



# CPUs, Memory, Motherboards and Buses

CompTIA A+ 220-1201 domain 3.0 and beyond | x86/ARM, sockets, DDR4/DDR5, ECC, PCIe, USB4 | CPU security features (ANSSI DAT-24)

#CPU #Memory #Motherboards #HardwareSecurity

## CPU architectures and what the exam asks

### Scope and sources

CompTIA A+ Core 1 exam **220-1201**, objective domain 3.0 Hardware (CPUs, RAM, motherboards, expansion buses), extended with 2024-2026 platforms and the CPU security features ANSSI (Agence nationale de la sécurité des systèmes d'information, the French national cybersecurity agency) asks for in its x86 hardware-configuration note DAT-24 (2015). Every acronym is expanded at first use; an acronym decoder closes the sheet.

| x86-64 (CISC)                                                                                                                 | ARM64 / AArch64 (RISC)                                                                                       | RISC-V                                                                                                                               |
|-------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| Intel Core / Core Ultra / Xeon, AMD Ryzen / EPYC                                                                              | Apple M1-M4, Qualcomm Snapdragon X, AWS Graviton, phones                                                     | open ISA (instruction set architecture = the machine-language contract), royalty-free; microcontrollers, SSD controllers, early SBCs |
| CISC (complex instruction set computer): variable-length instructions, decoded internally to micro-ops                        | RISC (reduced instruction set computer): fixed-length load/store instructions, low power per op              | modular base + extensions (RV64GC)                                                                                                   |
| Runs every legacy Windows binary natively                                                                                     | Windows on ARM emulates x64 (Prism); drivers must be ARM64                                                   | no mainstream desktop Windows                                                                                                        |
| Virtualization: Intel VT-x + EPT (Extended Page Tables), AMD-V + NPT/RVI (Nested Page Tables / Rapid Virtualization Indexing) | EL2 (exception level 2 = hypervisor privilege), SMMU (System MMU, filters device DMA = direct memory access) | H extension (hypervisor)                                                                                                             |
| BIOS/UEFI firmware (Basic Input/Output System / Unified Extensible Firmware Interface), socketed CPU on desktops              | SoC (system on chip): CPU, GPU, NPU, memory controller on one die, soldered                                  | SoC, soldered                                                                                                                        |

**Core vs thread** — A core is a physical execution unit; SMT (simultaneous multithreading: Intel **Hyper-Threading**, AMD SMT) exposes 2 logical threads per core. 8 cores / 16 threads = 16 logical processors in Task Manager.

**Hybrid (big.LITTLE)** — **P-cores** (performance) + **E-cores** (efficiency) since Intel 12th gen (2021, Thread Director) and all ARM SoCs. Intel Core Ultra 200S (Arrow Lake, 2024) dropped Hyper-Threading on P-cores.

**Cache** — L1 (per core, split I/D, ~32-64 KB), L2 (per core, 1-3 MB), L3 (shared, tens of MB). AMD **X3D** parts stack extra L3 (3D V-Cache).

**TDP / PL1 / PL2** — Thermal design power sizes the cooler; Intel PL1 = sustained, PL2 = turbo burst. Undersized cooler = thermal throttling at Tjmax (maximum junction temperature of the die, ~95-105 C): the CPU lowers its clock to protect itself.

**NPU** — Neural processing unit for on-device AI; Microsoft **Copilot+ PC** requires an NPU of 40+ TOPS (tera = 10<sup>12</sup> operations per second, the usual NPU speed metric) (Snapdragon X, Core Ultra 200V, Ryzen AI 300).

