Introduction
In order to receive CompTIA A+ certification a candidate must pass two exams. The first exam is the CompTIA A+ 220-902 Certification Exam. The CompTIA A+ 220-902 Certification Exam is the second exam required in order for CompTIA A+ certification candidates to complete their certification.

The CompTIA A+ 220-902 examination measures necessary competencies for an entry-level IT professional with the equivalent knowledge of at least 12 months of hands-on experience in the lab or field.

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.

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. The following CompTIA A+ 220-902 certification exam objectives result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an entry-level IT professional. The percentages in this document represent the relative importance of the subject areas (domains) in the associated body of knowledge, and together establish the foundation of an entry-level IT professional.

This examination blueprint includes domain weighting, test objectives, and example content. Example topics and concepts are included to clarify the test objectives and should not be construed as a comprehensive listing of all the content of this examination.

Candidates are encouraged to use this document to guide their studies. The table below lists the domains measured by this examination and the extent to which they are represented. The CompTIA A+ 220-902 certification exam is based on these objectives.

<table>
<thead>
<tr>
<th>Domain</th>
<th>Percentage of Examination</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0 Windows Operating Systems</td>
<td>29%</td>
</tr>
<tr>
<td>2.0 Other Operating Systems &amp; Technologies</td>
<td>12%</td>
</tr>
<tr>
<td>3.0 Security</td>
<td>22%</td>
</tr>
<tr>
<td>4.0 Software Troubleshooting</td>
<td>24%</td>
</tr>
<tr>
<td>5.0 Operational Procedures</td>
<td>13%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>
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 webpage:

http://certification.comptia.org/Training/testingcenters/policies.aspx

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 (http://certification.comptia.org/Training/testingcenters/policies/agreement.aspx) at the time of exam delivery.

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: http://www.certguard.com/search.asp

**Note: The lists of examples provided in bulleted format below each objective 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.
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, bit-locker, 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, Power Shell, 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
  o Computer management
  o Device manager
  o Local Users and Groups
  o Local security policy
  o Performance monitor
  o Services
  o System configuration
  o Task scheduler
  o Component services
  o Data sources
  o Print management
  o Windows memory diagnostics
  o Windows firewall
  o Advanced security
• MSCONFIG
  o General
  o 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
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
  - Dialups
  - 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/ Antimalware 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/ Antimalware updates

- Tools
  - Backup/Time Machine
  - Restore/snapshot
  - Image recovery
  - Disk maintenance utilities
  - Shell/Terminal
  - Screen sharing
  - Force Quit

- Features
  - 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
2.2 Given a scenario, setup 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
  - DNS server
  - Proxy server
  - Mail server
  - Authentication server
- Internet appliance
  - UTM
  - IDS
  - IPS
- Legacy / embedded systems

2.5 Identify basic features of mobile operating systems.
- Android vs. iOS vs. Windows
  - Open source vs. closed source/vendor specific
  - App source (play store, app store and store)
  - Screen orientation (accelerometer/gyroscope)
  - Screen calibration
  - GPS and geotagging
  - WiFi calling
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
     o Spyware
     o Viruses
     o Worms
     o Trojans
     o Rootkits
     o 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
     o Lock doors
     o Mantrap
     o Cable locks
     o Securing physical documents/passwords/shredding
     o Biometrics
     o ID badges
     o Key fobs
     o RFID badge
     o Smart card
     o Tokens
     o Privacy filters
     o Entry control roster
   • Digital security
     o Antivirus/Antimalware
     o Firewalls
     o User authentication/strong passwords
     o Multifactor authentication
     o Directory permissions
     o VPN
     o DLP
     o Disabling ports
     o Access control lists
     o Smart card
     o Email filtering
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 attempts restrictions
- Antivirus/Antimalware
- 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 user-names 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/pin wheel)
  - 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 NTLD
- 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
- DEFRA
- 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
  o Antivirus software
  o Antimalware software
  o Recovery console
  o Terminal
  o System restore/Snapshot
  o Pre-installation environments
  o Event viewer
  o Refresh/restore
  o 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 antimalware 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
  o Dim display
  o Intermittent wireless
  o No wireless connectivity
  o No bluetooth connectivity
  o Cannot broadcast to external monitor
  o Touchscreen non-responsive
  o Apps not loading
  o Slow performance
  o Unable to decrypt email
  o Extremely short battery life
  o Overheating
  o Frozen system
  o No sound from speakers
  o Inaccurate touch screen response
  o System lockout

