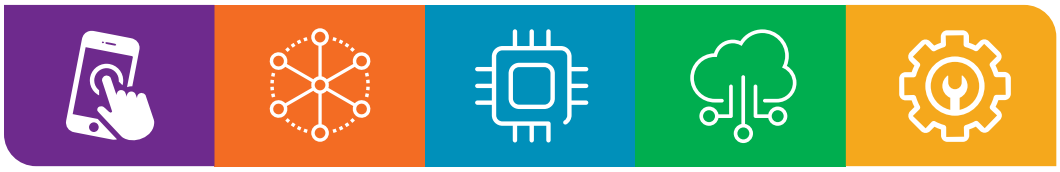
Catalog

CompTIA A+ Certification Exam Core 1 Objectives

EXAM NUMBER: CORE 1 (220-1101)



CompTIA

About the Exam

Candidates are encouraged to use this document to help prepare for the CompTIA A+ Core 1 (220-1101) certification exam. In order to receive the CompTIA A+ certification, you must pass two exams: Core 1 (220-1101) and Core 2 (220-1102). The CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) certification exams will verify the successful candidate has the knowledge and skills required to:

- Install, configure, and maintain computer equipment, mobile devices, and software for end users
- Service components based on customer requirements
- Understand networking basics and apply basic cybersecurity methods to mitigate threats
- Properly and safely diagnose, resolve, and document common hardware and software issues
- Apply troubleshooting skills and provide customer support using appropriate communication skills
- Understand the basics of scripting, cloud technologies, virtualization, and multi-OS deployments in corporate environments

This is equivalent to 12 months of hands-on experience working in a help desk support technician, desktop support technician, or field service technician job role. 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 A+ Core 1 (220-1101) 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 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.

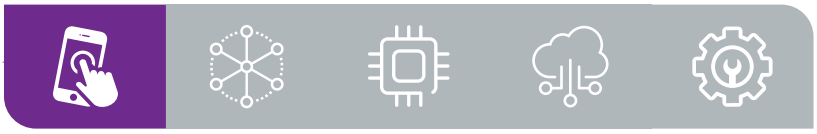
TEST DETAILS

Required exam	A+ Core 1 (220-1101)
Number of questions	Maximum of 90
Types of questions	Multiple-choice and performance-based
Length of test	90 minutes
Recommended experience	12 months of hands-on experience in a help desk support technician, desktop support technician, or field service technician job role
Passing score	675 (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	Mobile Devices	15%
2.0	Networking	20%
3.0	Hardware	25%
4.0	Virtualization and Cloud Computing	11%
5.0	Hardware and Network Troubleshooting	29%
Total		**100%**



1.0 Mobile Devices

1.1 Given a scenario, install and configure laptop hardware and components.

- **Hardware/device replacement**
  - Battery
  - Keyboard/keys
  - Random-access memory (RAM)
  - Hard disk drive (HDD)/solid-state drive (SSD) migration
  - HDD/SSD replacement
  - Wireless cards
- **Physical privacy and security components**
  - Biometrics
  - Near-field scanner features

1.2 Compare and contrast the display components of mobile devices.

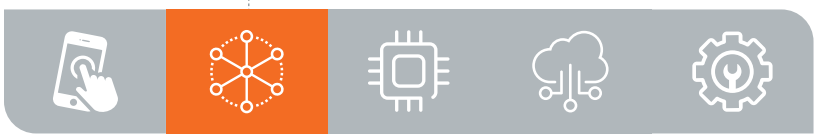
- **Types**
  - Liquid crystal display (LCD)
    - In-plane switching (IPS)
    - Twisted nematic (TN)
    - Vertical alignment (VA)
  - Organic light-emitting diode (OLED)
- **Mobile display components**
- **WiFi antenna connector/ placement**
- **Camera/webcam**
- **Microphone**
- **Touch screen/digitizer**
- **Inverter**

1.3 Given a scenario, set up and configure accessories and ports of mobile devices.

- **Connection methods**
  - Universal Serial Bus (USB)/ USB-C/microUSB/miniUSB
  - Lightning
  - Serial interfaces
  - Near-field communication (NFC)
  - Bluetooth
  - Hotspot
- **Accessories**
  - Touch pens
  - Headsets
  - Speakers
  - Webcam
- **Docking station**
- **Port replicator**
- **Trackpad/drawing pad**

1.4 Given a scenario, configure basic mobile-device network connectivity and application support.

- **Wireless/cellular data network (enable/disable)**
  - 2G/3G/4G/5G
  - Hotspot
  - Global System for Mobile Communications (GSM) vs. code-division multiple access (CDMA)
  - Preferred Roaming List (PRL) updates
- **Bluetooth**
  - Enable Bluetooth
  - Enable pairing
  - Find a device for pairing
  - Enter the appropriate PIN code
  - Test connectivity
- **Location services**
  - Global Positioning System (GPS) services
  - Cellular location services
- **Mobile device management (MDM)/mobile application management (MAM)**
  - Corporate email configuration
  - Two-factor authentication
  - Corporate applications
- **Mobile device synchronization**
  - Account setup
    - Microsoft 365
    - Google Workspace
    - iCloud
  - Data to synchronize
    - Mail
    - Photos
    - Calendar
    - Contacts
    - Recognizing data caps



2.0 Networking

2.1 Compare and contrast Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports, protocols, and their purposes.

- **Ports and protocols**
  - 20/21 – File Transfer Protocol (FTP)
  - 22 – Secure Shell (SSH)
  - 23 – Telnet
  - 25 – Simple Mail Transfer Protocol (SMTP)
  - 53 – Domain Name System (DNS)
  - 67/68 – Dynamic Host Configuration Protocol (DHCP)
  - 80 – Hypertext Transfer Protocol (HTTP)
  - 110 – Post Office Protocol 3 (POP3)
  - 137/139 – Network Basic Input/Output System (NetBIOS)/NetBIOS over TCP/IP (NetBT)
  - 143 – Internet Mail Access Protocol (IMAP)
  - 161/162 – Simple Network Management Protocol (SNMP)
  - 389 – Lightweight Directory Access Protocol (LDAP)
  - 443 – Hypertext Transfer Protocol Secure (HTTPS)
  - 445 – Server Message Block (SMB)/Common Internet File System (CIFS)
  - 3389 – Remote Desktop Protocol (RDP)
- **TCP vs. UDP**
  - Connectionless
    - DHCP
    - Trivial File Transfer Protocol (TFTP)
  - Connection-oriented
    - HTTPS
    - SSH

2.2 Compare and contrast common networking hardware.

- **Routers**
- **Switches**
  - Managed
  - Unmanaged
- **Access points**
- **Patch panel**
- **Firewall**
- **Power over Ethernet (PoE)**
  - Injectors
  - Switch
  - PoE standards
- **Hub**
- **Cable modem**
- **Digital subscriber line (DSL)**
- **Optical network terminal (ONT)**
- **Network interface card (NIC)**
- **Software-defined networking (SDN)**

2.3 Compare and contrast protocols for wireless networking.

- **Frequencies**
  - 2.4GHz
  - 5GHz
- **Channels**
  - Regulations
  - 2.4GHz vs. 5GHz
- **Bluetooth**
- **802.11**
  - a
  - b
  - g
  - n
  - ac (WiFi 5)
  - ax (WiFi 6)
- **Long-range fixed wireless**
  - Licensed
  - Unlicensed
  - Power
  - Regulatory requirements for wireless power
- **NFC**
- **Radio-frequency identification (RFID)**

2.4 Summarize services provided by networked hosts.

- **Server roles**
  - DNS
  - DHCP
  - Fileshare
  - Print servers
  - Mail servers
  - Syslog
  - Web servers
  - Authentication, authorization, and accounting (AAA)
- **Internet appliances**
  - Spam gateways
  - Unified threat management (UTM)
  - Load balancers
  - Proxy servers
- **Legacy/embedded systems**
  - Supervisory control and data acquisition (SCADA)
- **Internet of Things (IoT) devices**

2.5 Given a scenario, install and configure basic wired/wireless small office/home office (SOHO) networks.

- **Internet Protocol (IP) addressing**
  - IPv4
    - Private addresses
    - Public addresses
  - IPv6
  - Automatic Private IP Addressing (APIPA)
  - Static
  - Dynamic
  - Gateway

2.6 Compare and contrast common network configuration concepts.

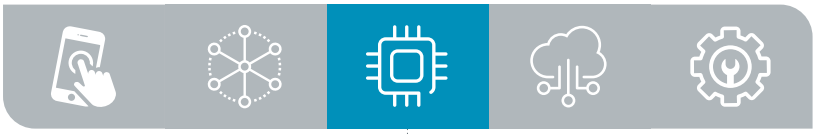
- **DNS**
  - Address
    - A
    - AAAA
  - Mail exchanger (MX)
  - Text (TXT)
    - Spam management
      (i) DomainKeys Identified Mail (DKIM)
      (ii) Sender Policy Framework (SPF)
      (iii) Domain-based Message Authentication, Reporting, and Conformance (DMARC)
- **DHCP**
  - Leases
  - Reservations
  - Scope
- **Virtual LAN (VLAN)**
- **Virtual private network (VPN)**

2.7 Compare and contrast Internet connection types, network types, and their features.

- **Internet connection types**
  - Satellite
  - Fiber
  - Cable
  - DSL
  - Cellular
  - Wireless Internet service provider (WISP)
- **Network types**
  - Local area network (LAN)
  - Wide area network (WAN)
  - Personal area network (PAN)
  - Metropolitan area network (MAN)
  - Storage area network (SAN)
  - Wireless local area network (WLAN)

2.8 Given a scenario, use networking tools.

- **Crimper**
- **Cable stripper**
- **WiFi analyzer**
- **Toner probe**
- **Punchdown tool**
- **Cable tester**
- **Loopback plug**
- **Network tap**



3.0 Hardware

3.1 Explain basic cable types and their connectors, features, and purposes.

- **Network cables**
  - Copper
    - Cat 5
    - Cat 5e
    - Cat 6
    - Cat 6a
    - Coaxial
    - Shielded twisted pair
      (i) Direct burial
    - Unshielded twisted pair
  - Plenum
  - Optical
    - Fiber
  - T568A/T568B
- **Peripheral cables**
  - USB 2.0
  - USB 3.0
  - Serial
  - Thunderbolt
- **Video cables**
  - High-Definition Multimedia Interface (HDMI)
  - DisplayPort
  - Digital Visual Interface (DVI)
  - Video Graphics Array (VGA)
- **Hard drive cables**
  - Serial Advanced Technology Attachment (SATA)
  - Small Computer System Interface (SCSI)
  - External SATA (eSATA)
  - Integrated Drive Electronics (IDE)
- **Adapters**
- **Connector types**
  - RJ11
  - RJ45
  - F type
  - Straight tip (ST)
  - Subscriber connector (SC)
  - Lucent connector (LC)
  - Punchdown block
  - microUSB
  - miniUSB
  - USB-C
  - Molex
  - Lightning port
  - DB9

3.2 Given a scenario, install the appropriate RAM.

- **RAM types**
  - Virtual RAM
  - Small outline dual inline memory module (SODIMM)
  - Double Data Rate 3 (DDR3)
  - Double Data Rate 4 (DDR4)
  - Double Data Rate 5 (DDR5)
  - Error correction code (ECC) RAM
- **Single-channel**
- **Dual-channel**
- **Triple-channel**
- **Quad-channel**

3.3 Given a scenario, select and install storage devices.

- **Hard drives**
  - Speeds
    - 5,400rpm
    - 7,200rpm
    - 10,000rpm
    - 15,000rpm
  - Form factor
    - 2.5
    - 3.5
- **SSDs**
  - Communications interfaces
    - Non-volatile Memory Express (NVMe)
    - SATA
    - Peripheral Component Interconnect Express (PCIe)
  - Form factors
    - M.2
    - mSATA
- **Drive configurations**
  - Redundant Array of Independent (or Inexpensive) Disks (RAID) 0, 1, 5, 10
- **Removable storage**
  - Flash drives
  - Memory cards
  - Optical drives

3.4 Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards.

