

# CompTIA Network+ Flashcards — Bonus Deck

Printable flashcard deck: 60 cards, generated from the TemplateForge concept list for this guide.

## HOW TO PRINT:

1. Print this file double-sided on Letter, flip on SHORT edge.
2. Front pages show the Terms; each back page shows that same page's answers in the identical grid layout.
3. Cut along the grid lines. The card number in the top-right corner matches each front to its back.

STUDY TIP: quiz yourself with the Anki deck (import the CSV into Anki — it's free — note type Basic, fields by comma). Review daily; space your reviews instead of cramming.

**Source: TemplateForge study guide concept list. Facts are the guide's own verified content — always confirm exam details at the official testing organization's website.**

# OSI Model

#1

## Layer 1 — Physical

#2

## Layer 2 — Data Link

#3

## Layer 3 — Network

#4

## Layer 4 — Transport

#5

## Layer 5 — Session

#6

#1

## OSI Model

Seven layers: Physical, Data Link, Network, Transport, Session, Presentation, Application — the reference for how network functions stack.

Tip: Memorize bottom-up: "Please Do Not Throw Sausage Pizza Away."

Example: A router operates at Layer 3, a switch at Layer 2, a repeater at Layer 1.

#2

## Layer 1 — Physical

Transmits bits as signals over media: voltage, light pulses, radio waves; defines connectors, cabling, encoding.

Tip: Layer 1 problems are cable/signal/connector problems.

Example: A damaged Cat6 patch cable causes CRC errors — a Layer 1 fault.

#3

## Layer 2 — Data Link

Frames with MAC addresses; switches, bridges, NICs; sublayers LLC and MAC; error detection via FCS.

Tip: MAC addresses are burned-in at Layer 2 and never cross routers.

Example: A switch learns MAC addresses from frame sources and forwards on the correct port.

#4

## Layer 3 — Network

Logical addressing (IP), routing between networks, packet forwarding, fragmentation.

Tip: Routers strip the Layer 2 frame and rebuild it per hop.

Example: 192.168.1.10 to 10.0.0.5: each router hop re-encapsulates the packet in a new frame.

#5

## Layer 4 — Transport

End-to-end delivery: TCP (reliable, connection-oriented) vs UDP (connectionless, fast); ports, segmentation, sequencing.

Tip: Match protocol to need: TCP for accuracy, UDP for speed.

Example: Streaming video uses UDP; a file download uses TCP.

#6

## Layer 5 — Session

Establishes, manages, terminates sessions (dialog control) between applications.

Tip: NetBIOS is a classic session-layer example.

Example: An online meeting creates a session between your video app and the server.

#7

## Layer 6 — Presentation

#8

## Layer 7 — Application

#9

## Encapsulation

#10

## Protocol Data Units

#11

## MAC vs IP Address

#12

## TCP/IP Model

#7

## Layer 6 — Presentation

Formatting, encryption, compression — data in a form apps understand.

Tip: Encryption for the wire is often cited at this layer.

Example: TLS encrypts at presentation-ish scope; the data arrives decrypted to the app.

#8

## Layer 7 — Application

Protocols that users interact with: HTTP, HTTPS, FTP, SMTP, DNS, DHCP.

Tip: Most "which layer?" questions land on 1, 2, 3, 4, or 7.

Example: Your browser speaks HTTP (L7) over TCP (L4) to a server's IP (L3).

#9

## Encapsulation

Each layer adds its header to the payload: segment → packet → frame → bits.

Tip: Reverse process is de-encapsulation on the receiver.

Example: An HTTP request wraps in TCP header, then IP header, then Ethernet header.

#10

## Protocol Data Units

Layer names for data: L4 segment, L3 packet, L2 frame, L1 bits.

Tip: "Segment at transport, packet at network" is a classic match.

Example: Wireshark shows frames at L2 and packets at L3 in the same capture.

#11

## MAC vs IP Address

MAC: 48-bit physical, flat, per NIC; IP: logical, hierarchical, routable.

Tip: ARP maps IP → MAC on the local network.

Example: Host A ARPs for its gateway's MAC to send a packet off-subnet.

#12

## TCP/IP Model

Four layers: Network Interface, Internet, Transport, Application — the practical model used by the TCP/IP suite.

Tip: Modern exams map OSI to TCP/IP: internet ~ network, link ~ data link+physical.

Example: DNS (application) uses UDP/TCP (transport) over IP (internet) over Ethernet (link).