• Tools
  o Hard reset
  o Soft reset
  o Close running applications
  o Reset to factory default
  o Adjust configurations/settings
  o Uninstall/reinstall apps
  o Force stop

4.4 Given a scenario, troubleshoot common mobile OS and application security issues with appropriate tools.
• Common symptoms
  o Signal drop/weak signal
  o 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
• Antimalware
• 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
o Surge suppressor

- Protection from airborne particles
  o Enclosures
  o Air filters/Mask

- Dust and debris
  o Compressed air
  o 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
  o First response
    - Identify
    - Report through proper channels
    - Data/device preservation
  o Use of documentation/documentation changes
  o Chain of custody
    - Tracking of evidence/documenting process

- Licensing / DRM / EULA
  o Open source vs. commercial license
  o 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, slang when applicable
- Maintain a positive attitude / Project confidence
- Actively listen (taking notes) and avoid interrupting the customer
- Be culturally sensitive
  o Use appropriate professional titles, when applicable
- Be on time (if late contact the customer)
- Avoid distractions
  o Personal calls
  o Texting / Social media sites
  o Talking to co-workers while interacting with customers
  o Personal interruptions
- Dealing with difficult customer or situation
  o Do not argue with customers and/or be defensive
  o Avoid dismissing customer problems
  o Avoid being judgmental
  o Clarify customer statements (ask open ended questions to narrow the scope of the problem, restate the issue or question to verify understanding)
  o Do not disclose experiences via social media outlets
- Set and meet expectations/timeline and communicate status with the customer
  o Offer different repair/replacement options if applicable
  o Provide proper documentation on the services provided
  o Follow up with customer/user at a later date to verify satisfaction
- Deal appropriately with customers confidential and private materials
  o 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**
Introduction
The following is a list of acronyms which 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.

