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 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: 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: 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:

<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><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>
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 boot, 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

- **Partitioning**
  - Dynamic
  - Basic
  - Primary
  - Extended
  - Logical
  - GPT

- **File system types/formatting**
  - exFAT
  - FAT32
  - NTFS

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

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

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**
- **GPRERESULT**
- **DIR**
- **EXIT**
- **HELP**
- **EXPAND**
- [command name] /?

CompTIA A+ Certification Exam Objectives Version 4.0 (Exam Number: 220-902)
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
- **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

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
- **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**
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)

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
  - 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
- 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 (Google Play Store, App Store, and Store)

- **Screen orientation**
  - (accelerometer/gyroscope)

- **Launcher/GUI**
  - Virtual assistant

- **Virtual assistant**
  - SDK/APK

- **GPS and geotracking**
  - Emergency notification

- **WiFi calling**
  - Mobile payment service

#### 2.5.1 Android vs. iOS vs. Windows

- Open source vs. closed source/vendor specific
- App source (Google Play Store, App Store, and Store)

#### 2.5.2 Android

- Static vs. dynamic vs. unified
- App store vs. Google Play
- Google Play Store
  - App store vs. App Store
  - App store vs. Store

#### 2.5.3 iOS

- Apple iOs
  - Apple iOs
  - Apple iOs

#### 2.5.4 Windows

- Windows Phone
  - Windows Phone
  - Windows Phone

### 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

- **Screen orientation**
  - (accelerometer/gyroscope)

- **GPS and geotracking**
  - Emergency notification

- **WiFi calling**
  - Mobile payment service

- **Launcher/GUI**
  - Virtual assistant

- **Virtual assistant**
  - SDK/APK

- **Emergency notification**
  - Mobile payment service

#### 2.6.1 Wireless/cellular data network (enable/disable)

- Hotspot
- Tethering
- Airplane mode

#### 2.6.2 Bluetooth

- Enable Bluetooth
- Enable pairing
- Find device for pairing

#### 2.6.3 Corporate and ISP email configuration

- POP3
- IMAP
- Port and SSL settings
- Exchange, S/MIME

#### 2.6.4 Integrated commercial provider email configuration

- Google/Inbox
- Yahoo
- Outlook.com
- iCloud

#### 2.6.5 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

#### 2.7.1 Synchronization methods

- Synchronize to the cloud
- Synchronize to the desktop

#### 2.7.2 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**
  - Antivirus/Anti-malware
  - Firewalls
  - User authentication/strong passwords
  - Multifactor authentication
  - Directory permissions
  - VPN
  - DLP
  - Disabling ports
  - Access control lists
  - Smart card
  - Email filtering
  - Trusted/untrusted software sources
- **User education/AUP**
  - Principle of least privilege

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
- **Shared files and folders**
  - Administrative shares vs. local shares
  - Permission propagation
  - Inheritance
- **System files and folders**
  - Moving vs. copying folders and files
  - File attributes
- **User authentication**
  - Single sign-on
  - Run as administrator vs. standard user
  - BitLocker
  - BitLocker-To-Go
  - EFS
**3.0 Security**

**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 usernames/passwords
  - Screensaver required password
  - BIOS/UEFI passwords
- **Account management**
  - Requiring passwords
  - Restricting user permissions
  - Login time restrictions
  - Disabling guest account
  - Failed attempts lockout
  - Timeout/screen lock
- **Account management**
  - 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**
  - 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

- **Tools**
  - BIOS/UEFI
  - SFC
  - Logs
  - System recovery options
  - Repair disks
  - Pre-installation environments
  - MSCONFIG
  - DEFrag
  - Regsvr32
  - 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
Given a scenario, troubleshoot common mobile OS and application issues with appropriate tools.

### 4.3 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 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
- Compliance to local government regulations
5.0 Operational Procedures

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

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

- Deal appropriately with customers confidential and private materials
  - Located on a computer, desktop, printer, etc
## 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.

