



# CompTIA A+ Certification Exam Objectives

**EXAM NUMBER: 220-902**



# About the Exam

Candidates are encouraged to use this document to help prepare for CompTIA A+ 220-902. In order to receive the CompTIA A+ certification, you must pass two exams: 220-901 and 220-902. CompTIA A+ 220-902 measures the necessary skills for an entry-level IT professional. Successful candidates will have the knowledge required to:

- Assemble components based on customer requirements
- Install, configure and maintain devices, PCs and software for end users
- Understand the basics of networking and security/forensics
- Properly and safely diagnose, resolve and document common hardware and software issues
- Apply troubleshooting skills
- Provide appropriate customer support
- Understand the basics of virtualization, desktop imaging and deployment

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

CompTIA A+ 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 perform a search using CertGuard’s engine, found [here](#).

## 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	CompTIA A+ 220-902
Number of questions	Maximum of 90
Types of questions	Multiple choice and performance-based
Length of test	90 minutes
Recommended experience	Six to 12 months hands-on experience in the lab or field
Passing score	CompTIA A+ 220-902: 700 (on a scale of 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 Windows Operating Systems	29%
2.0 Other Operating Systems & Technologies	12%
3.0 Security	22%
4.0 Software Troubleshooting	24%
5.0 Operational Procedures	13%
<b>Total</b>	<b>100%</b>



# 1.0 Windows Operating Systems

## 1.1 Compare and contrast various features and requirements of Microsoft Operating Systems (Windows Vista, Windows 7, Windows 8, Windows 8.1).

### • Features:

- 32-bit vs. 64-bit
- Aero, gadgets, user account control, BitLocker, shadow copy, system restore, ready boost, sidebar, compatibility mode, virtual XP mode, easy transfer, administrative tools, defender, Windows firewall,

- security center, event viewer, file structure and paths, category view vs. classic view
- Side-by-side apps, Metro UI, Pinning, One Drive, Windows store, multimonitor task bars, charms, Start Screen, PowerShell, Live sign in, Action Center

- Upgrade paths – differences between in place upgrades, compatibility tools, Windows upgrade OS advisor

## 1.2 Given a scenario, install Windows PC operating systems using appropriate methods.

### • Boot methods

- USB
- CD-ROM
- DVD
- PXE
- Solid state/flash drives
- Netboot
- External/hot swappable drive
- Internal hard drive (partition)

### • Type of installations

- Unattended installation
- Upgrade
- Clean install
- Repair installation
- Multiboot

- Remote network installation
- Image deployment
- Recovery partition
- Refresh/restore

### • Partitioning

- Dynamic
- Basic
- Primary
- Extended
- Logical
- GPT

### • File system types/formatting

- exFAT
- FAT32
- NTFS

- CDFS
- NFS
- ext3, ext4
- Quick format vs. full format

- Load alternate third-party drivers when necessary
- Workgroup vs. domain setup
- Time/date/region/language settings
- Driver installation, software and windows updates
- Factory recovery partition
- Properly formatted boot drive with the correct partitions/format

## 1.3 Given a scenario, apply appropriate Microsoft command line tools.

- TASKKILL
- BOOTREC
- SHUTDOWN
- TASKLIST
- MD
- RD
- CD
- DEL
- FORMAT

- COPY
- XCOPY
- ROBOCOPY
- DISKPART
- SFC
- CHKDSK
- GPUPDATE
- GPRESULT
- DIR

- EXIT
- HELP
- EXPAND
- [command name] /?
- Commands available with standard privileges vs. administrative privileges



## 1.4 Given a scenario, use appropriate Microsoft operating system features and tools.

- **Administrative**
  - Computer management
  - Device manager
  - Local users and groups
  - Local security policy
  - Performance monitor
  - Services
  - System configuration
  - Task scheduler
  - Component services
  - Data sources
  - Print management
  - Windows memory diagnostics
  - Windows firewall
  - Advanced security
- **MSCONFIG**
  - General
  - Boot
  - Services
- Startup
- Tools
- **Task Manager**
  - Applications
  - Processes
  - Performance
  - Networking
  - Users
- **Disk management**
  - Drive status
  - Mounting
  - Initializing
  - Extending partitions
  - Splitting partitions
  - Shrink partitions
  - Assigning/changing drive letters
  - Adding drives
  - Adding arrays
  - Storage spaces
- **Other**
  - User State Migration tool (USMT)
  - Windows Easy Transfer
  - Windows Upgrade Advisor
- **System utilities**
  - REGEDIT
  - COMMAND
  - SERVICES.MSC
  - MMC
  - MSTSC
  - NOTEPAD
  - EXPLORER
  - MSINFO32
  - DXDIAG
  - DEFRAG
  - System restore
  - Windows Update