- **Motherboard form factor**
  - Advanced Technology eXtended (ATX)
  - Information Technology eXtended (ITX)
- **Motherboard connector types**
  - Peripheral Component Interconnect (PCI)
  - PCI Express (PCIe)
  - Power connectors
  - SATA
  - eSATA
  - Headers
  - M.2
- **Motherboard compatibility**
  - CPU sockets
    - Advanced Micro Devices, Inc. (AMD)
    - Intel
  - Server
  - Multisocket
  - Desktop
  - Mobile
- **Basic Input/Output System (BIOS)/Unified Extensible Firmware Interface (UEFI) settings**
  - Boot options
  - USB permissions
  - Trusted Platform Module (TPM) security features
  - Fan considerations
  - Secure Boot
  - Boot password
- **Encryption**
  - TPM
  - Hardware security module (HSM)
- **CPU architecture**
  - x64/x86
  - Advanced RISC Machine (ARM)
  - Single-core
  - Multicore
  - Multithreading
  - Virtualization support
- **Expansion cards**
  - Sound card
  - Video card
  - Capture card
  - NIC
- **Cooling**
  - Fans
  - Heat sink
  - Thermal paste/pads
  - Liquid

3.5 Given a scenario, install or replace the appropriate power supply.

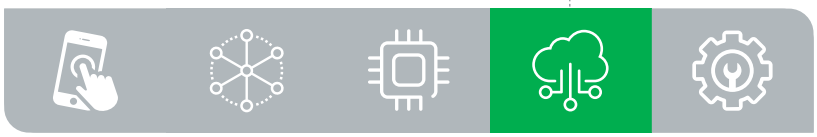
- **Input 110-120 VAC vs. 220-240 VAC**
- **Output 3.3V vs. 5V vs. 12V**
- **20-pin to 24-pin motherboard adapter**
- **Redundant power supply**
- **Modular power supply**
- **Wattage rating**

3.6 Given a scenario, deploy and configure multifunction devices/ printers and settings.

- **Properly unboxing a device – setup location considerations**
- **Use appropriate drivers for a given OS**
  - Printer Control Language (PCL) vs. PostScript
- **Device connectivity**
  - USB
  - Ethernet
  - Wireless
- **Public/shared devices**
  - Printer share
  - Print server
- **Configuration settings**
  - Duplex
  - Orientation
  - Tray settings
  - Quality
- **Security**
  - User authentication
  - Badging
  - Audit logs
  - Secured prints
- **Network scan services**
  - Email
  - SMB
  - Cloud services
- **Automatic document feeder (ADF)/flatbed scanner**

3.7 Given a scenario, install and replace printer consumables.

- **Laser**
  - Imaging drum, fuser assembly, transfer belt, transfer roller, pickup rollers, separation pads, duplexing assembly
  - Imaging process: processing, charging, exposing, developing, transferring, fusing, and cleaning
  - Maintenance: Replace toner, apply maintenance kit, calibrate, clean
- **Inkjet**
  - Ink cartridge, print head, roller, feeder, duplexing assembly, carriage belt
  - Calibration
  - Maintenance: Clean heads, replace cartridges, calibrate, clear jams
- **Thermal**
  - Feed assembly, heating element
  - Special thermal paper
  - Maintenance: Replace paper, clean heating element, remove debris
  - Heat sensitivity of paper
- **Impact**
  - Print head, ribbon, tractor feed
  - Impact paper
  - Maintenance: Replace ribbon, replace print head, replace paper
- **3-D printer**
  - Filament
  - Resin
  - Print bed



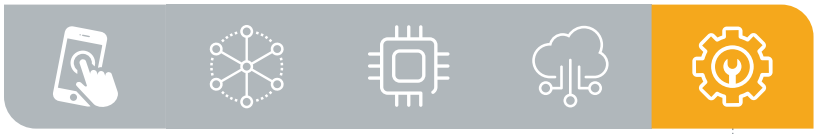
4.0 Virtualization and Cloud Computing

4.1 Summarize cloud-computing concepts.

- **Common cloud models**
  - Private cloud
  - Public cloud
  - Hybrid cloud
  - Community cloud
  - Infrastructure as a service (IaaS)
  - Software as a service (SaaS)
  - Platform as a service (PaaS)
- **Cloud characteristics**
  - Shared resources
  - Metered utilization
  - Rapid elasticity
  - High availability
  - File synchronization
- **Desktop virtualization**
  - Virtual desktop infrastructure (VDI) on premises
  - VDI in the cloud

4.2 Summarize aspects of client-side virtualization.

- **Purpose of virtual machines**
  - Sandbox
  - Test development
  - Application virtualization
    - Legacy software/OS
    - Cross-platform virtualization
- **Resource requirements**
- **Security requirements**



5.0 Hardware and Network Troubleshooting

5.1 Given a scenario, apply the best practice methodology to resolve problems.

- **Always consider corporate policies, procedures, and impacts before implementing changes**
  1. Identify the problem
     - Gather information from the user, identify user changes, and, if applicable, perform backups before making changes
     - Inquire regarding environmental or infrastructure changes
  2. Establish a theory of probable cause (question the obvious)
     - If necessary, conduct external or internal research based on symptoms
  3. Test the theory to determine the cause
     - Once the theory is confirmed, determine the next steps to resolve the problem
     - If the theory is not confirmed, re-establish a new theory or escalate
  4. Establish a plan of action to resolve the problem and implement the solution
     - Refer to the vendor's instructions for guidance
  5. Verify full system functionality and, if applicable, implement preventive measures
  6. Document the findings, actions, and outcomes

5.2 Given a scenario, troubleshoot problems related to motherboards, RAM, CPU, and power.

- **Common symptoms**
  - Power-on self-test (POST) beeps
  - Proprietary crash screens (blue screen of death [BSOD]/ pinwheel)
  - Black screen
  - No power
  - Sluggish performance
  - Overheating
  - Burning smell
  - Intermittent shutdown
  - Application crashes
  - Grinding noise
  - Capacitor swelling
  - Inaccurate system date/time

5.3 Given a scenario, troubleshoot and diagnose problems with storage drives and RAID arrays.

- **Common symptoms**
  - Light-emitting diode (LED) status indicators
  - Grinding noises
  - Clicking sounds
  - Bootable device not found
  - Data loss/corruption
  - RAID failure
  - Self-monitoring, Analysis, and Reporting Technology (S.M.A.R.T.) failure
  - Extended read/write times
  - Input/output operations per second (IOPS)
  - Missing drives in OS

5.4 Given a scenario, troubleshoot video, projector, and display issues.

- **Common symptoms**
  - Incorrect data source
  - Physical cabling issues
  - Burned-out bulb
  - Fuzzy image
  - Display burn-in
  - Dead pixels
  - Flashing screen
  - Incorrect color display
  - Audio issues
  - Dim image
  - Intermittent projector shutdown

5.5 Given a scenario, troubleshoot common issues with mobile devices.

- **Common symptoms**
  - Poor battery health
  - Swollen battery
  - Broken screen
  - Improper charging
  - Poor/no connectivity
  - Liquid damage
  - Overheating
  - Digitizer issues
  - Physically damaged ports
  - Malware
  - Cursor drift/touch calibration

5.6 Given a scenario, troubleshoot and resolve printer issues.

- **Common symptoms**
  - Lines down the printed pages
  - Garbled print
  - Toner not fusing to paper
  - Paper jams
  - Faded print
  - Incorrect paper size
  - Paper not feeding
  - Multipage misfeed
  - Multiple prints pending in queue
  - Speckling on printed pages
  - Double/echo images on the print
  - Incorrect color settings
  - Grinding noise
  - Finishing issues
    - Staple jams
    - Hole punch
  - Incorrect page orientation

5.7 Given a scenario, troubleshoot problems with wired and wireless networks.

- **Common symptoms**
  - Intermittent wireless connectivity
  - Slow network speeds
  - Limited connectivity
  - Jitter
  - Poor Voice over Internet Protocol (VoIP) quality
  - Port flapping
  - High latency
  - External interference

CompTIA A+ Core 1 (220-1101) Acronym List

The following is a list of acronyms that appear on the CompTIA A+ Core 1 (220-1101) 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	Alternating Current
ACL	Access Control List
ADF	Automatic Document Feeder
AES	Advanced Encryption Standard
AP	Access Point
APFS	Apple File System
APIPA	Automatic Private Internet Protocol Addressing
APK	Android Package
ARM	Advanced RISC [Reduced Instruction Set Computer] Machine
ARP	Address Resolution Protocol
ATA	Advanced Technology Attachment
ATM	Asynchronous Transfer Mode
ATX	Advanced Technology Extended
AUP	Acceptable Use Policy
BIOS	Basic Input/Output System
BSOD	Blue Screen of Death
BYOD	Bring Your Own Device
CAD	Computer-aided Design
CAPTCHA	Completely Automated Public Turing Test to Tell Computers and Humans Apart
CD	Compact Disc
CDFS	Compact Disc File System
CDMA	Code-Division Multiple Access
CERT	Computer Emergency Response Team
CIFS	Common Internet File System
CMD	Command Prompt
CMOS	Complementary Metal-Oxide Semiconductor
CPU	Central Processing Unit
CRL	Certificate Revocation List
DC	Direct Current
DDoS	Distributed Denial of Service
DDR	Double Data Rate
DHCP	Dynamic Host Configuration Protocol
DIMM	Dual Inline Memory Module
DKIM	DomainKeys Identified Mail
DMA	Direct Memory Access
DMARC	Domain-based Message Authentication, Reporting, and Conformance
DNS	Domain Name System
DoS	Denial of Service
DRAM	Dynamic Random-Access Memory
DRM	Digital Rights Management
DSL	Digital Subscriber Line
DVI	Digital Visual Interface
DVI-D	Digital Visual Interface-Digital
ECC	Error Correcting Code
EFS	Encrypting File System
EMI	Electromagnetic Interference
EOL	End-of-Life
eSATA	External Serial Advanced Technology Attachment
ESD	Electrostatic Discharge
EULA	End-User License Agreement
exFAT	Extensible File Allocation Table
ext	Extended File System
FAT	File Allocation Table
FAT12	12-bit File Allocation Table
FAT16	16-bit File Allocation Table
FAT32	32-bit File Allocation Table
FSB	Front-Side Bus
FTP	File Transfer Protocol
GFS	Grandfather-Father-Son
GPS	Global Positioning System
GPT	GUID [Globally Unique Identifier] Partition Table
GPU	Graphics Processing Unit
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
GUID	Globally Unique Identifier
HAL	Hardware Abstraction Layer
HAV	Hardware-assisted Virtualization