<table>
<thead>
<tr>
<th>ACRONYM</th>
<th>SPELLED OUT</th>
<th>ACRONYM</th>
<th>SPELLED OUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC</td>
<td>Alternating Current</td>
<td>CIDR</td>
<td>Classless Inter-Domain Routing</td>
</tr>
<tr>
<td>ACL</td>
<td>Access Control List</td>
<td>CIFS</td>
<td>Common Internet File System</td>
</tr>
<tr>
<td>ACPI</td>
<td>Advanced Configuration Power Interface</td>
<td>CLI</td>
<td>Command Line Interface</td>
</tr>
<tr>
<td>ACT</td>
<td>Activity</td>
<td>CMOS</td>
<td>Complementary Metal-Oxide Semiconductor</td>
</tr>
<tr>
<td>ADSL</td>
<td>Asymmetrical Digital Subscriber Line</td>
<td>CNR</td>
<td>Communications and Networking Riser</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
<td>COMx</td>
<td>Communication Port (x=Port Number)</td>
</tr>
<tr>
<td>AGP</td>
<td>Accelerated Graphics Port</td>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>AHCI</td>
<td>Advanced Host Controller Interface</td>
<td>CRT</td>
<td>Cathode Ray Tube</td>
</tr>
<tr>
<td>AP</td>
<td>Access Point</td>
<td>DAC</td>
<td>Discretionary Access Control</td>
</tr>
<tr>
<td>APIPA</td>
<td>Automatic Private Internet Protocol Addressing</td>
<td>DB-25</td>
<td>Serial Communications D-Shell Connector, 25 Pins</td>
</tr>
<tr>
<td>APM</td>
<td>Advanced Power Management</td>
<td>DB-9</td>
<td>9 Pin D Shell Connector</td>
</tr>
<tr>
<td>ARP</td>
<td>Address Resolution Protocol</td>
<td>DC</td>
<td>Direct Current</td>
</tr>
<tr>
<td>ASR</td>
<td>Automated System Recovery</td>
<td>DDoS</td>
<td>Distributed Denial of Service</td>
</tr>
<tr>
<td>ATA</td>
<td>Advanced Technology Attachment</td>
<td>DDR</td>
<td>Double Data Rate</td>
</tr>
<tr>
<td>ATAPI</td>
<td>Advanced Technology Attachment Packet Interface</td>
<td>DDR RAM</td>
<td>Double Data Rate Random-Access Memory</td>
</tr>
<tr>
<td>ATM</td>
<td>Asynchronous Transfer Mode</td>
<td>DDR SDRAM</td>
<td>Double Data Rate Synchronous Dynamic Access Memory</td>
</tr>
<tr>
<td>ATSC</td>
<td>Advanced Television Systems Committee</td>
<td>DFS</td>
<td>Distributed File System</td>
</tr>
<tr>
<td>ATX</td>
<td>Advanced Technology Extended</td>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>AUP</td>
<td>Acceptable Use Policy</td>
<td>DIMM</td>
<td>Dual Inline Memory Module</td>
</tr>
<tr>
<td>A/V</td>
<td>Audio Video</td>
<td>DIN</td>
<td>Deutsche Industrie Norm</td>
</tr>
<tr>
<td>BD-R</td>
<td>Blu-ray Disk Recordable</td>
<td>DLL</td>
<td>Dynamic Link Library</td>
</tr>
<tr>
<td>BIOS</td>
<td>Basic Input/Output System</td>
<td>DLT</td>
<td>Digital Linear Tape</td>
</tr>
<tr>
<td>BNC</td>
<td>Bayonet-Neill-Concelman or British Naval Connector</td>
<td>DLP</td>
<td>Digital Light Processing or Data Loss Prevention</td>
</tr>
<tr>
<td>BTX</td>
<td>Balanced Technology Extended</td>
<td>DMA</td>
<td>Direct Memory Access</td>
</tr>
<tr>
<td>CAD</td>
<td>Computer Aided Design</td>
<td>DMZ</td>
<td>Demilitarized Zone</td>
</tr>
<tr>
<td>CAPTCHA</td>
<td>Completely Automated Public Turing Test to tell Computers and Humans Apart</td>
<td>DNAT</td>
<td>Destination Network Address Translation</td>
</tr>
<tr>
<td>CCFL</td>
<td>Cold Cathode Fluorescent Lamp</td>
<td>DNS</td>
<td>Domain Name Service or Domain Name Server</td>
</tr>
<tr>
<td>CD</td>
<td>Compact Disc</td>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>CD-ROM</td>
<td>Compact Disc-Read-Only Memory</td>
<td>DRAM</td>
<td>Dynamic Random Access Memory</td>
</tr>
<tr>
<td>CD-RW</td>
<td>Compact Disc-Rewritable</td>
<td>DRM</td>
<td>Digital Rights Management</td>
</tr>
<tr>
<td>CDFS</td>
<td>Compact Disc File System</td>
<td>DSL</td>
<td>Digital Subscriber Line</td>
</tr>
<tr>
<td>CERT</td>
<td>Computer Emergency Response Team</td>
<td>DVD</td>
<td>Digital Video Disc or Digital Versatile Disc</td>
</tr>
<tr>
<td>CFS</td>
<td>Central File System or Common File System or Command File System</td>
<td>DVD-ROM</td>
<td>Digital Video Disc-Read-Only Memory</td>
</tr>
</tbody>
</table>