## 1.5 Given a scenario, use Windows Control Panel utilities.

- **Internet options**
  - Connections
  - Security
  - General
  - Privacy
  - Programs
  - Advanced
- **Display/display settings**
  - Resolution
  - Color depth
  - Refresh rate
- **User accounts**
- **Folder options**
  - View hidden files
- Hide extensions
- General options
- View options
- **System**
  - Performance (virtual memory)
  - Remote settings
  - System protection
- **Windows firewall**
- **Power options**
  - Hibernate
  - Power plans
  - Sleep/suspend
  - Standby
- **Programs and features**
- **HomeGroup**
- **Devices and printers**
- **Sound**
- **Troubleshooting**
- **Network and Sharing Center**
- **Device Manager**



## 1.6 Given a scenario, install and configure Windows networking on a client/desktop.

- HomeGroup vs. WorkGroup
  - Domain setup
  - Network shares/administrative shares/mapping drives
  - Printer sharing vs. network printer mapping
  - Establish networking connections
    - VPN
    - Dial-ups
    - Wireless
    - Wired
    - WWAN (Cellular)
  - Proxy settings
  - Remote Desktop Connection
  - Remote Assistance
  - Home vs. work vs. public network settings
  - Firewall settings
    - Exceptions
    - Configuration
    - Enabling/disabling Windows firewall
  - Configuring an alternative IP address in Windows
    - IP addressing
    - Subnet mask
  - DNS
  - Gateway
  - Network card properties
    - Half duplex/full duplex/auto
    - Speed
    - Wake-on-LAN
    - QoS
    - BIOS (on-board NIC)
- 

## 1.7 Perform common preventive maintenance procedures using the appropriate Windows OS tools.

- Best practices
  - Scheduled backups
  - Scheduled disk maintenance
  - Windows updates
  - Patch management
  - Driver/firmware updates
  - Antivirus/Anti-malware updates
- Tools
  - Backup
  - System restore
  - Recovery image
  - Disk maintenance utilities



## 2.0 Other Operating Systems and Technologies

### 2.1 Identify common features and functionality of the Mac OS and Linux operating systems.

- **Best practices**
  - Scheduled backups
  - Scheduled disk maintenance
  - System updates/App Store
  - Patch management
  - Driver/firmware updates
  - Antivirus/anti-malware updates
- **Tools**
  - Backup/Time Machine
  - Restore/snapshot
  - Image recovery
  - Disk maintenance utilities
  - Shell/Terminal
  - Screen sharing
- **Features**
  - Force Quit
  - Multiple desktops/Mission Control
  - Key Chain
  - Spot Light
  - iCloud
  - Gestures
  - Finder
  - Remote Disc
  - Dock
  - Boot Camp
- **Basic Linux commands**
  - ls
  - grep
  - cd
  - shutdown
  - pwd vs. passwd
  - mv
  - cp
  - rm
  - chmod
  - chown
  - iwconfig/ifconfig
  - ps
  - su/sudo
  - apt-get
  - vi
  - dd

### 2.2 Given a scenario, set up and use client-side virtualization.

- Purpose of virtual machines
- Resource requirements
- Emulator requirements
- Security requirements
- Network requirements
- Hypervisor

### 2.3 Identify basic cloud concepts.

- SaaS
- IaaS
- PaaS
- Public vs. Private vs. Hybrid vs. Community
- Rapid Elasticity
- On-demand
- Resource pooling
- Measured service

### 2.4 Summarize the properties and purpose of services provided by networked hosts.

- **Server roles**
  - Web server
  - File server
  - Print server
  - DHCP server
- **Internet appliance**
  - DNS server
  - Proxy server
  - Mail server
  - Authentication server
- **Legacy/embedded systems**
  - UTM
  - IDS
  - IPS