Acronym	Definition
HCL	Hardware Compatibility List
HDCP	High-bandwidth Digital Content Protection
HDD	Hard Disk Drive
HDMI	High-Definition Multimedia Interface
HSM	Hardware Security Module
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I/O	Input/Output
IaaS	Infrastructure as a Service
ICR	Intelligent Character Recognition
IDE	Integrated Drive Electronics
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IMAP	Internet Mail Access Protocol
IOPS	Input/Output Operations Per Second
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IPS	In-plane Switching
IPSec	Internet Protocol Security
IR	Infrared
IrDA	Infrared Data Association
IRP	Incident Response Plan
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITX	Information Technology eXtended
KB	Knowledge Base
KVM	Keyboard-Video-Mouse
LAN	Local Area Network
LC	Lucent Connector
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LED	Light-emitting Diode
MAC	Media Access Control/Mandatory Access Control
MAM	Mobile Application Management
MAN	Metropolitan Area Network
MBR	Master Boot Record
MDM	Mobile Device Management
MFA	Multifactor Authentication
MFD	Multifunction Device
MFP	Multifunction Printer
MMC	Microsoft Management Console
MOU	Memorandum of Understanding
MSDS	Material Safety Data Sheet
MSRA	Microsoft Remote Assistance

Acronym	Definition
MX	Mail Exchange
NAC	Network Access Control
NAT	Network Address Translation
NDA	Non-disclosure Agreement
NetBIOS	Networked Basic Input/Output System
NetBT	NetBIOS over TCP/IP [Transmission Control Protocol/Internet Protocol]
NFC	Near-field Communication
NFS	Network File System
NIC	Network Interface Card
NTFS	New Technology File System
NVMe	Non-volatile Memory Express
OCR	Optical Character Recognition
OLED	Organic Light-emitting Diode
ONT	Optical Network Terminal
OS	Operating System
PaaS	Platform as a Service
PAN	Personal Area Network
PC	Personal Computer
PCIe	Peripheral Component Interconnect Express
PCL	Printer Command Language
PE	Preinstallation Environment
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PoE	Power over Ethernet
POP3	Post Office Protocol 3
POST	Power-on Self-Test
PPP	Point-to-Point Protocol
PRL	Preferred Roaming List
PSU	Power Supply Unit
PXE	Preboot Execution Environment
RADIUS	Remote Authentication Dial-in User Service
RAID	Redundant Array of Independent (or Inexpensive) Disks
RAM	Random-access Memory
RDP	Remote Desktop Protocol
RF	Radio Frequency
RFI	Radio-Frequency Interference
RFID	Radio-Frequency Identification
RJ11	Registered Jack Function 11
RJ45	Registered Jack Function 45
RMM	Remote Monitoring and Management
RTO	Recovery Time Objective
SaaS	Software as a Service
SAN	Storage Area Network
SAS	Serial Attached SCSI [Small Computer System Interface]
SATA	Serial Advanced Technology Attachment

Acronym	Definition
SC	Subscriber Connector
SCADA	Supervisory Control and Data Acquisition
SCP	Secure Copy Protection
SCSI	Small Computer System Interface
SDN	Software-defined Networking
SFTP	Secure File Transfer Protocol
SIM	Subscriber Identity Module
SIMM	Single Inline Memory Module
S.M.A.R.T.	Self-monitoring Analysis and Reporting Technology
SMB	Server Message Block
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SODIMM	Small Outline Dual Inline Memory Module
SOHO	Small Office/Home Office
SPF	Sender Policy Framework
SQL	Structured Query Language
SRAM	Static Random-access Memory
SSD	Solid-State Drive
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-on
ST	Straight Tip
STP	Shielded Twisted Pair
TACACS	Terminal Access Controller Access-Control System
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TN	Twisted Nematic
TPM	Trusted Platform Module
UAC	User Account Control
UDP	User Datagram Protocol
UEFI	Unified Extensible Firmware Interface
UNC	Universal Naming Convention
UPnP	Universal Plug and Play
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
UTM	Unified Threat Management
UTP	Unshielded Twisted Pair
VA	Vertical Alignment
VDI	Virtual Desktop Infrastructure
VGA	Video Graphics Array
VLAN	Virtual LAN [Local Area Network]
VM	Virtual Machine
VNC	Virtual Network Computer
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VRAM	Video Random-access Memory
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WISP	Wireless Internet Service Provider
WLAN	Wireless LAN [Local Area Network]
WMN	Wireless Mesh Network
WPA	WiFi Protected Access
WWAN	Wireless Wide Area Network
XSS	Cross-site Scripting

CompTIA A+ Core 1 (220-1101) Proposed Hardware and Software List

**CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the A+ Core 1 (220-1101) exam. This list may also be helpful for training companies that wish to create a lab component to their training offering. The bulleted lists below each topic are sample lists and are not exhaustive.

Equipment

- Apple tablet/smartphone
- Android tablet/smartphone
- Windows tablet
- Chromebook
- Windows laptop/Mac laptop/Linux laptop
- Windows desktop/Mac desktop/Linux desktop
- Windows server with Active Directory and Print Management
- Monitors
- Projectors
- SOHO router/switch
- Access point
- VoIP phone
- Printer
  - Laser/inkjet
  - Wireless
  - 3-D printer
  - Thermal
- Surge suppressor
- Uninterruptible power supply (UPS)
- Smart devices (IoT devices)
- Server with a hypervisor
- Punchdown block
- Patch panel
- Webcams
- Speakers
- Microphones

Spare parts/hardware

- Motherboards
- RAM
- Hard drives
- Power supplies
- Video cards
- Sound cards
- Network cards
- Wireless NICs
- Fans/cooling devices/heat sink
- CPUs
- Assorted connectors/cables
  - USB
  - HDMI
  - DisplayPort
  - DVI
  - VGA
- Adapters
  - Bluetooth adapter
- Network cables
- Unterminated network cable/connectors
- Alternating current (AC) adapters
- Optical drives
- Screws/standoffs
- Cases
- Maintenance kit
- Mice/keyboards
- Keyboard-video-mouse (KVM)
- Console cable
- SSD

Tools

- Screwdriver
- Multimeter
- Wire cutters
- Punchdown tool
- Crimper
- Power supply tester
- Cable stripper
- Standard technician toolkit
- Electrostatic discharge (ESD) strap
- Thermal paste
- Cable tester
- Cable toner
- WiFi analyzer
- SATA to USB connectors

Software

- Operating systems
  - Linux
  - Chrome OS
  - Microsoft Windows
  - macOS
  - Android
  - iOS
- Preinstallation environment (PE) disk/live compact disc (CD)
- Antivirus software
- Virtualization software
- Anti-malware
- Driver software

CompTIA

CompTIA A+ Certification Exam Core 2 Objectives

EXAM NUMBER: CORE 2 (220-1102)

CompTIA

About the Exam

Candidates are encouraged to use this document to help prepare for the CompTIA A+ 220-1102 certification exam. In order to receive the CompTIA A+ certification, you must pass two exams: Core 1 (220-1101) and Core 2 (220-1102). The CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) certification exams will verify the successful candidate has the knowledge and skills required to:

- Install, configure, and maintain computer equipment, mobile devices, and software for end users
- Service components based on customer requirements
- Understand networking basics and apply basic cybersecurity methods to mitigate threats
- Properly and safely diagnose, resolve, and document common hardware and software issues
- Apply troubleshooting skills and provide customer support using appropriate communication skills
- Understand the basics of scripting, cloud technologies, virtualization, and multi-OS deployments in corporate environments

This is equivalent to 12 months of hands-on experience working in a help desk support, desktop support technician, or field service technician job role. 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 A+ Core 2 (220-1102) 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 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	A+ Core 2 (220-1102)
Number of questions	Maximum of 90
Types of questions	Multiple-choice and performance-based
Length of test	90 minutes
Recommended experience	12 months of hands-on experience in a help desk support technician, desktop support technician, or field service technician job role
Passing score	700 (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	Operating Systems	31%
2.0	Security	25%
3.0	Software Troubleshooting	22%
4.0	Operational Procedures	22%
Total		**100%**

NOTE ON WINDOWS 11

Versions of Microsoft® Windows® that are not end of Mainstream Support (as determined by Microsoft), up to and including Windows 11, are intended content areas of the certification. As such, objectives in which a specific version of Microsoft Windows is not indicated in the main objective title can include content related to Windows 10 and Windows 11, as it relates to the job role.

1.0 Operating Systems

1.1 Identify basic features of Microsoft Windows editions.

- **Windows 10 editions**
  - Home
  - Pro
  - Pro for Workstations
  - Enterprise
- **Feature differences**
  - Domain access vs. workgroup
  - Desktop styles/user interface
  - Availability of Remote Desktop Protocol (RDP)
  - Random-access memory (RAM) support limitations
  - BitLocker
  - gpedit.msc
- **Upgrade paths**
  - In-place upgrade

1.2 Given a scenario, use the appropriate Microsoft command-line tool.

- **Navigation**
  - cd
  - dir
  - md
  - rmdir
  - Drive navigation inputs:
    - C: or D: or x:
- **Command-line tools**
  - ipconfig
  - ping
  - hostname
  - netstat
  - nslookup
  - chkdsk
  - net user
  - net use
  - tracert
  - format
  - xcopy
  - copy
  - robocopy
  - gpupdate
  - gpresult
  - shutdown
  - sfc
  - [command name] /?
  - diskpart
  - pathping
  - winver

1.3 Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS).

- **Task Manager**
  - Services
  - Startup
  - Performance
  - Processes
  - Users
- **Microsoft Management Console (MMC) snap-in**
  - Event Viewer (eventvwr.msc)
  - Disk Management (diskmgmt.msc)
  - Task Scheduler (taskschd.msc)
  - Device Manager (devmgmt.msc)
  - Certificate Manager (certmgr.msc)
  - Local Users and Groups (lusrmgr.msc)
  - Performance Monitor (perfmon.msc)
  - Group Policy Editor (gpedit.msc)
- **Additional tools**
  - System Information (msinfo32.exe)
  - Resource Monitor (resmon.exe)
  - System Configuration (msconfig.exe)
  - Disk Cleanup (cleanmgr.exe)
  - Disk Defragment (dfrgui.exe)
  - Registry Editor (regedit.exe)

1.4 Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility.

