About the Exam

Candidates are encouraged to use this document to help prepare for CompTIA A+ Core 2. In order to receive the CompTIA A+ certification, you must pass two exams: Core 1 (220-1001) and Core 2 (220-1002). CompTIA A+ Core 2 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 PCs, mobile devices, 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 scripting, 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 testing exam objectives. Please know that all related exam preparation materials will still be valid.
TEST DETAILS

Required exam: Core 2  
Number of questions: Maximum of 90  
Types of questions: Multiple choice and performance-based  
Length of test: 90 minutes  
Recommended experience: 12 months of experience as an IT support specialist  
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 Operating Systems</td>
<td>27%</td>
</tr>
<tr>
<td>2.0 Security</td>
<td>24%</td>
</tr>
<tr>
<td>3.0 Software Troubleshooting</td>
<td>26%</td>
</tr>
<tr>
<td>4.0 Operational Procedures</td>
<td>23%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>
1.0 Operating Systems

1.1 Compare and contrast common operating system types and their purposes.
- 32-bit vs. 64-bit
  - RAM limitations
  - Software compatibility
- Workstation operating systems
  - Microsoft Windows
  - Apple Macintosh OS
  - Linux
- Cell phone/tablet operating systems
  - Microsoft Windows
  - Android
  - iOS
  - Chrome OS
- Vendor-specific limitations
  - End-of-life
  - Update limitations
- Compatibility concerns between operating systems

1.2 Compare and contrast features of Microsoft Windows versions.
- Windows 7
- Windows 8
- Windows 8.1
- Windows 10
- Corporate vs. personal needs
  - Domain access
  - BitLocker
  - Media center
- BranchCache
- EFS
- Desktop styles/user interface

1.3 Summarize general OS installation considerations and upgrade methods.
- Boot methods
  - Optical disc (CD-ROM, DVD, Blu-ray)
  - External drive/flash drive (USB/eSATA)
  - Network boot (PXE)
  - Internal fixed disk (HDD/SSD)
  - Internal hard drive (partition)
- Type of installations
  - Unattended installation
  - In-place 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
  - HFS
  - Swap partition
- 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
- Prerequisites/hardware compatibility
- Application compatibility
- OS compatibility/upgrade path
1.4 Given a scenario, use appropriate Microsoft command line tools.

- Navigation
  - dir
  - cd
  - ..
- ipconfig
- ping
- tracert
- netstat
- nslookup

- shutdown
- dism
- sfc
- chkdsk
- diskpart
- taskkill
- gpupdate
- gpretresult
- format
- copy
- xcopy
- robocopy
- net use
- net user
- [command name] /?
- Commands available with standard privileges vs. administrative privileges

1.5 Given a scenario, use 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
  - Event Viewer
  - User Account Management

- 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

- System utilities
  - Regedit
  - Command
  - Services.msc
  - MMC
  - MSTSC
  - Notepad
  - Explorer
  - Msinfo32
  - DxDiag
  - Disk Defragmenter
  - System Restore
  - Windows Update

1.6 Given a scenario, use Microsoft Windows Control Panel utilities.

- Internet Options
  - Connections
  - Security
  - General
  - Privacy
  - Programs
  - Advanced
- 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
- Credential Manager
- Programs and features
- HomeGroup
- Devices and Printers
- Sound
- Troubleshooting
- Network and Sharing Center
- Device Manager
- BitLocker
- Sync Center
1.7 Summarize application installation and configuration concepts.

- System requirements
  - Drive space
  - RAM
- OS requirements
  - Compatibility
- Methods of installation and deployment
  - Local (CD/USB)
  - Network-based
- Local user permissions
  - Folder/file access for installation
- Security considerations
  - Impact to device
  - Impact to network

1.8 Given a scenario, configure Microsoft 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)

1.9 Given a scenario, use features and tools of the Mac OS and Linux client/desktop 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
  - 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
  - rm
  - chmod
  - chown
  - iwconfig/ifconfig
  - ps
  - su/sudo
  - apt-get
  - vi
  - dd
  - kill
2.0 Security

2.1 Summarize the importance of physical security measures.

- Mantrap
- Badge reader
- Smart card
- Security guard
- Door lock

- Biometric locks
- Hardware tokens
- Cable locks
- Server locks
- USB locks

- Privacy screen
- Key fobs
- Entry control roster

2.2 Explain logical security concepts.

- Active Directory
  - Login script
  - Domain
  - Group Policy/Updates
  - Organizational Units
  - Home Folder
  - Folder redirection
  - Software tokens