## Router

#13

## Switch

#14

## Static Routing

#15

## Dynamic Routing

#16

## OSPF

#17

## EIGRP

#18

#13

**Router**

Layer 3 device that forwards packets between networks using IP addressing and routing tables.

Tip: Default gateway of a host = the router's address.

Example: A home router connects your LAN (192.168.1.0/24) to your ISP's network.

#14

**Switch**

Layer 2 device that forwards frames by MAC address; segments collision domains.

Tip: Each switch port is its own collision domain.

Example: A 24-port switch gives 24 devices full-duplex dedicated bandwidth.

#15

**Static Routing**

Manually configured routes; predictable, no protocol overhead, but no automatic failover.

Tip: Use static for small nets and default routes; default route 0.0.0.0/0.

Example: A branch router has a static default route to its ISP gateway.

#16

**Dynamic Routing**

Protocols exchange routes and adapt to topology changes automatically.

Tip: Interior (IGP) vs exterior (EGP) — BGP is the EGP.

Example: OSPF reconverges around a failed link without an admin touching config.

#17

**OSPF**

Open Shortest Path First: link-state IGP, cost = inverse bandwidth, areas for scale.

Tip: OSPF floods LSAs and runs SPF; fast convergence in campus/enterprise.

Example: A campus runs OSPF area 0 core; each building is another area.

#18

**EIGRP**

Cisco proprietary (now open) hybrid distance-vector IGP; metrics from bandwidth + delay.

Tip: Cisco shops: EIGRP; non-Cisco: OSPF.

Example: A Cisco-only network runs EIGRP with successor/feasible-successor loop prevention.

## BGP

#19

## Route Selection

#20

## Administrative Distance

#21

## NAT

#22

## PAT (Overload)

#23

## FHRP

#24

#19

**BGP**

Border Gateway Protocol: path-vector EGP, used between autonomous systems; TCP 179.

Tip: BGP = internet routing; attributes like AS-PATH, LOCAL\_PREF pick paths.

Example: An ISP advertises its customer prefixes to peers via eBGP.

#20

**Route Selection**

Longest-prefix match wins; then administrative distance, then metric.

Tip: A /32 host route beats any summary — longest prefix always first.

Example: A router has 0.0.0.0/0 and 10.1.0.0/16: packet to 10.1.2.3 uses the /16.

#21

**Administrative Distance**

Trust rating of route sources (e.g., connected 0, static 1, OSPF 110) — lower wins.

Tip: AD breaks ties between protocols; metric breaks ties within one.

Example: A static route (AD 1) beats OSPF (AD 110) to the same prefix.

#22

**NAT**

Network Address Translation maps private IPs to public ones — many-to-one with overloading (PAT).

Tip: NAT/PAT lets an entire LAN share one public IP.

Example: 50 home devices all reach the internet through one WAN IP via PAT.

#23

**PAT (Overload)**

Port Address Translation: unique source ports distinguish translations of the same public IP.

Tip: Without PAT, one public IP = one outbound translation.

Example: Two laptops browsing simultaneously use different source ports behind the same public IP.

#24

**FHRP**

First-Hop Redundancy Protocol (HSRP, VRRP, GLBP): two routers share a virtual IP for gateway failover.

Tip: The virtual IP is the hosts' default gateway.

Example: Router A dies; the standby takes over the virtual gateway IP in seconds.

#25

## Virtual IP (VIP)

#26

## Subinterfaces and Router-on-a-Stick

#27

## Physical vs Logical Diagrams

#28

## Rack Diagrams

#29

## Cable Maps and Network Diagrams

#30

## Asset Inventory

#25

## Virtual IP (VIP)

An IP not bound to a physical interface — used by FHRP, load balancers, HA clusters.

Tip: VIP moves between devices transparently to clients.

Example: A load balancer fronts four web servers with one VIP.

#26

## Subinterfaces and Router-on-a-Stick

One physical interface split into logical subinterfaces, each tagged with a VLAN — trunking for routing.

Tip: Router-on-a-stick routes between VLANs on one trunk link.

Example: SWITCH trunk → router Gi0/0.10 (VLAN 10) and Gi0/0.20 (VLAN 20) routes inter-VLAN traffic.

#27

## Physical vs Logical Diagrams

Physical = devices, ports, locations, cabling; logical = addressing, VLANs, protocols, zones.

Tip: Keep both current — they answer different questions.

Example: A logical diagram shows VLAN 10 = 192.168.10.0/24; the physical shows which switch port serves each desk.

#28

## Rack Diagrams

Show equipment placement in racks: which RU, which device, power and network connections.