- **Internet Options**
- **Devices and Printers**
- **Programs and Features**
- **Network and Sharing Center**
- **System**
- **Windows Defender Firewall**
- **Mail**
- **Sound**
- **User Accounts**
- **Device Manager**
- **Indexing Options**
- **Administrative Tools**
- **File Explorer Options**
  - Show hidden files
  - Hide extensions
  - General options
  - View options
- **Power Options**
  - Hibernate
  - Power plans
  - Sleep/suspend
  - Standby
  - Choose what closing the lid does
  - Turn on fast startup
  - Universal Serial Bus (USB) selective suspend
- **Ease of Access**

1.5 Given a scenario, use the appropriate Windows settings.

- **Time and Language**
- **Update and Security**
- **Personalization**
- **Apps**
- **Privacy**
- **System**
- **Devices**
- **Network and Internet**
- **Gaming**
- **Accounts**

1.6 Given a scenario, configure Microsoft Windows networking features on a client/desktop.

- **Workgroup vs. domain setup**
  - Shared resources
  - Printers
  - File servers
  - Mapped drives
- **Local OS firewall settings**
  - Application restrictions and exceptions
  - Configuration
- **Client network configuration**
  - Internet Protocol (IP) addressing scheme
  - Domain Name System (DNS) settings
  - Subnet mask
  - Gateway
  - Static vs. dynamic
- **Establish network connections**
  - Virtual private network (VPN)
  - Wireless
  - Wired
  - Wireless wide area network (WWAN)
- **Proxy settings**
- **Public network vs. private network**
- **File Explorer navigation – network paths**
- **Metered connections and limitations**

1.7 Given a scenario, apply application installation and configuration concepts.

- **System requirements for applications**
  - 32-bit vs. 64-bit dependent application requirements
  - Dedicated graphics card vs. integrated
  - Video random-access memory (VRAM) requirements
  - RAM requirements
  - Central processing unit (CPU) requirements
  - External hardware tokens
  - Storage requirements
- **OS requirements for applications**
  - Application to OS compatibility
  - 32-bit vs. 64-bit OS
- **Distribution methods**
  - Physical media vs. downloadable
  - ISO mountable
- **Other considerations for new applications**
  - Impact to device
  - Impact to network
  - Impact to operation
  - Impact to business

1.8 Explain common OS types and their purposes.

- **Workstation OSs**
  - Windows
  - Linux
  - macOS
  - Chrome OS
- **Cell phone/tablet OSs**
  - iPadOS
  - iOS
  - Android
- **Various filesystem types**
  - New Technology File System (NTFS)
  - File Allocation Table 32 (FAT32)
  - Third extended filesystem (ext3)
  - Fourth extended filesystem (ext4)
  - Apple File System (APFS)
  - Extensible File Allocation Table (exFAT)
- **Vendor life-cycle limitations**
  - End-of-life (EOL)
  - Update limitations
- **Compatibility concerns between OSs**

1.9 Given a scenario, perform OS installations and upgrades in a diverse OS environment.

- **Boot methods**
  - USB
  - Optical media
  - Network
  - Solid-state/flash drives
  - Internet-based
  - External/hot-swappable drive
  - Internal hard drive (partition)
- **Types of installations**
  - Upgrade
  - Recovery partition
  - Clean install
  - Image deployment
  - Repair installation
  - Remote network installation
  - Other considerations
    - Third-party drivers
- **Partitioning**
  - GUID [globally unique identifier] Partition Table (GPT)
  - Master boot record (MBR)
- **Drive format**
- **Upgrade considerations**
  - Backup files and user preferences
  - Application and driver support/ backward compatibility
  - Hardware compatibility
- **Feature updates**
  - Product life cycle

1.10 Identify common features and tools of the macOS/desktop OS.

- **Installation and uninstallation of applications**
  - File types
    - .dmg
    - .pkg
    - .app
  - App Store
  - Uninstallation process
- **Apple ID and corporate restrictions**
- **Best practices**
  - Backups
  - Antivirus
  - Updates/patches
- **System Preferences**
  - Displays
  - Networks
  - Printers
  - Scanners
  - Privacy
  - Accessibility
  - Time Machine
- **Features**
  - Multiple desktops
  - Mission Control
  - Keychain
  - Spotlight
  - iCloud
  - Gestures
  - Finder
  - Remote Disc
  - Dock
- **Disk Utility**
- **FileVault**
- **Terminal**
- **Force Quit**

1.11 Identify common features and tools of the Linux client/desktop OS.

- **Common commands**
  - ls
  - pwd
  - mv
  - cp
  - rm
  - chmod
  - chown
  - su/sudo
  - apt-get
  - yum
  - ip
  - df
  - grep
  - ps
  - man
  - top
  - find
  - dig
  - cat
  - nano
- **Best practices**
  - Backups
  - Antivirus
  - Updates/patches
- **Tools**
  - Shell/terminal
  - Samba

2.0 Security

2.1 Summarize various security measures and their purposes.

- **Physical security**
  - Access control vestibule
  - Badge reader
  - Video surveillance
  - Alarm systems
  - Motion sensors
  - Door locks
  - Equipment locks
  - Guards
  - Bollards
  - Fences
- **Physical security for staff**
  - Key fobs
  - Smart cards
  - Keys
  - Biometrics
    - Retina scanner
    - Fingerprint scanner
    - Palmprint scanner
  - Lighting
  - Magnetometers
- **Logical security**
  - Principle of least privilege
  - Access control lists (ACLs)
  - Multifactor authentication (MFA)
  - Email
  - Hard token
  - Soft token
  - Short message service (SMS)
  - Voice call
  - Authenticator application
- **Mobile device management (MDM)**
- **Active Directory**
  - Login script
  - Domain
  - Group Policy/updates
  - Organizational units
  - Home folder
  - Folder redirection
  - Security groups

2.2 Compare and contrast wireless security protocols and authentication methods.

- **Protocols and encryption**
  - WiFi Protected Access 2 (WPA2)
  - WPA3
  - Temporal Key Integrity Protocol (TKIP)
  - Advanced Encryption Standard (AES)
- **Authentication**
  - Remote Authentication Dial-In User Service (RADIUS)
  - Terminal Access Controller Access-Control System (TACACS+)
  - Kerberos
  - Multifactor

2.3 Given a scenario, detect, remove, and prevent malware using the appropriate tools and methods.

- **Malware**
  - Trojan
  - Rootkit
  - Virus
  - Spyware
  - Ransomware
  - Keylogger
  - Boot sector virus
  - Cryptominers
- **Tools and methods**
  - Recovery mode
  - Antivirus
  - Anti-malware
  - Software firewalls
  - Anti-phishing training
  - User education regarding common threats
  - OS reinstallation

2.4 Explain common social-engineering attacks, threats, and vulnerabilities.

- **Social engineering**
  - Phishing
  - Vishing
  - Shoulder surfing
  - Whaling
  - Tailgating
  - Impersonation
  - Dumpster diving
  - Evil twin
- **Threats**
  - Distributed denial of service (DDoS)
  - Denial of service (DoS)
  - Zero-day attack
  - Spoofing
  - On-path attack
  - Brute-force attack
  - Dictionary attack
  - Insider threat
  - Structured Query Language (SQL) injection
  - Cross-site scripting (XSS)
- **Vulnerabilities**
  - Non-compliant systems
  - Unpatched systems
  - Unprotected systems (missing antivirus/missing firewall)
  - EOL OSs
  - Bring your own device (BYOD)

2.5 Given a scenario, manage and configure basic security settings in the Microsoft Windows OS.

- **Defender Antivirus**
  - Activate/deactivate
  - Updated definitions
- **Firewall**
  - Activate/deactivate
  - Port security
  - Application security
- **Users and groups**
  - Local vs. Microsoft account
  - Standard account
  - Administrator
  - Guest user
  - Power user
- **Login OS options**
  - Username and password
  - Personal identification number (PIN)
  - Fingerprint
  - Facial recognition
  - Single sign-on (SSO)
- **NTFS vs. share permissions**
  - File and folder attributes
  - Inheritance
- **Run as administrator vs. standard user**
  - User Account Control (UAC)
- **BitLocker**
- **BitLocker To Go**
- **Encrypting File System (EFS)**

2.6 Given a scenario, configure a workstation to meet best practices for security.

- **Data-at-rest encryption**
- **Password best practices**
  - Complexity requirements
    - Length
    - Character types
  - Expiration requirements
  - Basic input/output system (BIOS)/ Unified Extensible Firmware Interface (UEFI) passwords
- **End-user best practices**
  - Use screensaver locks
  - Log off when not in use
  - Secure/protect critical hardware (e.g., laptops)
  - Secure personally identifiable information (PII) and passwords
- **Account management**
  - Restrict user permissions
  - Restrict login times
  - Disable guest account
  - Use failed attempts lockout
  - Use timeout/screen lock
- **Change default administrator's user account/password**
- **Disable AutoRun**
- **Disable AutoPlay**

2.7 Explain common methods for securing mobile and embedded devices.

- **Screen locks**
  - Facial recognition
  - PIN codes
  - Fingerprint
  - Pattern
  - Swipe
- **Remote wipes**
- **Locator applications**
- **OS updates**
- **Device encryption**
- **Remote backup applications**
- **Failed login attempts restrictions**
- **Antivirus/anti-malware**
- **Firewalls**
- **Policies and procedures**
  - BYOD vs. corporate owned
  - Profile security requirements
- **Internet of Things (IoT)**

2.8 Given a scenario, use common data destruction and disposal methods.

- **Physical destruction**
  - Drilling
  - Shredding
  - Degaussing
  - Incinerating
- **Recycling or repurposing best practices**
  - Erasing/wiping
  - Low-level formatting
  - Standard formatting
- **Outsourcing concepts**
  - Third-party vendor
  - Certification of destruction/recycling

2.9 Given a scenario, configure appropriate security settings on small office/home office (SOHO) wireless and wired networks.

- **Home router settings**
  - Change default passwords
  - IP filtering
  - Firmware updates
  - Content filtering
  - Physical placement/secure locations
  - Dynamic Host Configuration Protocol (DHCP) reservations
  - Static wide-area network (WAN) IP
  - Universal Plug and Play (UPnP)
  - Screened subnet
- **Wireless specific**
  - Changing the service set identifier (SSID)
  - Disabling SSID broadcast
  - Encryption settings
  - Disabling guest access
  - Changing channels
- **Firewall settings**
  - Disabling unused ports
  - Port forwarding/mapping

2.10 Given a scenario, install and configure browsers and relevant security settings.

- **Browser download/installation**
  - Trusted sources
    - Hashing
  - Untrusted sources
- **Extensions and plug-ins**
  - Trusted sources
  - Untrusted sources
- **Password managers**
- **Secure connections/sites – valid certificates**
- **Settings**
  - Pop-up blocker
  - Clearing browsing data
  - Clearing cache
  - Private-browsing mode
  - Sign-in/browser data synchronization
  - Ad blockers

3.0 Software Troubleshooting

3.1 Given a scenario, troubleshoot common Windows OS problems.

- **Common symptoms**
  - Blue screen of death (BSOD)
  - Sluggish performance
  - Boot problems
  - Frequent shutdowns
  - Services not starting
  - Applications crashing
  - Low memory warnings
  - USB controller resource warnings
  - System instability
  - No OS found
  - Slow profile load
  - Time drift
- **Common troubleshooting steps**
  - Reboot
  - Restart services
  - Uninstall/reinstall/update applications
  - Add resources
  - Verify requirements
  - System file check
  - Repair Windows
  - Restore
  - Reimage
  - Roll back updates
  - Rebuild Windows profiles

3.2 Given a scenario, troubleshoot common personal computer (PC) security issues.

- **Common symptoms**
  - Unable to access the network
  - Desktop alerts
  - False alerts regarding antivirus protection
  - Altered system or personal files
    - Missing/renamed files
  - Unwanted notifications within the OS
  - OS update failures
- **Browser-related symptoms**
  - Random/frequent pop-ups
  - Certificate warnings
  - Redirection