- MDM policies
- Port security
- MAC address filtering
- Certificates
- Antivirus/Anti-malware
- Firewalls
- User authentication/strong passwords
- Multifactor authentication

- Directory permissions
- VPN
- DLP
- Access control lists
- Smart card
- Email filtering
- Trusted/untrusted software sources
- Principle of least privilege

2.3 Compare and contrast wireless security protocols and authentication methods.

- Protocols and encryption
  - WEP
  - WPA
  - WPA2
  - TKIP
  - AES

- Authentication
  - Single-factor
  - Multifactor
  - RADIUS
  - TACACS

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

- Malware
  - Ransomware
  - Trojan
  - Keylogger
  - Rootkit
  - Virus

- Tools and methods
  - Antivirus
  - Anti-malware

- Botnet
- Worm
- Spyware

- Recovery console
- Backup/restore
- End user education
- Software firewalls
- DNS configuration
2.0 Security

2.5 Compare and contrast social engineering, threats, and vulnerabilities.

- Social engineering
  - Phishing
  - Spear phishing
  - Impersonation
  - Shoulder surfing
  - Tailgating
  - Dumpster diving
- DDoS
- DoS
- Zero-day
- Man-in-the-middle
- Brute force
- Dictionary
- Rainbow table
- Spoofing
- Non-compliant systems
- Zombie

2.6 Compare and contrast the differences of basic Microsoft 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

2.7 Given a scenario, implement security best practices to secure a workstation.

- Password best practices
  - Setting strong passwords
  - Password expiration
  - Screensaver required password
  - BIOS/UEFI passwords
  - Requiring passwords
- Account management
  - Restricting user permissions
  - Logon time restrictions
  - Disabling guest account
- Failed attempts lockout
- Timeout/screen lock
- Change default admin user account/password
- Basic Active Directory functions
  - Account creation
  - Account deletion
  - Password reset/unlock account
  - Disable account
- Disable autorun
- Data encryption
- Patch/update management
2.8 Given a scenario, implement 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/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

2.9 Given a scenario, implement 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

2.10 Given a scenario, configure security on 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
3.0 Software Troubleshooting

3.1 Given a scenario, troubleshoot Microsoft Windows OS problems.

- **Common symptoms**
  - Slow performance
  - Limited connectivity
  - Failure to boot
  - No OS found
  - Application crashes
  - Blue screens
  - Black screens
  - Printing issues
  - Services fail to start
  - Slow bootup
  - Slow profile load

- **Common solutions**
  - Defragment the hard drive
  - Reboot
  - Kill tasks
  - Restart services
  - Update network settings
  - Reimage/reload OS
  - Roll back updates
  - Roll back devices drivers
  - Apply updates
  - Repair application
  - Update boot order
  - Disable Windows services/applications
  - Disable application startup
  - Safe boot
  - Rebuild Windows profiles

3.2 Given a scenario, troubleshoot and resolve PC security issues.

- **Common symptoms**
  - Pop-ups
  - Browser redirection
  - Security alerts
  - Slow performance
  - Internet connectivity issues
  - PC/OS lockup
  - Application crash
  - OS updates failures
  - Rogue antivirus
  - Spam
  - Renamed system files
  - Disappearing files
  - File permission changes
  - Hijacked email
  - Responses from users regarding email
  - Automated replies from unknown sent email
  - Access denied
  - Invalid certificate (trusted root CA)
  - System/application log errors

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

1. Identify and research malware symptoms.
2. Quarantine the infected systems.
4. Remediate the infected systems.
   a. Update the anti-malware software.
   b. Scan and use removal techniques (safe mode, pre-installation environment).
5. Schedule scans and run updates.
6. Enable System Restore and create a restore point (in Windows).
7. Educate the end user.
Given a scenario, troubleshoot mobile OS and application issues.

