

IT SUPPORT CERTIFICATION

CompTIA A+

240+ High-Yield Terms & Concepts for Core 1 (220-1201) and Core 2 (220-1202): the two-exam V15 certification - up to 90 questions and 90 minutes per exam, passing at 675 (Core 1) and 700 (Core 2) on the 900 scale - covering mobile devices, networking, hardware, virtualization and cloud, hardware and network troubleshooting, operating systems, security, software troubleshooting, and operational procedures, each concept with key facts, a strategy tip, and a worked example



TemplateForge

IT Support Certification Series

240+ High-Yield Terms & Concepts for the 220-1201 (Core 1) and 220-1202 (Core 2) Exams

Price: \$29 | **Format:** Markdown + PDF Workbook

Category: IT Support Certifications (CompTIA A+, Core 1 220-1201, Core 2 220-1202)

Design: Slate steel blue

Important Disclaimer: This guide is an independent study aid. It is NOT affiliated with, endorsed by, or sponsored by CompTIA or any of CompTIA's programs. A+, Core 1, Core 2, and 220-1201/220-1202 refer to CompTIA's certification exams. Exam structure, content, scoring, fees, and policies can change - confirm current details on the official CompTIA website before registering.

How to Use This Guide

The CompTIA A+ certification is the entry-level credential for IT support roles such as help desk technician and technical support specialist. It is earned by passing TWO exams from the SAME exam series: Core 1 (220-1201) and Core 2 (220-1202), exam version V15, which launched March 25, 2025. Each exam has a maximum of 90 questions - multiple-choice, drag-and-drop, and performance-based - and 90 minutes on the clock. Core 1 passes at 675 on a 100-900 scale; Core 2 passes at 700. Both exams must be taken from the same version - no mixing old and new series. The certification is valid for 3 years and renews through CompTIA's CEU program (A+ requires 20 CEUs per cycle), by retaking current exams, or by earning a higher-level certification. This guide maps both exams the way they actually run. Part 1 covers the rules of the test itself: the two-exam structure, question types, scoring, domains, and renewal. Parts 2-4 cover Core 1 networking and mobile devices; Parts 5-7 cover Core 1 hardware; Part 8 covers virtualization and cloud; Part 9 covers Core 1 troubleshooting. Parts 10-12 cover Core 2 operating systems (Windows, macOS, Linux, mobile); Part 13 covers Core 2 security; Parts 14-16 cover software troubleshooting and operational procedures. Each concept pairs key facts with a strategy tip and a worked example, so the same page works for a first pass and a last-week review. Honest positioning: this is an independent study aid, NOT approved, endorsed, or produced by CompTIA. The official CompTIA exam objectives, the A+ page at [comptia.org](https://www.comptia.org), and the test-delivery partner (Pearson VUE) are the ground truth for everything administrative - domain percentages, fees, scheduling, and retirement dates change, so confirm them before you register.

Part 1: The A+ Certification & How It Works (17 Concepts)

High-yield domain terms from the Core 2 objectives that appear in exam questions.

#	Term	Key Facts	Strategy Tip	Example
1	CompTIA A+	Vendor-neutral entry-level IT certification requiring two exams from the same series: Core 1 (220-1201) and Core 2 (220-1202), V15, launched March 25 2025.	Treat A+ as the first rung on the CompTIA ladder - Network+ and Security+ build directly on it.	A help desk candidate passes both A+ exams, then studies Network+ for the same job family.
2	Core 1 (220-1201)	Hardware-focused exam: mobile devices, networking, hardware, virtualization and cloud, and hardware/network troubleshooting. Pass mark 675 on a 900 scale.	Study the five Core 1 domains in exam-weight order: troubleshooting (28%) and hardware (25%) first.	A candidate drills hardware and troubleshooting because they make up over half of Core 1.
3	Core 2 (220-1202)	Software-focused exam: operating systems, security, software troubleshooting, operational procedures. Pass mark 700 on a 900 scale.	OS and security are each 28% of Core 2 - give them the most review time.	Core 2 prep spends equal top weight on Windows administration and security fundamentals.
4	Same-version rule	Core 1 and Core 2 must be taken from the SAME exam version; mixing exam series (like 220-1101 with 220-1202) is not allowed.	Before registering for the second exam, confirm both vouchers match the 220-1200 series.	A candidate who started v14 must take both exams in v15 - not one in each.
5	Maximum of 90 questions	Each A+ exam can contain up to 90 questions: single-response and multi-response multiple choice, drag-and-drop, and performance-based questions (PBQs).	Budget roughly one minute per question; flag hard items and return if time remains.	A 90-minute exam at 90 questions gives about one minute per item before review time.
6	Performance-based questions	PBQs ask you to apply skill in a simulated environment: configure a network, order troubleshooting steps, or set up a device.	PBQs are often worth more time - attempt them first while the scenario is fresh.	A PBQ shows a Wi-Fi router screen and asks you to apply the correct encryption settings.
7	90-minute length	Each exam runs 90 minutes		

Use the on-screen review flag.

8	CompTIA A+ Study Guide	Passing scores	Core 1 passes at 675 and Core 2 passes at 700, both on a 100-900 scale. Scores are scaled, not raw percentages.	Do not assume both exams pass at the same number - Core 2 is the higher bar.	A 690 on Core 1 passes, while the same 690 on Core 2 fails because Core 2 needs 700.
		Recommended experience	CompTIA recommends about 12 months of hands-on experience in an IT support or help desk role before the exams.	Experience is recommended, not required - classroom or self-study candidates can still sit.	A college student with a home lab builds a year of practice before booking either exam.
10		Exam languages	Both exams are offered in English, German, and Japanese.	Choose the language you read fastest under time pressure, not your first language automatically.	A bilingual candidate sits the English version because they trained in English terms.
11		Retirement estimate	CompTIA usually retires an exam version three years after launch; the 220-1200 series is estimated to retire around 2028.	Plan to finish both exams well before any retirement date if you need the current objectives.	A candidate who delays 18 months still has time, but checks comptia.org for the current version.
12		Pearson VUE delivery	A+ exams are administered at Pearson VUE test centers (and online proctoring in some regions).	Book early - busy test centers fill weeks ahead before student deadlines.	A candidate schedules both exams on Pearson VUE, reserving Core 1 two weeks before Core 2.
13		3-year validity	The A+ certification expires three years after the date the certification is obtained (the later exam date).	Put a renewal reminder on your calendar the day you pass the second exam.	Someone certified in 2026 plans a 2029 renewal through CEUs or a current-exam retake.
14		CEU renewal	Renew by earning Continuing Education Units: A+ requires 20 CEUs across the three-year cycle, plus a maintenance fee.	Track CEUs in CompTIA's portal as you earn them, not the month before renewal.	A certified tech earns CEUs from vendor training and submits them to renew A+ without retesting.
15		Alternative renewals	Renew by retaking the current A+ exams, or by earning a higher-level CompTIA certification that covers A+.	If you plan Network+ anyway, it can renew A+ and is often the cheaper path.	A tech passes Network+ and never pays a separate A+ maintenance fee that cycle.
16		ANSI accreditation	The A+ program is accredited against ISO/IEC 17024 by the American National Standards Institute (ANSI).	You can state A+ is ANSI-accredited in a resume summary - it is a verified fact.	A job post asks for a vendor-neutral credential; the ANSI accreditation supports A+.
17		DoD 8140 roles	A+ maps to U.S. DoD 8140 approved work roles: technical support specialist, system administrator, and cyber defense infrastructure support.	Government-contract job hunters should list the matching DoD 8140 role names.	A cleared technician matches A+ to the technical support specialist work role in a job application.

Part 2: Core 1 - Mobile Devices (14 Concepts)

High-yield domain terms from the Core 1 objectives that appear in exam questions.