**32 vs 64-bit** — 32-bit OS addresses 4 GB (about 3.2-3.5 GB usable). Windows 11 exists only as x64 and ARM64.

| Socket   | Type                                   | CPUs (2021-2026)                     | Memory                                                                                         |
|----------|----------------------------------------|--------------------------------------|------------------------------------------------------------------------------------------------|
| LGA 1700 | LGA (land grid array), pins on board   | Intel Core 12th-14th gen             | DDR4 or DDR5 (board-specific)                                                                  |
| LGA 1851 | LGA                                    | Intel Core Ultra 200S (Arrow Lake)   | DDR5 only, CUDIMM support (clocked unbuffered DIMM: clock driver on the module for 8000+ MT/s) |
| AM4      | PGA (pin grid array) 1331, pins on CPU | AMD Ryzen 1000-5000                  | DDR4                                                                                           |
| AM5      | LGA 1718                               | AMD Ryzen 7000-9000                  | DDR5 only                                                                                      |
| SP5      | LGA 6096                               | AMD EPYC 9004 / 9005                 | DDR5 RDIMM, 12 channels                                                                        |
| LGA 4677 | LGA                                    | Intel Xeon Sapphire / Emerald Rapids | DDR5 RDIMM, 8 channels                                                                         |

### EXAM TIP

LGA = pins in the **socket** (bent socket pins = board RMA); PGA = pins on the **CPU**. Mobile CPUs are **BGA** (ball grid array: soldered) and cannot be upgraded. A socket match is not enough: the **chipset BIOS** must list the CPU (update the BIOS before swapping in a newer CPU).

### Virtualization extensions

VT-x / AMD-V (run guests), SLAT (second-level address translation): EPT / NPT, hardware guest page tables, required by client Hyper-V; VT-d / AMD-Vi **IOMMU** (input/output memory management unit: device passthrough, blocks rogue device DMA). Often **disabled by default** in firmware.

### Microcode

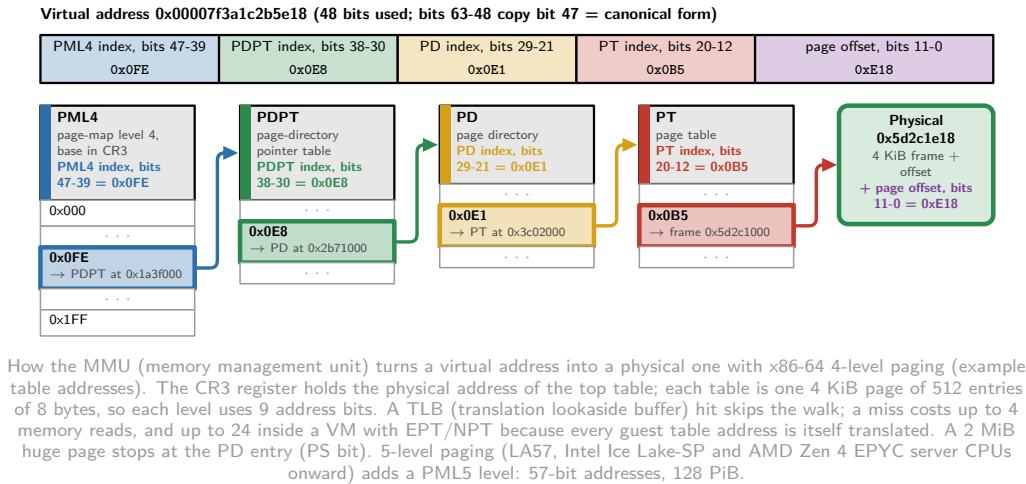
CPU firmware patch loaded by UEFI or OS early boot. Fixes side channels and bugs (Intel 13th/14th gen Vmin instability, 2024: excessive voltage degraded CPUs, fixed by microcode 0x12B). Delivered inside UEFI updates and Windows Update / Linux intel-microcode.