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC</td>
<td>alternating current</td>
</tr>
<tr>
<td>ACL</td>
<td>access control list</td>
</tr>
<tr>
<td>ACPI</td>
<td>advanced configuration power interface</td>
</tr>
<tr>
<td>ACT</td>
<td>activity</td>
</tr>
<tr>
<td>ADSL</td>
<td>asymmetrical digital subscriber line</td>
</tr>
<tr>
<td>AGP</td>
<td>accelerated graphics port</td>
</tr>
<tr>
<td>AHCI</td>
<td>Advanced host controller interface</td>
</tr>
<tr>
<td>AP</td>
<td>Access point</td>
</tr>
<tr>
<td>APIPA</td>
<td>automatic private internet protocol addressing</td>
</tr>
<tr>
<td>APM</td>
<td>advanced power management</td>
</tr>
<tr>
<td>ARP</td>
<td>address resolution protocol</td>
</tr>
<tr>
<td>ASR</td>
<td>automated system recovery</td>
</tr>
<tr>
<td>ATA</td>
<td>advanced technology attachment</td>
</tr>
<tr>
<td>ATAPI</td>
<td>advanced technology attachment packet interface</td>
</tr>
<tr>
<td>ATM</td>
<td>asynchronous transfer mode</td>
</tr>
<tr>
<td>ATX</td>
<td>advanced technology extended</td>
</tr>
<tr>
<td>AUP</td>
<td>Acceptable Use Policy</td>
</tr>
<tr>
<td>A/V</td>
<td>Audio Video</td>
</tr>
<tr>
<td>BIOS</td>
<td>basic input/output system</td>
</tr>
<tr>
<td>BNC</td>
<td>Bayonet-Neill-Concelman or British Naval Connector</td>
</tr>
<tr>
<td>BTX</td>
<td>balanced technology extended</td>
</tr>
<tr>
<td>CAPTCHA</td>
<td>Completely Automated Public Turing Test To Tell Computers and Humans Apart</td>
</tr>
<tr>
<td>CCFL</td>
<td>Cold Cathode Fluorescent Lamp</td>
</tr>
<tr>
<td>CD</td>
<td>compact disc</td>
</tr>
<tr>
<td>CD-ROM</td>
<td>compact disc-read-only memory</td>
</tr>
<tr>
<td>CD-RW</td>
<td>compact disc-rewritable</td>
</tr>
<tr>
<td>CDFS</td>
<td>compact disc file system</td>
</tr>
<tr>
<td>CFS</td>
<td>Central File System, Common File System, Command File System</td>
</tr>
<tr>
<td>CIFS</td>
<td>Common Internet File System</td>
</tr>
<tr>
<td>CMOS</td>
<td>complementary metal-oxide semiconductor</td>
</tr>
<tr>
<td>CNR</td>
<td>Communications and Networking Riser</td>
</tr>
<tr>
<td>COMx</td>
<td>communication port (x=port number)</td>
</tr>
<tr>
<td>CPU</td>
<td>central processing unit</td>
</tr>
<tr>
<td>CRT</td>
<td>cathode-ray tube</td>
</tr>
<tr>
<td>DAC</td>
<td>discretionary access control</td>
</tr>
<tr>
<td>DB-25</td>
<td>serial communications D-shell connector, 25 pins</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>DB-9</td>
<td>9 pin D shell connector</td>
</tr>
<tr>
<td>DC</td>
<td>direct current</td>
</tr>
<tr>
<td>DDOS</td>
<td>distributed denial of service</td>
</tr>
<tr>
<td>DDR</td>
<td>double data-rate</td>
</tr>
<tr>
<td>DDR RAM</td>
<td>double data-rate random access memory</td>
</tr>
<tr>
<td>DDR</td>
<td>double data-rate synchronous dynamic random access memory</td>
</tr>
<tr>
<td>DFS</td>
<td>distributed file system</td>
</tr>
<tr>
<td>DHCP</td>
<td>dynamic host configuration protocol</td>
</tr>
<tr>
<td>DIMM</td>
<td>dual inline memory module</td>
</tr>
<tr>
<td>DIN</td>
<td>Deutsche Industrie Norm</td>
</tr>
<tr>
<td>DLT</td>
<td>digital linear tape</td>
</tr>
<tr>
<td>DLP</td>
<td>digital light processing</td>
</tr>
<tr>
<td>DMA</td>
<td>direct memory access</td>
</tr>
<tr>
<td>DMZ</td>
<td>demilitarized zone</td>
</tr>
<tr>
<td>DNS</td>