#	Term	Key Facts	Strategy Tip	Example
18	Mobile device hardware	Laptop and tablet internals: replaceable batteries, cameras, Wi-Fi and Bluetooth antennas, and add-on storage.	Know which laptop parts are field-serviceable (RAM, storage, battery) versus soldered.	A tech swaps a laptop's M.2 SSD and RAM while the CPU stays soldered to the board.
19	Battery management	Lithium-ion batteries degrade by charge cycles and heat; calibrate by full discharge only when the vendor asks.	Keep laptops cool and avoid leaving them at 100% for months to extend battery life.	A fleet of docks runs cool and is charged to 80%, doubling average battery lifespan.
20	Wi-Fi/Bluetooth antennas	Laptops hide antenna wires along the display bezel for Wi-Fi and Bluetooth signals.	Reconnect antennas after display work - a loose wire explains a sudden Wi-Fi drop.	After replacing a laptop screen, the tech reseats the two antenna leads and Wi-Fi returns.
21	USB ports on mobile	Laptops and tablets use USB-A and USB-C for data, charging, and docking; USB-C also carries video over alternate mode.	Check cable and port standards before assuming a device is broken - USB versions matter.	A USB-C laptop needs a DisplayPort-capable USB-C cable to drive an external monitor.
22	Bluetooth pairing	Short-range wireless pairing under 30 feet; pairs keyboards, mice, headsets, and phones.	Remove and re-pair a stubborn device instead of fighting driver settings blindly.	A wireless mouse stops responding; the tech removes the pairing and re-pairs it in 30 seconds.
23	NFC	Near-field communication works at under a few centimeters for taps: payments, tags, and pairing.	Enable NFC for tap-to-pair accessories and mobile payments on supported phones.	A phone taps a payment terminal; NFC completes the transaction in seconds.
24	Docking stations	A dock adds ports (video, Ethernet, USB) through one connection and manages external displays and charging.	For mismatched display behavior, update dock firmware first - it fixes most port quirks.	A dock powers the laptop, two monitors, and a wired network from a single USB-C cable.
25	Mobile network setup	Configure cellular data, Wi-Fi, Bluetooth, and synchronization		

Use airplane mode to isolate a cell-data problem from Wi-Fi

A tablet fails to sync; the tech
toggles cellular data and

Match sync frequency to

27	MDM	Mobile Device Management: enrolls company devices, pushes policies, and can wipe lost units remotely.	Name the MDM feature set: enrollment, policy, app control, and remote wipe in answers.	A lost company phone is remotely wiped through MDM within minutes of the report.
28	BYOD vs corporate-owned	Bring-your-own-device and corporate-owned models differ in policy control, app management, and separation of personal data.	On exam questions, pick answers that separate work data policies from personal use.	A BYOD phone gets a work profile (container) so personal apps stay outside company policy.
29	Mobile anti-malware	Mobile security apps scan apps, block malicious links, and help manage app permissions.	On mobile, review app permissions, not just the antivirus, for real risk.	A phone asks for SMS access; the tech denies it because the app only needs storage.
30	Laptop batteries and chargers	Match voltage and connector type; USB-C PD (power delivery) charges many modern laptops.	Never force a different-brand barrel charger into a port - voltage mismatches can damage boards.	A traveler borrows a USB-C PD charger rated for the laptop wattage and charges safely.
31	Mobile print options	Print from phones via Wi-Fi Direct, vendor cloud print, and NFC tap-to-print on supported printers.	Use Wi-Fi Direct for one-off printing without putting the phone on the office network.	A sales rep prints a receipt by tapping the phone to the printer's NFC pad.

Part 3: Core 1 - Networking Part 1: Protocols & Ports (16 Concepts)

High-yield domain terms from the Core 1 objectives that appear in exam questions.

#	Term	Key Facts	Strategy Tip	Example
32	TCP vs UDP	TCP is connection-oriented with guaranteed delivery; UDP is fast, connectionless, and loss-tolerant.	Match the protocol to the job: files need TCP, streaming and VOIP use UDP.	Video call audio runs over UDP so a dropped packet becomes a blip, not a stall.
33	Port 20/21 - FTP	FTP transfers files on port 21 (control) and 20 (data) in plaintext - no encryption by default.	Prefer FTPS or SFTP in answers where security matters; port 21 marks plaintext FTP.	A legacy device only supports FTP on port 21, so the tech wraps it in a VPN.
34	Port 22 - SSH	Secure Shell: encrypted remote administration and secure file transfer (SFTP rides on 22).	Port 22 is the safe remote-management answer versus plaintext Telnet on 23.	An admin manages a Linux server over SSH from a laptop on the same LAN.
35	Port 23 - Telnet	Legacy plaintext remote terminal protocol - unencrypted and discouraged.	Flag Telnet as insecure; any modern answer uses SSH instead.	A router still offers Telnet; the tech disables it and enables SSH.
36	Port 25 - SMTP	Simple Mail Transfer Protocol: sending mail between servers on port 25.	SMTP is for sending; receiving uses POP3 or IMAP mailboxes.	An email server relays outbound mail to another server on port 25.
37	Port 53 - DNS	Domain Name System resolves names to IP addresses on UDP (and TCP for large transfers).	A name-resolution failure answers point back to port 53 / DNS servers.	Typing a web address fails; the tech checks the DNS server setting and the 53 traffic.
38	Port 80 - HTTP	Hypertext Transfer Protocol: unencrypted web traffic.	Any web answer favoring security steers to HTTPS on 443 instead of 80.	A legacy dashboard is served over HTTP; a tech puts it behind HTTPS.
39	Port 443 - HTTPS	HTTP over TLS: encrypted web traffic and the default for modern sites.	443 is the safe web answer; when a site must be secure, choose 443.	An online store encrypts all checkout traffic over port 443.
40	Port 110 - POP3	Post Office Protocol v3: downloads mail to the local client; copies typically leave the server.	POP3 fits single-device mail; IMAP (143) is the multi-device answer.	A home user reads mail on one PC; POP3 keeps the mailbox small on the server.
41	Port 143 - IMAP	Internet Message Access Protocol: mail stays on the server and syncs across devices.	Choose IMAP whenever the user needs the same inbox on phone and desktop.	A sales rep reads the same inbox on laptop and phone through IMAP.
42	Port 3389 - RDP	Remote Desktop Protocol: Windows remote GUI access on 3389.	RDP is the Windows remote-desktop answer; enable it only when needed and change defaults.	A tech supports a user remotely by connecting over RDP to the workstation.
43	Port 445/139 - SMB	Server Message Block: Windows file and printer sharing (445 modern, 139 NetBIOS legacy).	File-sharing questions point to SMB; check if the question wants the modern port.	A mapped drive serves documents over SMB from a Windows file server.
44	Port 123 - NTP	Network Time Protocol keeps device clocks synchronized on UDP 123.	Clock skew breaks authentication - point to NTP when logins fail across servers.	A workstation's time drifts; NTP resyncs it so Kerberos tickets validate.
45	Port 161 - SNMP	Simple Network Management Protocol: monitoring network devices on UDP 161.	SNMP is the management-and-monitoring answer in network questions.	A switch reports interface errors to a monitoring tool via SNMP.
46	Ports 389/636 - LDAP/LDAPS	Lightweight Directory Access Protocol for directory lookups; 636 is the TLS-encrypted		

Choose LDAPS (636) over LDAP when credentials cross the wire.	A help desk validates user accounts against the directory over LDAPS.
---	---

47	CompTIA A+ Study Guide	DHCP	Dynamic Host Configuration Protocol hands out IP address, subnet mask, gateway, and DNS on UDP 67/68.	When a device has no valid IP (169.254), the first fix is checking DHCP.	A new laptop joins Wi-Fi and pulls an address, gateway, and DNS automatically from DHCP.
----	------------------------	------	---	--	--

Part 4: Core 1 - Networking Part 2: SOHO, Wireless & Tools (16 Concepts)

High-yield domain terms from the Core 1 objectives that appear in exam questions.