### Security features

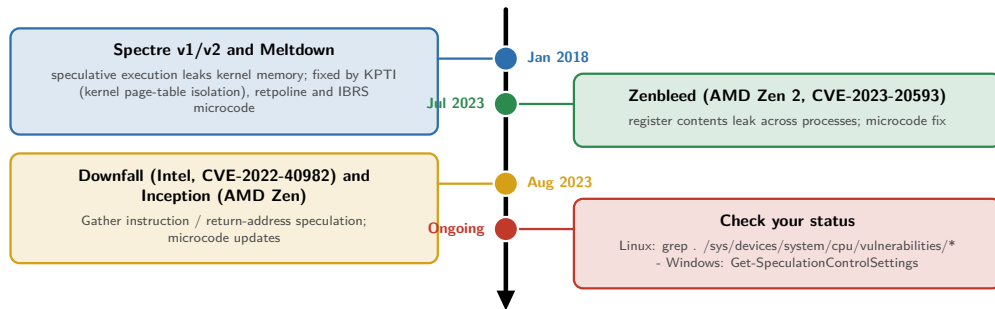
NX/XD bit (no-execute pages, used by Windows DEP = Data Execution Prevention), SMEP/SMAP (kernel may not execute / read user pages), CET (Control-flow Enforcement Technology) shadow stacks, AES-NI (hardware AES instructions), TME/SME (Intel Total / AMD Secure Memory Encryption), confidential-computing enclaves SGX / SEV-SNP / TDX, Microsoft **Pluton** security processor.

### Cooling fit

Cooler bracket must match socket (AM4 vs AM5 mostly compatible; LGA 1700 vs 1851 same mounting). Thin even paste layer; remove protective film from cold plate.



#### CPU side channels worth naming (patch = microcode + OS)



#### Memory: DDR4, DDR5, ECC, channels and timings

| Property                                              | DDR4                      | DDR5                                                                                         |
|-------------------------------------------------------|---------------------------|----------------------------------------------------------------------------------------------|
| DIMM pins / SO-DIMM pins                              | 288 / 260                 | 288 / 262 (notch moved: not interchangeable)                                                 |
| Voltage                                               | 1.2 V (XMP up to 1.35 V+) | 1.1 V, regulated by a <b>PMIC</b> (power management IC) on the module                        |
| JEDEC speeds                                          | 1600-3200 MT/s            | 4800-8800 MT/s                                                                               |
| Channels per DIMM (DIMM = dual in-line memory module) | one 64-bit channel        | two independent 32-bit subchannels                                                           |
| Burst length                                          | BL8                       | BL16                                                                                         |
| On-die ECC                                            | no                        | yes, internal to chips; <b>not</b> system ECC                                                |
| Max per UDIMM                                         | 32 GB                     | 64 GB (non-binary 24/48 GB sizes exist)                                                      |
| Laptop variants                                       | SO-DIMM, LPDDR4X soldered | SO-DIMM, LPDDR5/5X soldered, CAMM2 / LPCAMM2 (compression-attached, thin replaceable module) |

| Calculation                | Formula                                                                                                                                                                                                                                                                                                                                                                                                            | Worked example                                     |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|
| Peak bandwidth per channel | $MT/s \times 8 \text{ bytes}$                                                                                                                                                                                                                                                                                                                                                                                      | DDR4-3200 = 25.6 GB/s (module name PC4-25600)      |
| System bandwidth           | $MT/s \times 8 \times \text{channels}$                                                                                                                                                                                                                                                                                                                                                                             | DDR5-6000 dual channel = 96 GB/s                   |
| True CAS latency (ns)      | $\frac{CL \times 2000}{MT/s}$                                                                                                                                                                                                                                                                                                                                                                                      | DDR4-3200 CL16 = 10 ns; DDR5-6000 CL30 = 10 ns     |
| Clock vs data rate         | $f_{clock} = \frac{MT/s}{2}$                                                                                                                                                                                                                                                                                                                                                                                       | DDR5-4800 runs a 2400 MHz clock (double data rate) |
| Timings CL-tRCD-trP-tRAS   | e.g. 30-38-38-96: CAS latency, RAS-to-CAS delay, row precharge, row active time, in clock cycles. Lower = faster at the same MT/s.                                                                                                                                                                                                                                                                                 |                                                    |
| XMP / EXPO                 | Intel Extreme Memory Profile / AMD EXtended Profiles for Overclocking: stored in the SPD (serial presence detect) chip of the module, one click in UEFI. Without them DIMMs run at JEDEC base (DDR5-4800).                                                                                                                                                                                                         |                                                    |
| Channels                   | Dual channel = one DIMM per channel in the colour-coded slots (usually <b>A2 + B2</b> ). Four DDR5 DIMMs often force lower speeds. Mixed kits may fail training.                                                                                                                                                                                                                                                   |                                                    |
| ECC                        | Error-correcting code: detects 2-bit, corrects 1-bit errors per word (SECEDED = single-error correction, double-error detection); needs CPU + chipset + board support (Xeon, EPYC, many Ryzen). Corrected errors logged as WHEA (Windows Hardware Error Architecture) event 19 on Windows, by EDAC (Error Detection and Correction driver, edac-util) on Linux. A rising count = replace the DIMM before it fails. |                                                    |
| RDIMM / LRDIMM             | Registered (buffered) server memory; DDR5 RDIMM and UDIMM are keyed differently. Never mix registered and unbuffered.                                                                                                                                                                                                                                                                                              |                                                    |