<td>domain name service or domain name server</td>
</tr>
<tr>
<td>DOS</td>
<td>denial of service</td>
</tr>
<tr>
<td>DRAM</td>
<td>dynamic random access memory</td>
</tr>
<tr>
<td>DSL</td>
<td>digital subscriber line</td>
</tr>
<tr>
<td>DVD</td>
<td>digital video disc or digital versatile disc</td>
</tr>
<tr>
<td>DVD-RAM</td>
<td>digital video disc-random access memory</td>
</tr>
<tr>
<td>DVD-ROM</td>
<td>digital video disc-read only memory</td>
</tr>
<tr>
<td>DVD-R</td>
<td>digital video disc-recordable</td>
</tr>
<tr>
<td>DVD-RW</td>
<td>digital video disc-re-writable</td>
</tr>
<tr>
<td>DVI</td>
<td>digital visual interface</td>
</tr>
<tr>
<td>ECC</td>
<td>error correcting code/error checking and correction</td>
</tr>
<tr>
<td>ECP</td>
<td>extended capabilities port</td>
</tr>
<tr>
<td>EEPROM</td>
<td>electrically erasable programmable read-only memory</td>
</tr>
<tr>
<td>EFS</td>
<td>encrypting file system</td>
</tr>
<tr>
<td>EIDE</td>
<td>enhanced integrated drive electronics</td>
</tr>
<tr>
<td>EMI</td>
<td>electromagnetic interference</td>
</tr>
<tr>
<td>EMP</td>
<td>electromagnetic pulse</td>
</tr>
<tr>
<td>EPROM</td>
<td>erasable programmable read-only memory</td>
</tr>
<tr>
<td>EPP</td>
<td>enhanced parallel port</td>
</tr>
<tr>
<td>ERD</td>
<td>emergency repair disk</td>
</tr>
<tr>
<td>ESD</td>
<td>electrostatic discharge</td>
</tr>
<tr>
<td>EVGA</td>
<td>extended video graphics adapter/array</td>
</tr>
<tr>
<td>EVDO</td>
<td>evolution data optimized or evolution data only</td>
</tr>
<tr>
<td>FAT</td>
<td>file allocation table</td>
</tr>
<tr>
<td>FAT12</td>
<td>12-bit file allocation table</td>
</tr>
<tr>
<td>FAT16</td>
<td>16-bit file allocation table</td>
</tr>
<tr>
<td>FAT32</td>
<td>32-bit file allocation table</td>
</tr>
<tr>
<td>FDD</td>
<td>floppy disk drive</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Fn</td>
<td>Function (referring to the function key on a laptop)</td>
</tr>
<tr>
<td>FPM</td>
<td>fast page-mode</td>
</tr>
<tr>
<td>FRU</td>
<td>field replaceable unit</td>
</tr>
<tr>
<td>FSB</td>
<td>Front Side Bus</td>
</tr>
<tr>
<td>FTP</td>
<td>file transfer protocol</td>
</tr>
<tr>
<td>FQDN</td>
<td>fully qualified domain name</td>
</tr>
<tr>
<td>Gb</td>
<td>gigabit</td>
</tr>
<tr>
<td>GB</td>
<td>gigabyte</td>
</tr>
<tr>
<td>GDI</td>
<td>graphics device interface</td>
</tr>
<tr>
<td>GHz</td>
<td>gigahertz</td>
</tr>
<tr>
<td>GUI</td>
<td>graphical user interface</td>
</tr>
<tr>
<td>GPS</td>
<td>global positioning system</td>
</tr>
<tr>
<td>GSM</td>
<td>global system for mobile communications</td>
</tr>
<tr>
<td>HAL</td>
<td>hardware abstraction layer</td>
</tr>
<tr>
<td>HAV</td>
<td>Hardware Assisted Virtualization</td>
</tr>
<tr>
<td>HCL</td>
<td>hardware compatibility list</td>
</tr>
<tr>
<td>HDD</td>
<td>hard disk drive</td>
</tr>
<tr>
<td>HDMI</td>
<td>high definition media interface</td>
</tr>
<tr>
<td>HPFS</td>
<td>high performance file system</td>
</tr>
<tr>
<td>HTML</td>
<td>hypertext markup language</td>
</tr>
<tr>
<td>HTPC</td>
<td>home theater PC</td>
</tr>
<tr>
<td>HTTP</td>
<td>hypertext transfer protocol</td>
</tr>
<tr>
<td>HTTPS</td>
<td>hypertext transfer protocol over secure sockets layer</td>
</tr>
<tr>
<td>I/O</td>
<td>input/output</td>
</tr>
<tr>