#	Term	Key Facts	Strategy Tip	Example
48	Router	Forwards packets between networks, serves as the gateway, and usually hosts DHCP and NAT at home or small office.	Label the router as the gateway-plus-DHCP device in SOHO topology answers.	A home router gives every device an address and sends traffic to the internet.
49	Switch	Connects devices on the same LAN, forwarding frames by MAC address.	Switches extend LAN ports; routers move between networks - keep the two separate.	Four desktops plug into a switch that uplinks to the router.
50	Access point	Bridges wireless clients onto the wired network using SSIDs and encryption.	In a wireless question, the access point is the device that actually serves Wi-Fi.	An office installs an access point so a conference room gets Wi-Fi coverage.
51	SOHO network design	Small office/home office topology: modem to router to switch to devices, with wired and wireless segments.	Draw the flow modem - router - switch - devices to answer topology questions fast.	A home network runs modem gateway router switch, then two PCs wired and phones on Wi-Fi.
52	IP addressing	IPv4 32-bit dotted decimal plus subnet mask; private ranges 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16.	Private ranges are the 'inside' answer; the internet side gets a public address.	A home LAN uses 192.168.1.x; the WAN side uses the ISP's public address.
53	APIPA 169.254	Automatic Private IP Addressing: when DHCP fails, Windows self-assigns 169.254.x.x, meaning no server answered.	Seeing 169.254 means 'check DHCP,' not 'restart the browser.'	A user has no internet; ipconfig shows 169.254.x.x, so the tech checks the DHCP service.
54	IPv6 basics	128-bit addressing with a global unicast prefix, link-local fe80::/10 addresses, and no NAT by default.	Link-local fe80 answers local-communication questions; global addresses route publicly.	Two PCs on a LAN use fe80 addresses to talk without any router.
55	VPN	Virtual Private Network encrypts traffic in a tunnel between a remote client and the office network.	VPN is the remote-worker security answer for using office resources from home.	A field tech connects over VPN, then reaches the file server securely.
56	Wi-Fi standards	802.11ax (Wi-Fi 6) and later are current; 802.11ac (Wi-Fi 5) and older still appear in legacy networks.	Match the fastest standard the device supports - both ends must share it.	A Wi-Fi 6 laptop on an 802.11ax router negotiates the fastest link.
57	2.4 vs 5 vs 6 GHz	2.4 GHz reaches farther with more interference; 5 and 6 GHz are faster with shorter range.	For speed choose 5/6 GHz; for range through walls choose 2.4 GHz.	A desktop far from the router uses 2.4 GHz; a laptop near it uses 5 GHz.
58	Wireless security	WPA3 is current; WPA2 is the legacy minimum - never WEP or open networks.	Security answers pick the strongest supported option shared by all clients.	An office with old printers stays on WPA2; a new deployment chooses WPA3.
59	SSID	Service Set Identifier: the visible network name clients select.	Hide the SSID only as a minor control - it is not real security.	A guest network broadcasts its own SSID with separate credentials.
60	PoE	Power over Ethernet delivers power and data over one cable to devices like access points and cameras.	PoE answers: one cable for power plus data; check the switch provides PoE.	A ceiling access point is powered entirely by its Ethernet cable via PoE.
61	VLAN	Virtual LAN segments traffic logically on one switch, isolating groups without extra hardware.	VLANs separate voice, data, and guests - isolation without new switches.	A switch splits office traffic and guest traffic onto two VLANs on one device.
62	Network tools	Crimpers terminate cable ends; cable testers certify wiring; Wi-Fi analyzers find interference and channel use.	Match the tool to the symptom: bad termination - crimper; weak signal - analyzer.	A flaky cable is re-terminated with a crimper, then verified with a cable tester.
63	Loopback plug	A loopback plug shortens TX to RX on a port to test it in isolation.	Use loopback to confirm a port works before blaming the switch.	A tech plugs a loopback into a suspect port; link lights prove the port functions.

Part 5: Core 1 - Hardware Part 1: Motherboards, CPUs & RAM (16 Concepts)

High-yield domain terms from the Core 1 objectives that appear in exam questions.

#	Term	Key Facts	Strategy Tip	Example
64	Motherboard form factors	ATX, micro-ATX, and mini-ITX define board size, mounting holes, and expansion slots.	Match the form factor to the case; mini-ITX means fewer slots, not less power.	A small build uses mini-ITX in a compact case with a single PCIe slot.
65	Chipset	The chipset routes data between CPU, RAM, storage, and peripherals and defines supported features.	Chipset questions: it manages the motherboard's feature set and connectivity.	A chipset decides how many USB ports and M.2 slots the board can offer.
66	CPU sockets	Sockets (like LGA) must match the CPU generation; they define pin layout and cooler mounting.	Match CPU and motherboard by socket - never force a CPU into the wrong socket.	An LGA1700 CPU only fits an LGA1700 board; the tech verifies before installing.
67	Cores and threads	Cores are physical processing units; threads (Hyper-Threading/SMT) let each core handle two tasks.	More cores helps multitasking; thread count matters for virtualization workloads.	An 8-core CPU with SMT shows 16 logical processors in the OS.
68	CPU cache	On-die memory levels L1, L2, L3; larger cache speeds repeated access to hot data.	Cache answers favor the fastest, closest storage layer being checked first.	A benchmark improves after enabling a CPU's larger L3 cache window.
69	Cooling the CPU	Air coolers, liquid AIO (all-in-one) coolers, and thermal paste transfer heat from the IHS to the heatsink.	Fresh thermal paste and a seated cooler fix most sudden thermal throttling.	After reseating the cooler with new paste, a CPU stops throttling under load.
70	RAM types	DDR4 and DDR5 are current desktop RAM; SODIMM is the laptop module; speeds are matched to the board.	Match DIMM generation and speed to the motherboard - do not mix DDR4 and DDR5.	Upgrading a DDR4 board, the tech installs DDR4 modules, never DDR5.
71	Dual channel	Running RAM in matched pairs (same capacity and speed in paired slots) doubles memory bandwidth.	Install matching pairs in the correct slots; mismatched sticks run single channel.	Two identical 8 GB sticks in paired slots give dual-channel 16 GB.
72	ECC RAM	Error-correcting code memory detects and corrects single-bit errors; used in servers, rarely in desktops.	Choose ECC for data-integrity answers (servers), non-ECC for consumer builds.	A file server runs ECC RAM so a single-bit memory error is corrected silently.
73	Memory capacity planning	Match capacity to workload: web and office in 8-16 GB, design and VMs in 16-32 GB or more.	Size memory to the heaviest app plus the OS and a margin.	A video editor upgrades to 32 GB so previews and exports stop swapping.
74	BIOS/UEFI	Firmware that initializes hardware and boots the OS; UEFI is modern, with Secure Boot and GPUs/disk support.	UEFI answers pair with Secure Boot and GPT; BIOS pairs with legacy MBR.	A new PC boots in UEFI mode with Secure Boot enabled from the factory.
75	CMOS and battery	The CMOS battery keeps BIOS settings and the clock when the PC is unplugged; a dead battery resets settings.	When the clock resets or BIOS settings vanish, suspect the CMOS battery.	A PC loses time and boot order; a new CR2032 battery fixes both.
76	Power button and POST	Pressing power runs Power-On Self-Test: the system checks CPU, RAM, video, and storage before booting.	POST beep patterns identify failing hardware - look them up per vendor.	A PC beeps once and proceeds; a new build beeps repeatedly, pointing to RAM.
77	Expansion slots	PCIe x16 (graphics), x4/x1 (add-in cards); physical size and lanes matter for bandwidth.	Install GPUs in x16; lower-bandwidth cards work in smaller slots.	A capture card fits a PCIe x1 slot; the GPU stays in the x16 slot.
78	Onboard video vs GPU	Integrated graphics use system RAM; discrete GPUs add dedicated VRAM for heavy rendering.	Choose discrete GPU answers for gaming and video work; integrated for office use.	A designer adds a discrete GPU so 3D renders stop stuttering.
79	Troubleshooting memory	Fault symptoms: random crashes, BSODs, and beep codes; test sticks one at a time and reseat.	Reseat and test one stick per slot to isolate a bad module quickly.	A PC BSODs randomly; removing one stick stops the crashes - that stick is bad.