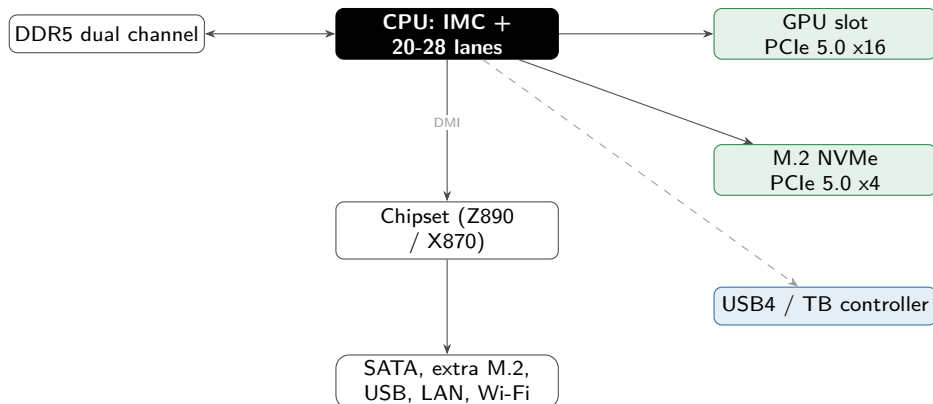
#### Memory symptoms

- **Long black screen on first DDR5 boot** memory training (up to minutes); normal, do not power off
- **Continuous beeps / memory LED (DRAM) lit** reseat, test one DIMM in slot A2, then swap
- **BSOD MEMORY\_MANAGEMENT, random app crashes** disable XMP/EXPO, run MemTest86 4 passes or mdsched.exe
- **Less RAM shown than installed** 32-bit OS, iGPU reserved memory, unseated DIMM, board limit

#### ⚠ WARNING

**Rowhammer** (2014): repeated row activation flips bits in neighbouring rows, enabling privilege escalation. DDR4 TRR (Target Row Refresh, in-DRAM counter that refreshes victim rows) was bypassed by TRRespass (2020). Mitigations: ECC memory, higher refresh rate, vendor firmware; against **cold-boot** attacks (DRAM keeps data seconds to minutes after power-off, longer when chilled, so keys can be read from a stolen running machine) use full memory encryption (TME/SME) and BitLocker with pre-boot PIN.

## Motherboards, chipsets, PCIe and external buses



Typical 2025 desktop: CPU lanes vs chipset lanes. IMC = integrated memory controller; the chipset uplink (Intel DMI = Direct Media Interface 4.0 x8, AMD PCIe 4.0 x4) is shared by everything below it

| PCIe gen | Rate / lane | Encoding    | x1 (GB/s, one way) | x16 (GB/s) |
|----------|-------------|-------------|--------------------|------------|
| 1.0      | 2.5 GT/s    | 8b/10b      | 0.25               | 4          |
| 2.0      | 5 GT/s      | 8b/10b      | 0.5                | 8          |
| 3.0      | 8 GT/s      | 128b/130b   | ~0.985             | ~15.8      |
| 4.0      | 16 GT/s     | 128b/130b   | ~1.97              | ~31.5      |
| 5.0      | 32 GT/s     | 128b/130b   | ~3.94              | ~63        |
| 6.0      | 64 GT/s     | PAM4 + FLIT | ~7.5               | ~121       |

### NOTE

GT/s = giga-transfers per second on one lane (raw signalling). Encoding overhead: 8b/10b loses 20 %, 128b/130b about 1.5 %. PCIe 6.0 switches to **PAM4** (4 voltage levels = 2 bits per symbol) with fixed-size FLIT packets (flow-control units) and forward error correction.

