CompTIA A+ (220-1201 / 220-1202 (V15)) — One-Page Study Guide

BareMetalCyber.com | Cybersecurity Audio Academy
baremetalcyber.com/cybersecurity-audio-academy

A) Exam Snapshot

- **Issuer:** CompTIA | **Target level:** Beginner / entry-level IT support
- **Exams:** Core 1 (220-1201) + Core 2 (220-1202) — pass both for certification
- **Time limit:** 90 minutes per exam | **Max questions:** 90 per exam
- **Question types:** multiple-choice (single & multiple response), drag-and-drop, performance-based questions (PBQs)
- **Scoring:** scaled 100–900 | **Pass:** 675 (Core 1), 700 (Core 2)

B) Domain Weights

Domain (Core 1 — 220-1201)	Weight
Mobile devices	13%
Networking	23%
Hardware	25%
Virtualization & cloud computing	11%
Hardware & network troubleshooting	28%

Domain (Core 2 — 220-1202)	Weight
Operating systems	28%
Security	28%
Software troubleshooting	23%
Operational procedures	21%

C) Core Workflow (How the exam thinks)

- Identify the problem: gather symptoms, environment, and recent changes; confirm the scope.
- Establish a theory of probable cause; start broad, then narrow with one purposeful test.
- Test the theory to determine the cause; use the result to rule options in or out.
- Plan the fix: choose the least risky next step; consider downtime, data loss, and escalation.
- Implement the solution (or escalate) and record what changed (settings, parts, versions).
- Verify full functionality and apply preventive measures (updates, security baseline, backups).
- Document findings, actions taken, outcomes, and user confirmation in the ticket.

D) High-Yield Concepts

- Hardware basics: CPU vs RAM vs storage, form factors, expansion, and common failure symptoms.
- Storage: HDD vs SSD vs NVMe; partition style (MBR vs GPT); file systems (NTFS vs exFAT).
- Cables & connectors: USB-C vs USB-A, HDMI vs DisplayPort, RJ45 vs fiber, power and adapters.
- Printers: laser vs inkjet, consumables, calibration, jams, and common print quality defects.
- Networking: IP addressing, subnetting basics, DHCP vs DNS, NAT, VPN, VLAN concepts, and SOHO gear.
- Wireless: 2.4 GHz vs 5/6 GHz tradeoffs; Wi■Fi standards; WPA2/WPA3; roaming and interference.
- Virtualization & cloud: hypervisor/VM concepts; resource allocation; snapshots; IaaS/PaaS/SaaS.
- Operating systems: install/upgrade paths, drivers, updates, recovery tools, and account types.
- Windows tools to recognize: Task Manager, Device Manager, Disk Management, Event Viewer, Services.
- Security: least privilege, MFA, encryption, malware types, secure authentication, and safe disposal.
- Troubleshooting mindset: isolate layer (power, hardware, OS, network, app); prove root cause before big changes.
- Operational procedures: change control, documentation, professionalism, and safety (ESD, hazards).

E) Common Traps

- Missing the command word: *best* vs *first* vs *most likely* changes the right answer.
- Skipping safety: no ESD control, no power removal, or no data protection before invasive work.
- Confusing DHCP vs DNS symptoms (no IP vs no name resolution) and choosing the wrong first fix.
- Treating Wi■Fi issues as internet issues: separate client, access point, and upstream provider.
- Overusing “reinstall/reset” before checking logs, rollback options, safe mode, or known-good parts.
- Mixing up authentication vs authorization (sign-in vs permissions) in access and security scenarios.
- Forgetting physical basics: wrong display input, loose cable, disabled NIC, airplane mode, muted mic.
- Selecting a tool that doesn’t test the hypothesis (doing work that won’t change the uncertainty).

F) Cheat Sheet (commands / ports / artifacts)

- Ports to recognize: DNS 53; DHCP 67/68; HTTP 80; HTTPS 443; RDP 3389; SMB 445; SSH 22; SMTP 25; IMAP 143; POP3 110; FTP 20/21.
- Wi■Fi quick rule: 2.4 GHz favors range; 5/6 GHz favors speed; interference favors channel planning.
- Network CLI: *ipconfig*/*ifconfig*, *ping*, *tracert*/*traceroute*, *nslookup*/*dig*, *netstat*, *arp*.
- Windows repair: *chkdsk*, *sfc*, *DISM*, recovery environment, restore points, safe mode.
- Disk concepts: MBR vs GPT; NTFS vs exFAT; encryption basics (BitLocker/FileVault) and recovery keys.
- Printer essentials: replace consumables first when indicated; then calibrate/clean; then check driver/spooler.
- Cable sanity: match connector + standard (USB/Thunderbolt/video); confirm power rating and orientation.
- User/account basics: standard vs admin rights; local vs domain; UAC prompts; password and lockout flow.
- Security defaults: update first, least privilege, strong authentication, verify cert/wireless settings.
- Ticket notes: symptom, scope, steps tried, fix applied, validation result, and user sign■off.

G) Exam-Day Tactics

- Plan two sittings: treat Core 1 and Core 2 as separate tests with separate weak spots.
- PBQs: read the required end state, do the quick wins first, then move on before time drains.
- First pass: answer the sure questions quickly; flag anything slow or ambiguous for later.
- Use elimination: remove answers that don’t address the symptom, violate safety, or ignore constraints.
- Watch for small mismatches: Mbps vs MBps, 32■bit vs 64■bit, 2.4 vs 5/6 GHz, user vs admin.
- When stuck, pick the least invasive next step that gathers evidence or reduces risk.
- Keep a review buffer: reserve the last 10–15 minutes to revisit flags and PBQs.
- Re-read the last line before submitting: confirm the question you answered is the one asked.

H) 30-Minute Final Review Plan

- 5 min: ports, protocols, and Wi■Fi security (WPA2/WPA3, bands, common symptoms).
- 5 min: CompTIA troubleshooting flow and “tool matches the hypothesis” discipline.
- 5 min: Windows utilities + what each is used for (Task Manager, Event Viewer, Disk Management).
- 5 min: hardware quick hits (storage types, connectors, display basics, printer issues).
- 5 min: security and ops basics (least privilege, MFA, encryption, ESD, documentation).

Source: official exam objectives & exam details. Quick review only; practice required.