## 2.5 Identify basic features of mobile operating systems.

- **Android vs. iOS vs. Windows**
    - Open source vs. closed source/vendor specific
    - App source (Google Play Store, App Store, and Store)
  - Screen orientation (accelerometer/gyroscope)
  - Screen calibration
  - GPS and geotracking
  - WiFi calling
  - Launcher/GUI
  - Virtual assistant
  - SDK/APK
  - Emergency notification
  - Mobile payment service
- 

## 2.6 Install and configure basic mobile device network connectivity and email.

- **Wireless/cellular data network (enable/disable)**
    - Hotspot
    - Tethering
    - Airplane mode
  - **Bluetooth**
    - Enable Bluetooth
    - Enable pairing
    - Find device for pairing
  - Enter appropriate pin code
  - Test connectivity
  - **Corporate and ISP email configuration**
    - POP3
    - IMAP
    - Port and SSL settings
    - Exchange, S/MIME
  - **Integrated commercial provider email configuration**
  - Google/Inbox
  - Yahoo
  - Outlook.com
  - iCloud
  - **PRI updates/PRL updates/Baseband updates**
  - **Radio firmware**
  - **IMEI vs. IMSI**
  - **VPN**
- 

## 2.7 Summarize methods and data related to mobile device synchronization.

- **Types of data to synchronize**
  - Contacts
  - Programs
  - Email
  - Pictures
  - Music
  - Videos
  - Calendar
  - Bookmarks
- Documents
- Location data
- Social media data
- eBooks
- **Synchronization methods**
  - Synchronize to the Cloud
  - Synchronize to the Desktop
- **Mutual authentication for multiple services (SSO)**
- **Software requirements to install the application on the PC**
- **Connection types to enable synchronization**



## 3.0 Security

### 3.1 Identify common security threats and vulnerabilities.

- **Malware**
  - Spyware
  - Viruses
  - Worms
  - Trojans
  - Rootkits
  - Ransomware
- **Phishing**
- **Spear phishing**
- **Spoofing**
- **Social engineering**
- **Shoulder surfing**
- **Zero-day attack**
- **Zombie/botnet**
- **Brute forcing**
- **Dictionary attacks**
- **Non-compliant systems**
- **Violations of security best practices**
- **Tailgating**
- **Man-in-the-middle**

### 3.2 Compare and contrast common prevention methods.

- **Physical security**
  - Lock doors
  - Mantrap
  - Cable locks
  - Securing physical documents/ passwords/shredding
  - Biometrics
  - ID badges
  - Key fobs
  - RFID badge
- **Digital security**
  - Smart card
  - Tokens
  - Privacy filters
  - Entry control roster
  - Antivirus/Anti-malware
  - Firewalls
  - User authentication/strong passwords
  - Multifactor authentication
  - Directory permissions
- **User education/AUP**
- **Principle of least privilege**
- VPN
- DLP
- Disabling ports
- Access control lists
- Smart card
- Email filtering
- Trusted/untrusted software sources

### 3.3 Compare and contrast differences of basic Windows OS security settings.

- **User and groups**
  - Administrator
  - Power user
  - Guest
  - Standard user
- **NTFS vs. Share permissions**
  - Allow vs. deny
- **Moving vs. copying folders and files**
- **File attributes**
- **Shared files and folders**
  - Administrative shares vs. local shares
  - Permission propagation
  - Inheritance
- **System files and folders**
- **User authentication**
  - Single sign-on
- **Run as administrator vs. standard user**
- **BitLocker**
- **BitLocker-To-Go**
- **EFS**

### 3.4 Given a scenario, deploy and enforce security best practices to secure a workstation.

- **Password best practices**
    - Setting strong passwords
    - Password expiration
    - Changing default user names/passwords
    - Screensaver required password
  - BIOS/UEFI passwords
  - Requiring passwords
  - **Account management**
    - Restricting user permissions
    - Login time restrictions
    - Disabling guest account
  - Failed attempts lockout
  - Timeout/screen lock
  - **Disable autorun**
  - **Data encryption**
  - **Patch/update management**
- 