### TIP

Rule of thumb: each generation **doubles** bandwidth; cards and slots are backward/forward compatible at the **lowest common** generation and width. A x16 card in a x16-sized slot wired x4 runs x4: read LnkSta in lspci -vv or GPU-Z 'Bus interface'. Populating some M.2 slots **disables SATA ports or halves the GPU slot** (lane sharing): check the manual's lane table.

| Bus                          | Signalling rate          | Notes                                                      |
|------------------------------|--------------------------|------------------------------------------------------------|
| USB 2.0 Hi-Speed             | 480 Mb/s                 | 5 m cable max; 500 mA                                      |
| USB 3.2 Gen 1 (USB 5Gbps)    | 5 Gb/s                   | blue port (Type-A), 900 mA                                 |
| USB 3.2 Gen 2 (USB 10Gbps)   | 10 Gb/s                  | Type-A or Type-C                                           |
| USB 3.2 Gen 2x2 (USB 20Gbps) | 20 Gb/s                  | Type-C only, two lanes                                     |
| USB4 (USB 40Gbps)            | 20 or 40 Gb/s            | tunnels PCIe, DisplayPort, USB; Type-C only                |
| USB4 v2 (USB 80Gbps)         | 80 Gb/s (120 asymmetric) | same C connector, new cables                               |
| Thunderbolt 3 / 4            | 40 Gb/s                  | TB4 mandates 32 Gb/s PCIe, two 4K displays, DMA protection |

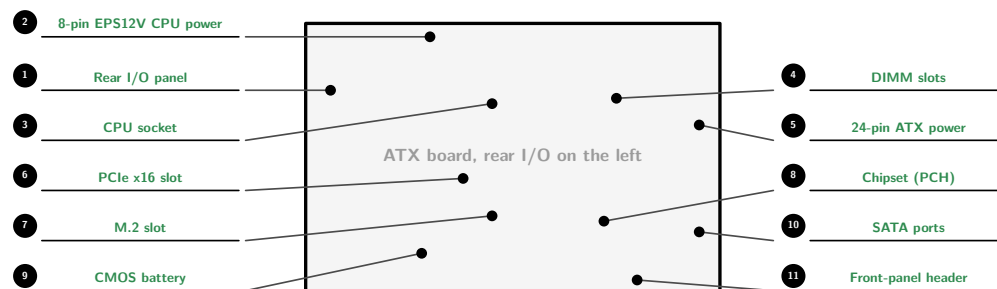
### Thunderbolt 5

USB PD 3.0 / 3.1 EPR  
(Power Delivery, Extended Power Range)