<td>ICMP</td>
<td>internet control message protocol</td>
</tr>
<tr>
<td>ICR</td>
<td>intelligent character recognition</td>
</tr>
<tr>
<td>IDE</td>
<td>integrated drive electronics</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IIS</td>
<td>Internet Information Services</td>
</tr>
<tr>
<td>IMAP</td>
<td>internet mail access protocol</td>
</tr>
<tr>
<td>IP</td>
<td>internet protocol</td>
</tr>
<tr>
<td>IPCONFIG</td>
<td>internet protocol configuration</td>
</tr>
<tr>
<td>IPP</td>
<td>internet printing protocol</td>
</tr>
<tr>
<td>IPSEC</td>
<td>internet protocol security</td>
</tr>
<tr>
<td>IR</td>
<td>infrared</td>
</tr>
<tr>
<td>IrDA</td>
<td>Infrared Data Association</td>
</tr>
<tr>
<td>IRQ</td>
<td>interrupt request</td>
</tr>
<tr>
<td>ISDN</td>
<td>integrated services digital network</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization/Industry Standards Organization</td>
</tr>
<tr>
<td>ISP</td>
<td>internet service provider</td>
</tr>
<tr>
<td>JBOD</td>
<td>just a bunch of disks</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Kb</td>
<td>kilobit</td>
</tr>
<tr>
<td>KB</td>
<td>Kilobyte or knowledge base</td>
</tr>
<tr>
<td>LAN</td>
<td>local area network</td>
</tr>
<tr>
<td>LBA</td>
<td>logical block addressing</td>
</tr>
<tr>
<td>LC</td>
<td>Lucent connector</td>
</tr>
<tr>
<td>LCD</td>
<td>liquid crystal display</td>
</tr>
<tr>
<td>LDAP</td>
<td>lightweight directory access protocol</td>
</tr>
<tr>
<td>LED</td>
<td>light emitting diode</td>
</tr>
<tr>
<td>Li-on</td>
<td>lithium-ion</td>
</tr>
<tr>
<td>LPD/LPR</td>
<td>line printer daemon / line printer remote</td>
</tr>
<tr>
<td>LPT</td>
<td>line printer terminal</td>
</tr>
<tr>
<td>LVD</td>
<td>low voltage differential</td>
</tr>
<tr>
<td>MAC</td>
<td>media access control / mandatory access control</td>
</tr>
<tr>
<td>MAPI</td>
<td>messaging application programming interface</td>
</tr>
<tr>
<td>MAU</td>
<td>media access unit, media attachment unit</td>
</tr>
<tr>
<td>Mb</td>
<td>megabit</td>
</tr>
<tr>
<td>MB</td>
<td>megabyte</td>
</tr>
<tr>
<td>MBR</td>
<td>master boot record</td>
</tr>
<tr>
<td>MBSA</td>
<td>Microsoft Baseline Security Analyzer</td>
</tr>
<tr>
<td>MFD</td>
<td>multi-function device</td>
</tr>
<tr>
<td>MFP</td>
<td>multi-function product</td>
</tr>
<tr>
<td>MHz</td>
<td>megahertz</td>
</tr>
<tr>
<td>MicroDIMM</td>
<td>micro dual inline memory module</td>
</tr>
<tr>
<td>MIDI</td>
<td>musical instrument digital interface</td>
</tr>
<tr>
<td>MIME</td>
<td>multipurpose internet mail extension</td>
</tr>
<tr>
<td>MIMO</td>
<td>Multiple Input Multiple Output</td>
</tr>
<tr>
<td>MMC</td>
<td>Microsoft management console</td>
</tr>
<tr>
<td>MP3</td>
<td>Moving Picture Experts Group Layer 3 Audio</td>
</tr>
<tr>
<td>MP4</td>
<td>Moving Picture Experts Group Layer 4</td>
</tr>
<tr>
<td>MPEG</td>
<td>Moving Picture Experts Group</td>
</tr>
<tr>
<td>MSConfig</td>
<td>Microsoft configuration</td>
</tr>
<tr>
<td>MSDS</td>
<td>material safety data sheet</td>
</tr>
<tr>
<td>MUI</td>
<td>multilingual user interface</td>
</tr>
<tr>
<td>NAC</td>
<td>network access control</td>
</tr>
<tr>
<td>NAS</td>
<td>network-attached storage</td>
</tr>
<tr>
<td>NAT</td>
<td>network address translation</td>
</tr>
<tr>
<td>NetBIOS</td>