3.3 Given a scenario, use best practice procedures for malware removal.

1. **Investigate and verify malware symptoms**
2. **Quarantine infected systems**
3. **Disable System Restore in Windows**
4. **Remediate infected systems**
   a. Update anti-malware software
   b. Scanning and removal techniques (e.g., safe mode, preinstallation environment)
5. **Schedule scans and run updates**
6. **Enable System Restore and create a restore point in Windows**
7. **Educate the end user**

3.4 Given a scenario, troubleshoot common mobile OS and application issues.

- **Common symptoms**
  - Application fails to launch
  - Application fails to close/crashes
  - Application fails to update
  - Slow to respond
  - OS fails to update
  - Battery life issues
  - Randomly reboots
  - Connectivity issues
    - Bluetooth
    - WiFi
    - Near-field communication (NFC)
    - AirDrop
  - Screen does not autorotate

3.5 Given a scenario, troubleshoot common mobile OS and application security issues.

- **Security concerns**
  - Android package (APK) source
  - Developer mode
  - Root access/jailbreak
  - Bootleg/malicious application
    - Application spoofing
- **Common symptoms**
  - High network traffic
  - Sluggish response time
  - Data-usage limit notification
  - Limited Internet connectivity
  - No Internet connectivity
  - High number of ads
  - Fake security warnings
  - Unexpected application behavior
  - Leaked personal files/data

4.0 Operational Procedures

4.1 Given a scenario, implement best practices associated with documentation and support systems information management.

- **Ticketing systems**
  - User information
  - Device information
  - Description of problems
  - Categories
  - Severity
  - Escalation levels
  - Clear, concise written communication
    - Problem description
    - Progress notes
    - Problem resolution
- **Asset management**
  - Inventory lists
  - Database system
  - Asset tags and IDs
  - Procurement life cycle
  - Warranty and licensing
  - Assigned users
- **Types of documents**
  - Acceptable use policy (AUP)
  - Network topology diagram
  - Regulatory compliance requirements
    - Splash screens
  - Incident reports
  - Standard operating procedures
    - Procedures for custom installation of software package
  - New-user setup checklist
  - End-user termination checklist
- **Knowledge base/articles**

4.2 Explain basic change-management best practices.

- **Documented business processes**
  - Rollback plan
  - Sandbox testing
  - Responsible staff member
- **Change management**
  - Request forms
  - Purpose of the change
  - Scope of the change
  - Date and time of the change
  - Affected systems/impact
  - Risk analysis
    - Risk level
  - Change board approvals
  - End-user acceptance

4.3 Given a scenario, implement workstation backup and recovery methods.

- **Backup and recovery**
  - Full
  - Incremental
  - Differential
  - Synthetic
- **Backup testing**
  - Frequency
- **Backup rotation schemes**
  - On site vs. off site
  - Grandfather-father-son (GFS)
  - 3-2-1 backup rule

4.4 Given a scenario, use common safety procedures.

- **Electrostatic discharge (ESD) straps**
- **ESD mats**
- **Equipment grounding**
- **Proper power handling**
- **Proper component handling and storage**
- **Antistatic bags**
- **Compliance with government regulations**
- **Personal safety**
  - Disconnect power before repairing PC
  - Lifting techniques
  - Electrical fire safety
  - Safety goggles
  - Air filtration mask

4.5 Summarize environmental impacts and local environmental controls.

- **Material safety data sheet (MSDS)/documentation for handling and disposal**
  - Proper battery disposal
  - Proper toner disposal
  - Proper disposal of other devices and assets
- **Temperature, humidity-level awareness, and proper ventilation**
  - Location/equipment placement
  - Dust cleanup
  - Compressed air/vacuums
- **Power surges, under-voltage events, and power failures**
  - Battery backup
  - Surge suppressor

4.6 Explain the importance of prohibited content/activity and privacy, licensing, and policy concepts.

- **Incident response**
  - Chain of custody
  - Inform management/law enforcement as necessary
  - Copy of drive (data integrity and preservation)
  - Documentation of incident
- **Licensing/digital rights management (DRM)/end-user license agreement (EULA)**
  - Valid licenses
  - Non-expired licenses
  - Personal use license vs. corporate use license
  - Open-source license
- **Regulated data**
  - Credit card transactions
  - Personal government-issued information
  - PII
  - Healthcare data
  - Data retention requirements

4.7 Given a scenario, use proper communication techniques and professionalism.

- **Professional appearance and attire**
  - Match the required attire of the given environment
    - Formal
    - Business casual
- **Use proper language and avoid jargon, acronyms, and slang, when applicable**
- **Maintain a positive attitude/ project confidence**
- **Actively listen, take notes, and avoid interrupting the customer**
- **Be culturally sensitive**
  - Use appropriate professional titles, when applicable
- **Be on time (if late, contact the customer)**
- **Avoid distractions**
  - Personal calls
  - Texting/social media sites
  - Personal interruptions
- **Dealing with difficult customers or situations**
  - Do not argue with customers or be defensive
  - Avoid dismissing customer problems
  - Avoid being judgmental
  - Clarify customer statements (ask open-ended questions to narrow the scope of the problem, restate the issue, or question to verify understanding)
  - Do not disclose experience via social media outlets
- **Set and meet expectations/time line and communicate status with the customer**
  - Offer repair/replacement options, as needed
  - Provide proper documentation on the services provided
  - Follow up with customer/user at a later date to verify satisfaction
- **Deal appropriately with customers' confidential and private materials**
  - Located on a computer, desktop, printer, etc.

4.8 Identify the basics of scripting.

- **Script file types**
  - .bat
  - .ps1
  - .vbs
  - .sh
  - .js
  - .py
- **Use cases for scripting**
  - Basic automation
  - Restarting machines
  - Remapping network drives
  - Installation of applications
  - Automated backups
  - Gathering of information/data
  - Initiating updates
- **Other considerations when using scripts**
  - Unintentionally introducing malware
  - Inadvertently changing system settings
  - Browser or system crashes due to mishandling of resources

4.9 Given a scenario, use remote access technologies.

- **Methods/tools**
  - RDP
  - VPN
  - Virtual network computer (VNC)
  - Secure Shell (SSH)
  - Remote monitoring and management (RMM)
  - Microsoft Remote Assistance (MSRA)
  - Third-party tools
    - Screen-sharing software
    - Video-conferencing software
    - File transfer software
    - Desktop management software
- **Security considerations of each access method**

CompTIA A+ Core 2 (220-1102) Acronym List

The following is a list of acronyms that appear on the CompTIA A+ Core 2 (220-1102) 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	Alternating Current
ACL	Access Control List
ADF	Automatic Document Feeder
AES	Advanced Encryption Standard
AP	Access Point
APFS	Apple File System
APIPA	Automatic Private Internet Protocol Addressing
APK	Android Package
ARM	Advanced RISC [Reduced Instruction Set Computer] Machine
ARP	Address Resolution Protocol
ATA	Advanced Technology Attachment
ATM	Asynchronous Transfer Mode
ATX	Advanced Technology Extended
AUP	Acceptable Use Policy
BIOS	Basic Input/Output System
BSOD	Blue Screen of Death
BYOD	Bring Your Own Device
CAPTCHA	Completely Automated Public Turing Test to Tell Computers and Humans Apart
CD	Compact Disc
CDFS	Compact Disc File System
CDMA	Code-Division Multiple Access
CERT	Computer Emergency Response Team
CIFS	Common Internet File System
CMD	Command Prompt
CMOS	Complementary Metal-Oxide Semiconductor
CPU	Central Processing Unit
CRL	Certificate Revocation List
DC	Direct Current
DDoS	Distributed Denial of Service
DDR	Double Data Rate
DHCP	Dynamic Host Configuration Protocol
DIMM	Dual Inline Memory Module
DKIM	DomainKeys Identified Mail
DMA	Direct Memory Access
DMARC	Domain-based Message Authentication, Reporting, and Conformance
DNS	Domain Name System
DoS	Denial of Service
DRAM	Dynamic Random-Access Memory
DRM	Digital Rights Management
DSL	Digital Subscriber Line
DVI	Digital Visual Interface
DVI-D	Digital Visual Interface-Digital
ECC	Error Correcting Code
EFS	Encrypting File System
EMI	Electromagnetic Interference
EOL	End-of-Life
eSATA	External Serial Advanced Technology Attachment
ESD	Electrostatic Discharge
EULA	End-User License Agreement
exFAT	Extensible File Allocation Table
ext	Extended File System
FAT	File Allocation Table
FAT12	12-bit File Allocation Table
FAT16	16-bit File Allocation Table
FAT32	32-bit File Allocation Table
FSB	Front-Side Bus
FTP	File Transfer Protocol
GFS	Grandfather-Father-Son
GPS	Global Positioning System
GPT	GUID [Globally Unique Identifier] Partition Table
GPU	Graphics Processing Unit
GSM	Global System for Mobile Communications
GUI	Graphical User Interface

Acronym	Definition
GUID	Globally Unique Identifier
HAL	Hardware Abstraction Layer
HAV	Hardware-assisted Virtualization
HCL	Hardware Compatibility List
HDCP	High-bandwidth Digital Content Protection
HDD	Hard Disk Drive
HDMI	High-Definition Multimedia Interface
HSM	Hardware Security Module
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I/O	Input/Output
IaaS	Infrastructure as a Service
ICR	Intelligent Character Recognition
IDE	Integrated Drive Electronics
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IMAP	Internet Mail Access Protocol
IOPS	Input/Output Operations Per Second
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IPS	In-plane Switching
IPSec	Internet Protocol Security
IR	Infrared
IrDA	Infrared Data Association
IRP	Incident Response Plan
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITX	Information Technology eXtended
KB	Knowledge Base
KVM	Keyboard-Video-Mouse
LAN	Local Area Network
LC	Lucent Connector
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LED	Light-emitting Diode
MAC	Media Access Control/Mandatory Access Control
MAM	Mobile Application Management
MAN	Metropolitan Area Network
MBR	Master Boot Record
MDM	Mobile Device Management
MFA	Multifactor Authentication
MFD	Multifunction Device
MFP	Multifunction Printer
MMC	Microsoft Management Console
MOU	Memorandum of Understanding
MSDS	Material Safety Data Sheet
MSRA	Microsoft Remote Assistance
MX	Mail Exchange
NAC	Network Access Control
NAT	Network Address Translation
NDA	Non-disclosure Agreement
NetBIOS	Networked Basic Input/Output System
NetBT	NetBIOS over TCP/IP [Transmission Control Protocol/Internet Protocol]
NFC	Near-field Communication
NFS	Network File System
NIC	Network Interface Card
NTFS	New Technology File System
NVMe	Non-volatile Memory Express
OCR	Optical Character Recognition
OLED	Organic Light-emitting Diode
ONT	Optical Network Terminal
OS	Operating System
PaaS	Platform as a Service
PAN	Personal Area Network
PC	Personal Computer
PCIe	Peripheral Component Interconnect Express
PCL	Printer Command Language
PE	Preinstallation Environment
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PoE	Power over Ethernet
POP3	Post Office Protocol 3
POST	Power-on Self-Test
PPP	Point-to-Point Protocol
PRL	Preferred Roaming List
PSU	Power Supply Unit
PXE	Preboot Execution Environment
RADIUS	Remote Authentication Dial-in User Service
RAID	Redundant Array of Independent (or Inexpensive) Disks
RAM	Random-access Memory
RDP	Remote Desktop Protocol
RF	Radio Frequency
RFI	Radio Frequency Interference
RFID	Radio Frequency Identification
RJ11	Registered Jack Function 11
RJ45	Registered Jack Function 45
RMM	Remote Monitoring and Management
RTO	Recovery Time Objective
SaaS	Software as a Service
SAN	Storage Area Network

