EXAM CRAM

The CompTIA® A+® CramSheet

This Cram Sheet contains the distilled, key facts about the CompTIA A+ Core 1 (220-1101) and Core 2 (220-1102) exams. Review this information as the last step before you enter the testing center, paying special attention to those areas in which you think that you need the most review.

220-1101

1. Laptops are smaller, portable versions of desktop PCs with replaceable items such as keyboards and touchpads. Fn key for implementing secondary key functions, 2.5" or 1.8" hard drives (SSD, HDD, or hybrid), M.2 and Mini PCIe cards, and SODIMM RAM: DDR3 (204-pin), DDR4 (260-pin), DDR5 (262-pin).
2. Smartphones and tablets are mobile devices that have ARM-based CPUs, internal flash memory, multitouch displays, and Li-ion batteries. Often IP68-compliant (dust and watertight). Android = USB-C or microUSB; iOS = USB-C or Lightning connector.
3. GPS and geotracking provide location information about mobile devices.
4. Mobile devices connect to Internet via cellular WWAN (example: 5G, 4G, LTE, CDMA, GSM), WISP, and Wi-Fi (WLAN).
5. LAN = local area network. WAN = wide area network. MAN = metropolitan area network. PAN = personal area network. SAN = storage area network. WMN = wireless mesh network. WLAN = wireless local area network.
6. Switches connect computers together in a LAN. Routers connect two or more LANs and connect LANs to the Internet. Firewalls protect individual computers and networks from unwanted intrusion. IDS = intrusion detection system. IPS = intrusion prevention system.
7. **Networking connectors:** twisted pair (RJ45, RJ11); fiber optic (SC, ST, and LC); coaxial (RG-6, F-connector).
8. **T568B standard:** 1. White/orange, 2. Orange, 3. White/green, 4. Blue, 5. White/blue, 6. Green, 7. White/brown, 8. Brown. 568A reverses the orange and green. (Straight through cable = 568B to 568B; crossover cable = 568B to 568A).
9. IPv4 addresses are 32-bit dotted-decimal numbers (example: 192.168.1.1) and can be statically (manually) inputted or dynamically (automatically) assigned (DHCP).

   127.0.0.1 is the loopback address

   APIPA is 169.254.x.x (also known as link-local)
10. IPv6 addresses are 128-bit hexadecimal numbers (example: 2001:7120:0000:8001:0000:0000:0000:1F10).

    ::1 is the loopback address.

    Link-local addresses begin with FE80::/10 prefix.
11. Common network speeds are 1000 Mbps (Gigabit Ethernet) and 10 Gbps (10 Gbps Ethernet).
12. **Networking protocols include**
    - FTP (File Transfer Protocol). Port 20/21

      Secure versions: FTPS on port 989/990 and SFTP on port 22
    - SSH (Secure Shell). Port 22
    - Telnet. Port 23 (not secure)
    - SMTP (Simple Mail Transfer Protocol). Port 25

      Secure version uses SSL/TLS on port 587 or 465
    - DNS (Domain Naming System). Port 53
    - DHCP (Dynamic Host Configuration Protocol). Port 67/68
    - HTTP (Hypertext Transfer Protocol). Port 80
    - POP3 (Post Office Protocol). Port 110

      Secure version uses SSL/TLS on port 995
    - NetBIOS/NetBT (NetBIOS over TCP/IP). Ports 137–139
    - IMAP (Internet Message Access Protocol). Port 143

      Secure version uses SSL/TLS on port 993
    - SNMP (Simple Network Management Protocol). Port 161/162
    - LDAP (Lightweight Directory Access Protocol). Port 389

