

How the Internet Works: Cheat Sheet

The 12 lessons of the full course, in exam-ready form. Aligned with objectives of CompTIA A+ Core 1 (220-1201), A+ Core 2 (220-1202) and Network+ (N10-009).

IT Unpacked

youtube.com/@ITUnpacked

1 Router, modem & switch

- **Modem:** converts your ISP's signal (cable, DSL). On fibre, an **ONT** does that job.
- **Router:** joins your network to the internet; usually also DHCP, NAT and a firewall.
- **Switch:** connects devices inside one network, using MAC addresses (Layer 2).
- Your ISP box is usually all three in one. Two routers in a row = **double NAT**; fix with bridge or AP mode.

2 IP addresses

- IPv4: four numbers 0–255, e.g. 192.168.1.23 (32 bits, ~4.3 billion).
- **Private** (RFC 1918): 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16. Not routed on the internet.
- **NAT:** the router shares one public IP with every private device.
- Loopback 127.0.0.1. APIPA 169.254.x.x = no DHCP server reached.
- IPv6: 128 bits. fe80:: = link-local (your network only); addresses starting with 2 are usually public.

3 DNS

- Turns names into IP addresses: the internet's contacts app.
- Order: browser cache → OS cache → resolver; if the resolver hasn't cached it: root → TLD (.com) → authoritative server.
- Answers are cached for their **TTL**. DNS uses port 53.
- Try it: nslookup youtube.com

4 DHCP

- Hands out IP address, subnet mask, default gateway and DNS servers.
- **DORA:** Discover, Offer, Request, Acknowledge. Addresses are **leased**; renewal starts at 50%.
- UDP 67 (server) / 68 (client). **Reservation** = same address for one device every time.
- Try it: ipconfig /all. To watch DORA: ipconfig /release then ipconfig /renew in Command Prompt run as administrator (your connection drops for a few seconds).

5 Wi-Fi

- Wi-Fi 4/5/6/7 = 802.11n / ac / ax / be. Wi-Fi 6E adds 6 GHz.
- 2.4 GHz: further, slower, crowded. 5 and 6 GHz: faster, shorter range.
- Non-overlapping 2.4 GHz channels (exam answer): **1, 6, 11**.
- Security: **WPA3** best, WPA2 OK, never WEP or open.
- Try it: netsh wlan show interfaces (Win 11 may need Location turned on).

6 Ports: TCP vs UDP

IP gets data to the device; the **port** gets it to the right app (0–65,535). TCP = reliable (handshake); UDP = fast, no handshake.

Port	Protocol	Port	Protocol
20/21	FTP	110	POP3
22	SSH / SFTP	143	IMAP
23	Telnet	389	LDAP
25	SMTP	443	HTTPS
53	DNS	445	SMB
67/68	DHCP	3389	RDP
80	HTTP	587	SMTPTS: mail submission (STARTTLS)

Try it: netstat -an (the number after the last colon is the port).

7 What happens when you type a URL

- 0 DHCP (already done) → 1 **DNS** finds the IP → 2 default gateway, NAT, hops across the internet → 3 **TCP** handshake (SYN, SYN-ACK, ACK) + **TLS** on 443 → 4 **HTTP** GET → 200 OK.
- HTTP/3 runs over QUIC (UDP), so it skips the TCP handshake.
- Try it: tracert youtube.com

8 HTTPS & the padlock

- Certificate proves the name; it's usually issued by a **middle (intermediate) CA** that chains back to a **root** your device trusts.
- Key exchange in public (asymmetric), then fast **symmetric** encryption (e.g. AES) for the data.
- Padlock = private and genuine name, **not** an honest site. Phishing sites have padlocks too.
- Revocation checks: CRL, OCSP. Try it: certmgr.msc

9 The OSI model

#	Layer	Examples
7	Application	HTTP, DNS, DHCP
6	Presentation	encryption, formats (TLS is often placed at 6)
5	Session	opening/closing conversations
4	Transport	TCP, UDP, ports (segment/datagram)
3	Network	IP, routers (packet)
2	Data link	MAC, switches (frame)
1	Physical	cables, radio, hubs (bits)

Mnemonic (1→7): **Please Do Not Throw Sausage Pizza Away**. Try it: arp -a

10 Subnet masks

CIDR	Mask	Usable hosts
/16	255.255.0.0	65,534
/24	255.255.255.0	254
/25	255.255.255.128	126

- Usable hosts = $2^{\text{host bits}} - 2$ (network + broadcast addresses).
- Same network part = deliver directly; different = send to the **default gateway**.

11 VLANs

- A separate network made inside a switch (guest, CCTV, office on one box).
- **Access port:** one VLAN, untagged. **Trunk:** many VLANs, **802.1Q** tags.
- VLANs talk only through a **router** or **Layer 3 switch** (inter-VLAN routing).
- Moved desk, now on the guest range? Wrong VLAN on the port, not a bad cable.