Acronym	Definition
SAS	Serial Attached SCSI [Small Computer System Interface]
SATA	Serial Advanced Technology Attachment
SC	Subscriber Connector
SCADA	Supervisory Control and Data Acquisition
SCP	Secure Copy Protection
SCSI	Small Computer System Interface
SDN	Software-defined Networking
SFTP	Secure File Transfer Protocol
SIM	Subscriber Identity Module
SIMM	Single Inline Memory Module
S.M.A.R.T.	Self-monitoring Analysis and Reporting Technology
SMB	Server Message Block
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SODIMM	Small Outline Dual Inline Memory Module
SOHO	Small Office/Home Office
SPF	Sender Policy Framework
SQL	Structured Query Language
SRAM	Static Random-access Memory
SSD	Solid-State Drive
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-on
ST	Straight Tip
STP	Shielded Twisted Pair
TACACS	Terminal Access Controller Access-Control System
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TN	Twisted Nematic
TPM	Trusted Platform Module
UAC	User Account Control
UDP	User Datagram Protocol
UEFI	Unified Extensible Firmware Interface
UNC	Universal Naming Convention
UPnP	Universal Plug and Play
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
UTM	Unified Threat Management
UTP	Unshielded Twisted Pair
VA	Vertical Alignment
VDI	Virtual Desktop Infrastructure
VGA	Video Graphics Array
VLAN	Virtual LAN [Local Area Network]
VM	Virtual Machine
VNC	Virtual Network Computer
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VRAM	Video Random-access Memory
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WISP	Wireless Internet Service Provider
WLAN	Wireless LAN [Local Area Network]
WMN	Wireless Mesh Network
WPA	WiFi Protected Access
WWAN	Wireless Wide Area Network
XSS	Cross-site Scripting

CompTIA A+ Core 2 (220-1102) Proposed Hardware and Software List

**CompTIA has included this sample list of hardware and software to assist candidates as they prepare for the A+ Core 2 (220-1102) exam. This list may also be helpful for training companies that wish to create a lab component to their training offering. The bulleted lists below each topic are sample lists and are not exhaustive.

Equipment

- Apple tablet/smartphone
- Android tablet/smartphone
- Windows tablet
- Chromebook
- Windows laptop/Mac laptop/Linux laptop
- Windows desktop/Mac desktop/Linux desktop
- Windows server with Active Directory and Print Management
- Monitors
- Projectors
- SOHO router/switch
- Access point
- Voice over Internet Protocol (VoIP) phone
- Printer
  - Laser/inkjet
  - Wireless
  - 3-D printer
  - Thermal
- Surge suppressor
- Uninterruptible power supply (UPS)
- Smart devices (Internet of Things [IoT] devices)
- Server with a hypervisor
- Punchdown block
- Patch panel
- Webcams
- Speakers
- Microphones

Spare parts/hardware

- Motherboards
- RAM
- Hard drives
- Power supplies
- Video cards
- Sound cards
- Network cards
- Wireless network interface cards (NICs)
- Fans/cooling devices/heat sink
- CPUs
- Assorted connectors/cables
  - USB
  - High-Definition Multimedia Interface (HDMI)
  - DisplayPort
  - Digital visual interface (DVI)
  - Video graphics array (VGA)
- Adapters
  - Bluetooth adapter
- Network cables
- Unterminated network cable/connectors
- Alternating current (AC) adapters
- Optical drives
- Screws/standoffs
- Cases
- Maintenance kit
- Mice/keyboards
- Keyboard-video-mouse (KVM)
- Console cable
- Solid-state drive (SSD)

Tools

- Screwdriver
- Multimeter
- Wire cutters
- Punchdown tool
- Crimper
- Power supply tester
- Cable stripper
- Standard technician toolkit
- Electrostatic discharge (ESD) strap
- Thermal paste
- Cable tester
- Cable toner
- WiFi analyzer
- Serial advanced technology attachment (SATA) to USB connectors

Software

- OSs
  - Linux
  - Chrome OS
  - Microsoft Windows
  - macOS
  - Android
  - iOS
- Preinstallation environment (PE) disk/live compact disc (CD)
- Antivirus software
- Virtualization software
- Anti-malware
- Driver software

CompTIA

CompTIA Network+ Certification Exam Objectives

EXAM NUMBER: N10-008

CompTIA

About the Exam

Candidates are encouraged to use this document to help prepare for the CompTIA Network+ (N10-008) certification exam. The CompTIA Network+ certification exam will verify the successful candidate has the knowledge and skills required to:

- **Establish network connectivity by deploying wired and wireless devices**
- **Understand and maintain network documentation**
- **Understand the purpose of network services**
- **Understand basic datacenter, cloud, and virtual networking concepts**
- **Monitor network activity, identifying performance and availability issues**
- **Implement network hardening techniques**
- **Manage, configure, and troubleshoot network infrastructure**

This is equivalent to 9–12 months of hands-on experience working in a junior network administrator/network support technician job role. 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+ (N10-008) 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 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	N10-008
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 9–12 months of hands-on experience working in a junior network administrator/ network support technician job role
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 Fundamentals	24%
2.0 Network Implementations	19%
3.0 Network Operations	16%
4.0 Network Security	19%
5.0 Network Troubleshooting	22%
Total	**100%**

1.0 Networking Fundamentals

1.1 Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.

- **OSI model**
  - Layer 1 – Physical
  - Layer 2 – Data link
  - Layer 3 – Network
  - Layer 4 – Transport
  - Layer 5 – Session
  - Layer 6 – Presentation
  - Layer 7 – Application
- **Data encapsulation and decapsulation within the OSI model context**
  - Ethernet header
  - Internet Protocol (IP) header
  - Transmission Control Protocol (TCP)/ User Datagram Protocol (UDP) headers
  - TCP flags
  - Payload
  - Maximum transmission unit (MTU)

1.2 Explain the characteristics of network topologies and network types.

- **Mesh**
- **Star/hub-and-spoke**
- **Bus**
- **Ring**
- **Hybrid**
- **Network types and characteristics**
  - Peer-to-peer
  - Client-server
  - Local area network (LAN)
  - Metropolitan area network (MAN)
  - Wide area network (WAN)
  - Wireless local area network (WLAN)
  - Personal area network (PAN)
  - Campus area network (CAN)
  - Storage area network (SAN)
  - Software-defined wide area network (SDWAN)
  - Multiprotocol label switching (MPLS)
  - Multipoint generic routing encapsulation (mGRE)
- **Service-related entry point**
  - Demarcation point
  - Smartjack
- **Virtual network concepts**
  - vSwitch
  - Virtual network interface card (vNIC)
  - Network function virtualization (NFV)
  - Hypervisor
- **Provider links**
  - Satellite
  - Digital subscriber line (DSL)
  - Cable
  - Leased line
  - Metro-optical

1.3 Summarize the types of cables and connectors and explain which is the appropriate type for a solution.

- **Copper**
  - Twisted pair
    - Cat 5
    - Cat 5e
    - Cat 6
    - Cat 6a
    - Cat 7
    - Cat 8
  - Coaxial/RG-6
  - Twinaxial
  - Termination standards
    - TIA/EIA-568A
    - TIA/EIA-568B
- **Fiber**
  - Single-mode
  - Multimode
- **Connector types**
  - Local connector (LC), straight tip (ST), subscriber connector (SC), mechanical transfer (MT), registered jack (RJ)
    - Angled physical contact (APC)
    - Ultra-physical contact (UPC)
  - RJ11
  - RJ45
  - F-type connector
  - Transceivers/media converters
  - Transceiver type
    - Small form-factor pluggable (SFP)
    - Enhanced form-factor pluggable (SFP+)
    - Quad small form-factor pluggable (QSFP)
    - Enhanced quad small form-factor pluggable (QSFP+)
- **Cable management**
  - Patch panel/patch bay
  - Fiber distribution panel
  - Punchdown block
    - 66
    - 110
    - Krone
    - Bix
- **Ethernet standards**
  - Copper
    - 10BASE-T
    - 100BASE-TX
    - 1000BASE-T
    - 10GBASE-T
    - 40GBASE-T
  - Fiber
    - 100BASE-FX
    - 100BASE-SX
    - 1000BASE-SX
    - 1000BASE-LX
    - 10GBASE-SR
    - 10GBASE-LR
    - Coarse wavelength division multiplexing (CWDM)
    - Dense wavelength division multiplexing (DWDM)
    - Bidirectional wavelength division multiplexing (WDM)

1.4 Given a scenario, configure a subnet and use appropriate IP addressing schemes.

- **Public vs. private**
  - RFC1918
  - Network address translation (NAT)
  - Port address translation (PAT)
- **IPv4 vs. IPv6**
  - Automatic Private IP Addressing (APIPA)
  - Extended unique identifier (EUI-64)
  - Multicast
  - Unicast
  - Anycast
  - Broadcast
  - Link local
  - Loopback
  - Default gateway
- **IPv4 subnetting**
  - Classless (variable-length subnet mask)
  - Classful
    - A
    - B
    - C
    - D
    - E
  - Classless Inter-Domain Routing (CIDR) notation
- **IPv6 concepts**
  - Tunneling
  - Dual stack
  - Shorthand notation
  - Router advertisement
  - Stateless address autoconfiguration (SLAAC)
- **Virtual IP (VIP)**
- **Subinterfaces**

1.5 Explain common ports and protocols, their application, and encrypted alternatives.

Protocols	Ports
File Transfer Protocol (FTP)	20/21
Secure Shell (SSH)	22
Secure File Transfer Protocol (SFTP)	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
Post Office Protocol v3 (POP3)	110
Network Time Protocol (NTP)	123
Internet Message Access Protocol (IMAP)	143
Simple Network Management Protocol (SNMP)	161/162
Lightweight Directory Access Protocol (LDAP)	389
Hypertext Transfer Protocol Secure (HTTPS) [Secure Sockets Layer (SSL)]	443
HTTPS [Transport Layer Security (TLS)]	443
Server Message Block (SMB)	445
Syslog	514
SMTP TLS	587
Lightweight Directory Access Protocol (over SSL) (LDAPS)	636
IMAP over SSL	993
POP3 over SSL	995
Structured Query Language (SQL) Server	1433
SQLnet	1521
MySQL	3306
Remote Desktop Protocol (RDP)	3389
Session Initiation Protocol (SIP)	5060/5061

- **IP protocol types**
  - Internet Control Message Protocol (ICMP)
  - TCP
  - UDP
  - Generic Routing Encapsulation (GRE)
  - Internet Protocol Security (IPSec)
    - Authentication Header (AH)/Encapsulating Security Payload (ESP)
- **Connectionless vs. connection-oriented**