Part 6: Core 1 - Hardware Part 2: Storage, Power & Cooling (16 Concepts)

High-yield domain terms from the Core 1 objectives that appear in exam questions.

#	Term	Key Facts	Strategy Tip	Example
80	HDD	Hard disk drives store data on spinning platters; large capacity at low cost, slower, mechanical.	Choose HDD for bulk archiving; SSD for anything performance-sensitive.	A NAS archives video files on 8 TB HDDs because capacity beats speed there.
81	SSD	Solid-state drives use NAND flash with no moving parts; fast boots, low power, shock resistant.	SSD is the default performance answer for OS drives and laptops.	An old laptop gets an SSD, and boot time drops from minutes to seconds.
82	NVMe and M.2	M.2 is the small card form factor; NVMe is the PCIe-based protocol with very		

NVMe/M.2 = fastest storage answer; SATA M.2 exists but is slower.	A new workstation boots from a 1 TB NVMe M.2 drive with multi-gigabyte speeds.
---	--

83	SATA	Serial ATA connects drives at up to 6 Gbps; the common interface for 2.5-inch SSDs and HDDs.	SATA answers suit mechanical drives and 2.5-inch SSDs; NVMe answers for speed.	A data drive (HDD) and an OS drive (SATA SSD) both connect over SATA ports.
84	RAID levels	RAID 0 stripes for speed, RAID 1 mirrors for redundancy, RAID 5 stripes with parity, RAID 10 mirrors stripes.	Match RAID to the need: redundancy - RAID 1/5/10; speed only - RAID 0.	Two drives in RAID 1 keep a copy; one drive failing loses nothing.
85	RAID controllers	Hardware controllers handle RAID on their own processor; software RAID (like Windows Storage Spaces) uses the OS.	Hardware RAID survives OS changes; software RAID is cheaper and good for desktops.	A small office uses Windows Storage Spaces for a two-drive mirror.
86	PSU	Power supply converts AC to DC (12V, 5V, 3.3V rails) and must supply enough wattage with headroom.	Calculate wattage as peak load plus 20-30 percent headroom for stability.	A 650 W PSU comfortably serves a mid-range build peaking near 450 W.
87	PSU form factors	ATX and SFX sizes fit standard and small cases; modular supplies attach only needed cables.	Small cases need SFX; modular PSUs make cable management easier.	An ITX build fits an SFX PSU and leaves room for airflow.
88	80 Plus rating	Efficiency certification: Bronze, Silver, Gold, Platinum, Titanium - higher ratings waste less heat.	Gold or better for builds that run long hours; it saves power over years.	A NAS runs 24/7 on a Gold PSU, trimming annual electricity cost.
89	Cooling systems	Case airflow, CPU coolers, case fans, and liquid cooling keep components under thermal limits.	Positive-ish airflow (more intake than exhaust) reduces dust and hot spots.	Two intakes and one exhaust keep a gaming case cool under load.
90	Thermal paste	Paste fills microscopic gaps between CPU and cooler; old dried paste raises temperatures.	Replace dried paste when a cooler is reseated - it is cheap insurance.	A CPU hits 95C; new paste and a reseal bring it back under 80C.
91	Case and fans	Cases host drives and airflow; fan size and RPM trade noise for cooling.	Match fan direction to case flow arrows; front intake, rear exhaust.	A quiet office build uses larger 140 mm fans spinning slower and quieter.
92	Storage performance tuning	Defragment HDDs (not SSDs), trim SSDs, and keep free space above about 15 percent for steady write speed.	Never defrag SSD - TRIM is the right maintenance command there.	A half-full SSD is trimmed monthly; the HDD is defragmented on schedule.
93	Storage health signs	Symptoms of failing storage: clicking HDDs, slow reads, SMART warnings, and disappearing partitions.	Back up immediately and replace the drive when SMART reports pending failures.	A drive shows SMART reallocated sectors; the tech images it and swaps it.
94	Power protection	Surge suppressors absorb spikes; UPSes provide battery backup and clean power during outages.	Servers and file storage sit on UPS; surge-only is fine for cheap peripherals.	A crash-free file server runs on a UPS that bridges short outages.
95	Storage connectors in practice	SATA data plus power, M.2 slots, and external USB enclosures cover most installs.	For cloning, image to a USB adapter or second internal slot to avoid boot conflicts.	A tech clones an HDD to an NVMe drive, then boots from the new drive.

Part 7: Core 1 - Hardware Part 3: Cables, Connectors & Peripherals (16 Concepts)

High-yield domain terms from the Core 1 objectives that appear in exam questions.

#	Term	Key Facts	Strategy Tip	Example
96	USB generations	USB 2.0 at 480 Mbps, USB 3.x at 5/10/20 Gbps, USB4/Thunderbolt at 40 Gbps; Type-A and Type-C connectors.	Match USB speed to the peripheral: external SSDs want USB 3.x or newer.	A backup SSD over USB 3.2 runs far faster than the same drive on USB 2.0.
97	USB-C	Reversible, power-delivery capable, and carries video, data, and charging in one cable.	USB-C is the modern 'one cable' answer for docking and charging.	A laptop connects to a dock over a single USB-C cable for power, video, and data.
98	Thunderbolt	Intel/Apple standard over USB-C: up to 40 Gbps, daisy-chaining, and external GPU support.	Thunderbolt answers pair with 40 Gbps and daisy-chained high-speed devices.	A video editor daisy-chains two 4K monitors from one Thunderbolt port.
99	HDMI	Digital audio/video port common on TVs and monitors; carries uncompressed video plus audio.	HDMI is the display answer for TVs and consumer monitors.	A conference TV mirrors a laptop over HDMI.
100	DisplayPort	Digital display connector with higher bandwidth and daisy-chain (MST) support on monitors.	DisplayPort suits high-refresh and multi-monitor setups.	A 144 Hz gaming monitor runs at full refresh over DisplayPort.
101	Ethernet cabling	Cat5e at 1 Gbps, Cat6 at 10 Gbps short runs; RJ45 connectors; distances to 100		

Ethernet > 30 m or gigabit: choose Cat5e/Cat6 - Wi-Fi cannot match it.	A workshop desktop is wired with Cat6 for a stable gigabit link.
--	--

102	Fiber optic	LC/SC connectors, single-mode for long distances, multi-mode for short runs; immune to EMI.	Fiber is the answer for long, high-speed, EMI-heavy runs.	A campus backbone links buildings with single-mode fiber.
103	Printer interfaces	USB, Ethernet, Wi-Fi, and Bluetooth connect printers; network queues serve many users.	Networked printers get a static IP or DHCP reservation so users find them.	An office printer gets a DHCP reservation so every workstation can map it.
104	Laser printer	Uses toner, a drum, and a fuser; fast text printing; components include imaging drum and fuser.	Laser answers for high-volume text; keep spare toner and check the fuser for smears.	A reception desk prints hundreds of labels on a laser printer with a toner cartridge.
105	Inkjet printer	Sprays ink through nozzles; good for color photos; ink dries out if idle.	Print regularly or store ink carts sealed; nozzle clogs cause streaked output.	A home photo printer streaks after months idle - a nozzle cleaning fixes it.
106	Thermal printer	Heat burns images onto thermal paper; used for receipts and labels, no ink or toner.	Thermal answers: receipts and labels, plain thermal paper, no cartridges.	A point-of-sale printer outputs receipts on thermal paper.
107	3D printer	Additive printing builds objects layer by layer from filament or resin.	3D printing answers: layer-by-layer additive manufacturing.	A lab prints prototype brackets on a filament 3D printer.
108	Scanners	Flatbed and sheet-fed scanners digitize documents at chosen DPI.	Scan at appropriate DPI: text around 300 DPI, photos higher.	An office scans signed contracts at 300 DPI to PDF.
109	Keyboard and mouse	Wired, Bluetooth, and RF receivers; ergonomic and accessibility variants exist.	RF receiver and Bluetooth are wireless answers; USB for wired simplicity.	A cashier uses a USB keyboard and mouse that need no pairing.
110	KVM switch	Keyboard, video, mouse switch lets one console control multiple computers.	KVM is the answer when one monitor and keyboard must drive several machines.	An admin manages two servers from one keyboard, monitor, and mouse via KVM.
111	Display cables vs ports	Match cable to port: HDMI, DisplayPort, USB-C alt mode, VGA legacy, DVI legacy.	Older projectors need VGA or HDMI adapters; check both ends before diagnosing.	A legacy projector connects through a DisplayPort-to-HDMI adapter.

