VPWEB.DEV · STUDY PLAN

CompTIA A+

Exam 220-1201 & 220-1202 (V15)

CompTIA A+ is the industry-standard entry credential for IT support. It is two exams — Core 1 (220-1201) and Core 2 (220-1202) — and you must pass both. This plan breaks down every domain, gives you a realistic schedule, and packs the reference material you will rely on most.

Exam at a glance

EXAMS	Two — Core 1 (220-1201) + Core 2 (220-1202). Both required.
PASSING SCORE	Core 1: 675 / 900 · Core 2: 700 / 900 (scale 100–900)
LENGTH	Up to 90 questions, 90 minutes, per exam
QUESTION TYPES	Multiple choice (single/multi) + performance-based (PBQs)
COST (APPROX.)	·$253 USD per exam voucher — check CompTIA for current pricing
RETAKE POLICY	2nd attempt immediate; 14-day wait before a 3rd attempt
VALIDITY	Good for 3 years; renew with continuing education (CE)
BEST FOR	Help desk, desktop support, field service technician

Every domain, in depth

CORE 1 · DOMAIN 1 — 13%

Mobile Devices

Laptops and mobile hardware, displays, accessories, and connectivity.

- Install/replace laptop hardware: battery, keyboard, RAM, storage, wireless cards
- Laptop display components: LCD vs OLED, webcam, microphone, digitizer, Wi-Fi antenna
- Accessories & ports: USB-C, Lightning, NFC, docking stations, touch pens
- Mobile connectivity: cellular (4G/5G), Bluetooth pairing, hotspot/tethering, airplane mode
- Account & app configuration and synchronization (corporate vs personal email)

CORE 1 · DOMAIN 2 — 23%

Networking

Ports, protocols, hardware, wireless, and SOHO network configuration.

- TCP/UDP ports & protocols (see cheat sheet) — know them cold
- Hardware: routers, switches, access points, firewalls, modems, PoE, patch panels
- Wireless: 802.11 a/b/g/n/ac/ax, 2.4/5/6 GHz bands, channels, WPA2/WPA3
- Services: DNS, DHCP, NTP, and common server roles
- IP addressing: static vs dynamic, APIPA, subnet mask, default gateway, IPv4 vs IPv6
- Internet connection types: fiber, cable, DSL, satellite, cellular/WISP
- Tools: cable tester, crimper, punchdown, toner probe, loopback plug

CORE 1 · DOMAIN 3

25%

Hardware

The physical components — cables, RAM, storage, motherboards, power, printers.

- Cables & connectors: USB, SATA, RJ45, fiber, HDMI, DisplayPort, Thunderbolt
- RAM: DDR3/DDR4/DDR5, SODIMM, ECC vs non-ECC, single/dual/quad channel
- Storage: HDD (5400/7200 RPM), SSD (SATA, M.2, NVMe), RAID 0/1/5/10
- Motherboards & CPUs: ATX/ITX form factors, sockets, BIOS/UEFI, CMOS, x64 vs ARM
- Power supplies: wattage, connectors, modular vs non-modular, redundancy
- Printers: laser imaging process (7 steps), inkjet, thermal, impact, 3D + maintenance

CORE 1 · DOMAIN 4

11%

Virtualization & Cloud Computing

Cloud service/deployment models and client-side virtualization.

- Service models: IaaS, PaaS, SaaS — who manages what
- Deployment models: public, private, hybrid, community
- Cloud characteristics: shared/elastic resources, metered usage, high availability, file sync
- Client-side virtualization: purpose (sandbox, test, legacy), Type 1 vs Type 2 hypervisors
- Resource requirements: CPU virtualization support, RAM, storage, networking

CORE 1 · DOMAIN 5

28%

Hardware & Network Troubleshooting

The biggest domain — diagnosing failures with a repeatable method.

- The six-step troubleshooting methodology (see cheat sheet) — tested directly
- Motherboard/RAM/CPU/power: no power, no POST, beep codes, overheating, swelling
- Storage & RAID: clicking, SMART failures, RAID not found, slow performance
- Display/video: dim, flickering, dead pixels, no image, artifacts
- Mobile: battery/charging, overheating, broken digitizer, poor connectivity
- Printers: paper jams, ghosting/streaks, low quality, network printing
- Networks: intermittent connectivity, high latency, limited/no connectivity

CORE 2 · DOMAIN 1

28%

Operating Systems

Windows-heavy — editions, tools, command line, plus macOS and Linux.

- Windows editions: Home, Pro, Pro for Workstations, Enterprise
- Command line: ipconfig, ping, tracert, netstat, nslookup, chkdsk, sfc, gpupdate, diskpart
- Tools: Task Manager, MSConfig, regedit, services.msc, MMC, Event Viewer, perfmon
- Control Panel vs Settings; user/group management; Windows networking (workgroup vs domain)
- Install/upgrade: boot methods, clean vs in-place, partitioning (GPT/MBR), file systems
- File systems: NTFS, exFAT, FAT32, ext4, APFS
- macOS: Time Machine, Mission Control, Keychain, Disk Utility; Linux: ls, cd, chmod, sudo, apt/yum, grep

CORE 2 · DOMAIN 2

28%

Security

Physical and logical security, malware, social engineering, and best practices.

