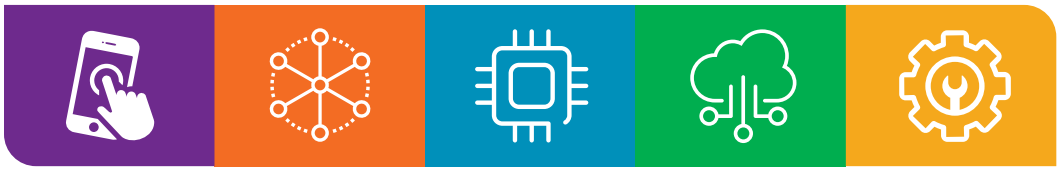
CompTIA A+ Certification Exam Core 1 Objectives

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.

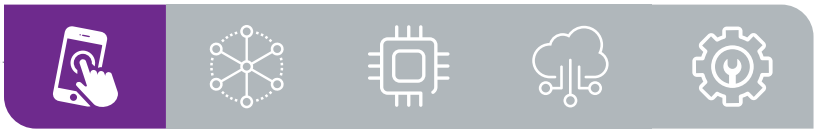
TEST DETAILS

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.

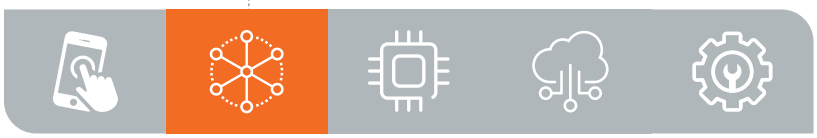
- **Types**
  - Liquid crystal display (LCD)
    - In-plane switching
    - Twisted nematic (TN)
    - Vertical alignment (VA)
  - Organic light-emitting diode (OLED)
- **Mobile display components**
- **WiFi antenna connector/ placement**
- **Camera/webcam**
- **Microphone**
- **Touch screen/digitizer**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

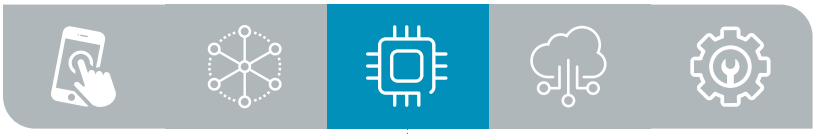
- **DNS**
  - Address
    - A
    - AAAA
  - Mail exchanger (MX)
  - Text (TXT)
    - Spam management
      (i) DomainKeys Identified Mail (DKIM)
      (ii) Sender Policy Framework (SPF)
      (iii) Domain-based Message Authentication, Reporting, and Conformance (DMARC)
- **DHCP**
  - Leases
  - Reservations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

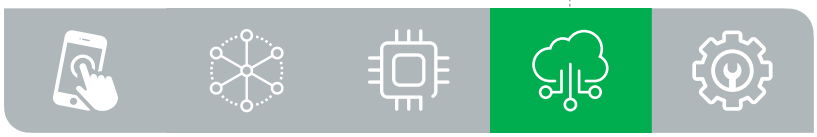
- **Input 110-120 VAC vs. 220-240 VAC**
- **Output 3.3V vs. 5V vs. 12V**
- **20-pin to 24-pin motherboard adapter**
- **Redundant power supply**
- **Modular power supply**
- **Wattage rating**

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



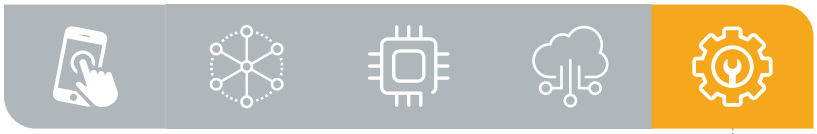
4.0 Virtualization and Cloud Computing

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+ Certification Exam Core 2 Objectives

EXAM NUMBER: CORE 2 (220-1102)

CompTIA

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
AV	Antivirus
BIOS	Basic Input/Output System
BSOD	Blue Screen of Death
BYOD	Bring Your Own Device
CA	Certificate Authority
CAPTCHA	Completely Automated Public Turing Test to Tell Computers and Humans Apart
CAD	Computer-aided Design
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
CNAME	Canonical Name
CPU	Central Processing Unit
CRL	Certificate Revocation List
DaaS	Data as a Service

Acronym	Definition
DBaaS	Database as a Service
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
DOS	Disk Operating System
DRaaS	Disaster Recovery as a Service
DRAM	Dynamic Random-Access Memory
DRM	Digital Rights Management
DSL	Digital Subscriber Line
DVI	Digital Visual Interface
DVI-D	Digital Visual Interface-Digital
EAP	Extensible Authentication Protocol
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

Acronym	Definition
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
HCL	Hardware Compatibility List
HDCP	High-bandwidth Digital Content Protection
HDD	Hard Disk Drive
HDMI	High-Definition Multimedia Interface
HHD	Hybrid Hard Drive
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
ICMP	Internet Message Control Protocol
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
IPSec	Internet Protocol Security
IR	Infrared
IrDA	Infrared Data Association
IRP	Incident Response Plan
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
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
LEAP	Lightweight Extensible Protocol
LED	Light-emitting Diode
LTE	Long Term Evolution
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
mSATA	Mini-serial Advanced Technology Attachment
MSDS	Material Safety Data Sheet
MSP	Managed Service Provider
MSRA	Microsoft Remote Assistance
MTBF	Meantime Between Failure
MX	Mail Exchange
NAC	Network Access Control
NAS	Network Attached Storage
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
NTP	Network Time Protocol
NVMe	Non-volatile Memory Express
OCR	Optical Character Recognition
OEM	Original Equipmet Manufacturer
OLED	Organic Light-emitting Diode
ONT	Optical Network Terminal
OS	Operating System
PaaS	Platform as a Service
PAN	Personal Area Network
PC	Personal Computer
PCI	Payment Card Industry
PCIe	Peripheral Component Interconnect Express
PCL	Printer Command Language
PDU	Power Distribution Unit
PE	Preinstallation Environment
PEAP	Protected Extensible Protocol
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
PSK	Preshared Key
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

Acronym	Definition
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
S/MIME	Secure/Multipurpose Internet Mail Extensions
SaaS	Software as a Service
SAN	Storage Area Network
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
SD	Secure Digital
SDD	Super Density Disk
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
SOA	Start of Authority
SODIMM	Small Outline Dual Inline Memory Module
SOHO	Small Office/Home Office
SOP	Standard Operating Procedure
SPF	Sender Policy Framework
SQL	Structured Query Language
SRAM	Static Random-access Memory
SRV	Service
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
USB-C	Universal Serial Bus Type C
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
WAP	Wireless Access Point
WEP	Wired Equivalent Privacy
WISP	Wireless Internet Service Provider
WLAN	Wireless LAN [Local Area Network]
WMN	Wireless Mesh Network
WPA	WiFi Protected Access
WPS	Wi-Fi Protected Service
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