Tip: Essential for remote hands and capacity planning.

Example: A rack diagram shows server C-03 in RU 12 with PDU A and B feeds.

#29

## Cable Maps and Network Diagrams

Cable maps trace physical cabling run by run; network diagrams show topology and links.

Tip: Update after every change, or both drift.

Example: A technician pulls the wrong cable after trusting an outdated cable map.

#30

## Asset Inventory

Register devices: model, serial, location, firmware, owner, lifecycle dates.

Tip: Feeds licensing, support renewals, and audits.

Example: An inventory flag shows 40 switches past EOL needing replacement.

**IPAM**

#31

**SLA**

#32

**Wireless Surveys (Documented)**

#33

**EOL and EOS**

#34

**Software and Firmware  
Management**

#35

**Decommissioning**

#36

#31

**IPAM**

IP Address Management: structured records of subnets and assigned addresses.

Tip: Prevents overlap conflicts and eases DHCP/DNS integration.

Example: IPAM shows 192.168.50.0/24 with 60% utilization — time to plan a new subnet.

#32

**SLA**

Service Level Agreement: promised uptime, performance, response times, penalties.

Tip: The SLA defines what "we're compliant" means.

Example: An ISP SLA promises 99.9% uptime; a month with 1.5h outage is a breach.

#33

**Wireless Surveys (Documented)**

Heatmaps and coverage reports kept as baseline documentation.

Tip: Useful for later troubleshoots and capacity adds.

Example: A survey map shows -67 dBm worst-case coverage in the warehouse.

#34

**EOL and EOS**

End of Life (no longer sold) / End of Support (no updates, no support).

Tip: Budget refresh BEFORE EOS — unsupported gear is a risk.

Example: A switch line hits EOS; the admin plans replacement before the security patches stop.

#35

**Software and Firmware Management**

Patch/firmware cycles per policy; staged rollout; rollback plans.

Tip: Test firmware in a lab before production.

Example: Switch firmware updates run on a maintenance window with a rollback image saved.

#36

**Decommissioning**

Remove retired gear safely: config wipe, data sanitization, disposal/recycling.

Tip: Wipe configs and persistent storage before disposal.

Example: A retired router has its config erased and drives securely wiped before recycling.

#37

## Baseline Documentation

#38

## CIA Triad

#39

## Risk, Vulnerability, Exploit, Threat

#40

## Least Privilege

#41

## Zero Trust

#42

## Defense in Depth

#37

## Baseline Documentation

Performance baselines (CPU, bandwidth, latency) captured at normal operation for later comparison.

Tip: Baselines make anomalies obvious.

Example: A 20% link-utilization baseline doubles to 40% — investigation is triggered.

#38

## CIA Triad

Confidentiality (secrecy), Integrity (unmodified), Availability (accessible) — the security triangle.

Tip: Rank which C is most at risk per scenario.

Example: Encryption serves confidentiality; hashes serve integrity; redundant links serve availability.

#39

## Risk, Vulnerability, Exploit, Threat

Threat = actor/capability; vulnerability = weakness; exploit = the act; risk = likelihood × impact.

Tip: Sequence: threat exploits vulnerability → risk realized.

Example: An unpatched firewall (vulnerability) is exploited by a scanner (threat) → breach (risk).

#40

## Least Privilege

Users get only the permissions needed to do their job — nothing more.

Tip: Apply to accounts, ACLs, and service accounts alike.

Example: A helpdesk tech can reset passwords but cannot change firewall rules.

#41

## Zero Trust

Trust nothing by default; verify every request regardless of location.

Tip: "Never trust, always verify" — micro-segmentation and MFA.

Example: An internal file share still requires MFA and per-request auth in zero trust.

#42

## Defense in Depth

Multiple layered controls — if one fails, others still protect.

Tip: Layers: perimeter, network, host, app, data.

Example: A server is behind a firewall, an IDS, host firewall, and encrypted at rest.

#43

## **Data in Transit vs at Rest**

#44

## **Authentication vs Authorization**

#45

## **Accounting**

#46

## **AAA Protocols**

#47

## **Troubleshooting Methodology**

#48

## **Identifying the Problem**

#43

### Data in Transit vs at Rest

In transit: moving over networks (encrypt with TLS/IPsec); at rest: stored data (encrypt disks/DBs).

Tip: Match encryption to the state of the data.

Example: HTTPS encrypts web traffic in transit; BitLocker encrypts the laptop disk at rest.

#44

### Authentication vs Authorization

Authentication proves identity; authorization decides what identity may do.