### 3.5 Compare and contrast various methods for securing mobile devices.

- **Screen locks**
    - Fingerprint lock
    - Face lock
    - Swipe lock
    - Passcode lock
  - **Remote wipes**
  - **Locator applications**
  - **Remote backup applications**
  - **Failed login attempt restrictions**
  - **Antivirus/anti-malware**
  - **Patching/OS updates**
  - **Biometric authentication**
  - **Full device encryption**
  - **Multifactor authentication**
  - **Authenticator applications**
  - **Trusted sources vs. untrusted sources**
  - **Firewalls**
  - **Policies and procedures**
    - BYOD vs. corporate owned
    - Profile security requirements
- 

### 3.6 Given a scenario, use appropriate data destruction and disposal methods.

- **Physical destruction**
    - Shredder
    - Drill/hammer
    - Electromagnetic (Degaussing)
    - Incineration
    - Certificate of destruction
  - **Recycling or repurposing best practices**
    - Low level format vs. standard format
    - Overwrite
    - Drive wipe
- 

### 3.7 Given a scenario, secure SOHO wireless and wired networks.

- **Wireless specific**
  - Changing default SSID
  - Setting encryption
  - Disabling SSID broadcast
  - Antenna and access point placement
  - Radio power levels
  - WPS
- **Change default usernames and passwords**
- **Enable MAC filtering**
- **Assign static IP addresses**
- **Firewall settings**
- **Port forwarding/mapping**
- **Disabling ports**
- **Content filtering/parental controls**
- **Update firmware**
- **Physical security**



## 4.0 Software Troubleshooting

### 4.1 Given a scenario, troubleshoot PC operating system problems with appropriate tools.

#### • Common symptoms

- Proprietary crash screens (BSOD/pinwheel)
- Failure to boot
- Improper shutdown
- Spontaneous shutdown/restart
- Device fails to start/detected
- Missing DLL message
- Services fails to start
- Compatibility error
- Slow system performance
- Boots to safe mode
- File fails to open

- Missing NTLDR
- Missing boot configuration data
- Missing operating system
- Missing graphical interface
- Missing GRUB/LILO
- Kernel panic
- Graphical Interface fails to load
- Multiple monitor misalignment/orientation

#### • Tools

- BIOS/UEFI
- SFC
- Logs

- System Recovery Options
- Repair disks
- Pre-installation environments
- MSCONFIG
- DEFRAG
- REGSRV32
- REGEDIT
- Event viewer
- Safe mode
- Command prompt
- Uninstall/reinstall/repair

### 4.2 Given a scenario, troubleshoot common PC security issues with appropriate tools and best practices.

#### • Common symptoms

- Pop-ups
- Browser redirection
- Security alerts
- Slow performance
- Internet connectivity issues
- PC/OS lock up
- Application crash
- OS updates failures
- Rogue antivirus
- Spam
- Renamed system files
- Files disappearing
- File permission changes
- Hijacked email
  - Responses from users regarding email
  - Automated replies from unknown sent email
- Access denied
- Invalid certificate (trusted root CA)

#### • Tools

- Antivirus software
- Anti-malware software
- Recovery console
- Terminal
- System restore/Snapshot
- Pre-installation environments
- Event viewer
- Refresh/restore
- MSCONFIG/Safe boot

#### • Best practice procedure for malware removal

1. Identify malware symptoms
2. Quarantine infected system
3. Disable system restore (in Windows)
4. Remediate infected systems
  - a. Update anti-malware software
  - b. Scan and removal techniques (safe mode, pre-installation environment)
5. Schedule scans and run updates
6. Enable system restore and create restore point (in Windows)
7. Educate end user



### 4.3 Given a scenario, troubleshoot common mobile OS and application issues with appropriate tools.

- **Common symptoms**
    - Dim display
    - Intermittent wireless
    - No wireless connectivity
    - No Bluetooth connectivity
    - Cannot broadcast to external monitor
    - Touchscreen non-responsive
    - Apps not loading
    - Slow performance
    - Unable to decrypt email
  - Extremely short battery life
  - Overheating
  - Frozen system
  - No sound from speakers
  - Inaccurate touch screen response
  - System lockout
  - **Tools**
    - Hard reset
    - Soft reset
    - Close running applications
  - Reset to factory default
  - Adjust configurations/settings
  - Uninstall/reinstall apps
  - Force stop
- 