CompTIA A+ Certification Exam Objectives Version 4.0 (Exam Number: 220-902)
<table>
<thead>
<tr>
<th>ACRONYM</th>
<th>SPELLED OUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>DVD-R</td>
<td>Digital Video Disc-Recordable</td>
</tr>
<tr>
<td>DVD-RW</td>
<td>Digital Video Disc-Rewritable</td>
</tr>
<tr>
<td>DVI</td>
<td>Digital Visual Interface</td>
</tr>
<tr>
<td>ECC</td>
<td>Error Correcting Code or</td>
</tr>
<tr>
<td></td>
<td>Error Checking and Correction</td>
</tr>
<tr>
<td>ECP</td>
<td>Extended Capabilities Port</td>
</tr>
<tr>
<td>EDO</td>
<td>Extended Data Out (RAM)</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>eSATA</td>
<td>External Serial Advanced Technology Attachment</td>
</tr>
<tr>
<td>ESD</td>
<td>Electrostatic Discharge</td>
</tr>
<tr>
<td>EULA</td>
<td>End-User License Agreement</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>Ext2</td>
<td>Second Extended File System</td>
</tr>
<tr>
<td>exFAT</td>
<td>Extended File Allocation Table</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>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>GPO</td>
<td>Group Policy Object</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>GPT</td>
<td>GUID Partition Table</td>
</tr>
<tr>
<td>GPU</td>
<td>Graphics Processing Unit</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>HFS</td>
<td>Hierarchical File System</td>
</tr>
<tr>
<td>HPFS</td>
<td>High-Performance File System</td>
</tr>
<tr>
<td>HSF</td>
<td>Heat Sink and Fan</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</td>
</tr>
<tr>
<td></td>
<td>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>ICS</td>
<td>Internet Connection Sharing</td>
</tr>
<tr>
<td>IDE</td>
<td>Integrated Drive Electronics</td>
</tr>
<tr>
<td>IDF</td>
<td>Intermediate Distribution Frame</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and</td>
</tr>
<tr>
<td></td>
<td>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>IMEI</td>
<td>International Mobile Equipment</td>
</tr>
<tr>
<td>IMSI</td>
<td>International Mobile Subscriber</td>
</tr>
<tr>
<td>IOPS</td>
<td>Input/Output Per Second</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>IPS</td>
<td>In-Plane Switching or Intrusion</td>
</tr>
<tr>
<td></td>
<td>Prevention System</td>
</tr>
<tr>
<td>IPSEC</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>IR</td>
<td>Infrared</td>
</tr>
<tr>
<td>IRA</td>
<td>Infrared Data Association</td>
</tr>
<tr>
<td>IRP</td>
<td>Incident Response Plan</td>
</tr>
<tr>
<td>IRQ</td>
<td>Interrupt Request</td>
</tr>
<tr>
<td>ISDN</td>
<td>Integrated Services Digital</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for</td>
</tr>
<tr>
<td></td>
<td>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>Kb</td>
<td>Kilobit</td>
</tr>
<tr>
<td>KB</td>
<td>Kilobyte or Knowledge Base</td>
</tr>
<tr>
<td>KVM</td>
<td>Kernel-based Virtual Machine</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</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>LVDS</td>
<td>Low Voltage Differential Signaling</td>
</tr>
<tr>
<td>ACRONYM</td>
<td>SPELLED OUT</td>
</tr>
<tr>
<td>----------</td>
<td>----------------</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control or Mandatory Access Control</td>
</tr>
<tr>
<td>MAPI</td>
<td>Messaging Application Programming Interface</td>
</tr>
<tr>
<td>MAU</td>
<td>Media Access Unit or 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>MDM</td>
<td>Master Data Management</td>
</tr>
<tr>
<td>MFA</td>
<td>Multifactor Authentication</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>MSRA</td>
<td>Microsoft Remote Assistance</td>
</tr>
<tr>
<td>MSTSC</td>