      Secure version uses SSL/TLS on port 636
    - HTTPS (HTTP Secure). Port 443
    - SMB/CIFS (Server Message Block/Common Internet File System). Port 445
    - RDP (Remote Desktop Protocol). Port 3389
13. **Twisted pair cabling standards (maximum 328 feet/100 meters):**
    - Category 5: Rated for 100 Mbps
    - Category 5e: Rated for 100 Mbps and Gigabit networks
    - Category 6/6a: Rated for Gigabit and 10 Gbps networks
    - Plenum-rated cable: Fire-resistant cable designed for airways, conduits, and areas sprinklers cannot reach.
    - Direct burial cable is used outdoors, 8 inches underground, 8 inches away from power lines.
14. **Wireless Ethernet:**
    - 802.11a, 5 GHz
    - 802.11b, 2.4 GHz
    - 802.11g, 2.4 GHz
    - 802.11n, 5 and 2.4 GHz
    - 802.11ac (Wi-Fi 5), 5 GHz
    - 802.11ax (Wi-Fi 6), 5 GHz
    - 2.4 GHz channels: 1–11
    - 5 GHz channels: 36, 40, 44, 48, 149, 153, 157, 161, 165
15. Bluetooth is a short-range technology aimed at simplifying communications and synchronization among network devices.

    Bluetooth classes: Class I maximum transmission range: 100 meters; Class II (most common) range: 10 meters; Class III range: 1 meter. Class 4 range: .5 meter.
16. **NAT (Network Address Translation):** process of modifying an IP address as it crosses a router. Translates from one network to another.
17. Port forwarding forwards an external network port to an internal IP address and port.
18. **Screened subnet (aka DMZ):** Area of network for servers, not within LAN but between LAN and the Internet.
19. **QoS (quality of service):** Prioritizes computers or applications.
20. **PoE (Power over Ethernet):** 802.3af PoE devices send Ethernet data *and* power over twisted pair cable to compliant devices (for example, a PoE injector).
21. Video cards typically connect to motherboards by way of x16 PCIe expansion slots. Video connector types include DVI, VGA, HDMI, Mini-HDMI, DisplayPort.
22. USB (Universal Serial Bus). Type A/Type B connectors are used by desktops/laptops, microUSB and USB-C connectors are used by tablets/smartphones, etc.
    USB 2.0 (high-speed) = 480 Mbps. USB 3.0 (SuperSpeed) = 5 Gbps.
    USB 3.1 (SuperSpeed+) = 10 Gbps. USB 3.2 = 10/20 Gbps (requires USB-C).
23. **Thunderbolt:** Ver 1 = 10 Gbps and uses DisplayPort; Ver 2 = 20 Gbps (also DisplayPort); Ver 3 = 40 Gbps and uses USB Type C. Apple mobile devices use 8-pin Lightning connector (USB 3.0 speeds)
24. **Random access memory (RAM):** DIMMs include DDR3 (240 pins), DDR4 (288 pins), and DDR5 (288 pins), none are backward compatible. Example of DDR transfer rate: DDR4-2666 = 21,333 MB/s. Dual-channel is double width, 128-bit bus. Triple-channel is 3x the width, 192-bit bus. Quad-channel is 4x the width, 256-bit bus. ECC detects and corrects errors.
25. Storage drives are nonvolatile devices that store data. Types of drives and interfaces include:
    - **HDD:** Hard disk drive (magnetic-based)
    - **SSD:** Solid-state drive (flash-based). Can be SATA or M.2
    - **SATA:** Serial ATA uses a 15-pin power connector and 7-pin data connector. Rev 3 = 6 Gb/s, Rev 3.2 (SATA Express) = 16 Gbps.
26. **RAID:** Redundant array of independent disks. RAID 0 = striping (not fault tolerant), RAID 1 = mirroring, and RAID 5 = striping with parity. RAID 10 is mirrored sets that are striped.
27. ATX 12V 2.x power supplies connect to motherboard (24-pin cable). CPU (4-pin/8-pin). PCIe video (6 or 8-pin). SATA (15-pin). Molex (4-pin).
28. BIOS/UEFI identifies, tests, and initializes components and boots to storage drive, optical disc, USB flash drive, or network via PXE. CR2032 lithium battery provides backup power.