### 4.4 Given a scenario, troubleshoot common mobile OS and application security issues with appropriate tools.

- **Common symptoms**
  - Signal drop/weak signal
  - Power drain
  - Slow data speeds
  - Unintended WiFi connection
  - Unintended Bluetooth pairing
  - Leaked personal files/data
  - Data transmission overlimit
  - Unauthorized account access
  - Unauthorized root access
- Unauthorized location tracking
- Unauthorized camera/microphone activation
- High resource utilization
- **Tools**
  - Anti-malware
  - App scanner
  - Factory reset/clean install
  - Uninstall/reinstall apps
  - WiFi analyzer
- Force stop
- Cell tower analyzer
- Backup/restore
  - iTunes/iCloud/Apple Configurator
  - Google Sync
  - One Drive



## 5.0 Operational Procedures

### 5.1 Given a scenario, use appropriate safety procedures.

- **Equipment grounding**
- **Proper component handling and storage**
  - Antistatic bags
  - ESD straps
  - ESD mats
  - Self-grounding
- **Toxic waste handling**
  - Batteries
  - Toner
  - CRT
- **Personal safety**
  - Disconnect power before repairing PC
  - Remove jewelry
  - Lifting techniques
  - Weight limitations
  - Electrical fire safety
  - Cable management
  - Safety goggles
  - Air filter mask
- **Compliance with local government regulations**

### 5.2 Given a scenario with potential environmental impacts, apply the appropriate controls.

- **MSDS documentation for handling and disposal**
- **Temperature, humidity level awareness and proper ventilation**
- **Power surges, brownouts, blackouts**
  - Battery backup
  - Surge suppressor
- **Protection from airborne particles**
  - Enclosures
  - Air filters/mask
- **Dust and debris**
  - Compressed air
  - Vacuums
- **Compliance to local government regulations**

### 5.3 Summarize the process of addressing prohibited content/activity, and explain privacy, licensing and policy concepts.

- **Incident Response**
  - First response
    - Identify
    - Report through proper channels
    - Data/device preservation
  - Use of documentation/documentation changes
  - Chain of custody
    - Tracking of evidence/documenting process
- **Licensing/DRM/EULA**
  - Open source vs. commercial license
  - Personal license vs. enterprise licenses
- **Personally Identifiable Information**
- **Follow corporate end-user policies and security best practices**

**5.4 Demonstrate proper communication techniques and professionalism.**

- **Use proper language – avoid jargon, acronyms and slang when applicable**
- **Maintain a positive attitude/project confidence**
- **Actively listen (taking 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
  - Talking to co-workers while interacting with customers
  - Personal interruptions
- **Dealing with difficult customer or situation**
  - Do not argue with customers and/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 experiences via social media outlets
- **Set and meet expectations/timeline and communicate status with the customer**
  - Offer different repair/replacement options if applicable
- 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

**5.5 Given a scenario, explain the troubleshooting theory.**

- **Always consider corporate policies, procedures and impacts before implementing changes.**
  1. Identify the problem
    - Question the user and identify user changes to computer and perform backups before making 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 cause
    - Once theory is confirmed, determine next steps to resolve problem
    - If theory is not confirmed, re-establish new theory or escalate
  4. Establish a plan of action to resolve the problem and implement the solution
  5. Verify full system functionality and if applicable implement preventive measures
  6. Document findings, actions and outcomes

