A+ Exam Glossary

Find more at BareMetalCyber.com

1. **Access control**
   Access control is how a system decides who can use a resource and what actions they are allowed to take. On the exam, it shows up as choosing the right control for a situation (accounts, permissions, MFA) and avoiding "everyone gets admin" defaults.

2. **Access Control List (ACL)**
   An ACL is a set of rules attached to a resource (like a file share, firewall, or network device) that permits or denies specific traffic or access. Exam questions often test whether you recognize that an ACL is about *allow/deny logic* and rule order, not identity proofing.

3. **Airplane mode**
   Airplane mode is a device setting that disables wireless radios (typically cellular, Wi-Fi, and Bluetooth), sometimes with manual re-enable options. It's a common troubleshooting "trapdoor" on the exam because it can look like a network failure when the real cause is a local radio disable.

4. **Antimalware**
   Antimalware is software designed to detect, block, and remove malicious code (viruses, spyware, ransomware, and more). On the exam, the decision point is often *contain first* (stop spread), then remediate, and confirm normal operation without disabling protections long-term.

5. **APIPA (Automatic Private IP Addressing)**
   APIPA is when a device self-assigns an IP address because it cannot reach a DHCP server, usually resulting in limited connectivity. A+ questions use this to test whether you correctly diagnose "no DHCP lease" versus "DNS problem" and pick the right first check.

6. **ARP (Address Resolution Protocol)**
   ARP maps an IP address to a device's physical MAC address on a local network segment so traffic can be delivered on the LAN. On the exam, it commonly appears in scenarios where local connectivity is inconsistent and you must identify whether the issue is local-layer addressing versus routing or DNS.

7. **Attenuation**
   Attenuation is signal loss as it travels through distance, walls, or interference,

especially in wireless networks. Exam items use it to separate “weak signal” causes from “wrong password” causes and to justify moving closer, changing band, or adjusting placement rather than changing IP settings.

8. **Authentication**
   Authentication is proving identity, such as with a password, token, certificate, or biometrics. The exam often tests the difference between “can’t sign in” (authentication failure) and “signed in but can’t access” (authorization problem).

9. **Authorization**
   Authorization is the permission to do something after identity is verified, such as read/write access to a folder or permission to install software. On the exam, it shows up in access-denied scenarios where the user is real and logged in, but rights or group membership are wrong.

10. **Backup**
    A backup is a recoverable copy of data or system state used to restore after deletion, corruption, or device failure. Exam questions typically test choosing the safest next step before risky work (protect data) and recognizing that a backup is only useful if restores are possible and verified.

11. **BIOS (Basic Input Output System)**
    B I O S is firmware that initializes hardware at startup and hands control to the operating system boot process. On the exam, it shows up when you need the right “first step” for boot issues, hardware detection problems, or configuration changes like boot order and virtualization settings.

12. **BitLocker**
    BitLocker is Microsoft Windows full-disk encryption that protects data at rest if a device is lost or stolen. A+ questions often test recognizing when encryption is the right control and remembering that recovery keys and policy requirements can determine whether data is actually recoverable.

13. **Bluetooth**
    Bluetooth is a short-range wireless standard used for peripherals like headsets, keyboards, mice, and device-to-device sharing. On the exam it commonly appears in pairing and connectivity scenarios where the best next step is to verify pairing mode, profiles, interference, and whether the radio is enabled.

14. **Boot order**
    Boot order is the priority list a system uses to choose which device to start from, such as internal storage, USB, or network boot. Exam items use boot order as a

classic “wrong-first-step” trap when a system keeps booting the wrong device or fails to start after hardware changes.

15. **Bootable media**
    Bootable media is a USB drive or disc prepared with an installer or recovery environment that a system can start from. On the exam it matters for operating system installs, repairs, and password or startup recovery workflows, where choosing the correct tool is the key decision.

16. **Break-fix support**
    Break-fix is a support model where work is performed after a problem occurs, usually billed per incident rather than continuously managed. On A+, it can appear in operational procedure questions that compare service models, expectations, documentation, and escalation paths.

17. **Browser hijacker**
    A browser hijacker is unwanted software that changes browser settings such as homepage, search engine, or extensions to redirect traffic or inject ads. Exam questions typically test recognizing symptoms and choosing safe remediation steps instead of immediately reinstalling everything.

18. **Bring Your Own Device (BYOD)**
    B Y O D is an organization policy that allows personally owned devices to access company resources under defined rules. On the exam, it shows up as a governance and risk decision point, where acceptable use, access controls, and data protection requirements affect the recommended action.

19. **Buffer overflow**
    A buffer overflow is a software flaw where more data is written than a program expects, potentially causing crashes or enabling code execution. A+ tends to test it as a security concept you can recognize and classify, not as a deep exploit topic, and the decision is often patching and reducing exposure.