    BIOS/UEFI configurations: Time/date, boot device priority (boot order), passwords, power management, WOL, monitoring, clock and bus speeds, virtualization support (Intel VT or AMD-V), enable/disable devices, and intrusion detection. For BIOS/UEFI update, flash it with new firmware.
29. The central processing unit (CPU) or processor takes care of most calculations. Speed measured in GHz. PGA (AMD) = Pin Grid Array. LGA (Intel) = Land Grid Array. L1/L2 cache in each core. L3 cache is shared among entire CPU. Thermal paste is required whenever heat sink is installed. TDP = thermal design power (example: 140 watts).
30. **Laser-printing imaging process:** processing, charging, exposing, developing, transferring, fusing, and cleaning.
31. **Printer configuration settings:** duplexing = printing on both sides; orientation = portrait or landscape; quality = DPI (600 or 1200), tray settings (such as size = 8.5" x 11").
32. **Cloud types:** SaaS (software as a service), IaaS (infrastructure as a service), PaaS (platform as a service).
33. **Cloud concepts:** Metered utilization (service): only the services accessed are paid for. Rapid elasticity: ability to scale the network quickly.
34. **Virtualization:** *Type 1* hypervisor is native or bare metal (has direct access to hardware). *Type 2* is hosted; runs on top of OS. Examples: VMware, Hyper-V, VirtualBox. Network connectivity: bridged (direct access to Internet), NAT (separated access), host-only (private, no Internet), or no networking.
35. CompTIA 6-step *troubleshooting* methodology: Always consider corporate policies, procedures, and impacts before implementing changes.
    1. Identify the problem.
    2. Establish a theory of probable cause. (Question the obvious.)
    3. Test the theory to determine cause.
    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.
36. Time/date resets to earlier date? Check lithium battery. For OS, synchronize to a time server.
37. Trouble with CPU? Check CPU fan, heat sink and thermal compound, overclocking setting in BIOS, and whether CPU is secure.
38. Noisy computer? Check CPU fan, case fan, power supply fan, and use compressed air and vacuum.
39. RAM issue? Reseat modules; clean with compressed air. Overheating? Try RAM heat sinks. BIOS beep codes or displayed errors? Consult motherboard docs and analyze POST beep codes and numbers.
40. Power issues? Test AC outlet with receptacle tester. Test power supply with PSU tester: A power supply tester tests 3.3 V, 5 V, –5 V, 12 V, and –12 V. Do not open power supply; it is a FRU (field replaceable unit).
41. Slow storage drive? Defrag it, use disk cleanup, and scan drive with AV software. Drive isn't recognized? Check connections, check in BIOS/UEFI, initialize, partition, and format in Disk Management.
42. No second screen on laptop? Check Fn key. Laptop display blank? Check brightness, resolution settings (safe mode if necessary), and for older LCDs: inverter and backlight.
43. Printer paper jam? Power cycle, check paper tray, rollers, paper type, fuser, and entire paper path. Blank paper? Check toner cartridge and transfer corona wire. Lines or smearing? Check drum, primary corona wire, and replace toner cartridge. Toner not staying on paper? Check fusing assembly. Garbled print/garbage printout? Check driver. Ghosted image? Check drum and toner cartridge. Incorrect paper size? Check the tray and type of paper. No connectivity? Check power, network connection, whether printer is shared, proper IP address, and whether printer is set up as default in Windows.
44. Test network connections with patch tester, LAN cable tester, tone and probe kit. Test NIC or RJ45 jack/switch port with loopback plug.
45. No network connectivity? Check link light, patch cable, disabled NIC, wireless switch is off, IP configuration, and Windows Network Troubleshooter. Limited connectivity? Ping localhost, then move outward and use **ipconfig/all**. Poor wireless signal? Check distance, placement, antennas, and update hardware and software. APIPA or IP conflict? **ipconfig/release** and **/renew**; check DHCP server.