Part 8: Core 1 - Virtualization & Cloud (11 Concepts)

High-yield domain terms from the Core 1 objectives that appear in exam questions.

#	Term	Key Facts	Strategy Tip	Example
112	Virtual machine	A software-emulated computer running its own OS on shared host hardware.	VM answers: one physical host, many isolated guests.	A server runs Windows and Linux simultaneously in separate VMs.
113	Hypervisor	Software that creates and runs VMs: Type 1 bare-metal (ESXi, Hyper-V) or Type 2 hosted.	Type 1 runs directly on hardware; Type 2 runs inside an OS.	A lab uses VirtualBox (Type 2); a production host uses ESXi (Type 1).
114	Host vs guest	The host is the physical machine running the hypervisor; guests are the VMs inside it.	Name the physical box host and the VM guest in any virtualization question.	A host crash takes down all of its guest VMs together.
115	Desktop virtualization	VDI (Virtual Desktop Infrastructure) streams desktops from servers to thin clients.	VDI answers: central management, thin clients, any-device access.	A call center runs thin clients that log into virtual desktops.
116	Cloud service models	IaaS provides infrastructure (VMs), PaaS provides platforms, SaaS provides software.	Match the model to what the provider manages: infra, platform, or app.	Gmail is SaaS; an AWS VM is IaaS; a managed app runtime is PaaS.
117	Cloud characteristics	On-demand self-service, broad network access, resource pooling, rapid elasticity, measured service.	Pick these five NIST characteristics in cloud definition questions.	A team scales a web app up in minutes, paying only for what it uses.
118	Public vs private vs hybrid cloud	Public runs on a provider's infrastructure; private on your own; hybrid mixes both.	Hybrid answers: keep sensitive data private, burst to public for scale.	A bank runs core systems private and test environments in the public cloud.
119	vSwitch	A virtual switch connects VMs to each other and to physical networks inside the hypervisor.	vSwitch answers: VM-to-VM and VM-to-network connectivity.	Two VMs on the same host exchange traffic through the vSwitch without hitting a physical switch.
120	Resource allocation	VMs draw shared CPU, RAM, and storage; over-allocation causes performance contention.	Monitor host resources - oversubscribed CPU shows as guest stalls.	A host with four heavier VMs on two cores thrashes until cores are added.
121	Snapshots and clones	Snapshots capture VM state for rollback; clones copy a VM image for quick provisioning.	Snapshot before risky changes; clone for fast, consistent deployments.	A tech snapshots a VM before a driver update, then rolls back cleanly.
122	VM backup	Back up guest VMs consistently to avoid corrupted states during snapshots.	Use image or agent backups per VM; test restores on a schedule.	A nightly VM backup restores a corrupted guest in under an hour.

High-yield domain terms from the Core 1 objectives that appear in exam questions.

#	Term	Key Facts	Strategy Tip	Example
123	Troubleshooting methodology	Identify the problem, establish a theory, test the theory, plan and implement a fix, verify, document.	Answers that ask order: identify first, document last.	A no-internet ticket is worked in methodology order and the fix is documented.
124	Identifying the problem	Gather details: what changed, when it started, error messages, and who is affected.	Ask the user what changed - it beats guessing nine times out of ten.	A user says the network died 'after the storm,' pointing to a power or modem issue.
125	Establish a theory	Form a probable cause from symptoms before touching hardware: power, connection, settings.	Generate multiple theories, then test the cheapest one first.	No link light plus recent storm suggests a dead modem before a bad NIC.
126	Test the theory	Verify with tools: ping, link lights, cable tester, or swap-in known-good hardware.	Swapping a known-good cable or device isolates the failing part fast.	A ping fails on a wired PC; replacing the cable restores the link.
127	Plan and implement	Choose the least invasive fix, back up settings or data, and note rollback steps.	Prefer configuration fixes before hardware replacements.	The tech reconfigures DNS before ordering a new router.
128	Verify and document	Confirm the fix works, close the ticket, and record the root cause for future reference.	Documentation is the final methodology step and builds a knowledge base.	After verifying Wi-Fi, the tech logs the channel change in the KB.
129	POST beep patterns	BIOS beeps encode the failed component: RAM, video, or CPU vary by vendor.	Look up the vendor beep chart instead of guessing the beep meaning.	One long, three short beeps on a common BIOS points to missing video.
130	No display	Symptom: fans spin but screen stays black - check power, cable, input source, and GPU seating.	Check the monitor input source and cable before replacing anything.	A black screen fixes when the monitor input is switched from HDMI 1 to 2.
131	No POST / no power	Nothing happens on power: check wall outlet, PSU switch, power button header, and motherboard power.	Verify AC first - test the outlet with a lamp before opening the case.	A dead outlet trips no lights; a new outlet restores power.
132	BSOD (Blue Screen of Death)	Windows stop error; note the stop code and recent changes to trace the cause.	Write down the stop code, then roll back the latest driver or update.	A stop code after a GPU driver update rolls back to the previous driver.
133	Slow performance	Causes: low RAM, high disk usage, malware, overheating, or too many startup apps.	Check Task Manager resource hogs and disk health before buying new parts.	A slow PC improves after a rogue startup app is disabled.
134	Boot failures	Symptom: OS does not load - check boot order, boot device, and disk connections.	Enter BIOS to confirm the boot drive is detected and first in order.	A boot failure resolves once the NVMe drive is set first in boot order.
135	Network link lights	Solid link light means connected; blinking means traffic; no light means a cable or port fault.	No light = check cable, port, and NIC; light on = the problem is higher up.	A link light stays off; reseating the cable restores the LAN.
136	Weak Wi-Fi signal	Distance, walls, interference, channel congestion, and antenna issues reduce signal.	Move closer or change the channel; Wi-Fi analyzers find congestion.	An analyzer shows a crowded channel; switching to a clearer one doubles throughput.
137	Interface problems (Wi-Fi)	Symptoms: intermittent drops or no association - check SSID, security type, and drivers.	Verify the exact SSID and password before blaming range.	A phone joins nothing because the password saved is stale - re-entering fixes it.
138	Printer troubleshooting	Jams, paper feed, and smears: clear jams safely, align cartridges, clean heads, replace toner.	For laser smears check the fuser; for inkjet streaks clean the nozzles.	Streaked prints clear after an inkjet nozzle cleaning cycle.
139	Mobile diagnostic basics	Battery drain, heat, and app crashes: check settings, updates, and battery health first.	A hot, fast-draining phone usually means a runaway app or a failing battery.	Two apps updated recently drain the battery; uninstalling one stops the drain.
140	Tools recap	Multimeter tests power delivery; loopback plugs test ports; cable testers validate wiring.	Match the tool to the layer: power - multimeter; copper - tester; port - loopback.	A PSU with wrong voltages is caught by a multimeter before any part is replaced.

Part 10: Core 2 - Windows Part 1: Installation & Boot (16 Concepts)

High-yield domain terms from the Core 2 objectives that appear in exam questions.