1.6 Explain the use and purpose of network services.

- **DHCP**
  - Scope
  - Exclusion ranges
  - Reservation
  - Dynamic assignment
  - Static assignment
  - Lease time
  - Scope options
  - Available leases
  - DHCP relay
  - IP helper/UDP forwarding
- **DNS**
  - Record types
    - Address (A vs. AAAA)
    - Canonical name (CNAME)
    - Mail exchange (MX)
    - Start of authority (SOA)
    - Pointer (PTR)
    - Text (TXT)
    - Service (SRV)
    - Name server (NS)
  - Global hierarchy
    - Root DNS servers
  - Internal vs. external
  - Zone transfers
  - Authoritative name servers
  - Time to live (TTL)
  - DNS caching
  - Reverse DNS/reverse lookup/forward lookup
  - Recursive lookup/iterative lookup
- **NTP**
  - Stratum
  - Clients
  - Servers

1.7 Explain basic corporate and datacenter network architecture.

- **Three-tiered**
  - Core
  - Distribution/aggregation layer
  - Access/edge
- **Software-defined networking**
  - Application layer
  - Control layer
  - Infrastructure layer
  - Management plane
- **Spine and leaf**
  - Software-defined network
  - Top-of-rack switching
  - Backbone
- **Traffic flows**
  - North-South
  - East-West
- **Branch office vs. on-premises datacenter vs. colocation**
- **Storage area networks**
  - Connection types
    - Fibre Channel over Ethernet (FCoE)
    - Fibre Channel
    - Internet Small Computer Systems Interface (iSCSI)

1.8 Summarize cloud concepts and connectivity options.

- **Deployment models**
  - Public
  - Private
  - Hybrid
  - Community
- **Service models**
  - Software as a service (SaaS)
  - Infrastructure as a service (IaaS)
  - Platform as a service (PaaS)
  - Desktop as a service (DaaS)
- **Infrastructure as code**
  - Automation/orchestration
- **Connectivity options**
  - Virtual private network (VPN)
  - Private-direct connection to cloud provider
- **Multitenancy**
- **Elasticity**
- **Scalability**
- **Security implications**

2.0 Network Implementations

2.1 Compare and contrast various devices, their features, and their appropriate placement on the network.

- **Networking devices**
  - Layer 2 switch
  - Layer 3 capable switch
  - Router
  - Hub
  - Access point
  - Bridge
  - Wireless LAN controller
  - Load balancer
  - Proxy server
  - Cable modem
  - DSL modem
  - Repeater
  - Voice gateway
  - Media converter
  - Intrusion prevention system (IPS)/intrusion detection system (IDS) device
  - Firewall
  - VPN headend
- **Networked devices**
  - Voice over Internet Protocol (VoIP) phone
  - Printer
  - Physical access control devices
  - Cameras
  - Heating, ventilation, and air conditioning (HVAC) sensors
  - Internet of Things (IoT)
    - Refrigerator
    - Smart speakers
    - Smart thermostats
    - Smart doorbells
  - Industrial control systems/ supervisory control and data acquisition (SCADA)

2.2 Compare and contrast routing technologies and bandwidth management concepts.

- **Routing**
  - Dynamic routing
    - Protocols [Routing Internet Protocol (RIP), Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), Border Gateway Protocol (BGP)]
    - Link state vs. distance vector vs. hybrid
  - Static routing
  - Default route
  - Administrative distance
  - Exterior vs. interior
  - Time to live
- **Bandwidth management**
  - Traffic shaping
  - Quality of service (QoS)

2.3 Given a scenario, configure and deploy common Ethernet switching features.

- Data virtual local area network (VLAN)
- Voice VLAN
- Port configurations
  - Port tagging/802.1Q
  - Port aggregation
    - Link Aggregation Control Protocol (LACP)
  - Duplex
  - Speed
  - Flow control
  - Port mirroring
  - Port security
  - Jumbo frames
  - Auto-medium-dependent interface crossover (MDI-X)
- Media access control (MAC) address tables
- Power over Ethernet (PoE)/ Power over Ethernet plus (PoE+)
- Spanning Tree Protocol
- Carrier-sense multiple access with collision detection (CSMA/CD)

- **Address Resolution Protocol (ARP)**
- **Neighbor Discovery Protocol**

2.4 Given a scenario, install and configure the appropriate wireless standards and technologies.

- **802.11 standards**
  - a
  - b
  - g
  - n (WiFi 4)
  - ac (WiFi 5)
  - ax (WiFi 6)
- **Frequencies and range**
  - 2.4GHz
  - 5GHz
- **Channels**
  - Regulatory impacts
- **Channel bonding**
- **Service set identifier (SSID)**
  - Basic service set
  - Extended service set
  - Independent basic service set (Ad-hoc)
  - Roaming
- **Antenna types**
  - Omni
  - Directional
- **Encryption standards**
  - WiFi Protected Access (WPA)/ WPA2 Personal [Advanced Encryption Standard (AES)/ Temporal Key Integrity Protocol (TKIP)]
  - WPA/WPA2 Enterprise (AES/TKIP)
- **Cellular technologies**
  - Code-division multiple access (CDMA)
  - Global System for Mobile Communications (GSM)
  - Long-Term Evolution (LTE)
  - 3G, 4G, 5G
- **Multiple input, multiple output (MIMO) and multi-user MIMO (MU-MIMO)**

3.0 Network Operations

3.1 Given a scenario, use the appropriate statistics and sensors to ensure network availability.

- **Performance metrics/sensors**
  - Device/chassis
    - Temperature
    - Central processing unit (CPU) usage
    - Memory
  - Network metrics
    - Bandwidth
    - Latency
    - Jitter
- **SNMP**
  - Traps
  - Object identifiers (OIDs)
  - Management information bases (MIBs)
- **Network device logs**
  - Log reviews
    - Traffic logs
    - Audit logs
    - Syslog
  - Logging levels/severity levels
- **Interface statistics/status**
  - Link state (up/down)
  - Speed/duplex
  - Send/receive traffic
  - Cyclic redundancy checks (CRCs)
  - Protocol packet and byte counts
- **Interface errors or alerts**
  - CRC errors
  - Giants
  - Runts
  - Encapsulation errors
- **Environmental factors and sensors**
  - Temperature
  - Humidity
  - Electrical
  - Flooding
- **Baselines**
- **NetFlow data**
- **Uptime/downtime**

3.2 Explain the purpose of organizational documents and policies.

- **Plans and procedures**
  - Change management
  - Incident response plan
  - Disaster recovery plan
  - Business continuity plan
  - System life cycle
  - Standard operating procedures
- **Hardening and security policies**
  - Password policy
  - Acceptable use policy
  - Bring your own device (BYOD) policy
  - Remote access policy
  - Onboarding and offboarding policy
  - Security policy
  - Data loss prevention
- **Common documentation**
  - Physical network diagram
    - Floor plan
    - Rack diagram
    - Intermediate distribution frame (IDF)/main distribution frame (MDF) documentation
  - Logical network diagram
  - Wiring diagram
  - Site survey report
  - Audit and assessment report
  - Baseline configurations
- **Common agreements**
  - Non-disclosure agreement (NDA)
  - Service-level agreement (SLA)
  - Memorandum of understanding (MOU)

3.3 Explain high availability and disaster recovery concepts and summarize which is the best solution.

- **Load balancing**
- **Multipathing**
- **Network interface card (NIC) teaming**
- **Redundant hardware/clusters**
  - Switches
  - Routers
  - Firewalls
- **Facilities and infrastructure support**
  - Uninterruptible power supply (UPS)
  - Power distribution units (PDUs)
  - Generator
  - HVAC
  - Fire suppression
- **Redundancy and high availability (HA) concepts**
  - Cold site
  - Warm site
  - Hot site
  - Cloud site
  - Active-active vs. active-passive
    - Multiple Internet service providers (ISPs)/diverse paths
    - Virtual Router Redundancy Protocol (VRRP)/First Hop Redundancy Protocol (FHRP)
  - Mean time to repair (MTTR)
  - Mean time between failure (MTBF)
  - Recovery time objective (RTO)
  - Recovery point objective (RPO)
- **Network device backup/restore**
  - State
  - Configuration

4.0 Network Security

4.1 Explain common security concepts.

- **Confidentiality, integrity, availability (CIA)**
- **Threats**
  - Internal
  - External
- **Vulnerabilities**
  - Common vulnerabilities and exposures (CVE)
  - Zero-day
- **Exploits**
- **Least privilege**
- **Role-based access**
- **Zero Trust**
- **Defense in depth**
  - Network segmentation enforcement
  - Perimeter network [previously known as demilitarized zone (DMZ)]
  - Separation of duties
  - Network access control
  - Honeypot
- **Authentication methods**
  - Multifactor
  - Terminal Access Controller Access-Control System Plus (TACACS+)
  - Single sign-on (SSO)
  - Remote Authentication Dial-in User Service (RADIUS)
  - LDAP
  - Kerberos
  - Local authentication
  - 802.1X
  - Extensible Authentication Protocol (EAP)
- **Risk Management**
  - Security risk assessments
    - Threat assessment
    - Vulnerability assessment
    - Penetration testing
    - Posture assessment
  - Business risk assessments
    - Process assessment
    - Vendor assessment
- **Security information and event management (SIEM)**

4.2 Compare and contrast common types of attacks.

- **Technology-based**
  - Denial-of-service (DoS)/ distributed denial-of-service (DDoS)
    - Botnet/command and control
  - On-path attack (previously known as man-in-the-middle attack)
  - DNS poisoning
  - VLAN hopping
  - ARP spoofing
  - Rogue DHCP
  - Rogue access point (AP)
  - Evil twin
  - Ransomware
  - Password attacks
    - Brute-force
    - Dictionary
  - MAC spoofing
  - IP spoofing
  - Deauthentication
  - Malware
- **Human and environmental**
  - Social engineering
    - Phishing
    - Tailgating
    - Piggybacking
    - Shoulder surfing

4.3 Given a scenario, apply network hardening techniques.

- **Best practices**
  - Secure SNMP
  - Router Advertisement (RA) Guard
  - Port security
  - Dynamic ARP inspection
  - Control plane policing
  - Private VLANs
  - Disable unneeded switchports
  - Disable unneeded network services
  - Change default passwords
  - Password complexity/length
  - Enable DHCP snooping
  - Change default VLAN
  - Patch and firmware management
  - Access control list
  - Role-based access
  - Firewall rules
    - Explicit deny
    - Implicit deny
- **Wireless security**
  - MAC filtering
  - Antenna placement
  - Power levels
  - Wireless client isolation
  - Guest network isolation
  - Preshared keys (PSKs)
  - EAP
  - Geofencing
  - Captive portal
- **IoT access considerations**

4.4 Compare and contrast remote access methods and security implications.

- **Site-to-site VPN**
- **Client-to-site VPN**
  - Clientless VPN
  - Split tunnel vs. full tunnel
- **Remote desktop connection**
- **Remote desktop gateway**
- **SSH**
- **Virtual network computing (VNC)**
- **Virtual desktop**
- **Authentication and authorization considerations**
- **In-band vs. out-of-band management**