20. **Business continuity**
    Business continuity is the ability to keep essential services running during disruption, often supported by backups, redundancy, and recovery procedures. On the exam, it appears as choosing controls that reduce downtime and data loss and understanding why documentation and tested recovery steps matter.

11. **BIOS (Basic Input/Output System)**
    BIOS is firmware that initializes hardware during startup and starts the boot

process. On the exam, it shows up in boot failures, hardware detection issues, and settings like boot order or enabling/disabling onboard features.

12. **BitLocker**
    BitLocker is Windows full-disk encryption that protects data at rest if a device is lost or stolen. A+ questions often test when encryption is appropriate and why recovery keys and enterprise policy matter for support and data recovery.

13. **Bluetooth**
    Bluetooth is a short-range wireless technology used for peripherals such as headsets, keyboards, and mice. On the exam, it commonly appears in pairing and connectivity troubleshooting where you verify discoverable mode, profiles, interference, and that the radio is enabled.

14. **Boot order**
    Boot order is the priority list the system uses to decide which device to start from (internal drive, USB, network, etc.). Exam items use it as a "wrong-first-step" trap when the system keeps booting the wrong device or can't find a bootable OS.

15. **Bootable media**
    Bootable media is a USB drive or disc prepared with an installer or recovery environment that a PC can start from. On the exam, it matters for OS installs and repairs, and the key decision is choosing the right tool before taking invasive steps.

16. **Break-fix support**
    Break-fix is a support model where work happens after something fails, typically billed per incident. On A+, it can appear in operational procedure questions that compare support models, expectations, and documentation responsibilities.

17. **Browser hijacker**
    A browser hijacker is unwanted software that changes browser behavior like homepage, search provider, or extensions to redirect traffic or inject ads. Exam questions often test symptom recognition and safe remediation steps rather than immediately reinstalling the OS.

18. **Bring Your Own Device (BYOD)**
    BYOD is a policy that allows personally owned devices to access organizational resources under defined rules. On the exam, it shows up as a governance and risk decision where access controls, acceptable use, and data protection drive the recommended action.

19. **Buffer overflow**
    A buffer overflow is a software flaw where more data is written than a program expects, potentially causing a crash or enabling code execution. A+ typically tests it as a security concept to recognize and respond to with patching and risk reduction, not exploit development.

20. **Business continuity**
    Business continuity is the ability to keep critical operations running during and after a disruption. On the exam, it appears when choosing controls that reduce downtime and data loss, and when distinguishing continuity planning from simple backups.

21. **Cable tester**
    A cable tester checks whether a network or other cable is wired correctly and can carry signal end to end. On the exam, it's the "prove the physical layer" tool when symptoms point to bad terminations, broken pairs, or the wrong cable type.

22. **Cache**
    A cache is fast temporary storage that keeps frequently used data so systems can respond quicker. A+ questions use cache when troubleshooting performance, browsers, or applications, where clearing cache can fix stale data issues without changing core settings.

23. **CAPTCHA**
    A CAPTCHA is a challenge designed to separate humans from automated bots during sign-in or form submission. On the exam, it shows up as a security control that reduces automated abuse, and it can also appear as a user-experience friction point you must recognize.

24. **Category cable (Cat 5e/Cat 6/Cat 6a)**
    Category cable is twisted-pair Ethernet cabling rated for specific speeds and distances, with higher categories generally supporting higher performance. On the exam, it appears as a selection decision where the wrong cable choice creates speed drops, intermittent links, or failed runs.

25. **Certificate (digital certificate)**
    A digital certificate binds an identity to a public key so systems can support encryption and trust, commonly in TLS-secured connections. A+ questions often test what a certificate warning means and whether the right response is to verify trust and configuration rather than ignore it.

26. **Change management (change control)**
    Change management is the process of planning, approving, documenting, and

communicating changes to systems to reduce risk and outages. On the exam, it shows up when the “best” answer is to follow policy, get approval, and document outcomes instead of making an untracked fix.

27. **Chipset**
    A chipset is the set of controllers on a motherboard that helps manage communication between the CPU, memory, storage, and peripherals. Exam items use chipset concepts in compatibility and troubleshooting scenarios, where the right answer involves drivers, supported features, or board limitations.

28. **CMOS battery**
    A CMOS battery maintains system clock and firmware settings when power is removed. On the exam, it appears in symptoms like wrong time/date, lost BIOS settings, or boot configuration resets, where replacing the battery is the correct hardware fix.

29. **Command-line interface (CLI)**
    A CLI is a text-based way to run system tools and view configuration or status information. A+ questions use it to test tool selection, such as when command output is the fastest way to confirm IP settings, name resolution, or system integrity.

30. **Compression**
    Compression reduces file size by encoding data more efficiently, sometimes with lossless or lossy tradeoffs. On the exam, it shows up in storage and transfer decisions, where you must balance size, quality, compatibility, and performance impacts.