- Physical security: locks, badges, biometrics, access control vestibule, bollards
- Logical security: MFA, least privilege, ACLs, hard/soft tokens, group policy
- Wireless security: WPA2/WPA3, AES, RADIUS, TACACS+
- Malware: virus, worm, trojan, ransomware, rootkit, keylogger, spyware, botnet, cryptominer
- Social engineering & attacks: phishing/vishing, tailgating, shoulder surfing, DDoS, on-path, zero-day, SQL injection, XSS
- Best practices: password policy, account management, end-user education
- Data destruction: shredding, degaussing, wiping, recycling; SOHO + browser security

CORE 2 · DOMAIN 3

23%

Software Troubleshooting

Diagnosing OS, security, and mobile software problems.

- Windows problems: BSOD, slow boot/performance, services failing, profile issues
- Malware removal: the seven-step process (see cheat sheet)
- Mobile OS/app issues: crashing, battery drain, slow performance, connectivity
- Mobile security issues: data leaks, unauthorized access, fake/leaked notifications

CORE 2 · DOMAIN 4

21%

Operational Procedures

The professional, process, and safety side of IT — easy points if you read it.

- Documentation: knowledge base, network diagrams, SOPs, AUP, incident reports
- Change management: request forms, scope, risk analysis, rollback plan, approvals
- Backups: full, incremental, differential, synthetic; the 3-2-1 rule
- Safety: ESD straps/mats, equipment grounding, lifting, fire safety
- Environment: temperature/humidity, SDS sheets, proper disposal of batteries/toner
- Incident response: chain of custody, first response, documentation
- Communication, professionalism, basic scripting (.bat/.ps1/.sh/.py), remote access (RDP/VPN/SSH/RMM)

Week-by-week study plan

Weeks 1–2 Core 1: Hardware + Mobile Devices	• Study components, RAM, storage, cables • Daily flashcards (RAID, connectors, RAM types) • Open a real PC — identify every part
Weeks 3–4 Core 1: Networking + Virtualization & Cloud	• Memorize the ports table cold • Learn wireless standards and IP addressing • Build a SOHO network / VM lab
Week 5 Core 1: Troubleshooting + exam	• Drill the 6-step methodology • Practice exams until consistently ≥ 90% • Book and pass Core 1 (220-1201)
Weeks 6–7 Core 2: Operating Systems + Software Troubleshooting	• Windows tools and command line • Install Windows + a Linux distro in VMs • Practice the malware-removal steps
Weeks 8–9 Core 2: Security + Operational Procedures	• Malware types, social engineering, best practices • Read operational procedures carefully (easy points) • Domain-by-domain practice questions
Week 10 Core 2: Review + exam	• Full-length practice exams to ≥ 90% • Review weakest domains • Book and pass Core 2 — you are A+ certified

Cheat sheets

COMMON PORTS

PORT	SERVICE
20/21	FTP
22	SSH / SFTP
23	Telnet
25	SMTP
53	DNS
67/68	DHCP
80	HTTP
110	POP3
143	IMAP
161/162	SNMP
389	LDAP
443	HTTPS
445	SMB
3389	RDP

RAID LEVELS

RAID 0 Striping — speed, no redundancy (min 2 disks)

RAID 1 Mirroring — full redundancy (min 2 disks)

RAID 5 Striping with parity — 1 disk fault tolerance (min 3)

RAID 10 Mirror + stripe — speed and redundancy (min 4)

TROUBLESHOOTING METHODOLOGY

1. Identify the problem (and back up data first)
2. Establish a theory of probable cause
3. Test the theory to determine cause
4. Establish a plan of action & implement the solution
5. Verify full system functionality + preventive measures
6. Document findings, actions, and outcomes

MALWARE REMOVAL (7 STEPS)

1. Investigate and verify malware symptoms
2. Quarantine the infected system
3. Disable System Restore (Windows)
4. Remediate: update anti-malware, scan and remove
5. Schedule scans and run updates
6. Enable System Restore & create a restore point
7. Educate the end user

Acronyms to know

PBQ
Performance-Based Question

POST
Power-On Self-Test

UEFI
Unified Extensible Firmware Interface

NVMe
Non-Volatile Memory Express

SATA
Serial ATA

ECC
Error-Correcting Code

PoE
Power over Ethernet

APIPA
Automatic Private IP Addressing

DHCP
Dynamic Host Configuration Protocol

DNS
Domain Name System

NTFS
New Technology File System

MFA
Multi-Factor Authentication

UAC
User Account Control

RDP
Remote Desktop Protocol

VPN
Virtual Private Network

SODIMM
Small Outline Dual In-line Memory Module

IaaS
Infrastructure as a Service

SaaS
Software as a Service

ESD
Electrostatic Discharge

SDS
Safety Data Sheet

Recommended resources

- **Professor Messer** — free, complete video course covering every objective. Start here.
- **Practice exams** — the one paid resource worth buying; drill to a consistent 90% on fresh questions before booking (Jason Dion's are a community favorite).
- **Official CompTIA objectives PDF** — the literal exam blueprint; use it as your master checklist.
- **Hands-on labs** — VMs, a home lab, and real devices make concepts stick far better than reading alone.
- **Flashcards (Anki)** — for ports, acronyms, commands, and definitions via active recall.

The winning formula: follow the objectives top to bottom, get hands-on, and don't book the exam until you're consistently scoring 90%+ on fresh practice tests. For the full written walkthrough and career guidance, visit **vpweb.dev/blog**.