3.4

- **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
- App log errors

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

3.5

- **Common symptoms**
  - Signal drop/weak signal
  - Power drain
  - Slow data speeds
  - Unintended WiFi connection
  - Unintended Bluetooth pairing
  - Leaked personal files/data
  - Data transmission over limit
- Unauthorized account access
- Unauthorized location tracking
- Unauthorized camera/microphone activation
- High resource utilization

CompTIA A+ Certification Exam: Core 2 Objectives Version 4.0 (Exam Number: Core 2)
4.0 Operational Procedures

4.1 Compare and contrast best practices associated with types of documentation.

- Network topology diagrams
- Knowledge base/articles
- Incident documentation
- Regulatory and compliance policy
- Acceptable use policy
- Password policy
- Inventory management
  - Asset tags
  - Barcodes

4.2 Given a scenario, implement basic change management best practices.

- Documented business processes
  - Purpose of the change
  - Scope the change
  - Risk analysis
  - Plan for change
  - End-user acceptance
- Change board
  - Approvals
  - Backout plan
  - Document changes

4.3 Given a scenario, implement basic disaster prevention and recovery methods.

- Backup and recovery
  - Image level
  - File level
  - Critical applications
- Backup testing
- UPS
- Surge protector
- Cloud storage vs. local storage backups
- Account recovery options

4.4 Explain common safety procedures.

- Equipment grounding
- Proper component handling and storage
  - Antistatic bags
  - ESD straps
  - ESD mats
  - Self-grounding
- Toxic waste handling
  - Batteries
- Toner
- CRT
- Cell phones
- Tablets
- 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 government regulations
4.5 Explain environmental impacts and appropriate controls.

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

4.6 Explain the processes for addressing prohibited content/activity, and 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
- Regulated data
  - PII
  - PCI
  - GDPR
  - PHI
- Follow all policies and security best practices

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

- Use proper language and 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 coworkers while interacting with customers
  - Personal interruptions
- Dealing with difficult customers or situations
  - 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.
4.8 Identify the basics of scripting.

- Script file types
  - .bat
  - .ps1
  - .vbs
  - .sh
  - .py
  - .js

- Environment variables
- Comment syntax
- Basic script constructs
  - Basic loops
  - Variables