220-1102

1. Windows 10 min. requirements: CPU = 1 GHz; RAM = 2 GB; Free drive space = 32 GB.
2. Windows 11 min. requirements: CPU = 1 GHz; RAM = 4 GB; Free drive space = 64 GB; UEFI (secure boot) capable; TPM 2.0; DirectX 12; 720p resolution.
3. Common system tools include Device Manager, System Information, Task Manager, and **msconfig**.
4. Remote Desktop connection software (known as RDP) enables a user to see and control the GUI of a remote computer.
5. Workgroups are for small networks (20 maximum inbound sessions to a Windows client). Domains are for larger networks and are controlled by a domain controller that has Active Directory installed.
6. %systemroot% is C:\Windows by default.
7. In Windows, **DIR** is the directory command. Navigate with the **CD** command, including **CD..** and **CD**.
8. Files can be manipulated with: **del** (deletes), **copy** (copies files), **robocopy** (robust file copy, copies multiple files and directory trees).
9. Drives can be manipulated with: **format** (writes new file system), **diskpart** (does everything Disk Management does but in PowerShell/Command Prompt).
10. File checking command-line tools that can be used in Windows include **chkdsk** (**/F** fixes errors; **/R** locates bad sectors and recovers info) and **sfc** (System File Checker). **sfc /scannow** is common.
11. A storage drive using GPT (GUID partition table) can have 128 partitions and go beyond MBR's 2 TB limit. GPT is stored in multiple locations. Requires UEFI-compliant motherboard. A storage drive using MBR can have four partitions: up to four primary partitions but only one extended partition. Logical drives are sections of an extended partition. The Active partition is the one that is booted from; it usually contains the OS. Any section of a drive with a letter is called a volume. Volumes in dynamic drives can be resized, but not in basic drives. NTFS is the most common file system in Windows. exFAT for flash drives.
12. Backups can be accomplished with File History and Windows Backup.
13. System Restore can fix issues caused by defective hardware or software by reverting back to an earlier time.
14. The Windows Recovery Environment (Windows RE or WinRE) includes System Recovery Options such as Startup Repair, System Restore, Command Prompt, and Startup Settings.
15. Startup Settings brings up options such as Safe Mode, Enable low-resolution video, and Last Known Good Configuration. Safe Mode boots the system with minimal drivers.
16. The Event Viewer warns about possible issues and displays errors as they occur within three main log files: System, Application, and Security. Security displays auditing information.
17. A stop error (also known as a blue screen of death, or BSOD) completely halts the operating system and displays a blue screen with various text and code. Can be caused by faulty hardware or bad drivers. macOS's equivalent error is the spinning pinwheel.
18. **gpresult** displays policy information for the user/computer.
    gpupdate updates policies without having to log off and on.
19. Common Windows networking command-line tools include:
    - **ipconfig:** Displays current TCP/IP network configuration values; **ipconfig/all** shows additional Information such as MAC address.
    - **ping:** Tests whether another host is available over the network (example: **ping 192.168.1.1**). **ping 127.0.0.1** or **ping ::1** to test the local computer. **ping -t** is continuous, **ping -n** is a set of pings. **ping -l** changes the size of each ping, **ping -a** resolves IP address to hostname.
    - **tracert:** Sends packets to test destinations beyond the local computer's network. **pathping** is similar.
    - **netstat:** Shows the network statistics for the local computer. Displays TCP and UDP sessions by computer name (or IP) and port.
    - **nslookup:** Used to query DNS servers to find out DNS details, including the IP address of hosts.
    - **net:** Used to map network drives (**net use**), view computers (**net view**), view users (**net user**), start/stop services (**net start** and **net stop**), and synchronize time (**net time**).