#	Term	Key Facts	Strategy Tip	Example
141	Windows editions	Home, Pro, Enterprise, and Education differ in features like BitLocker, domain join, and group policy.	Pro/Enterprise answers carry BitLocker and domain join; Home lacks them.	A business workstation runs Windows 11 Pro to join the domain and use BitLocker.
142	Windows 11 requirements	Modern CPU, 4 GB RAM		

minimum, 64 GB storage, UEFI with Secure Boot, and TPM 2.0.

TPM 2.0 and Secure Boot are

143	Clean install vs upgrade	Clean installs wipe and load fresh; upgrades keep apps and settings in place.	Choose upgrade to preserve data; clean install for a fresh, consistent image.	A slow Windows 10 PC gets a clean Windows 11 install, losing no work after a backup.
144	In-place upgrade	Upgrade install keeps user files, apps, and settings while moving to a newer edition or version.	Answer in-place upgrade when data preservation is required.	A user upgrades Windows 10 to 11 in place and keeps all documents.
145	Installation media	Bootable USB or ISO created with Microsoft's media creation tool; boot order set in firmware.	Create media on a USB 3 flash drive; verify boot order in UEFI first.	A tech boots a laptop from a Windows 11 USB stick to install.
146	Partitions: MBR vs GPT	MBR supports legacy BIOS boot and smaller disks; GPT supports UEFI, Secure Boot, and 2 TB plus.	GPT is the modern answer; MBR only for legacy BIOS compatibility.	A 4 TB drive is initialized as GPT, not MBR, to use its full size.
147	UEFI vs BIOS	UEFI is modern firmware with Secure Boot, faster startup, and GPT support; BIOS is legacy.	Pair UEFI with GPT and Secure Boot in answers; BIOS with MBR.	Enabling Secure Boot in UEFI blocks unsigned boot loaders.
148	Secure Boot	UEFI feature that only allows signed, trusted boot loaders to run.	Secure Boot answers: prevents unauthorized OS at boot time.	A PC refuses a Linux USB until Secure Boot is configured or disabled.
149	TPM	Trusted Platform Module: hardware chip storing keys for BitLocker, Windows Hello, and Measured Boot.	TPM pairs with BitLocker and Hello; 2.0 is the modern requirement.	BitLocker uses the TPM to bind the drive to the machine.
150	Sysprep	System Preparation tool generalizes a Windows image for cloning to identical hardware.	Sysprep answers: prepare a master image for mass deployment.	An IT team runs Sysprep on one configured PC and clones the image fleet-wide.
151	Imaging and cloning	Capture a golden image (WIM or vendor format) and deploy it with tools like MDT or third-party imaging.	Imaging is the fastest fleet deployment answer after the image is prepared.	A lab rebuilds 40 PCs from a stored image in an afternoon.
152	Windows setup partitions	Installer creates system (EFI), MSR, recovery, and C: partitions; keep recovery intact.	Do not delete EFI or recovery partitions during installs.	A manual install keeps the EFI and recovery partitions and shrinks C:.
153	Boot process (UEFI)	Power - firmware - boot manager - Windows Boot Manager - kernel - services - shell.	Order questions: firmware first, shell last.	A startup repair fixes a broken boot manager chain after a failed update.
154	Boot Configuration Data	BCD stores boot entries; rebuilt with bootrec or bcdedit after boot corruption.	BCD corruption shows as boot loops - run bootrec /rebuildbcd.	A PC loops at boot; bootrec rebuilds BCD and it starts again.
155	Windows activation	Activation matches the license to the hardware (digital license) or product key.	Edition and license must match; upgrades carry the old license when eligible.	A digital license reactivates automatically after a motherboard swap in the linked account.
156	Post-install updates	Apply Windows Update patches, drivers, and then install applications after first boot.	Update order: OS, drivers, security, then apps - verify with a reboot.	A fresh install pulls updates, restarts, then installs the office suite.

Part 11: Core 2 - Windows Part 2: Tools & CLI (16 Concepts)

High-yield domain terms from the Core 2 objectives that appear in exam questions.

#	Term	Key Facts	Strategy Tip	Example
157	Task Manager	Shows processes, performance, startup apps, and lets you end tasks and change priorities.	Task Manager is the first stop for a slow PC - find the hog.	A runaway process pegs CPU; Task Manager ends it and the PC recovers.
158	Disk Management	Creates, formats, shrinks, and extends partitions; assigns drive letters; initializes disks.	Extend a volume only when adjacent unallocated space exists.	A tech extends C: by 50 GB from adjacent unallocated space in Disk Management.
159	Device Manager	Lists hardware, shows driver status, and updates or rolls back drivers.	Yellow warning in Device Manager = driver problem; update or roll back there.	A sound device shows an error; rolling back the driver restores audio.
160	System Configuration (msconfig)	Controls startup items, boot options, and services for troubleshooting.	Safe boot under msconfig is quick for diagnosis; uncheck it after.	Launching msconfig and selecting Safe Boot loads a minimal Windows.
161	System Information (msinfo32)	Reports hardware, drivers, and system summary for documentation and diagnosis.	Check msinfo32 for BIOS version and installed RAM before upgrades.	A tech reads the RAM slots count from msinfo32 before buying memory.
162	Command Prompt basics	cd, dir, copy, xcopy, robocopy, ipconfig, ping, and other CLI tools manage files and network.	Robocopy is the robust copy answer; ipconfig shows IP config instantly.	A tech copies a folder tree with robocopy /E and resumes interrupted copies.
163	ipconfig	Shows IP address, subnet, gateway, DNS, DHCP status; ipconfig /release and /renew		

ipconfig /renew is the quick answer when DHCP gave a bad address.

After renewing the lease, a workstation gets a valid 192.168 address instead of

164	ping	Tests reachability and round-trip time to an IP or hostname.	Ping the gateway first, then an external host, to find where the break is.	Ping to the router succeeds, while ping to a website fails - WAN is the issue.
165	tracert	Traces the route packets take, showing each hop; identifies where latency or loss starts.	A tracert hop with stars shows where the network path breaks.	Tracert shows normal hops then timeouts - pointing to the ISP segment.
166	netstat	Lists active connections, ports, and listeners; finds suspicious outbound links.	netstat -ano shows PID per connection for malware hunting.	A tech finds an unknown process connected to a foreign IP via netstat.
167	nslookup	Queries DNS records by name to confirm resolution.	nslookup names the failing DNS answer when browsing breaks but ping works.	nslookup fails to resolve a hostname - the DNS server setting is wrong.
168	diskpart	Disk partitioning tool: list, select, clean, create partition operations from CLI.	diskpart clean wipes a drive completely - use carefully.	A tech uses diskpart clean to remove all partitions before reimaging.
169	sfc /scannow	System File Checker repairs protected system files from the Windows image.	Run sfc after corruption; if it fails, add DISM restorehealth first.	A corrupted system DLL is repaired by sfc during a boot-loop fix.
170	chkdsk	Checks disk integrity and repairs file-system errors; /f fixes, /r finds bad sectors.	chkdsk /f needs an offline or scheduled run on the system drive.	After an unclean shutdown, chkdsk /f repairs the file system.
171	PowerShell	Command-line shell and scripting with cmdlet verbs; more powerful than CMD.	PowerShell answers for scripting and automation; CMD for quick legacy commands.	An admin writes a PowerShell script to inventory all workstations.
172	Windows Recovery Environment	WinRE offers Startup Repair, Safe Mode, System Restore, and command prompt for broken systems.	WinRE is the answer when Windows will not start normally.	A blue-screen loop is broken by booting into WinRE and running Startup Repair.

Part 12: Core 2 - macOS, Linux & Mobile OS (14 Concepts)

High-yield domain terms from the Core 2 objectives that appear in exam questions.