- Basic data types
  - Integers
  - Strings

4.9 Given a scenario, use remote access technologies.

- RDP
- Telnet
- SSH
- Third-party tools
  - Screen share feature
  - File share
- Security considerations of each access method
## 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>CGA</td>
<td>Computer Graphics and Applications</td>
</tr>
<tr>
<td>ACL</td>
<td>Access Control List</td>
<td>CIDR</td>
<td>Classless Inter-Domain Routing</td>
</tr>
<tr>
<td>ACPI</td>
<td>Advanced Configuration Power Interface</td>
<td>CIFS</td>
<td>Common Internet File System</td>
</tr>
<tr>
<td>ADF</td>
<td>Automatic Document Feeder</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>AHCI</td>
<td>Advanced Host Controller Interface</td>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>AP</td>
<td>Access Point</td>
<td>CRT</td>
<td>Cathode-Ray Tube</td>
</tr>
<tr>
<td>APIPA</td>
<td>Automatic Private Internet Protocol Addressing</td>
<td>DaaS</td>
<td>Data as a Service</td>
</tr>
<tr>
<td>APM</td>
<td>Advanced Power Management</td>
<td>DAC</td>
<td>Discretionary Access Control</td>
</tr>
<tr>
<td>ARP</td>
<td>Address Resolution Protocol</td>
<td>DB-25</td>
<td>Serial Communications D-Shell Connector, 25 pins</td>
</tr>
<tr>
<td>ASR</td>
<td>Automated System Recovery</td>
<td>DB-9</td>
<td>Serial Communications D-Shell Connector, 9 pins</td>
</tr>
<tr>
<td>ATA</td>
<td>Advanced Technology Attachment</td>
<td>DBaaS</td>
<td>Database as a Service</td>
</tr>
<tr>
<td>ATAPI</td>
<td>Advanced Technology Attachment Packet Interface</td>
<td>DC</td>
<td>Direct Current</td>
</tr>
<tr>
<td>ATM</td>
<td>Asynchronous Transfer Mode</td>
<td>DDoS</td>
<td>Distributed Denial of Service</td>
</tr>
<tr>
<td>ATX</td>
<td>Advanced Technology Extended</td>
<td>DDR</td>
<td>Double Data Rate</td>
</tr>
<tr>
<td>AUP</td>
<td>Acceptable Use Policy</td>
<td>DDR RAM</td>
<td>Double Data Rate Random Access Memory</td>
</tr>
<tr>
<td>A/V</td>
<td>Audio Video</td>
<td>DFS</td>
<td>Distributed File System</td>
</tr>
<tr>
<td>BD-R</td>
<td>Blu-ray Disc Recordable</td>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>BIOS</td>
<td>Basic Input/Output System</td>
<td>DIMM</td>
<td>Dual Inline Memory Module</td>
</tr>
<tr>
<td>BD-RE</td>
<td>Blu-ray Disc Rewritable</td>
<td>DIN</td>
<td>Deutsche Industrie Norm</td>
</tr>
<tr>
<td>BNC</td>
<td>Bayonet-Neill-Concelman</td>
<td>DLT</td>
<td>Digital Linear Tape</td>
</tr>
<tr>
<td>BSOD</td>
<td>Blue Screen of Death</td>
<td>DLP</td>
<td>Digital Light Processing or Data Loss Prevention</td>
</tr>
<tr>
<td>BYOD</td>
<td>Bring Your Own Device</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>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 Versatile Disc</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DVD-ROM</td>
<td>Digital Versatile Disc-Read Only Memory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DVD-R</td>
<td>Digital Versatile Disc-Recordable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DVD-RW</td>
<td>Digital Versatile Disc-Rewritable</td>
</tr>
<tr>
<td>ACRONYM</td>
<td>SPELLED OUT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DVI</td>
<td>Digital Visual Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DVI-D</td>
<td>Digital Visual Interface-Digital</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECC</td>
<td>Error Correcting Code</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECP</td>
<td>Extended Capabilities Port</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EEPROM</td>
<td>Electrically Erasable Programmable Read-Only Memory</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EIDE</td>
<td>Enhanced Integrated Drive Electronics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EMI</td>
<td>Electromagnetic Interference</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EMP</td>
<td>Electromagnetic Pulse</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EPROM</td>
<td>Erasable Programmable Read-Only Memory</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EPP</td>
<td>Enhanced Parallel Port</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ERD</td>
<td>Emergency Repair Disk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>eSATA</td>
<td>External Serial Advanced Technology Attachment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ESD</td>
<td>Electrostatic Discharge</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EULA</td>
<td>End User License Agreement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EVGA</td>
<td>Extended Video Graphics Adapter/Array</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ext2</td>
<td>Second Extended File System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>exFAT</td>
<td>Extended File Allocation Table</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FAT</td>
<td>File Allocation Table</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FAT12</td>
<td>12-bit File Allocation Table</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FAT16</td>
<td>16-bit File Allocation Table</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FAT32</td>
<td>32-bit File Allocation Table</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FDD</td>
<td>Floppy Disk Drive</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FPM</td>
<td>Fast Page Mode</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FSB</td>
<td>Front-Side Bus</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FQDN</td>
<td>Fully Qualified Domain Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GDDR</td>
<td>Graphics Double Data Rate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GDI</td>
<td>Graphics Device Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical User Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GUID</td>
<td>Globally Unique Identifier</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GPT</td>
<td>GUID Partition Table</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GPU</td>
<td>Graphics Processing Unit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HDD</td>
<td>Hard Disk Drive</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HDMI</td>
<td>High Definition Media Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HIPS</td>
<td>Host Intrusion Prevention System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HPFS</td>
<td>High Performance File System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTML</td>
<td>Hypertext Markup Language</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTPC</td>
<td>Home Theater PC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol Secure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>I/O</td>
<td>Input/Output</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IaaS</td>
<td>Infrastructure as a Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Message Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICR</td>
<td>Intelligent Character Recognition</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IDE</td>
<td>Integrated Drive Electronics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IIS</td>
<td>Internet Information Services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMAP</td>
<td>Internet Mail Access Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMEI</td>
<td>International Mobile Equipment Identity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMSI</td>
<td>International Mobile Subscriber Identity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPConfig</td>
<td>Internet Protocol Configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPP</td>
<td>Internet Printing Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPS</td>
<td>Intrusion Prevention System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPsec</td>
<td>Internet Protocol Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IR</td>
<td>Infrared</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IrDA</td>
<td>Infrared Data Association</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IRP</td>
<td>Incident Response Plan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IRQ</td>
<td>Interrupt Request</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISA</td>
<td>Industry Standard Architecture</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISDN</td>
<td>Integrated Services Digital Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
<td></td>
<td></td>
</tr>
<tr>
<td>JBOB</td>
<td>Just a Bunch of Disks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KB</td>
<td>Knowledge Base</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KVM</td>
<td>Kernel-based Virtual Machine</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KVM</td>
<td>Keyboard-Video-Mouse</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LBA</td>