# CompTIA A+ Acronyms

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

<b>ACRONYM</b>	<b>SPELLED OUT</b>	<b>ACRONYM</b>	<b>SPELLED OUT</b>
AC	Alternating Current	CPU	Central Processing Unit
ACL	Access Control List	CRT	Cathode Ray Tube
ACPI	Advanced Configuration Power Interface	DAC	Discretionary Access Control
ACT	Activity	DB-25	Serial Communications D-Shell Connector, 25 Pins
ADSL	Asymmetrical Digital Subscriber Line	DB-9	9 Pin D Shell Connector
AGP	Accelerated Graphics Port	DC	Direct Current
AHCI	Advanced Host Controller Interface	DDoS	Distributed Denial of Service
AP	Access Point	DDR	Double Data Rate
APIPA	Automatic Private Internet Protocol Addressing	DDR RAM	Double Data Rate Random-Access Memory
APM	Advanced Power Management	DDR SDRAM	Double Data Rate Synchronous Dynamic Random-Access Memory
ARP	Address Resolution Protocol	DFS	Distributed File System
ASR	Automated System Recovery	DHCP	Dynamic Host Configuration Protocol
ATA	Advanced Technology Attachment	DIMM	Dual Inline Memory Module
ATAPI	Advanced Technology Attachment Packet Interface	DIN	Deutsche Industrie Norm
ATM	Asynchronous Transfer Mode	DLT	Digital Linear Tape
ATX	Advanced Technology Extended	DLP	Digital Light Processing
AUP	Acceptable Use Policy	DMA	Direct Memory Access
A/V	Audio Video	DMZ	Demilitarized Zone
BIOS	Basic Input/Output System	DNS	Domain Name Service or Domain Name Server
BNC	Bayonet-Neill-Concelman or British Naval Connector	DoS	Denial of Service
BTX	Balanced Technology Extended	DRAM	Dynamic Random-Access Memory
CAPTCHA	Completely Automated Public Turing Test to tell Computers and Humans Apart	DRM	Digital Rights Management
CCFL	Cold Cathode Fluorescent Lamp	DSL	Digital Subscriber Line
CD	Compact Disc	DVD	Digital Video Disc or Digital Versatile Disc
CD-ROM	Compact Disc-Read-Only Memory	DVD-RAM	Digital Video Disc-Random-Access Memory
CD-RW	Compact Disc-Rewritable	DVD-ROM	Digital Video Disc-Read-Only Memory
CDFS	Compact Disc File System	DVD-R	Digital Video Disc-Recordable
CFS	Central File System or Common File System or Command File System	DVD-RW	Digital Video Disc-Rewritable
CIFS	Common Internet File System	DVI	Digital Visual Interface
CMOS	Complementary Metal-Oxide Semiconductor	ECC	Error Correcting Code or Error Checking and Correction
CNR	Communications and Networking Riser	ECP	Extended Capabilities Port
COMx	Communication Port (x=Port Number)	EEPROM	Electrically Erasable Programmable Read-Only Memory

<b>ACRONYM</b>	<b>SPELLED OUT</b>	<b>ACRONYM</b>	<b>SPELLED OUT</b>
EFS	Encrypting File System	IIS	Internet Information Services
EIDE	Enhanced Integrated Drive Electronics	IMAP	Internet Mail Access Protocol
EMI	Electromagnetic Interference	IMEI	International Mobile Equipment Identity
EMP	Electromagnetic Pulse	IMSI	International Mobile Subscriber Identity
EPROM	Erasable Programmable Read-Only Memory	IP	Internet Protocol
EPP	Enhanced Parallel Port	IPCONFIG	Internet Protocol Configuration
ERD	Emergency Repair Disk	IPP	Internet Printing Protocol
ESD	Electrostatic Discharge	IPS	In-Plane Switching
EULA	End-User License Agreement	IPSec	Internet Protocol Security
EVGA	Extended Video Graphics Adapter/Array	IR	Infrared
EVDO	Evolution Data Optimized or Evolution Data Only	IrDA	Infrared Data Association
FAT	File Allocation Table	IRP	Incident Response Plan
FAT12	12-Bit File Allocation Table	IRQ	Interrupt Request
FAT16	16-Bit File Allocation Table	ISDN	Integrated Services Digital Network
FAT32	32-Bit File Allocation Table	ISO	International Organization for Standardization or Industry Standards Organization
FDD	Floppy Disk Drive	ISP	Internet Service Provider
Fn	Function (referring to the function key on a laptop)	JBOD	Just a Bunch of Disks
FPM	Fast Page Mode	Kb	Kilobit
FRU	Field Replaceable Unit	KB	Kilobyte or Knowledge Base
FSB	Front Side Bus	LAN	Local Area Network
FTP	File Transfer Protocol	LBA	Logical Block Addressing
FQDN	Fully Qualified Domain Name	LC	Lucent Connector
Gb	Gigabit	LCD	Liquid Crystal Display
GB	Gigabyte	LDAP	Lightweight Directory Access Protocol
GDI	Graphics Device Interface	LED	Light Emitting Diode
GHz	Gigahertz	LI-ON	Lithium-Ion
GUI	Graphical User Interface	LPD/LPR	Line Printer Daemon/Line Printer Remote
GPS	Global Positioning System	LPT	Line Printer Terminal
GSM	Global System for Mobile communications	LVD	Low Voltage Differential
HAL	Hardware Abstraction Layer	MAC	Media Access Control/Mandatory Access Control
HAV	Hardware-Assisted Virtualization	MAPI	Messaging Application Programming Interface
HCL	Hardware Compatibility List	MAU	Media Access Unit or Media Attachment Unit
HDD	Hard Disk Drive	Mb	Megabit
HDMI	High-Definition Media Interface	MB	Megabyte
HPFS	High-Performance File System	MBR	Master Boot Record
HTML	Hypertext Markup Language	MBSA	Microsoft Baseline Security Analyzer
HTPC	Home Theater PC	MFD	Multi-Function Device
HTTP	Hypertext Transfer Protocol	MFP	Multi-Function Product
HTTPS	Hypertext Transfer Protocol Over Secure Sockets Layer	MHz	Megahertz
I/O	Input/Output	MicroDIMM	Micro Dual Inline Memory Module
ICMP	Internet Control Message Protocol	MIDI	Musical Instrument Digital Interface
ICR	Intelligent Character Recognition	MIME	Multipurpose Internet Mail Extension
IDE	Integrated Drive Electronics	MIMO	Multiple Input, Multiple Output
IDS	Intrusion Detection System	MMC	Microsoft Management Console
IEEE	Institute of Electrical and Electronics Engineers	MP3	Moving Picture Experts Group Layer 3 Audio