Tip: AuthN first, AuthZ second — always in that order.

Example: A user logs in (auth) and is granted read-only (authorization) to the share.

#45

### Accounting

Logging and auditing what users did — the third A of AAA.

Tip: Ties actions to identities for forensics and compliance.

Example: The firewall logs who changed rule #14 and when.

#46

### AAA Protocols

RADIUS (UDP 1812/1813) and TACACS+ (TCP 49, Cisco) — central auth/acct.

Tip: RADIUS = network access; TACACS+ = device admin + per-command auth.

Example: WPA2-Enterprise delivers RADIUS; network admins authenticate to routers via TACACS+.

#47

### Troubleshooting Methodology

Official flow: identify the problem → establish a theory of probable cause → test the theory → establish a plan of action and implement it → verify functionality → document findings.

Tip: Work the steps in order; escalate if theory fails.

Example: Link is down: identify scope, theorize cabling, test with a known-good cable, verify, document.

#48

### Identifying the Problem

Gather information, duplicate the issue, question users, identify recent changes, determine scope.

Tip: "Ask, gather, duplicate" beats guessing.

Example: A user reports slow internet; helpdesk asks when it started and what changed yesterday.

#49

## Establish a Theory

#50

## Testing the Theory

#51

## Plan and Implement

#52

## Verify Functionality

#53

## Document Findings

#54

## Escalation

#49

## Establish a Theory

Generate probable causes from evidence, not from thin air; most probable first.

Tip: Split-half testing narrows the search fast.

Example: Slow for one user → theory: client-side; slow for everyone → theory: WAN or server.

#50

## Testing the Theory

Confirm or eliminate causes: ping, traceroute, replacement, monitoring.

Tip: If a theory is disproven, escalate or form a new one.

Example: Pinging the gateway succeeds while the internet fails → theory shifts to WAN path.

#51

## Plan and Implement

Write the fix, assess impact, apply in a maintenance window if needed, include rollback.

Tip: Smallest change that fixes it first.

Example: Replace the suspected patch cable with a known-good one, then verify.

#52

## Verify Functionality

Confirm the fix works AND nothing else regressed; check from the user's perspective.

Tip: Test beyond the symptom: full workflow, not just ping.

Example: After the cable swap, the user downloads a file and opens the app successfully.

#53

## Document Findings

Record symptoms, cause, resolution, and prevention — the knowledge base grows.

Tip: Documentation is the step most skipped and most valuable.

Example: The ticket logs: "port 12 bad patch cable replaced — future: re-test port after moves."

#54

## Escalation

When scope is beyond you, hand off with solid evidence and notes.

Tip: Include what was tested and ruled out.

Example: The helpdesk escalates a WAN latency issue to the ISP with traceroute evidence.

**Incorrect Cable Type**

#55

**Signal Degradation and Attenuation**

#56

**Improper Termination**

#57

**TX/RX Transposed**

#58

**Damaged Connectors**

#59

**EMI and Crosstalk**

#60

#55

### Incorrect Cable Type

Wrong category, straight vs crossover, fiber mode mismatch (SM vs MM), wrong connector.

Tip: Modern switches auto-MDIX, but category still matters.

Example: A 10G run installed with Cat5e negotiates down to 1G — wrong category for the need.

#56

### Signal Degradation and Attenuation

Long runs, bad terminations, EMI, poor splices weaken signals.

Tip: Check length (<100 m copper), cable damage, interference sources.

Example: A 110-m run produces CRC errors — run is past copper's practical limit; use fiber or a switch.

#57

### Improper Termination

Wrong pairs, untwisted too far, partial pin seating, mis-crimped RJ45.

Tip: Re-terminate with minimal untwist per T568A/B.

Example: Every pair works but throughput stalls: 1-2 pair swapped at the jack — re-terminate.

#58

### TX/RX Transposed

Two ends not crossed correctly (or wrong crossover) — link fails to pass traffic.

Tip: Auto-MDIX fixes most; older gear needs crossover.

Example: Two switches won't pass traffic until a crossover replaces the straight cable.

#59

### Damaged Connectors

Bent pins, loose jack, broken clip, dirty contacts.

Tip: Replace the cable — repairs rarely hold.

Example: A laptop loses link on every movement: the RJ45 clip is broken — swap the cable.

#60

### EMI and Crosstalk

Electrical interference from motors/fluorescent lights; crosstalk between adjacent pairs.

Tip: Keep data away from power; shield or use fiber near noise.

Example: A cable run beside a motor causes flapping — reroute the cable.