#	Term	Key Facts	Strategy Tip	Example
173	macOS fundamentals	Unix-based OS with Finder, Dock, System Settings, and Gatekeeper app security.	macOS answers pair with Gatekeeper, Time Machine, and Spotlight.	A Mac blocks an unsigned app via Gatekeeper until the user allows it.
174	Time Machine	macOS built-in backup to external drive or network share, with hourly snapshots.	Time Machine is the macOS backup answer; restore from it after drive failure.	A Mac recovers an accidentally deleted file from Time Machine.
175	macOS recovery	Command-R boots macOS Recovery for reinstalls, disk utility, and restore.	Command-R answers: recovery and reinstall without a bootable USB.	A Mac with a failing OS is reinstalled from Recovery.
176	Linux distributions	Ubuntu, CentOS, Debian, and Fedora share the Linux kernel but differ in package managers and defaults.	Match distro-specific answers to their package tool: apt (Debian/Ubuntu), dnf/yum (Fedora/CentOS).	A Ubuntu server installs packages with apt update and apt install.
177	Linux file structure	/etc holds configs, /home user files, /var logs and mail, /tmp temporary files, /bin executables.	Know the big directories - /etc config, /var logs, /home users.	A tech edits a service config in /etc and reads its log in /var/log.
178	Linux permissions	rxw flags in three sets (owner, group, other); chmod changes them, chown changes owner.	chmod 755 + chown root:root is the common service file setup.	A script fails to run until chmod +x grants execute permission.
179	Linux CLI basics	ls, cd, cp, mv, rm, grep, ps, top, and man cover daily administration.	grep filters command output; ps and top show processes.	A tech runs ps aux and greps the log to find a crashing process.
180	Package management	apt/dnf/yum install, update, and remove software from repositories; dependencies resolve automatically.	Package answers pair with the distro family - apt for Debian.	Ubuntu installs nginx with apt install nginx from its repository.
181	Mobile OS basics	iOS and Android manage apps, storage, settings, and updates; each has its own restore and reset paths.	Know the mobile reset hierarchy: app settings, OS update, factory reset.	A broken Android app is fixed by clearing its cache before a full reset.
182	Mobile connectivity settings	Wi-Fi, cellular, Bluetooth, hotspot, and VPN are controlled in OS settings on both platforms.	Toggle airplane mode to reinitialize radios when a device drops all connectivity.	A phone stuck offline recovers after airplane mode is toggled.
183	iCloud and Google backup	Cloud backup syncing: iCloud on iOS, Google account backup on Android.	Cloud backup answers: reinstall brings back settings and data from the account.	After a factory reset, an iPhone restores from the latest iCloud backup.
184	Mobile resets	Soft reset, force restart, and factory reset differ in data loss; back up before factory reset.	Step up in severity: app reset, soft reset, then factory reset.	A frozen phone force-restarts; only later does the tech consider factory reset.
185	Screen and lock settings	Passcode, biometric (Face ID, fingerprint), auto-lock, and Find My Device security settings.	Biometric + passcode is the recommended lock answer on mobile.	A lost phone is located and wiped using Find My Device.
186	Cross-platform integration	Synchronizing email, calendar, and files across Windows,		

IMAP, CalDAV, and sync
clients keep multiple platforms

A user's calendar shows the same events on Android and

High-yield domain terms from the Core 2 objectives that appear in exam questions.

#	Term	Key Facts	Strategy Tip	Example
187	CIA triad	Confidentiality, Integrity, Availability - the three security goals framing most controls.	Map controls to the triad in questions: encryption = confidentiality.	Backups support availability; hashes verify integrity; passwords protect confidentiality.
188	Encryption basics	Symmetric uses one key; asymmetric uses a public/private pair; TLS protects data in transit.	Encryption answers: at rest - BitLocker/FileVault; in transit - TLS/VPN.	A laptop's drive is encrypted with BitLocker; web traffic uses TLS.
189	BitLocker	Windows full-disk encryption tied to TPM; requires Pro/Enterprise editions.	BitLocker pairs with TPM and Pro editions; Home cannot run it.	A stolen Pro laptop yields nothing because BitLocker encrypts the drive.
190	FileVault	macOS full-disk encryption with FileVault on Apple Silicon or Intel Macs.	FileVault is the macOS full-disk encryption answer.	A Mac's data stays unreadable without the FileVault recovery key.
191	Authentication factors	Something you know (password), something you have (token), something you are (biometric).	MFA answers combine two different factors.	Login requires a password plus a phone code - that is MFA.
192	Password best practices	Long unique passwords or passphrases, password managers, and no reuse across sites.	Password-manager answers beat in-head memory for every account.	A user's reused password leaks; a password manager generates fresh ones per site.
193	Access control	Least privilege gives users only what their job needs; RBAC groups users by role.	Least-privilege and RBAC are the access-control answers.	A finance role gets accounting shares but not HR folders.
194	Biometrics	Face, fingerprint, and iris authentication; convenient but need a fallback method.	Biometric answers pair with a passcode fallback.	An employee logs in with fingerprint plus PIN when the sensor fails.
195	Wireless security settings	WPA3 with strong passphrases; disable WPS; isolate guests from the main network.	WPA3, WPS off, guest isolation are the modern wireless security answers.	A SOHO router runs WPA3 and a separate guest SSID with isolation.
196	Malware types	Virus, worm, Trojan, ransomware, spyware, adware, rootkit, and keyloggers each behave differently.	Match malware to behavior: locks files - ransomware; hides deep - rootkit.	A screen demands payment to unlock files - that is ransomware.
197	Ransomware	Encrypts files and demands payment; prevent with backups, updates, and email filtering.	Ransomware answers: offline backups are the key recovery path.	A workstation is restored from an offline backup after a ransomware attack.
198	Anti-malware software	Antivirus/EDR scans, quarantines, and blocks malware; keep definitions current.	Update signatures plus full scan is the standard removal follow-through.	A periodic scan catches a Trojan before it spreads on the network.
199	Firewalls	Host and network firewalls filter traffic by rules; Windows Defender Firewall is built in.	Default-deny firewall answers block everything not explicitly allowed.	A server's firewall blocks inbound 445 except from the admin subnet.
200	Windows Defender	Built-in antivirus plus firewall and tamper protection in Windows 10/11.	Defender answers: keep real-time protection on and definitions updated.	Defender flags an unknown downloaded file and quarantines it.
201	Phishing and social engineering	Emails and calls trick users into revealing credentials or installing malware; verify unexpected requests.	Human-layer answers: verify by another channel, never click unsolicited links.	A fake invoice email is reported and deleted before anyone clicks.
202	Zero-day and updates	Exploits for unknown flaws; patching promptly closes most practical risks.	Patch-management answers reduce exposure to known and zero-day attacks.	A Tuesday patch cycle closes a browser flaw exploited over the weekend.
203	Account lockout and auditing	Failed-login thresholds and audit logs detect brute force and unauthorized access.	Auditing answers: review logs for repeated failures and odd hours.	A lockout policy trips after five failed attempts, blocking a brute-force run.
204	Physical security	Locks, badge access, and cable locks protect devices; full-disk encryption protects the data after theft.	Physical + encryption answers cover both device and data loss.	A data center uses badge entry, and laptops run full-disk encryption.

Part 14: Core 2 - Software Troubleshooting (16 Concepts)

High-yield domain terms from the Core 2 objectives that appear in exam questions.

