**Part 1 – Networking Basics (1–25)**

**1. What is computer networking?
The practice of connecting computers and devices to share resources and data.**

**2. What is an IP address?
A unique number assigned to a device for communication in a network.**

**3. What is IPv4 vs IPv6?**

* **IPv4: 32-bit addresses (e.g., 192.168.1.1)**
* **IPv6: 128-bit addresses (e.g., 2001:db8::1)**

**4. What is the difference between public and private IP addresses?**

* **Public: Reachable over the internet**
* **Private: Used within local networks**

**5. What is a subnet mask?
A number that defines the network and host portion of an IP address.**

**6. What is a MAC address?
A unique hardware identifier for a network interface card.**

**7. What is DNS?
Domain Name System — translates domain names into IP addresses.**

**8. What is DHCP?
Dynamic Host Configuration Protocol — automatically assigns IP addresses.**

**9. What is the difference between TCP and UDP?**

* **TCP: Reliable, connection-based.**
* **UDP: Faster, connectionless, no guaranteed delivery.**

**10. What is HTTP vs HTTPS?
HTTPS is HTTP with encryption using SSL/TLS.**

**11. What is FTP?
File Transfer Protocol — transfers files between computers.**

**12. What is SMTP?
Simple Mail Transfer Protocol — sends emails.**

**13. What is IMAP vs POP3?**

* **IMAP: Keeps email on the server.**
* **POP3: Downloads and removes email from the server.**

**14. What is a firewall?
A security system that filters network traffic.**

**15. What is a proxy server?
An intermediary between a client and the internet.**

**16. What is NAT?
Network Address Translation — maps private IPs to public IPs.**

**17. What is a VPN?
Virtual Private Network — encrypts and tunnels network traffic securely.**

**18. What is ping?
A tool to check connectivity between devices.**

**19. What is traceroute?
A tool that shows the path packets take to reach a destination.**

**20. What is bandwidth?
The maximum amount of data transferable over a network in a given time.**

**21. What is latency?
The delay between sending and receiving data.**

**22. What is jitter?
Variation in packet delay times.**

**23. What is packet loss?
When network packets fail to reach their destination.**

**24. What is a port number?
A numeric identifier for a specific process or service in a device.**

**25. What are common TCP ports QA engineers should know?
HTTP (80), HTTPS (443), FTP (21), SMTP (25), DNS (53).**

**Part 2 – Network Models & Protocols (26–50)**

**26. What is the OSI model?
A 7-layer framework for understanding network communication.**

**27. What are the OSI model layers?
Physical, Data Link, Network, Transport, Session, Presentation, Application.**

**28. What is the TCP/IP model?
A 4-layer model: Network Interface, Internet, Transport, Application.**

**29. Which OSI layer does HTTP work on?
Application layer.**

**30. Which OSI layer does IP work on?
Network layer.**

**31. Which OSI layer does TCP/UDP work on?
Transport layer.**

**32. Which OSI layer does Ethernet work on?
Data Link layer.**

**33. What is ARP?
Address Resolution Protocol — maps IP addresses to MAC addresses.**

**34. What is ICMP?
Internet Control Message Protocol — used for diagnostic tools like ping.**

**35. What is SSL/TLS?
Protocols for securing data over the internet.**

**36. What is WebSocket?
A protocol for persistent two-way communication between client and server.**

**37. What is REST API communication protocol?
Usually HTTP/HTTPS over TCP/IP.**

**38. What is MQTT?
A lightweight messaging protocol for IoT devices.**

**39. What is SNMP?
Simple Network Management Protocol — manages network devices.**

**40. What is the difference between unicast, multicast, and broadcast?**

* **Unicast: One-to-one**
* **Multicast: One-to-many (selected)**
* **Broadcast: One-to-all**

**41. What is a VLAN?
Virtual Local Area Network — segments networks for better management and security.**

**42. What is QoS?
Quality of Service — prioritizes certain network traffic.**

**43. What is load balancing?
Distributing traffic across multiple servers.**

**44. What is failover?
Switching to a backup system during failure.**

**45. What is a CDN?
Content Delivery Network — distributes content closer to users for speed.**

**46. What is IPv6 better than IPv4?
Larger address space, better security, auto-configuration.**

**47. What is a packet sniffer?
A tool for capturing network traffic (e.g., Wireshark).**

**48. What is a socket in networking?
An endpoint for sending or receiving data.**

**49. What is DNS caching?
Storing DNS lookups locally to improve speed.**

**50. What is reverse DNS lookup?
Finding the domain name for a given IP address.**

**Part 3 – QA Testing & Networking (51–75)**

**51. Why should QA engineers understand networking?
To troubleshoot connectivity issues and verify application performance.**