31. **CPU (Central Processing Unit)**
    The CPU is the main processor that executes instructions and coordinates work across the system. On the exam, it shows up in performance and compatibility questions, especially when symptoms point to thermal throttling, insufficient cores, or the wrong platform support.

32. **Crash dump (memory dump)**
    A crash dump is a saved snapshot of system memory and state taken when an operating system fails. On the exam, it matters because it’s evidence for troubleshooting, and the decision point is knowing when logs and dumps help confirm a driver, hardware, or OS-level root cause.

33. **Credential stuffing**
    Credential stuffing is an attack where stolen username and password pairs are tried across many sites to find reused credentials. On A+, it commonly appears as a

security scenario where the best response involves MFA, password resets, and recognizing that lockouts can be a sign of automated attempts.

34. **Default gateway**
    The default gateway is the router address a device uses to reach networks outside its local subnet. Exam questions use it to test whether you can distinguish "local network works" from "can't reach the internet," and to avoid confusing gateway issues with DNS issues.

35. **Device Manager**
    Device Manager is a Windows tool used to view hardware, driver status, and device error codes. On the exam, it's a go-to choice for troubleshooting missing devices, driver conflicts, and verifying whether a device is disabled or failing.

36. **DHCP (Dynamic Host Configuration Protocol)**
    DHCP automatically assigns IP configuration such as IP address, subnet mask, gateway, and DNS servers. On the exam, it's central to diagnosing "no network" problems, where the correct first step is often verifying the lease process before changing unrelated settings.

37. **Disk Management**
    Disk Management is a Windows utility for viewing disks, partitions, volumes, and basic formatting tasks. On the exam, it shows up when a drive is present but not usable, and the key confusion is "the disk exists" versus "it's not initialized, partitioned, or assigned a letter."

38. **DisplayPort**
    DisplayPort is a digital video interface commonly used on PCs and monitors, often supporting high resolutions and refresh rates. On the exam, it appears in display troubleshooting and adapter selection, where the wrong connector standard can cause no signal or limited capability.

39. **DNS (Domain Name System)**
    DNS translates human-friendly names (like a website) into IP addresses so devices can connect. A+ questions often test the difference between "internet is down" and "names won't resolve," where switching to an IP test or checking DNS settings is the correct move.

40. **Driver**
    A driver is software that lets the operating system communicate correctly with hardware like a GPU, NIC, or printer. On the exam, it's a frequent root cause for

instability and missing features, and the decision point is whether to update, roll back, or reinstall based on what changed.

41. **EDR (Endpoint Detection and Response)**
    EDR is a security capability that monitors endpoint activity to detect suspicious behavior and support investigation and response. On the exam, it shows up as a "best control" choice when basic antivirus is not enough and when visibility and containment are needed.

42. **EFS (Encrypting File System)**
    EFS is a Windows feature that encrypts individual files or folders using user-based keys. On the exam, it's often compared to full-disk encryption, and the key decision is understanding when per-file protection is useful versus when whole-drive protection is required.

43. **Electrostatic discharge (ESD)**
    ESD is a sudden flow of static electricity that can damage sensitive computer components. A+ questions frequently test correct safety practices—like grounding and using an anti-static strap—because ignoring ESD is a common "trap" answer.

44. **Event Viewer**
    Event Viewer is a Windows tool that displays system, application, and security logs. On the exam, it's a high-value troubleshooting step because it provides evidence, and it helps you choose the next action based on specific error patterns rather than guessing.

45. **ExFAT (Extended File Allocation Table)**
    ExFAT is a file system designed for removable media with broad cross-platform support and fewer limits than older FAT variants. On the exam, it often appears in "best choice for a USB drive used on multiple operating systems" scenarios.

46. **FAT32 (File Allocation Table 32)**
    FAT32 is an older file system with broad compatibility but strict limits such as a 4 GB maximum single file size. A+ questions use it as a common confusion point when a large file won't copy to a flash drive.

47. **Firmware**
    Firmware is low-level software stored on hardware (like a motherboard, router, or SSD) that controls basic device operation. On the exam, it shows up in stability, compatibility, and security scenarios where updating firmware can fix issues—but also carries risk if done improperly.

48. **Firewall**
    A firewall is a control that allows or blocks network traffic based on rules such as ports, protocols, addresses, or applications. On the exam, it's often the correct explanation for "service works locally but not remotely," and the key is selecting the right rule change without opening unnecessary access.

49. **GPUPDATE**
    GPUPDATE is a Windows command that refreshes Group Policy settings without waiting for the normal update cycle. A+ questions use it in domain-managed environments where settings are not applying, and it tests whether you recognize policy-driven behavior versus local misconfiguration.

50. **GPT (GUID Partition Table)**
    GPT is a modern disk partitioning scheme that supports large disks and more partitions than MBR, and it's commonly used with UEFI. On the exam, it appears in installation and boot scenarios where selecting GPT vs MBR affects compatibility and boot behavior.