<td>Logical Block Addressing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LC</td>
<td>Lucent Connector</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LCD</td>
<td>Liquid Crystal Display</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LED</td>
<td>Light Emitting Diode</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LPD/LPR</td>
<td>Line Printer Daemon/Line Printer Remote</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LPT</td>
<td>Line Printer Terminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LVD</td>
<td>Low Voltage Differential</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control/Mandatory Access Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAN</td>
<td>Metropolitan Area Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAPI</td>
<td>Messaging Application Programming Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mATX</td>
<td>Micro Advanced Technology Extended</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAU</td>
<td>Media Access Unit/Media Attachment Unit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MBR</td>
<td>Master Boot Record</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MBSA</td>
<td>Microsoft Baseline Security Analyzer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ACRONYM</td>
<td>SPELLED OUT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MDM</td>
<td>Mobile Device Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MFA</td>
<td>Multifactor Authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MFD</td>
<td>Multifunction Device</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MFP</td>
<td>Multifunction Product</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MicroDIMM</td>
<td>Micro Dual Inline Memory Module</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MIDI</td>
<td>Musical Instrument Digital Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MIME</td>
<td>Multipurpose Internet Mail Extension</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MIMO</td>
<td>Multiple Input Multiple Output</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MMC</td>
<td>Microsoft Management Console</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MP3</td>
<td>Moving Picture Experts Group Layer 3 Audio</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MP4</td>
<td>Moving Picture Experts Group Layer 4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPEG</td>
<td>Moving Picture Experts Group</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MSConfig</td>
<td>Microsoft Configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MSDS</td>
<td>Material Safety Data Sheet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MT-RJ</td>
<td>Mechanical Transfer Registered Jack</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MUI</td>
<td>Multilingual User Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NaaS</td>
<td>Network as a Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAC</td>
<td>Network Access Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAS</td>
<td>Network-Attached Storage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NetBIOS</td>
<td>Networked Basic Input/Output System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NetBEUI</td>
<td>Networked Basic Input/Output System Extended User Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NFC</td>
<td>Near Field Communication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NFS</td>
<td>Network File System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NIC</td>
<td>Network Interface Card</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NiCd</td>
<td>Nickel Cadmium</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NiMH</td>
<td>Nickel Metal Hydride</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NLX</td>
<td>New Low-profile Extended</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NNTP</td>
<td>Network News Transfer Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTFS</td>
<td>New Technology File System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTLDR</td>
<td>New Technology Loader</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTSC</td>
<td>National Transmission Standards Committee</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NVMe</td>
<td>Non-volatile Memory Express</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OCR</td>
<td>Optical Character Recognition</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OEM</td>
<td>Original Equipment Manufacturer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OLED</td>
<td>Organic Light Emitting Diode</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PaaS</td>
<td>Platform as a Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAL</td>
<td>Phase Alternating Line</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAN</td>
<td>Personal Area Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAT</td>
<td>Port Address Translation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCI</td>
<td>Peripheral Component Interconnect</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCI</td>
<td>Payment Card Industry</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCIe</td>
<td>Peripheral Component Interconnect Express</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCIX</td>
<td>Peripheral Component Interconnect Extended</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCL</td>
<td>Printer Command Language</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCMCIA</td>
<td>Personal Computer Memory Card</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PE</td>
<td>Preinstallation Environment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PGA</td>
<td>Pin Grid Array</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PGA2</td>
<td>Pin Grid Array 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PGP</td>
<td>Pretty Good Protection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PII</td>
<td>Personally Identifiable Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PHI</td>
<td>Personal Health Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PnP</td>
<td>Plug and Play</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PoE</td>
<td>Power over Ethernet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>POP3</td>
<td>Post Office Protocol 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PoS</td>
<td>Point of Sale</td>
<td></td>
<td></td>
</tr>
<tr>
<td>POST</td>
<td>Power-On sSelf-tTest</td>
<td></td>
<td></td>
</tr>
<tr>
<td>POTS</td>
<td>Plain Old Telephone Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PPM</td>
<td>Pages Per Minute</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PPP</td>
<td>Point-to-Point Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PPTP</td>
<td>Point-to-Point Tunneling Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PRI</td>
<td>Primary Rate Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PROM</td>
<td>Programmable Read-Only Memory</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PS/2</td>
<td>Personal System/2 connector</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PSTN</td>
<td>Public Switched Telephone Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PSU</td>
<td>Power Supply Unit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PVA</td>
<td>Patterned Vertical Alignment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PVC</td>
<td>Permanent Virtual Circuit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PXE</td>
<td>Preboot Execution Environment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial-In User Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RAID</td>
<td>Redundant Array of Independent (or inexpensive) Discs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RAM</td>
<td>Random Access Memory</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RAS</td>
<td>Remote Access Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RDP</td>
<td>Remote Desktop Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RFI</td>
<td>Radio Frequency Interference</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RFID</td>
<td>Radio Frequency Identification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RGB</td>
<td>Red Green Blue</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RIP</td>
<td>Routing Information Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RIS</td>
<td>Remote Installation Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RISC</td>
<td>Reduced Instruction Set Computer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RJ-11</td>
<td>Registered Jack Function 11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RJ-45</td>
<td>Registered Jack Function 45</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