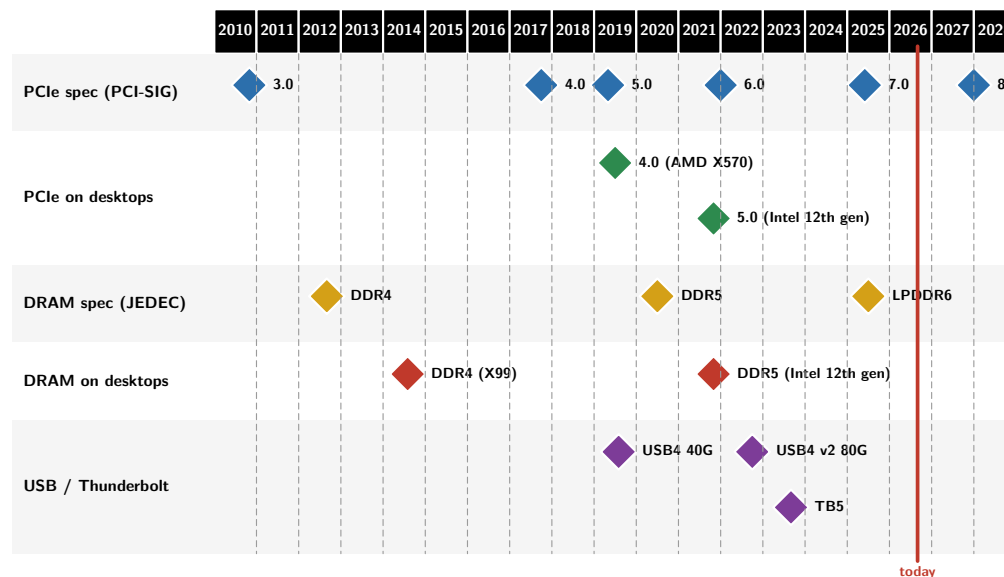
80 Gb/s (120 boost)  
100 W / 240 W

based on USB4 v2, 2024 devices  
20 V 5 A, EPR 48 V 5 A with 240 W e-marked cable (chip in the plug declares its rating)

### Label the ATX motherboard



Typical ATX layout (positions vary). Cues: EPS12V feeds the CPU regulators; the CR2032 coin cell keeps clock and settings (dead = date and boot order reset); M.2 often shares lanes with SATA ports



Specification year vs first mainstream desktop platform: a gap of 2-4 years. PCIe 7.0 (128 GT/s) was released in June 2025; PCIe 8.0 (256 GT/s) targets 2028 and LPDDR6 (JEDEC JESD209-6, 2025) first ships in phones (verify these recent dates)

### Motherboard install and security checks

✓ baseline / mandatory    □ recommended – verify in your context

- ✓ Standoffs only under board mounting holes (stray standoff = short, no POST)
- ✓ 24-pin ATX and 8-pin EPS (4+4) CPU power both connected
- ✓ Front-panel header (PWR\_SW, RESET, LEDs) per manual pinout
- **SHOULD** ARGB 3-pin 5 V vs RGB 4-pin 12 V: wrong header burns LEDs

- ☐ **MUST** Update UEFI before installing a newer-generation CPU (BIOS Flashback if no POST)
- ☐ **MUST** Enable IOMMU (VT-d/AMD-Vi), TPM (Trusted Platform Module: firmware fTPM on AMD, PTT on Intel), Secure Boot (only signed boot loaders run) IOMMU blocks DMA attacks from Thunderbolt/PCIe devices; TPM stores BitLocker keys; Secure Boot stops bootkits
- ☐ **MUST** Set a firmware setup password, unique per machine (ANSSI DAT-24 R11), and lock boot order to the system disk only (R13) otherwise anyone at the keyboard boots a USB stick or disables Secure Boot; a shared password leaks fleet-wide
- ☐ **SHOULD** Enable VT-x/AMD-V only where hypervisors or VBS are used (ANSSI R9/R15 keep it off when not needed); keep NX/XD on (R14) Windows 11 VBS/HVCI (virtualization-based security) needs VT-x on, so most fleets enable it
- ☐ **SHOULD** Disable unused onboard devices, radios and external boot; set Thunderbolt security level

| Inventory command                                         | What it shows                                                                     |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------|
| lscpu ; grep -Ec 'vmx svm' /proc/cpuinfo                  | model, cores/threads, flags; >0 = VT-x or AMD-V present                           |
| sudo dmidecode -t memory   grep -E 'Size Speed Locator'   | DIMMs per slot, rated and configured speed                                        |
| sudo lspci -vv   grep -E 'LnkCap LnkSta'                  | PCIe link capability vs negotiated speed/width                                    |
| lsusb -t ; boltctl list                                   | USB tree with speeds; Thunderbolt devices and authorisation                       |
| gcim Win32_Processor   fl Name,Number*,Virt*              | cores, logical processors, VirtualizationFirmwareEnabled (gcim = Get-CimInstance) |
| gcim Win32_PhysicalMemory   ft Bank Label,Capacity,*Speed | Windows DIMM inventory (wmic is deprecated)                                       |
| msinfo32 ; systeminfo                                     | BIOS mode (UEFI), Secure Boot, Kernel DMA Protection, Hyper-V requirements        |

Q1

Peak bandwidth of DDR5-5600 in dual channel?