4.5 Explain the importance of physical security.

- **Detection methods**
  - Camera
  - Motion detection
  - Asset tags
  - Tamper detection
- **Prevention methods**
  - Employee training
  - Access control hardware
    - Badge readers
    - Biometrics
  - Locking racks
  - Locking cabinets
  - Access control vestibule (previously known as a mantrap)
  - Smart lockers
- **Asset disposal**
  - Factory reset/wipe configuration
  - Sanitize devices for disposal

5.0 Network Troubleshooting

5.1 Explain the network 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 the theory is confirmed, determine the next steps to resolve the problem
  - If the theory is not confirmed, reestablish 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, if applicable, implement preventive measures**
- **Document findings, actions, outcomes, and lessons learned**

5.2 Given a scenario, troubleshoot common cable connectivity issues and select the appropriate tools.

- **Specifications and limitations**
  - Throughput
  - Speed
  - Distance
- **Cable considerations**
  - Shielded and unshielded
  - Plenum and riser-rated
- **Cable application**
  - Rollover cable/console cable
  - Crossover cable
  - Power over Ethernet
- **Common issues**
  - Attenuation
  - Interference
  - Decibel (dB) loss
  - Incorrect pinout
  - Bad ports
  - Open/short
  - Light-emitting diode (LED) status indicators
  - Incorrect transceivers
  - Duplexing issues
  - Transmit and receive (TX/RX) reversed
  - Dirty optical cables
- **Common tools**
  - Cable crimper
  - Punchdown tool
  - Tone generator
  - Loopback adapter
  - Optical time-domain reflectometer (OTDR)
  - Multimeter
  - Cable tester
  - Wire map
  - Tap
  - Fusion splicers
  - Spectrum analyzers
  - Snips/cutters
  - Cable stripper
  - Fiber light meter

5.3 Given a scenario, use the appropriate network software tools and commands.

- **Software tools**
  - WiFi analyzer
  - Protocol analyzer/packet capture
  - Bandwidth speed tester
  - Port scanner
  - iperf
  - NetFlow analyzers
  - Trivial File Transfer Protocol (TFTP) server
  - Terminal emulator
  - IP scanner
- **Command line tool**
  - ping
  - ipconfig/ifconfig/ip
  - nslookup/dig
  - traceroute/tracert
  - arp
  - netstat
  - hostname
  - route
  - telnet
  - tcpdump
  - nmap
- **Basic network platform commands**
  - show interface
  - show config
  - show route

5.4 Given a scenario, troubleshoot common wireless connectivity issues.

- **Specifications and limitations**
  - Throughput
  - Speed
  - Distance
  - Received signal strength indication (RSSI) signal strength
  - Effective isotropic radiated power (EIRP)/power settings
- **Considerations**
  - Antennas
    - Placement
    - Type
    - Polarization
  - Channel utilization
  - AP association time
  - Site survey
- **Common issues**
  - Interference
    - Channel overlap
  - Antenna cable attenuation/signal loss
  - RF attenuation/signal loss
  - Wrong SSID
  - Incorrect passphrase
  - Encryption protocol mismatch
  - Insufficient wireless coverage
  - Captive portal issues
  - Client disassociation issues

5.5 Given a scenario, troubleshoot general networking issues.

- **Considerations**
  - Device configuration review
  - Routing tables
  - Interface status
  - VLAN assignment
  - Network performance baselines
- **Common issues**
  - Collisions
  - Broadcast storm
  - Duplicate MAC address
  - Duplicate IP address
  - Multicast flooding
  - Asymmetrical routing
  - Switching loops
  - Routing loops
  - Rogue DHCP server
  - DHCP scope exhaustion
  - IP setting issues
    - Incorrect gateway
    - Incorrect subnet mask
    - Incorrect IP address
    - Incorrect DNS
  - Missing route
  - Low optical link budget
  - Certificate issues
  - Hardware failure
  - Host-based/network-based firewall settings
  - Blocked services, ports, or addresses
  - Incorrect VLAN
  - DNS issues
  - NTP issues
  - BYOD challenges
  - Licensed feature issues
  - Network performance issues

Network+ (N10-008) 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 part of a comprehensive exam preparation program.

ACRONYM	SPELLED OUT
AAAA	Authentication, Authorization, Accounting, Auditing
ACL	Access Control List
AES	Advanced Encryption Standard
AH	Authentication Header
AP	Access Point
APC	Angled Physical Contact
APIPA	Automatic Private Internet Protocol Addressing
ARP	Address Resolution Protocol
AUP	Acceptable Use Policy
BGP	Border Gateway Protocol
BNC	British Naval Connector/Bayonet Neill-Concelman
BYOD	Bring Your Own Device
CAM	Content Addressable Memory (table)
CAN	Campus Area Network
CDMA	Code Division Multiple Access
CIA	Confidentiality, Integrity, and Availability
CIDR	Classless Inter-Domain Routing
CLI	Command-Line Interface
CNAME	Canonical Name
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier-Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier-Sense Multiple Access with Collision Detection
CSU	Channel Service Unit
CVE	Common Vulnerabilities and Exposures
CWDM	Coarse Wavelength Division Multiplexing
DaaS	Desktop as a Service
dB	Decibel
DDoS	Distributed Denial-of-Service
DHCP	Dynamic Host Configuration Protocol
DLP	Data Loss Prevention
DNS	Domain Name System
DoS	Denial-of-Service
DSL	Digital Subscriber Line
DSU	Data Service Unit
DWDM	Dense Wavelength Division Multiplexing
EAP	Extensible Authentication Protocol
EIA	Electronic Industries Association
EIGRP	Enhanced Interior Gateway Routing Protocol
EIRP	Effective Isotropic Radiated Power
ESP	Encapsulating Security Payload
EUI	Extended Unique Identifier
FCoE	Fibre Channel over Ethernet
FHRP	First Hop Redundancy Protocol
FTP	File Transfer Protocol
GBIC	Gigabit Interface Converter
GRE	Generic Routing Encapsulation
GSM	Global System for Mobile Communications
HA	High Availability
HDMI	High-Definition Multimedia Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HVAC	Heating, Ventilation, and Air Conditioning
IaaS	Infrastructure as a Service
ICMP	Internet Control Message Protocol
ICS	Industrial Control System
IDF	Intermediate Distribution Frame
IDS	Intrusion Detection System
IGMP	Internet Group Management Protocol
IMAP	Internet Message Access Protocol
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
iSCSI	Internet Small Computer Systems Interface
ISP	Internet Service Provider
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LC	Local Connector
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol (over SSL)
LED	Light-Emitting Diode
LTE	Long-Term Evolution
MAC	Media Access Control/Medium Access Control
MAN	Metropolitan Area Network
MDF	Main Distribution Frame
MDIX	Medium Dependent Interface Crossover
mGRE	Multipoint Generic Routing Encapsulation
MIB	Management Information Base

ACRONYM	SPELLED OUT
MIMO	Multiple Input, Multiple Output
MU-MIMO	Multiuser - Multiple Input, Multiple Output
MOU	Memorandum of Understanding
MPLS	Multiprotocol Label Switching
MTBF	Mean Time Between Failure
MT-RJ	Mechanical Transfer - Registered Jack
MTTR	Mean Time to Repair
MTU	Maximum Transmission Unit
MX	Mail Exchange
NAC	Network Access Control
NAS	Network Attached Storage
NAT	Network Address Translation
NDA	Non-Disclosure Agreement
NFV	Network Function Virtualization
NGFW	Next-Generation Firewall
NIC	Network Interface Card
NS	Name Server
NTP	Network Time Protocol
OID	Object Identifier
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OTDR	Optical Time Domain Reflectometer
PaaS	Platform as a Service
PAN	Personal Area Network
PAT	Port Address Translation
PDU	Power Distribution Unit
PoE	Power over Ethernet
POP3	Post Office Protocol version 3
PSK	Pre-Shared Key
PTR	Pointer Record
QoS	Quality of Service
QSFP	Quad Small Form-factor Pluggable
RA	Router Advertisements
RADIUS	Remote Authentication Dial-In User Service
RAID	Redundant Array of Inexpensive (or Independent) Disks
RDP	Remote Desktop Protocol
RF	Radio Frequency
RFC	Request for Comment
RG	Radio Guide
RIP	Routing Internet Protocol
RJ	Registered Jack
RPO	Recovery Point Objective
RSSI	Received Signal Strength Indication
RTO	Recovery Time Objective
RTSP	Real Time Streaming Protocol
SaaS	Software as a Service
SAN	Storage Area Network
SC	Standard Connector/Subscriber Connector
SCADA	Supervisory Control and Data Acquisition
SDN	Software-Defined Network
SDWAN	Software-Defined WAN

ACRONYM	SPELLED OUT
SFP	Small Form-factor Pluggable
SFTP	Secure File Transfer Protocol
SIEM	Security Information and Event Management
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLAAC	Stateless Address Auto-Configuration
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOA	Start of Authority
SOHO	Small Office Home Office
SQL	Structured Query Language
SRV	Service Record
SSD	Solid-State Drive
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-On
ST	Straight Tip or Snap Twist
STP	Spanning Tree Protocol
SYSLOG	System Log
TACACS+	Terminal Access Controller Access Control System Plus
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TIA/EIA	Telecommunications Industry Association/Electronic Industries Alliance
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTL	Time to Live
TX/RX	Transmit and Receive
UDP	User Datagram Protocol
UPC	Ultra-Physical Contact
UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTP	Unshielded Twister Pair
VIP	Virtual IP
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNC	Virtual Network Computing
vNIC	virtual Network Interface Card
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WAP	Wireless Access Point
WDM	Wavelength Division Multiplexing
WLAN	Wireless Local Area Network
WPA	WiFi Protected Access

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 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

- Optical and copper patch panels
- Punchdown blocks
- Layer 2 switch
- Layer 3 switch
- PoE switch
- Router
- Firewall
- VPN headend
- Wireless access point
- Basic laptops that support virtualization
- Tablet/cell phone
- Media converters
- VoIP system (including a phone)

SPARE HARDWARE

- NICs
- Power supplies
- GBICs
- SFPs
- Managed switch
- Wireless access point
- UPS
- PoE injector

SPARE PARTS

- Patch cables
- RJ11 connectors
- RJ45 connectors, modular jacks
- Unshielded twisted pair cable spool
- Coaxial cable spool
- F connectors
- Fiber connectors
- Antennas
- Bluetooth/wireless adapters
- Console cables (RS-232 to USB serial adapter)

TOOLS

- Telco/network crimper
- Cable tester
- Punchdown tool
- Cable stripper
- Coaxial crimper
- Wire cutter
- Tone generator
- Fiber termination kit
- Optical power meter

SOFTWARE

- Protocol analyzer/packet capture
- Terminal emulation software
- Linux OS/Windows OS
- Software firewall
- Software IDS/IPS
- Network mapper
- Hypervisor software
- Virtual network environment
- WiFi analyzer
- Spectrum analyzer
- Network monitoring tools
- DHCP service
- DNS service
- NetFlow analyzer
- TFTP server
- Firmware backups for upgrades

OTHER

- Sample network documentation
- Sample logs
- Defective cables
- Cloud network diagrams

CompTIA