CompTIA A+ Certification Exam: Core 2 Objectives Version 4.0 (Exam Number: Core 2)
<table>
<thead>
<tr>
<th>ACRONYM</th>
<th>SPELLED OUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>RMA</td>
<td>Returned Materials Authorization</td>
</tr>
<tr>
<td>ROM</td>
<td>Read-Only Memory</td>
</tr>
<tr>
<td>RPO</td>
<td>Recovery Point Objective</td>
</tr>
<tr>
<td>RTC</td>
<td>Real-Time Clock</td>
</tr>
<tr>
<td>RTO</td>
<td>Recovery Time Objective</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software as a Service</td>
</tr>
<tr>
<td>SAN</td>
<td>Storage Area Network</td>
</tr>
<tr>
<td>SAS</td>
<td>Serial Attached SCSI</td>
</tr>
<tr>
<td>SATA</td>
<td>Serial Advanced Technology Attachment</td>
</tr>
<tr>
<td>SC</td>
<td>Subscription Channel</td>
</tr>
<tr>
<td>SCP</td>
<td>Secure Copy Protection</td>
</tr>
<tr>
<td>SCsi</td>
<td>Small Computer System Interface</td>
</tr>
<tr>
<td>SCSi ID</td>
<td>Small Computer System Interface Identifier</td>
</tr>
<tr>
<td>SD card</td>
<td>Secure Digital Card</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>SIM</td>
<td>Subscriber Identity Module</td>
</tr>
<tr>
<td>SIMM</td>
<td>Single In-Line Memory Module</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</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>SSID</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>TACACS</td>
<td>Terminal Access Controller Access-Control System</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>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACRONYM</th>
<th>SPELLED OUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>TKIP</td>
<td>Temporal Key Integrity Protocol</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</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>UXGA</td>
<td>Ultra Extended Graphics Array</td>
</tr>
<tr>
<td>VA</td>
<td>Vertical Alignment</td>
</tr>
<tr>
<td>VDC</td>
<td>Volts DC</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>VLAN</td>
<td>Virtual LAN</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>VNC</td>
<td>Virtual Network Computer</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>WMN</td>
<td>Wireless Mesh Network</td>
</tr>
<tr>
<td>WPA</td>
<td>Wireless 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>WWAN</td>
<td>Wireless Wide Area Network</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 that wish to create a lab component for 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
- Chromebook
- Windows laptop/Mac laptop/Linux laptop
- Windows desktop/Mac desktop/Linux desktop
- Windows Server w/Active Directory and Print Management
- Monitors
- Projectors
- SOHO router/switch
- Access point
- VoIP phone
- Printer
  - Laser/inkjet
  - Wireless
  - 3D printer
- Surge suppressor
- UPS
- VR headset
- Smart devices (IoT devices)

**SOFTWARE**
- Operating systems
  - Linux
  - Chrome OS
  - Microsoft Windows
  - Mac OS
  - Android
  - iOS
- PE Disk/Live CD
- Antivirus software
- Virtualization software
- Anti-malware
- Driver software

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

**SPARE PARTS/HARDWARE**
- Motherboards
- RAM
- Hard drives
- Power supplies
- Video cards
- Sounds cards
- Network cards
- Wireless NICs
- Fans/cooling devices/heat sink

© 2018 CompTIA Properties, LLC, used under license by CompTIA Certifications, LLC. All rights reserved. All certification programs and education related to such programs are operated exclusively by CompTIA Certifications, LLC. CompTIA is a registered trademark of CompTIA Properties, LLC in the U.S. and internationally. Other brands and company names mentioned herein may be trademarks or service marks of CompTIA Properties, LLC or of their respective owners. Reproduction or dissemination prohibited without written consent of CompTIA Properties, LLC. Printed in the U.S. 04992B-Apr2018