A

5600 x 8 bytes x 2 = 89.6 GB/s.

Q2

Which has lower true latency: DDR4-3600 CL18 or DDR5-6400 CL32?

A

Both 10 ns (18 x 2000 / 3600 and 32 x 2000 / 6400): equal latency, DDR5 has far more bandwidth.

Q3

Hyper-V refuses to start on a new PC with a supported CPU. First firmware setting to check?

A

Intel VT-x / AMD-V (SVM mode) disabled in UEFI; also SLAT support.

Q4

A GPU benchmarks at half its expected speed after adding a second NVMe drive. Likely cause?

A

Lane sharing: the M.2 slot took lanes from the x16 slot (now x8); check LnkSta or GPU-Z and the board manual.

Q5

DDR5 on-die ECC means the server has ECC memory. True?

A

False. On-die ECC corrects inside the chip only; system ECC needs ECC DIMMs plus CPU/board support.

Q6

Maximum USB PD power with an EPR cable?

A

240 W (48 V at 5 A, USB PD 3.1).

🔮 Upgrade procedure, CPU security features and acronym decoder

- 1

Check compatibility: socket, chipset, board CPU support list (QVL = qualified vendor list for RAM), wattage of the VRM and PSU
- 2

Update UEFI with the **old** CPU still installed (or use BIOS Flashback without CPU)
- 3

Power off, unplug, press power button to drain; wear an ESD (electrostatic discharge) strap on bare metal
- 4

Install the part; new thermal paste; plug the 8-pin EPS CPU power
- 5

First boot: let DDR5 memory training finish, then enable XMP/EXPO and check temperatures under load
- 6

Verify in OS: core count, RAM size and speed (msinfo32, lscpu, dmidecode), then re-enable Secure Boot / BitLocker if suspended

Safe CPU or RAM upgrade (A+ best-practice order)

| CPU feature (ANSSI DAT-24 rule) | What it does                                                                           | Setting |
|---------------------------------|----------------------------------------------------------------------------------------|---------|
| 64-bit x86 (R1, R2)             | larger address space for ASLR randomisation, NX always available                       | yes     |
| PAE if 32-bit (R3)              | Physical Address Extension: gives 32-bit OS the NX bit                                 | partial |
| NX/XD (R14)                     | data pages cannot be executed: blocks classic shellcode                                | yes     |
| SMEP / SMAP (R5, R6)            | kernel cannot run or read user-mode memory: blocks ret2usr kernel exploits             | yes     |
| AES-NI (R7)                     | constant-time hardware AES: fast disk encryption, no cache-timing leak                 | yes     |
| RDRAND / RDSEED (R8)            | hardware random numbers; mix with other sources, never use alone                       | partial |
| SMT / Hyper-Threading (R4)      | sibling threads share caches: disable when mutually distrustful workloads share a core | partial |
| VT-x / AMD-V (R9, R15)          | hardware virtualization; off unless hypervisor or VBS needs it                         | partial |
| VT-d / AMD-Vi IOMMU (R10, R16)  | filters device DMA: enable, then test that all devices still work                      | yes     |

**VRM** — Voltage regulator module: board circuitry converting 12 V to CPU core voltage; weak VRMs throttle high-end CPUs.

**SPD** — Serial presence detect: EEPROM on each DIMM holding its JEDEC timings and XMP/EXPO profiles.

**JEDEC** — Standards body that defines DRAM generations, speeds and module formats.

**MT/s** — Mega-transfers per second: DDR data rate, twice the real clock in MHz.

**IOMMU** — Input/output MMU: translates and filters memory accesses made by devices (Intel VT-d, AMD-Vi, ARM SMMU).

**SLAT** — Second-level address translation (EPT/NPT): hardware-walked guest page tables, needed for fast virtualization.

**ESD** — Electrostatic discharge: static shock that silently damages components; use a wrist strap and antistatic bags.