<td>Microsoft Terminal Services Client</td>
</tr>
<tr>
<td>MT-RJ</td>
<td>Mechanical Transfer Registered Jack</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</td>
</tr>
<tr>
<td>NFC</td>
<td>Near Field Communication</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>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>NVM HCI</td>
<td>Non-Volatile Memory Host Controller Interface</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>ACRONYM</td>
<td>SPELLED OUT</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>SD Card</td>
<td>Secure Digital Card</td>
</tr>
<tr>
<td>SDRAM</td>
<td>Synchronous Dynamic Random-Access Memory</td>
</tr>
<tr>
<td>SEC</td>
<td>Single Edge Connector</td>
</tr>
<tr>
<td>SFC</td>
<td>System File Checker</td>
</tr>
<tr>
<td>SFF</td>
<td>Small Form Factor</td>
</tr>
<tr>
<td>SFTP</td>
<td>Secure File Transfer Protocol</td>
</tr>
<tr>
<td>SLI</td>
<td>Scalable Link Interface or System Level Integration or Scanline Interleave Mode</td>
</tr>
<tr>
<td>S.M.A.R.T.</td>
<td>Self-Monitoring, Analysis, and Reporting Technology</td>
</tr>
<tr>
<td>SMB</td>
<td>Server Message Block or Small To Midsize Business</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SoDIMM</td>
<td>Small outline Dual Inline Memory Module</td>
</tr>
<tr>
<td>SOHO</td>
<td>Small Office, Home Office</td>
</tr>
<tr>
<td>SP</td>
<td>Service Pack</td>
</tr>
<tr>
<td>SPDIF</td>
<td>Sony/Philips Digital Interface Format</td>
</tr>
<tr>
<td>SPGA</td>
<td>Staggered Pin Grid Array</td>
</tr>
<tr>
<td>SRAM</td>
<td>Static Random-Access Memory</td>
</tr>
<tr>
<td>SSD</td>
<td>Solid State Drive</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>SSDID</td>
<td>Service Set Identifier</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>SSO</td>
<td>Single Sign-On</td>
</tr>
<tr>
<td>ST</td>
<td>Straight Tip</td>
</tr>
<tr>
<td>STP</td>
<td>Shielded Twisted Pair</td>
</tr>
<tr>
<td>SXGA</td>
<td>Super Extended Graphics Array</td>
</tr>
<tr>
<td>TB</td>
<td>Terabyte</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>Transmission Control Protocol/Internet Protocol</td>
</tr>
<tr>
<td>TDR</td>
<td>Time Domain Reflectometer</td>
</tr>
<tr>
<td>TFTP</td>
<td>Trivial File Transfer Protocol</td>
</tr>
<tr>
<td>TKIP</td>
<td>Temporal Key Integrity Protocol</td>
</tr>
<tr>
<td>TN</td>
<td>Twisted Nematic</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>UPnP</td>
<td>Universal Plug and Play</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>UTM</td>
<td>Unified Threat Management</td>
</tr>
<tr>
<td>UTP</td>
<td>Unshielded Twisted Pair</td>
</tr>
<tr>
<td>UUID</td>
<td>Universally Unique Identifier</td>
</tr>
<tr>
<td>UXGA</td>
<td>Ultra Extended Graphics Array</td>
</tr>
<tr>
<td>VDI</td>
<td>Virtual Desktop Infrastructure</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>VHD</td>
<td>Virtual Hard Disk</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 or 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>WOL</td>
<td>Wake-on-LAN</td>
</tr>
<tr>
<td>WPA</td>
<td>WiFi Protected Access</td>
</tr>
<tr>
<td>WPA2</td>
<td>WiFi Protected Access 2</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>XFS</td>
<td>Extended File System</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>Zig-zag 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 that wish to create a lab component to their training offering. The bulleted lists below each topic are sample lists and not exhaustive.

**EQUIPMENT**
- Apple tablet/smartphone
- Android tablet/smartphone
- Windows tablet/smartphone
- 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
- 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