100 Network Topics — Interview Study Sheet

Companion to **"100 Network Topics to Revise Before Your Interview"** · hmmnm.com · Prabhu Kalyan Samal

Free resource from the **HMMNM** weekly security briefing · **hmmnm.com**

1 · The topic map (what to cover, in order)

- **Essentials** — what a network is; the Internet and its origins; IP addresses; ports and the apps that use them; servers vs. clients.
- **TCP/IP protocol suite** — TCP (reliable, ordered, slower) vs. UDP (fast, connectionless) and when each is used.
- **OSI model** — the 7 layers and how traffic flows; TCP/IP vs. OSI mapping; how ports enable communication; MAC addresses; DNS (recursive vs. iterative); DHCP (allocation, dynamic vs. reservation); SSL; subnetting and IP classes; VPNs; network devices; ARP/RARP; broadcast vs. unicast vs. multicast.
- **Operations** — latency/loss/throughput; fiber optics; backup & restore; traffic management; anomaly detection; security best practices; monitoring policies; automation (Ansible/Puppet); segmentation; performance testing; virtualization (NSX/ACI); capacity planning; auditing; recovery strategies; alerting; ACLs; optimization tools; patching; incident response.
- **Architecture & design** — design principles; traffic analysis; monitoring automation (Nagios/Zabbix/PRTG); certifications (CCNA Security, CISSP); compliance (PCI DSS, HIPAA); configuration management; performance tuning; analysis & visualization (Wireshark/Splunk); threat landscape (malware, phishing, DDoS); disaster recovery; monitoring best practices.

How interviewers read this: they rarely ask all 100 — they pick 3–5 anchors (TCP vs UDP, OSI layers, DNS, DHCP, subnetting) and drill into how you reason, not what you memorize.

2 · The 20 ports that come up every single time

Port	Service	Why it matters in interviews / security
`tcp/20-21`	FTP	Cleartext file transfer — classic "replace with SFTP" answer.
`tcp/22`	SSH	Secure remote admin; key-based auth beats passwords.
`tcp/23`	Telnet	Cleartext remote shell — flag it as a finding wherever it's open.
`tcp/25`	SMTP	Mail relay; open relays = spam source.
`udp/53`	DNS	Name resolution; open resolvers feed amplification DDoS.
`tcp/80`	HTTP	Web traffic; expect the "redirect to 443" follow-up.
`tcp/110 / 143`	POP3 / IMAP	Mail retrieval; IMAP keeps server-side state.
`udp/123`	NTP	Time sync; logs are useless if clocks disagree.
`tcp/135-139`	RPC / NetBIOS	Legacy Windows surface — should not face the internet.
`tcp/1433`	MSSQL	Database engines never belong on public IPs.
`udp/161-162`	SNMP	Device management; default "public" community is a finding.
`tcp/389 / 636`	LDAP / LDAPS	Directory services; AD lives here.
`tcp/445`	SMB	File sharing — EternalBlue's door; must not be internet-facing.
`tcp/3306`	MySQL	Same rule as MSSQL: bound to localhost/private only.

`tcp/3389`	RDP	Windows remote desktop; brute-force & NLA discussions.
`udp/3389 etc.`	RDP (UDP mode)	Modern RDP also uses UDP for session reliability.
`tcp/443`	HTTPS	TLS everywhere; know SNI and certificate validation.
`tcp/465 / 587`	SMTP secure/submit	Modern mail submission with TLS.
`tcp/6379`	Redis	Unauthenticated by default — a recurring real-world breach.
`tcp/8080 / 8443`	HTTP alt	Proxies, admin panels, dev servers — always enumerate.

3 · Deep dives you should be able to narrate

TCP handshake — and how attacks abuse it

- SYN → SYN-ACK → ACK; sequence numbers make the stream reliable and ordered.
- **SYN flood:** attacker sends SYNs and never completes the handshake, exhausting half-open connection tables.
- **SYN cookies:** server encodes connection state into the sequence number instead of storing it — stateless defense.

DNS resolution — the full journey

- Browser/OS cache → recursive resolver → root ("ask .com") → TLD ("ask example's NS") → authoritative (the answer).
- Record types: A/AAAA (addresses), CNAME (alias), MX (mail), NS (delegation), TXT (proof/SPF/DKIM), PTR (reverse).
- Security angle: cache poisoning, DNSSEC's signing chain, and why open resolvers get abused for amplification.

Subnetting — the only formula you need

```
usable hosts = 2^(32 − prefix) − 2   →   /26 = 2^6 − 2 = 62 hosts
```

- Worked example A: /26 block 192.168.1.64/26 → range .65–.126, broadcast .127, 62 hosts.
- Worked example B: need 500 hosts → 2^9 − 2 = 510 → /23 (512 addresses).
- IP classes (A/B/C) are legacy; CIDR replaced them — say so, it scores points.

VLANs — segmentation as security

- VLANs split one physical switch into isolated broadcast domains (per team, per trust level).
- **VLAN hopping:** double-tagging or switch-spoofing (DTP) attacks; defense: disable auto-trunking, explicit native VLAN, unused-port shutdown.

Firewalls — stateful vs. next-gen

- Packet filter: per-packet rules, no memory of connections.
- Stateful: tracks sessions — replies are allowed only for connections it saw begin.
- NGFW: adds application awareness, TLS inspection, IPS, identity-based rules.

NAT — how it works and why it breaks things

- Static (1:1), dynamic (pool), PAT (many-to-one, port multiplexing — what home routers do).
- Breaks: inbound connections (need port-forwarding), protocols embedding IPs/ports (SIP, FTP active mode) → ALGs, STUN/TURN/ICE for WebRTC-style traversal.

4 · Prep plan by role (say this when asked "how do you keep up?")

- **DevOps / SRE:** subnetting & CIDR, NAT in VPCs, load balancers vs. reverse proxies, DNS TTLs during deploys, segmentation of admin planes.
- **Security analyst / SOC:** reading pcaps (handshakes, scans, exfil patterns), DNS as an exfil channel, segmentation & lateral-movement paths, log sources every device should emit.

- **Pentester:** service enumeration (the ports table), protocol abuse (SMB/LDAP/Redis), pivoting across VLANs, and explaining business impact of each finding.

Hands-on that makes this stick: run Wireshark through a full TCP handshake; resolve a domain with **nslookup**/dig and map the answer chain; traceroute your own site and explain every hop; subnet your home lab by hand; touch iptables/nftables once per rule type.

Companion to "100 Network Topics to Revise Before Your Interview" — read the full deep-dives at https://hmmnm.com/100-network-topics-revise-before-interview/ · Free weekly briefing at hmmnm.com · © 2026 Prabhu Kalyan Samal — share freely, keep it attributed.