<td>networked basic input/output system</td>
</tr>
<tr>
<td>NetBEUI</td>
<td>networked basic input/output system extended user interface</td>
</tr>
<tr>
<td>NFS</td>
<td>network file system</td>
</tr>
<tr>
<td>NIC</td>
<td>network interface card</td>
</tr>
<tr>
<td>NiCd</td>
<td>nickel cadmium</td>
</tr>
<tr>
<td>NiMH</td>
<td>nickel metal hydride</td>
</tr>
<tr>
<td>NLX</td>
<td>new low-profile extended</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>NNTP</td>
<td>network news transfer protocol</td>
</tr>
<tr>
<td>NTFS</td>
<td>new technology file system</td>
</tr>
<tr>
<td>NTLDR</td>
<td>new technology loader</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>OCR</td>
<td>optical character recognition</td>
</tr>
<tr>
<td>OEM</td>
<td>original equipment manufacturer</td>
</tr>
<tr>
<td>OLED</td>
<td>Organic Light Emitting Diode</td>
</tr>
<tr>
<td>OS</td>
<td>operating system</td>
</tr>
<tr>
<td>PAN</td>
<td>personal area network</td>
</tr>
<tr>
<td>PATA</td>
<td>parallel advanced technology attachment</td>
</tr>
<tr>
<td>PC</td>
<td>personal computer</td>
</tr>
<tr>
<td>PCI</td>
<td>peripheral component interconnect</td>
</tr>
<tr>
<td>PCIe</td>
<td>peripheral component interconnect express</td>
</tr>
<tr>
<td>PCIX</td>
<td>peripheral component interconnect extended</td>
</tr>
<tr>
<td>PCL</td>
<td>printer control language</td>
</tr>
<tr>
<td>PCMCIA</td>
<td>Personal Computer Memory Card International Association</td>
</tr>
<tr>
<td>PGA</td>
<td>pin grid array</td>
</tr>
<tr>
<td>PGA2</td>
<td>pin grid array 2</td>
</tr>
<tr>
<td>PII</td>
<td>Personally Identifiable Information</td>
</tr>
<tr>
<td>PIN</td>
<td>personal identification number</td>
</tr>
<tr>
<td>PKI</td>
<td>public key infrastructure</td>
</tr>
<tr>
<td>PnP</td>
<td>plug and play</td>
</tr>
<tr>
<td>POP3</td>
<td>post office protocol 3</td>
</tr>
<tr>
<td>PoS</td>
<td>Point of Sale</td>
</tr>
<tr>
<td>POST</td>
<td>power-on self test</td>
</tr>
<tr>
<td>POTS</td>
<td>plain old telephone service</td>
</tr>
<tr>
<td>PPP</td>
<td>point-to-point protocol</td>
</tr>
<tr>
<td>PPTP</td>
<td>point-to-point tunneling protocol</td>
</tr>
<tr>
<td>PRI</td>
<td>preferred roaming index</td>
</tr>
<tr>
<td>PRL</td>
<td>preferred roaming list</td>
</tr>
<tr>
<td>PROM</td>
<td>programmable read-only memory</td>
</tr>
<tr>
<td>PS/2</td>
<td>personal system/2 connector</td>
</tr>
<tr>
<td>PSTN</td>
<td>public switched telephone network</td>
</tr>
<tr>
<td>PSU</td>
<td>power supply unit</td>
</tr>
<tr>
<td>PVC</td>
<td>permanent virtual circuit</td>
</tr>
<tr>
<td>PXE</td>
<td>preboot execution environment</td>
</tr>
<tr>
<td>QoS</td>
<td>quality of service</td>
</tr>
<tr>
<td>RAID</td>
<td>redundant array of independent (or inexpensive) discs</td>
</tr>
<tr>
<td>RAM</td>
<td>random access memory</td>
</tr>
<tr>
<td>RAS</td>
<td>remote access service</td>
</tr>
<tr>
<td>RDP</td>
<td>Remote Desktop Protocol</td>
</tr>
<tr>
<td>RF</td>
<td>radio frequency</td>
</tr>
<tr>
<td>RFI</td>
<td>radio frequency interference</td>
</tr>
</tbody>
</table>
RGB  red green blue
RIP  routing information protocol
RIS  remote installation service
RISC reduced instruction set computer
RJ 11 registered jack function 11
RJ-45 registered jack function 45
RMA  returned materials authorization