#	Term	Key Facts	Strategy Tip	Example
205	Application won't start	Check compatibility, missing dependencies, corrupt files, and permissions; reinstall as last resort.	Repair install before full reinstall; check the event log for the error.	A legacy app fails until compatibility mode is set on the executable.
206	Slow application	Causes: low memory, runaway		

Close hogs and check disk

An email client crawls because

207	App crashes and freezes	Use Task Manager to end the task, check the app's logs, and apply the vendor fix or update.	Record the failure details from Event Viewer for accurate diagnosis.	A video app freezes on export until its GPU driver is updated.
208	Driver issues	Yellow device errors in Device Manager: update, roll back, or reinstall the matching driver.	Roll back the last driver change when a device broke right after an update.	A printer fails after a Windows update; rolling back the driver restores it.
209	System restore points	Windows snapshots registry and system files for rollback; created before updates and restores.	Restore before reinstalling - it undoes recent system changes fast.	An update breaks boot; a restore point returns Windows to working state.
210	Windows Update problems	Failed updates: run the troubleshooter, free space, and retry; check for pending reboots.	A pending reboot blocks updates - restart and retry before deeper fixes.	Windows Update fails repeatedly until a reboot completes pending changes.
211	Slow boot	Startup apps, disk health, and drivers affect boot time; disable unnecessary startup items.	Trim the startup list in Task Manager for the fastest boot win.	A PC boots in 40 seconds after nine startup apps are disabled.
212	Safe Mode	Starts Windows with minimal drivers and services for diagnosis of software issues.	Suspect drivers or malware - boot Safe Mode to test the theory.	A driver-induced crash disappears in Safe Mode, confirming the driver.
213	Malware removal process	Isolate the system, update definitions, scan, quarantine, and verify with a second tool.	Offline scan or Safe Mode beats scanning while malware runs.	A suspected infection is scanned offline, cleaned, and verified clean after reboot.
214	Unauthorized access	Signs: password changes and odd activity - reset credentials, audit logs, and enable MFA.	Immediately reset the account and revoke sessions when breached.	An account emails spam; the tech resets the password and signs out all devices.
215	Mobile app problems	Crashes and freezes on mobile: update the app, clear cache, check space, then reinstall.	Clear cache before uninstalling; reinstall only after the cheap fixes fail.	An Android app crashes until its cache is cleared and it is updated.
216	Mobile performance issues	Slow device: low storage, background apps, and old OS versions.	Free storage and close background apps before a factory reset.	A phone speeds up after 15 GB of videos are moved off device.
217	Connectivity app issues	Apps fail online: check Wi-Fi, date/time, and account sign-in state.	Wrong device time breaks TLS - check clock before network blame.	A mail app fails until the phone clock is corrected to the right zone.
218	Email client problems	Sent mail stuck, authentication failures, and server settings errors - verify ports and credentials.	Check SMTP/IMAP ports and app passwords for secure mail servers.	Outlook sends nothing until the SMTP port is changed to 587 with TLS.
219	Browser issues	Pages fail: cache, extensions, proxy settings, and DNS are the usual suspects.	Test in private mode and clear cache to isolate an extension fault.	A broken page works in a private window - an extension is the cause.
220	Script and macro warnings	Blocked macros and scripting prompts are security controls; enable only from trusted sources.	Never enable macros from email attachments.	A finance document's macros stay disabled because it arrived by email.

Part 15: Core 2 - Operational Procedures Part 1: Safety, Communication (12 Concepts)

High-yield domain terms from the Core 2 objectives that appear in exam questions.

#	Term	Key Facts	Strategy Tip	Example
221	ESD protection	Electrostatic discharge damages components; use ESD straps and mats when handling parts.	Wear the strap and touch the case before touching components.	A tech wearing an ESD strap installs RAM without zapping the board.
222	Power safety	Unplug before working inside; check for damaged cables and proper grounding.	Verify power is off and discharged before internal work.	A technician unplugs a PSU and presses power to drain capacitors before service.
223	Surge and UPS	Surge suppressors and UPSes protect equipment and keep servers up during dips.	Server and storage gear go on UPS; desktop workstations on surge protectors.	A brief brownout passes without a reboot thanks to the UPS.
224	Proper disposal	Recycle electronics, dispose of batteries and toner as hazardous material, and wipe data before disposal.	Erase data and recycle e-waste per local rules - toner and batteries are hazardous.	Old laptops have drives wiped, then go to a certified recycler.
225	Lifting and ergonomics	Lift with the legs, keep workstations at comfortable positions, and avoid prolonged strain.	Lift with the legs and take posture breaks - back injuries end careers.	Two techs lift a server tower using proper leg lift technique.
226	Ticketing systems	Tickets track incidents: priority, status, assignment, and resolution history.	Always create or update the ticket - it is the source of truth.	A help desk ticket moves from open to assigned to resolved with notes.
227	SLAs	Service Level Agreements define response and resolution targets; missed targets are tracked.	Match priority to SLA in questions: P1 fastest, P4 slowest.	A P1 outage is answered in 15 minutes per the SLA, while a P4 request waits a day.
228	Change management	Planned changes go through request, approval, testing,		

Change-management
answers: plan, approve, test,

A firewall rule change is approved, tested, deployed,

Write the resolution so the next

A ticket documents the exact

230	Professional communication	Be clear, patient, and honest; avoid jargon; set expectations for follow-up.	Explain what you are doing before you do it, and give honest timeframes.	A tech tells a user the repair takes 30 minutes and then delivers it.
231	Empathy and de-escalation	Acknowledge the user's frustration and keep the conversation focused on solving the issue.	Validate the frustration - 'I understand this is blocking your work' - then fix.	An angry caller calms once the tech repeats their problem back correctly.
232	Remote support tools	Screen-sharing, remote control, and chat tools enable support without a desk visit.	Get consent, share the session, and document what was changed remotely.	A support agent remote-controls a user's PC with permission to fix the printer.

Part 16: Core 2 - Operational Procedures Part 2: Backup, Recovery & Documentation (12 Concepts)

High-yield domain terms from the Core 2 objectives that appear in exam questions.

#	Term	Key Facts	Strategy Tip	Example
233	Backup types	Full backs up everything; incremental backs up changes since the last backup of any type; differential since the last full.	Full + incremental saves space; restoring takes full plus all incrementals.	A nightly incremental plus weekly full restores to Wednesday's state with two tapes.
234	3-2-1 backup rule	Three copies of data, on two different media, with one copy offsite.	Choose the 3-2-1 answer for resilient backup strategy questions.	A business keeps the NAS copy, an external disk, and a cloud copy.
235	Cloud backup	Offsite copies in cloud storage protect against fire, theft, and ransomware.	Cloud backup is the offsite leg of the 3-2-1 rule.	A small firm syncs critical folders to cloud storage nightly.
236	File History	Windows per-file backup of libraries and folders to an external drive or network location.	File History answers: user-file versioning on Windows.	A deleted spreadsheet is recovered from File History's hourly copies.
237	System image	A full drive image captures the OS, apps, and settings for bare-metal restore.	Images restore a whole machine; file backups restore individual files.	After a drive death, a system image rebuilds the PC in an hour.
238	Restore points vs backups	Restore points roll back system files and settings - not user data; backups protect data.	Restore point = system change; backup = data loss.	A bad driver is undone by a restore point; a deleted file needs a backup.
239	Recovery media	Bootable USB/ISO with the OS and tools to reinstall or recover.	Create recovery media before you need it - store it safely.	A dead OS is reinstalled from a pre-made recovery USB.
240	Disaster recovery plan	Documented procedures to restore systems and data within target recovery time (RTO).	DR answers: documented order of restore, tested regularly.	A flood forces restore from cloud; the DR plan's runbook makes it orderly.
241	Backup verification	Test restores and review logs so backups actually work when needed.	A backup you never restore is a hope, not a plan.	A quarterly restore test catches a corrupt backup chain before it matters.
242	Documentation standards	Label devices, document IPs and configs, and keep network maps current.	Good documentation turns a mystery into a 5-minute fix.	A labeled patch panel lets a tech trace a cable without re-terminating.
243	Inventory management	Track hardware, software licenses, warranties, and asset tags in an inventory system.	Keep the asset list current for audits and warranty claims.	An asset tag helps recover a lost laptop and claim its warranty.
244	Knowledge base	A shared repository of fixes and procedures that reduces repeat tickets.	Write KB articles for every recurring fix.	A KB article on the login loop cuts similar tickets by half.