<b>ACRONYM</b>	<b>SPELLED OUT</b>	<b>ACRONYM</b>	<b>SPELLED OUT</b>
MP4	Moving Picture Experts Group Layer 4	PRI	Preferred Roaming Index
MPEG	Moving Picture Experts Group	PRL	Preferred Roaming List
MSCONFIG	Microsoft Configuration	PROM	Programmable Read-Only Memory
MSDS	Material Safety Data Sheet	PS/2	Personal System/2
MUI	Multilingual User Interface	PSTN	Public Switched Telephone Network
NAC	Network Access Control	PSU	Power Supply Unit
NAS	Network Attached Storage	PVC	Permanent Virtual Circuit
NAT	Network Address Translation	PXE	Preboot Execution Environment
NETBIOS	Networked Basic Input/Output System	QoS	Quality of Service
NETBEUI	Networked Basic Input/Output System Extended User Interface	RAID	Redundant Array of Independent (or Inexpensive) Discs
NFS	Network File System	RAM	Random-Access Memory
NIC	Network Interface Card	RAS	Remote Access Service
NiCd	Nickel Cadmium	RDP	Remote Desktop Protocol
NiMH	Nickel Metal Hydride	RF	Radio Frequency
NLX	New Low Profile Extended	RFI	Radio Frequency Interference
NNTP	Network News Transfer Protocol	RGB	Red Green Blue
NTFS	New Technology File System	RIP	Routing Information Protocol
NTLDR	New Technology Loader	RIS	Remote Installation Service
NTP	Network Time Protocol	RISC	Reduced Instruction Set Computer
OCR	Optical Character Recognition	RJ-11	Registered Jack Function 11
OEM	Original Equipment Manufacturer	RJ-45	Registered Jack Function 45
OLED	Organic Light Emitting Diode	RMA	Returned Materials Authorization
OS	Operating System	ROM	Read-Only Memory
PAN	Personal Area Network	RTC	Real-Time Clock
PATA	Parallel Advanced Technology Attachment	SAN	Storage Area Network
PC	Personal Computer	SAS	Serial Attached SCSI
PCI	Peripheral Component Interconnect	SATA	Serial Advanced Technology Attachment
PCIe	Peripheral Component Interconnect express	SC	Subscription Channel
PCIX	Peripheral Component Interconnect Extended	SCP	Secure Copy Protection
PCL	Printer Control Language	SCSI	Small Computer System Interface
PCMCIA	Personal Computer Memory Card International Association	SCSI ID	Small Computer System Interface Identifier
PE	Preinstallation Environment	SD card	Secure Digital card
PGA	Pin Grid Array	SDRAM	Synchronous Dynamic Random Access Memory
PGA2	Pin Grid Array 2	SEC	Single Edge Connector
PII	Personally Identifiable Information	SFC	System File Checker
PIN	Personal Identification Number	SFF	Small Form Factor
PKI	Public Key Infrastructure	SLI	Scalable Link Interface or System Level Integration or Scanline Interleave mode
PnP	Plug and Play	S.M.A.R.T.	Self-Monitoring, Analysis, And Reporting Technology
POP3	Post Office Protocol 3	SMB	Server Message Block or Small-to-Midsize Business
PoS	Point of Sale	SMTP	Simple Mail Transfer Protocol
POST	Power-On Self Test	SNMP	Simple Network Management Protocol
POTS	Plain Old Telephone Service	SODIMM	Small Outline Dual Inline Memory Module
PPP	Point-to-Point Protocol	SOHO	Small Office, Home Office
PPTP	Point-to-Point Tunneling Protocol	SP	Service Pack

