
- 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



·3.0 Network Operations

- 3.1 Explain the purpose of organizational processes and 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.
 - Methods
 - SNMP
 - Traps
 - Management information base (MIB)
 - Versions
 - ▶ v2c
 - ▶ v3
 - Community strings
 - Authentication
 - 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

- Solutions
- Network discovery
 - Ad hoc
 - Scheduled
- Traffic analysis
- Performance monitoring
- Availability monitoring
- Configuration monitoring



3.3 Explain disaster recovery (DR) concepts.

- 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.

- 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
 - Address (A)
 - AAAA
 - Canonical name (CNAME)
 - Mail exchange (MX)
 - Text (TXT)
 - Nameserver (NS)
 - Pointer (PTR)

- Zone types
 - Forward
 - 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.

- 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



4.0 Network Security

4.1 Explain the importance of basic network security concepts.

- · 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 Dialin 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)
- · Network segmentation enforcement
- Internet of Things (IoT) and Industrial Internet of Things (IIoT)
- Supervisory control and data acquisition (SCADA), industrial control System (ICS), operational technology (OT)
- Guest
- Bring your own device (BYOD)

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

- 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
- Roque 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.
 - 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





- 5.0 Network Troubleshooting

- 5.1 Explain the troubleshooting methodology.
 - · 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)
 - Runts
 - Giants
 - Drops
- Port status
 - Error disabled
 - Administratively down
 - Suspended

- Hardware issues
- 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



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

ACRONYM	DEFINITION
---------	------------

Α Address

ACL Access Control List **Authentication Header** AΗ

AΡ Access Point

API **Application Programming Interface**

Automatic Private Internet Protocol Addressing **APIPA**

Address Resolution Protocol ARP **AUP** Acceptable Use Policy Border Gateway Protocol **BGP** Bayonet Neill-Concelman **BNC BSSID** Basic Service Set Identifier **BYOD** Bring Your Own Device CAM Content-addressable Memory Content Delivery Network CDN

Cisco Discovery Protocol CIA Confidentiality, Integrity, and Availability

CIDR Classless Inter-domain Routing

Command-line Interface CLI

CNAME Canonical Name

CDP

Central Processing Unit CPU CRC Cyclic Redundancy Check Direct Attach Copper DAC DAS Direct-attached Storage Data Center Interconnect DCI Distributed Denial-of-service DDoS

DHCP Dynamic Host Configuration Protocol

DLP **Data Loss Prevention** DNS Domain Name System

Domain Name System Security Extensions DNSSEC DNS over Hypertext Transfer Protocol Secure DoH

Denial-of-service DoS

DoT DNS over Transport Laver Security

DR Disaster Recovery

Extensible Authentication Protocol over LAN **EAPoL EIGRP Enhanced Interior Gateway Routing Protocol**

EOL End-of-life **EOS** End-of-support

FSP Encapsulating Security Payload Extended Service Set Identifier **ESSID** End User License Agreement **EULA**

FC Fibre Channel

FHRP First Hop Redundancy Protocol



ACRONYM DEFINITION

FTP File Transfer Protocol

GDPR General Data Protection Regulation
GRE Generic Routing Encapsulation
GUI Graphical User Interface
HTTP Hypertext Transfer Protocol

HTTPS Hypertext Transfer Protocol Secure

laaS Infrastructure as a Service laC Infrastructure as Code

IAM Identity and Access Management
ICMP Internet Control Message Protocol

ICSIndustrial Control SystemIDFIntermediate Distribution FrameIDSIntrusion Detection System

Internet of Things

IIoT Industrial Internet of Things
IKE Internet Key Exchange
IP Internet Protocol

IPAM Internet Protocol Address Management

IPS Intrusion Prevention System
IPSec Internet Protocol Security

IS-IS Intermediate System to Intermediate System

LACP Link Aggregation Control Protocol

LAN Local Area Network LC Local Connector

LDAP Lightweight Directory Access Protocol

LDAPS Lightweight Directory Access Protocol over SSL

LLDP Link Layer Discovery Protocol

MAC Media Access Control
MDF Main Distribution Frame

MDIX Medium Dependent Interface Crossover

MFA Multifactor Authentication
MIB Management Information Base

MPO Multifiber Push On

MTBF Mean Time Between Failure

MTTR Mean Time To Repair

MTU Maximum Transmission Unit MX Mail Exchange

NAC Network Access Control
NAS Network-attached Storage
NAT Network Address Translation
NFV Network Functions Virtualization

NIC Network Interface Cards

NS Name Server

NTP Network Time Protocol
NTS Network Time Security
OS Operating System

OSPF Open Shortest Path First
OSI Open Systems Interconnection

OT Operational Technology
PaaS Platform as a Service
PAT Port Address Translation

PCI DSS Payment Card Industry Data Security Standards

PDU Power Distribution Unit
PKI Public Key Infrastructure



ACRONYM DEFINITION

PoE Power over Ethernet PSK Pre-shared Key

PTP Precision Time Protocol

PTR Pointer

QoS Quality of Service

QSFP Quad Small Form-factor Pluggable

RADIUS Remote Authentication Dial-in User Service

RDP Remote Desktop Protocol
RFID Radio Frequency Identifier
RIP Routing Information Protocol

RJ Registered Jack

RPO Recovery Point Objective
RSTP Rapid Spanning Tree Protocol
RTO Recovery Time Objective

RX Receiver

SaaS Software as a Service

SAML Security Assertion Markup Language

SAN Storage Area Network
SASE Secure Access Service Edge

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
SFTP Secure File Transfer Protocol
SIP Session Initiation Protocol

SIEM Security Information and Event Management

SLA Service-level Agreement

SLAAC Stateless Address Autoconfiguration

SMB Server Message Block
SMTP Simple Mail Transfer Protocol

SMTPS Simple Mail Transfer Protocol Secure
SNMP Simple Network Management Protocol

SOA Start of Authority

SQL Structured Query Language SSE Security Service Edge

SSH Secure Shell

SSID Service Set Identifier
SSL Secure Socket Layer
SSO Single Sign-on
ST Straight Tip

STP Shielded Twisted Pair
SVI Switch Virtual Interface

TACAS+ Terminal Access Controller Access Control System Plus

TCP Transmission Control Protocol
TFTP Trivial File Transfer Protocol

TTL Time to Live TX Transmitter

TXT Text

UDP User Datagram Protocol
UPS Uninterruptible Power Supply
URL Uniform Resource Locator

USB Universal Serial Bus

UTM Unified Threat Management



ACRONYM DEFINITION

UTP Unshielded Twisted Pair

VIP Virtual IP

VLAN Virtual Local Area Network VLSM Variable Length Subnet Mask

VoIP Voice over IP

VPC Virtual Private Cloud
VPN Virtual Private Network
WAN Wide Area Network
WPA Wi-Fi Protected Access
WPS Wi-Fi Protected Setup
VXLAN Virtual Extensible LAN
ZTA Zero Trust Architecture



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
- laaS 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