ROM  read only memory
RTC  real-time clock
SAN  storage area network
SAS  Serial Attached SCSI
SATA  serial advanced technology attachment
SC  subscription channel
SCP  secure copy protection
SCSI  small computer system interface
SCSI ID  small computer system interface identifier
SD card  secure digital card
SDRAM  synchronous dynamic random access memory
SEC  single edge connector
SFC  system file checker
SFF  Small Form Factor
SLI  scalable link interface or system level integration or scanline interleave mode
S.M.A.R.T.  self-monitoring, analysis, and reporting technology
SMB  server message block or small to midsize business
SMTP  simple mail transfer protocol
SNMP  simple network management protocol
SoDIMM  small outline dual inline memory module
SOHO  small office/home office
SP  service pack
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
<table>
<thead>
<tr>
<th><strong>Abbreviation</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>TKIP</td>
<td>Temporal Key Integrity Protocol</td>
</tr>
<tr>
<td>TPM</td>
<td>trusted platform module</td>
</tr>
<tr>
<td>UAC</td>
<td>user account control</td>
</tr>
<tr>
<td>UDF</td>
<td>user defined functions or universal disk format or universal data format</td>
</tr>
<tr>
<td>UDP</td>
<td>user datagram protocol</td>
</tr>
<tr>
<td>UEFI</td>
<td>Unified Extensible Firmware Interface</td>
</tr>
<tr>
<td>UNC</td>
<td>universal naming convention</td>
</tr>
<tr>
<td>UPS</td>
<td>uninterruptible power supply</td>
</tr>
<tr>
<td>URL</td>
<td>uniform resource locator</td>
</tr>
<tr>
<td>USB</td>
<td>universal serial bus</td>
</tr>
<tr>
<td>USMT</td>
<td>user state migration tool</td>
</tr>
<tr>
<td>UTP</td>
<td>unshielded twisted pair</td>
</tr>
<tr>
<td>UXGA</td>
<td>ultra extended graphics array</td>
</tr>
<tr>
<td>VESA</td>
<td>Video Electronics Standards Association</td>
</tr>
<tr>
<td>VFAT</td>
<td>virtual file allocation table</td>
</tr>
<tr>
<td>VGA</td>
<td>video graphics array</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>VoIP</td>
<td>voice over internet protocol</td>
</tr>
<tr>
<td>VPN</td>
<td>virtual private network</td>
</tr>
<tr>
<td>VRAM</td>
<td>video random access memory</td>
</tr>
<tr>
<td>WAN</td>
<td>wide area network</td>
</tr>
<tr>
<td>WAP</td>
<td>wireless access protocol/wireless access point</td>
</tr>
<tr>
<td>WEP</td>
<td>wired equivalent privacy</td>
</tr>
<tr>
<td>WIFI</td>
<td>wireless fidelity</td>
</tr>
<tr>
<td>WINS</td>
<td>windows internet name service</td>
</tr>
<tr>
<td>WLAN</td>
<td>wireless local area network</td>
</tr>
<tr>
<td>WPA</td>
<td>wireless protected access</td>
</tr>
<tr>
<td>WPS</td>
<td>WiFi Protected Setup</td>
</tr>
<tr>
<td>WUXGA</td>
<td>wide ultra extended graphics array</td>
</tr>
<tr>
<td>XGA</td>
<td>extended graphics array</td>
</tr>
<tr>
<td>ZIF</td>
<td>zero-insertion-force</td>
</tr>
<tr>
<td>ZIP</td>
<td>zigzag inline package</td>
</tr>
</tbody>
</table>
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 / Smart phone
- Android tablet / Smart phone
- Windows tablet / Smart phone
- Windows Laptop / 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

CompTIA A+ 220-902 Objectives version6
- 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
- Antimalware
- Driver software