<b>ACRONYM</b>	<b>SPELLED OUT</b>
SPDIF	Sony-Philips Digital Interface Format
SPGA	Staggered Pin Grid Array
SRAM	Static Random Access Memory
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
ST	Straight Tip
STP	Shielded Twisted Pair
SXGA	Super Extended Graphics Array
TB	Terabyte
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDR	Time Domain Reflectometer
TFTP	Trivial File Transfer Protocol
TKIP	Temporal Key Integrity Protocol
TPM	Trusted Platform Module
UAC	User Account Control
UDF	User Defined Functions or Universal Disk Format or Universal Data Format
UDP	User Datagram Protocol
UEFI	Unified Extensible Firmware Interface
UNC	Universal Naming Convention
UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator

<b>ACRONYM</b>	<b>SPELLED OUT</b>
USB	Universal Serial Bus
USMT	User State Migration Tool
UTP	Unshielded Twisted Pair
UXGA	Ultra Extended Graphics Array
VESA	Video Electronics Standards Association
VFAT	Virtual File Allocation Table
VGA	Video Graphics Array
VM	Virtual Machine
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
VRAM	Video Random Access Memory
WAN	Wide Area Network
WAP	Wireless Access Protocol/Wireless Access Point
WEP	Wired Equivalent Privacy
WiFi	Wireless Fidelity
WINS	Windows Internet Name Service
WLAN	Wireless Local Area Network
WPA	Wireless Protected Access
WPS	WiFi Protected Setup
WUXGA	Wide Ultra Extended Graphics Array
XGA	Extended Graphics Array
ZIF	Zero-Insertion-Force
ZIP	Zigzag Inline Package

# A+ Proposed Hardware and Software List

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

## EQUIPMENT

- Apple tablet/smartphone
- Android tablet/smartphone
- Windows tablet/smartphone
- Windowslaptop/Mac laptop/Linux laptop
- Windows desktop/Mac desktop/Linux desktop
- Monitors
- Projectors
- SOHO router/switch
- Access point
- VoIP phone
- Printer
  - Laser/inkjet
  - Wireless
- Surge suppressor
- UPS

## SPARE PARTS/HARDWARE

- Motherboards
- RAM
- Hard drives
- Power supplies
- Video cards
- Sounds cards
- Network cards
- Wireless NICs
- Fans/cooling devices/heat sink
- CPUs
- Assorted connectors/cables
  - USB
  - HDMI
  - etc

- Adapters
- Network cables
- Unterminated network cable/connectors
- AC adapters
- Optical drives
- Screws/stand-offs
- Cases
- Maintenance kit
- Mice/keyboards

## TOOLS

- Screw drivers
- Multimeter
- Wire cutters
- Punchdown tool
- Crimper
- Power supply tester
- Cable stripper
- POST cards
- Standard technician toolkit
- ESD strap
- Thermal paste
- Cable tester
- WiFi analyzer
- SATA to USB connectors

## SOFTWARE

- Operating system disks
- Antivirus software
- Virtualization software
- Anti-malware
- Driver software