**52. What is network testing in QA?
Verifying an application works correctly over various network conditions.**

**53. How do you simulate slow networks?
Use tools like Network Link Conditioner or Chrome DevTools throttling.**

**54. How do you test API response times?
Use tools like Postman, JMeter, or cURL with timers.**

**55. How do you check network requests in a browser?
Use Developer Tools → Network tab.**

**56. What is packet inspection in QA testing?
Examining network traffic to validate requests and responses.**

**57. How do you test WebSocket communication?
Use browser dev tools or WebSocket test clients.**

**58. How do you verify HTTPS certificates?
Check certificate validity in the browser or using openssl.**

**59. How do you test DNS resolution?
Use nslookup or dig commands.**

**60. How do you check port connectivity?
Use telnet <host> <port> or nc (netcat).**

**61. How do you detect packet loss?
Use ping or network monitoring tools.**

**62. How do you check server latency?
Ping or traceroute to the server.**

**63. How do you simulate packet loss?
Use tools like tc (Linux) or WANem.**

**64. How do you test API under different network conditions?
Use JMeter or Charles Proxy to simulate latency and bandwidth changes.**

**65. How do you verify that an API request is secure?
Check for HTTPS, authentication, and encrypted payloads.**

**66. How do you capture mobile app network traffic?
Use tools like Charles Proxy or Fiddler with mobile proxy setup.**

**67. How do you troubleshoot a “connection refused” error?
Check server availability, firewall rules, and port status.**

**68. How do you verify load balancing?
Make repeated requests and check if they hit different servers.**

**69. How do you check API request size limits?
Send progressively larger requests and monitor responses.**

**70. How do you ensure API responses are cacheable?
Check HTTP cache headers.**

**71. How do you test for network security vulnerabilities?
Use tools like OWASP ZAP or Burp Suite.**

**72. How do you test a multi-region deployment?
Check performance from different geographic locations.**

**73. How do you check if a DNS change has propagated?
Use online DNS checkers or dig from multiple locations.**

**74. How do you test an application after a firewall change?
Validate all required ports and services are accessible.**

**75. How do you confirm API rate limiting?
Send multiple requests rapidly and check for 429 Too Many Requests.**

**Part 4 – Interview & Advanced Scenarios (76–100)**

**76. What’s the difference between TCP 3-way handshake and 4-way termination?**

* **Handshake: SYN → SYN-ACK → ACK**
* **Termination: FIN → ACK → FIN → ACK**

**77. What is MTU?
Maximum Transmission Unit — largest packet size that can be sent.**

**78. What is fragmentation in networking?
Splitting packets into smaller ones to fit MTU.**

**79. What is a keep-alive signal?
A periodic message to keep a connection open.**

**80. What is the difference between stateful and stateless protocols?**

* **Stateful: Maintains session info (TCP).**
* **Stateless: No session info (HTTP).**

**81. What is port forwarding?
Redirecting network traffic from one port to another.**

**82. What is a hop in networking?
A pass through a network device like a router.**

**83. What is load testing at the network level?
Simulating traffic to measure network capacity.**

**84. What is throughput testing?
Measuring actual data transfer rate.**

**85. What is a proxy vs reverse proxy?**

* **Proxy: Client → Proxy → Server**
* **Reverse Proxy: Client → Reverse Proxy → Multiple servers**

**86. What is a honeypot in networking?
A security trap to lure attackers.**

**87. What is IP spoofing?
Faking an IP address to disguise identity.**

**88. What is DDoS?
Distributed Denial of Service — flooding a server with traffic.**

**89. How does CDN improve performance?
By caching content closer to users.**

**90. What is content compression in networking?
Reducing data size (e.g., GZIP) before sending.**

**91. What is HTTP/2 vs HTTP/1.1?
HTTP/2 has multiplexing, better compression, and faster performance.**

**92. What is QUIC protocol?
A Google-developed protocol for faster web communication.**

**93. What is TLS handshake?
The process of establishing a secure HTTPS connection.**

**94. What is session persistence?
Keeping a user’s session tied to the same server.**

**95. What is sticky session in load balancing?
Ensuring a user’s requests always go to the same server.**

**96. What is failback in networking?
Returning traffic to the primary system after failover.**

**97. What is deep packet inspection?
Inspecting the data part of network packets for analysis or filtering.**

**98. What is an anycast IP address?
An IP assigned to multiple servers, routing to the nearest one.**

**99. What is zero trust networking?
Never trust, always verify — all traffic is authenticated.**

**100. Best networking practices for QA engineers**

* **Understand basic protocols**
* **Monitor with the right tools**
* **Test in real-world network conditions**
* **Keep security in mind**

**Part 1 – Networking & Number Systems (1–25)**

**1. What is binary in networking?**
Binary is the base-2 number system (0 and 1) used by computers to process data.

**2. Why is binary important in networking?**
IP addresses, MAC addresses, and data transmission are all represented in binary.