20. **Troubleshooting Windows:** Use WinRE startup settings, Startup Settings, MSConfig Safe Boot, use the Troubleshooter tool, restart services in services.msc (and with **net start**/**net stop**), end tasks in Task Manager, remove/repair applications in Programs and Features, enable/disable Windows components (such as Hyper-V and Telnet) in Windows Features. Analyze and remove certificates in certmgr.msc.
21. **macOS uses:** Dock (icons on the bottom), Finder (for locating applications and files), Key Chain (protected passwords/certificates), Mission Control (larger desktop perspective), Spotlight (the search tool), iCloud (for cloud storage, sync, and backup), Screen Sharing (view and take control of remote systems), Boot Camp (dual-boot to Windows), Time Machine (backup program/system state), and Terminal (similar to Linux).
22. **Linux** typically uses GPT and the ext4 file system. Paths use slashes (example: /Downloads/PDFs). Distros include Debian, Ubuntu, Fedora, Red Hat, CentOS, Kali, and Mint. Find the distro version by typing **cat /etc/os-release**.
    - **Linux Terminal tools: ip a**: Linux equivalent of **ipconfig**; **ls**: lists directory contents; **chmod**: modifies permissions; **chown**: changes file ownership; **ps**: displays process information; **apt-get** & **yum**: installs packages; **sudo**: executes commands as admin; **vi/Vim/nano**: opens text editor; **passwd**: changes password; **pwd**: displays full path/filename of working directory; **shutdown**: brings system down; **kill**: terminates processes; **cat**: displays file content; **grep**: searches for matching information; **df**: reports disk space usage; **man**: manual pages (help); **top**: analyzes running processes, CPU, and RAM; **find**: locates files; **dig**: finds out information related to DNS.
23. Wireless encryption protocols include:
    - WPA (Wi-Fi Protected Access), use version 2 or 3
    - AES (Advanced Encryption Standard)
    - Best combination is WPA3 with AES (as of writing of this book.)
    - PSK (pre-shared key) is stored on AP. RADIUS server is used (port 1812) for external authentication.
    - Deprecated protocols include WEP, WPA (version 1), and TKIP.
24. **Malicious software:** Known as malware, this includes:
    - **Virus:** Code that runs on a computer without the user's knowledge.
    - **Trojan horses:** Appear to perform desired functions but are actually performing malicious functions behind the scenes.
    - **Spyware:** Type of malicious software that is either downloaded unwittingly from a website or is installed along with some other third-party software.
    - **Rootkit:** Software designed to gain administrator-level access to the core of a system without being detected.
    - **Keylogger:** Hardware or software that captures the keystrokes of a keyboard.
    - **Ransomware:** Software designed to hold the computer hostage, encrypting files or locking the computer until the user pays the attacker. Often propagated by a Trojan.
    - **cryptominer:** Software that attempts to calculate hashes for cryptocurrency tokens. Can use up resources on a system making it perform sluggishly.
25. Best practice for malware removal:
    1. Identify and verify malware symptoms
    2. Quarantine infected systems
    3. Disable System Restore in Windows
    4. Remediate infected systems: update anti-malware, scan and use removal techniques (safe mode, preinstallation environment)
    5. Schedule scans and run updates
    6. Enable System Restore and create a restore point in Windows
    7. Educate the end user
26. **Social engineering:** The act of manipulating users into revealing confidential information or performing other actions detrimental to the user. Know phishing, vishing, whaling, impersonation, shoulder surfing, tailgating, and dumpster diving!
27. **Network attacks:** Know on-path attack, spoofing, zero-day, dictionary, and brute force. DDoS (distributed denial of service): enabled by a botnet. Evil twin: a rogue and malicious copy of a wireless access point.
28. **Authentication:** The verification of a person's identity; helps protect against unauthorized access. Broken down into: 1. Something the user knows (password or PIN); 2. Something the user has (a smart card or other security token); 3. Something the user is (biometric reading: fingerprint or retina scan); or 4. Something a user does (signature or voice print).