12 Firewalls

- Rules match IP, port, protocol, direction → allow or deny. On most network firewalls, the **first match wins**, with an **implicit deny** at the end. (Windows Defender Firewall has no rule order: a block rule always beats an allow rule.)
- **Stateful:** lets replies to your own connections back in.
- Packet filter (Layers 3–4) vs **NGFW** (sees apps, Layer 7).
- Can't stop you clicking a bad link. Try it: netsh advfirewall show currentprofile

Exam traps & first checks

- Every site shows a certificate warning → check the PC's **date and time**.
- 169.254.x.x → DHCP failed (APIPA): check cable / Wi-Fi first.
- Can reach an IP but not a name → **DNS**.
- Troubleshoot **bottom up**: link → IP address → ping gateway → DNS.
- New allow rule not working → a deny rule above it matches first.

How the Internet Works: Course Bonuses

The extra exam topic at the end of each lesson of the full course. Page 2 of the cheat sheet.

IT Unpacked

youtube.com/@ITUnpacked

B1 Hub vs switch

	Hub	Switch
Sends data	to every port	mostly to one port (learns MACs)
Talking	one at a time	all ports at once
OSI layer	Layer 1	Layer 2
Collision domain	one, shared	one per port

B2 The old address classes

Class	First number	Default mask
A	1–126	255.0.0.0
B	128–191	255.255.0.0
C	192–223	255.255.255.0
D	224–239	none (multicast)
E	240–255	none (experimental)

127 = loopback; 0 is reserved. Modern networks use CIDR (any prefix length) instead.

B3 DNS record types

- **A**: name → IPv4. **AAAA**: name → IPv6.
- **CNAME**: alias (www → main name). **MX**: the domain's mail server.
- **TXT**: text, e.g. domain proof, SPF, DKIM, DMARC.
- **PTR**: IP → name (reverse lookup).
- Try it: `nslookup -type=mx gmail.com`

B4 Scopes, exclusions & DHCP relay

- **Scope**: the range handed out, e.g. .100–.200.
- **Exclusion**: inside the scope, never handed out.
- **Reservation**: one address for one MAC address.
- Discover is a broadcast and routers don't forward broadcasts, so clients on another subnet need a **DHCP relay** (Cisco: **IP helper**).

B5 Personal vs Enterprise Wi-Fi

- **Personal** (PSK): one shared password, checked by the access point.
- **Enterprise**: each user's own login, checked by a **RADIUS** server (**802.1X**). Remove one account, only that user loses access.
- WPA3 Personal uses **SAE**: stops offline password guessing.
- Turn **WPS** off: its PIN can be cracked in hours.

B6 Port ranges

Range	Ports	Example
Well-known	0–1,023	443 HTTPS
Registered	1,024–49,151	3389 RDP
Dynamic / ephemeral	49,152–65,535	your side

Your PC uses a random high port for its side of each connection (Linux uses its own range). Try it: `netstat -an`

B7 HTTP status codes

2xx success	200 OK
3xx go elsewhere	301 Moved Permanently
4xx problem with the request	404 Not Found, 403 Forbidden
5xx problem on the server	500 Internal Error, 503 Unavailable

A 404 or 500 means you **did** reach the server: not a Wi-Fi problem.

B8 The secure twins

Plain text	Secure twin
HTTP 80	HTTPS 443
Telnet 23	SSH 22
FTP 20/21	SFTP 22 (over SSH), FTPS 990 (implicit)
LDAP 389	LDAPS 636
IMAP 143	IMAP over TLS 993
POP3 110	POP3 over TLS 995

Passwords captured on the network? Find the plain-text protocol and swap it for its twin.

B9 The TCP/IP model

TCP/IP layer	OSI	Examples
Application	5–7	HTTP, DNS, DHCP
Transport	4	TCP, UDP
Internet	3	IP, routers
Link / network access	1–2	cables, Wi-Fi, MAC

Some books split the bottom layer and count five. "A Layer 2 problem" means the OSI layer.

B10 Quick subnet maths

Prefix	Block	Usable	Mask
/24	256	254	255.255.255.0
/25	128	126	255.255.255.128
/26	64	62	255.255.255.192
/27	32	30	255.255.255.224

Usable = block – 2 (to /30). Last mask number = 256 – block. /26 blocks start at .0, .64, .128, .192, so .70 and .100 share the .64–.127 subnet.

B11 The native VLAN

- On a trunk every frame carries an **802.1Q** tag, except the **native VLAN**'s (untagged; Cisco default VLAN 1).
- Ends disagree on the native VLAN → traffic leaks between VLANs.
- **Double tagging**: a tag hidden inside a tag; a one-way VLAN hop.
- Fix: an unused native VLAN, the same on both ends; nothing in VLAN 1.

B12 The DMZ (screened subnet)

- A separate network between the internet and the office, with firewall rules on both sides.
- Internet → DMZ web server: **allowed**. DMZ → office (new connections): **blocked**.
- A home router's "DMZ host" is not a real DMZ: it sends every unsolicited connection to one device.