**3. What is hexadecimal in networking?**
Base-16 number system (0–9, A–F) often used for representing MAC and IPv6 addresses.

**4. What is the difference between binary and hexadecimal?**
Binary uses 2 symbols; hexadecimal uses 16 symbols for compact representation.

**5. How is an IP address stored in binary?**
Each octet of an IPv4 address is stored as 8 binary bits.

**6. How do you convert binary to decimal?**
Multiply each bit by 2ⁿ (where n is position from right) and sum up.

**7. How do you convert decimal to binary?**
Divide by 2 repeatedly and record remainders in reverse order.

**8. How is hexadecimal used in MAC addresses?**
A MAC address like 00:1A:2B:3C:4D:5E is represented in hex pairs.

**9. What is ASCII in networking?**
American Standard Code for Information Interchange — maps characters to binary values.

**10. What is Unicode?**
An encoding standard for text representation across languages.

**11. Why do network packets include binary headers?**
Headers store routing and protocol data in binary for fast processing.

**12. What is bit rate in networking?**
The number of bits transmitted per second.

**13. What is baud rate?**
Number of signal changes per second in data transmission.

**14. What is the difference between bits and bytes?**

* **Bit:** 1 binary digit
* **Byte:** 8 bits

**15. What is a nibble in binary?**
A group of 4 bits (half a byte).

**16. What is a dock station?**
A device that connects a laptop to multiple peripherals like monitors and network cables.

**17. How does a dock station help in QA testing?**
It allows connecting to wired networks, multiple devices, and external monitors easily.