    MFA = multi-factor authentication (Example: A password and a smart card).

    UAC (User Account Control) in Windows requires administrative login to perform higher tasks.
29. **Security techniques:** Access control vestibule or mantrap (quarantine area with two doors and surveillance), one-time password (OTP; card with changing code), RFID badge, biometric reader, smart cards, and ACLs (access control lists).
30. **Encryption:** The act of changing information using an algorithm known as a cipher to make it unreadable to anyone except users who possess the proper "key" to the data.
    - **Encrypting File System (EFS):** Encrypts one or more files or folders directly within the Properties page in Windows.
    - **BitLocker:** Encrypts an entire drive in Windows. Requires TPM (Trusted Platform Module). BitLocker To Go encrypts USB drives and other removable devices.
31. **Storage drive disposal:** Clearing (drive to be reused in-house), purging (sanitizing with Secure Erase, several passes of zeroing out data), and destruction (pulverizing/shredding, drilling holes in platters, incineration, degaussing, acquire certificate of destruction when complete).
32. BIOS/UEFI security includes administrator and user passwords, drivelock passwords, disabling removable media, UEFI Secure Boot (helps prevent rootkit access), and setting the boot device priority to storage drive first.
33. **Permissions:** The more restrictive takes effect (NTFS vs. share); Inheritance/propagation: If you create a folder, the default action it takes is to inherit permissions from the parent folder. (So, the parent propagates to the child.) If you move a folder within the same partition, it retains the permissions. If you move or copy a folder to another partition, the (new) folder inherits from the new parent.
34. **Mobile device security:** Screenlocks (pattern, PIN, password), invalid attempts lockout, remote wipe, remote backup, and antivirus. Disallow rooting and jailbreaking, which are removing limitations to Android and iOS to gain superuser capabilities.
35. **Wireless security:** Change admin password, change/disable SSID, reduce radio power, disable WPS, use WPA3/AES, enable MAC filtering, update firmware, enable firewall, disable ports, enable content filtering.
36. **Safety:** Do not open power supplies, test AC outlets before use, use Class C CO2-based, or BC fire extinguisher on electrical fires, and call 911. Employ cable management, MSDS = material safety datasheets, and consult when encountering a product with chemicals (toner cartridges, cleaners).
37. ESD = electrostatic discharge. Prevent with antistatic strap, mat, touch chassis, antistatic bags, unplug computer, and increase humidity.
38. UPS has battery backup for protection during electrical outages.
39. Trouble tickets include user/device information, description of problems, and severity and should be clearly written.
40. **Change management includes:** Purpose of change, scope of change, affected systems, risk analysis, end-user acceptance, change board approvals. Should also include rollback plan and sandbox testing.
41. **Incident response:** First response, identify what happened, report through proper channels, preserve data and devices, document, and set up chain of custody (chronological paper trail).
42. **Regulated data includes:** PII (personally identifiable information), PHI (protected health information), personal government-issued information (Social Security card, etc.), PCI DSS (Payment Card Industry Data Security Standards), and GDPR (General Data Protection Regulation). Store in a secure area with encryption and proper permissions, and lockouts.
43. **Professionalism:** Professional appearance, punctuality, listen to customer, take notes, clarify problems, positive attitude, speak clearly, project confidence, be culturally sensitive, set and meet expectations, avoid distractions (phone calls, texting, social media), and avoid confidential data.
44. Basic loops (such as **for**) tell a program to execute the same statement several times.
45. PowerShell and Bash always place a **$** before a variable.
46. **Scripting types:** Windows PowerShell (.ps1), batch file (.bat); Linux Bash (.sh); Python (.py); Visual Basic script (.vbs); JavaScript (.js).
47. **Remote access:** RDP (Remote Desktop Protocol, port 3389), SSH (Secure Shell, port 22), Virtual Network Computing (VNC).

Good luck! And be **confident!**
You can do this!