**18. What is a network interface card (NIC)?**
A hardware component that connects a device to a network.

**19. What is a switch in networking?**
A device that connects multiple devices in a LAN and forwards data.

**20. What is a hub in networking?**
A basic network device that broadcasts data to all connected devices.

**21. What is a router?**
A device that routes traffic between different networks.

**22. What is a modem?**
Converts digital data into signals for transmission over phone/cable lines.

**23. What is an access point?**
A device that extends wireless network coverage.

**24. What is PoE in networking?**
Power over Ethernet — delivering power and data through the same Ethernet cable.

**25. What is loopback address in networking?**
127.0.0.1 — used to test network communication within the same machine.

**Part 2 – Network Communication & Protocols (26–50)**

**26. What is a packet in networking?**
A unit of data sent over a network.

**27. What is encapsulation?**
Wrapping data with protocol headers before transmission.

**28. What is decapsulation?**
Removing protocol headers to retrieve data.

**29. What is a frame in networking?**
A data packet at the Data Link layer.

**30. What is the MTU?**
Maximum Transmission Unit — largest packet size allowed.

**31. What is port number in networking?**
A unique number identifying a specific application/service on a device.

**32. What are well-known ports?**
Ports 0–1023 (e.g., HTTP 80, HTTPS 443).

**33. What is ARP in networking?**
Maps an IP address to a MAC address.

**34. What is RARP?**
Reverse ARP — maps a MAC address to an IP address.

**35. What is ICMP?**
Protocol used for network diagnostics (e.g., ping).

**36. What is TCP handshake?**
Three-step connection setup: SYN → SYN-ACK → ACK.

**37. What is UDP?**
Connectionless transport protocol with no delivery guarantees.

**38. What is DHCP lease time?**
How long an IP address is assigned before renewal.

**39. What is TTL in networking?**
Time To Live — limits packet lifetime to prevent looping.

**40. What is DNS propagation?**
The time it takes for DNS changes to update worldwide.

**41. What is CDN?**
Content Delivery Network — caches content closer to users.

**42. What is NAT loopback?**
Accessing a public service using its external IP from inside the same network.

**43. What is VLAN trunking?**
Carrying multiple VLANs over a single network link.

**44. What is IGMP?**
Internet Group Management Protocol — manages multicast groups.

**45. What is network segmentation?**
Dividing a network into smaller parts for performance and security.

**46. What is QoS in networking?**
Prioritizing certain network traffic for better performance.

**47. What is SSL offloading?**
Moving SSL encryption/decryption from the server to another device.

**48. What is a reverse proxy?**
A proxy that routes traffic from clients to multiple backend servers.

**49. What is IPsec?**
A protocol suite for securing IP communications.

**50. What is MPLS?**
Multiprotocol Label Switching — speeds up network traffic flow.

**Part 3 – QA Engineer Networking Tasks (51–75)**

**51. Why is networking important for QA engineers?**
To test connectivity, security, and performance of applications.

**52. How do you check if a server is reachable?**
Use ping command.

**53. How do you check network path to a server?**
Use traceroute (Linux/Mac) or tracert (Windows).

**54. How do you test port availability?**
Use telnet host port or nc -zv host port.

**55. How do you capture HTTP traffic for testing?**
Use tools like Fiddler, Charles Proxy, or Wireshark.

**56. How do you simulate slow internet for testing?**
Use Chrome DevTools throttling or network simulation tools.

**57. How do you verify API HTTPS security?**
Check certificate validity and encryption strength.

**58. How do you test DNS changes?**
Use nslookup or dig.

**59. How do you monitor bandwidth usage?**
Use tools like iftop or Windows Task Manager.

**60. How do you test multiple network interfaces?**
Switch adapters and verify application behavior.

**61. How do you test mobile apps on different networks?**
Use Wi-Fi, 4G/5G, and simulate poor connections.

**62. How do you log network errors?**
Capture server and client logs during tests.

**63. How do you test firewall restrictions?**
Try accessing blocked services and verify access control.

**64. How do you test VPN impact on performance?**
Measure response times with and without VPN.

**65. How do you confirm load balancer distribution?**
Check server responses for session IDs or headers.

**66. How do you test network failover?**
Disconnect the primary link and check if backup works.

**67. How do you test SSL certificate renewal?**
Access the app after certificate update.

**68. How do you simulate packet loss?**
Use tc command in Linux or WANem.

**69. How do you test for cache freshness?**
Check if updated content appears without clearing cache.

**70. How do you test cloud-hosted applications?**
Verify latency, availability, and multi-region access.

**71. How do you confirm rate limiting?**
Send rapid requests and look for HTTP 429 errors.

**72. How do you capture mobile network requests?**
Route mobile traffic through a proxy tool.

**73. How do you test network APIs without backend?**
Mock responses using Postman or Mockoon.

**74. How do you verify multi-region failover?**
Shut down one region and check traffic routing.

**75. How do you validate WebSocket connections?**
Check persistent connection and message exchange in dev tools.

**Part 4 – Interview Networking Q&A (76–100)**

**76. What is a default gateway?**
A router that forwards traffic to other networks.

**77. What is a static IP address?**
An IP manually assigned to a device.

**78. What is a dynamic IP address?**
An IP assigned automatically by DHCP.

**79. What is a broadcast domain?**
A network segment where any broadcast reaches all devices.

**80. What is a collision domain?**
A network segment where devices compete for bandwidth.

**81. What is half-duplex?**
Communication in one direction at a time.

**82. What is full-duplex?**
Communication in both directions simultaneously.

**83. What is a patch cable?**
A short Ethernet cable used for connecting devices.

**84. What is a crossover cable?**
A cable with reversed wiring for connecting similar devices.

**85. What is 10/100/1000 Ethernet?**
Network speeds of 10 Mbps, 100 Mbps, and 1 Gbps.

**86. What is PoE switch?**
A switch that delivers both power and data via Ethernet.

**87. What is network throughput?**
The actual data transfer rate achieved.

**88. What is bandwidth throttling?**
Deliberately limiting available bandwidth.

**89. What is network topology?**
The arrangement of devices in a network (e.g., star, mesh).

**90. What is star topology?**
All devices connect to a central hub/switch.

**91. What is mesh topology?**
Each device connects to multiple others for redundancy.

**92. What is a network choke point?**
A bottleneck where traffic slows down.

**93. What is DNS spoofing?**
An attack that redirects DNS queries to malicious sites.

**94. What is ARP spoofing?**
An attack that sends false ARP messages to redirect traffic.

**95. What is packet fragmentation?**
Breaking large packets into smaller pieces for transmission.

**96. What is IPv6 address compression?**
Shortening 2001:0db8:0000:0000:0000:ff00:0042:8329 to 2001:db8::ff00:42:8329.

**97. What is a socket timeout?**
The time a network operation waits before failing.

**98. What is a captive portal?**
A web page shown before granting network access (e.g., public Wi-Fi login).

**99. What is network loop?**
When packets circulate endlessly due to faulty network design.

**100. Best networking habits for QA engineers**

* Understand protocols and ports
* Test in multiple network conditions
* Monitor performance regularly
* Stay updated on security threats