Networking Interview Questions with Answers

A Complete Guide for Recruiters, Hiring Managers & Candidates

This document covers all major networking interview questions: networking interview questions for freshers, networking interview questions PDF, computer network interview questions, network security interview questions, and routing protocol interview questions.

Networking Interview Questions for Freshers (ENTRY LEVEL · 0–2 YEARS)

Q1 What is a computer network?

A computer network is a group of interconnected devices- computers, servers, and routers that communicate and share resources. It enables data exchange, shared file access, and use of common peripherals like printers. Networks range from small home setups to large enterprise infrastructures.

Q2 What is the difference between LAN and WAN?

- LAN (Local Area Network): Connects devices within a limited area like a home, office, or school. High-speed, low-cost, shorter distances.
- WAN (Wide Area Network): Spans large geographic areas- cities, countries, or globally- using the internet or leased lines to link remote locations.

Q3 What is an IP address?

An IP (Internet Protocol) address is a unique numerical label assigned to each device on a network, enabling it to send and receive data.

- IPv4: 32-bit address (e.g., 192.168.1.1) — supports ~4.3 billion addresses
- IPv6: 128-bit address — designed to replace IPv4 with vastly more address space

Q4 How does DHCP work?

DHCP (Dynamic Host Configuration Protocol) automatically assigns IP addresses to devices joining a network.

A device sends a DHCP Discover broadcast → the server responds with an available IP and leases it for a set duration. This eliminates manual configuration and reduces administrative overhead.

Q5 What is the OSI model?

The OSI (Open Systems Interconnection) model is a conceptual 7-layer framework that standardizes how network components communicate.

Each layer handles a specific function from physical signal transmission to application-level interfaces helping engineers design, understand, and troubleshoot networks.

Q6 Name the 7 layers of the OSI model and their functions.

From bottom to top:

- Layer 1 – Physical: Transmits raw bits via cables or wireless signals
- Layer 2 – Data Link: Error-free transmission between directly connected nodes
- Layer 3 – Network: Routes packets across networks (IP lives here)
- Layer 4 – Transport: Reliable end-to-end delivery (TCP/UDP lives here)
- Layer 5 – Session: Manages connections between applications
- Layer 6 – Presentation: Data formatting, encryption, and compression
- Layer 7 – Application: Network services for apps like HTTP, DNS, FTP

Q7 What is TCP/IP?

TCP/IP is the foundational communication protocol suite of the internet.

- TCP (Transmission Control Protocol): Ensures reliable, ordered, error-checked delivery
- IP (Internet Protocol): Handles addressing and routing of packets between networks

Together, they define how data is packaged, addressed, transmitted, and received.

Q8 What is the function of a router?

A router forwards data packets between different networks. It reads each packet's destination IP address and uses routing tables to select the best path forward.

Routers are essential for connecting networks, managing traffic, and enabling internet communication.

Q9 What is the difference between a hub and a switch?

- Hub: Broadcasts all incoming data to EVERY connected device- causes collisions, inefficient
- Switch: Forwards data only to the INTENDED device using its MAC address- reduces collisions, improves performance

Switches are the standard choice for modern networks due to their targeted, efficient data delivery.

Q10 What is a MAC address?

A MAC (Media Access Control) address is a unique 48-bit hexadecimal hardware identifier assigned to each network interface card (NIC) by its manufacturer.

It acts as the physical address of a device on a local network. Switches use MAC addresses to forward data to the correct destination.

Q11 What is ARP (Address Resolution Protocol)?

ARP resolves IP addresses to their corresponding MAC addresses within a local network.

When a device needs to communicate on the same subnet, it broadcasts an ARP request asking 'Who has IP X?' The device with that IP responds with its MAC address, enabling data link layer communication.

Q12 What is DNS and how does it work?

DNS (Domain Name System) translates human-readable domain names (e.g., google.com) into IP addresses computers use to locate each other.

User types a URL → Browser queries a DNS resolver → Resolver contacts DNS servers → Returns the IP → Browser connects to the correct server. DNS is essentially the internet's phone book.

Q13 What is a subnet mask?

A subnet mask is a 32-bit number that divides an IP address into its network and host portions.

It tells a device whether a destination IP is on the same local network or must be routed through a gateway. Example: 255.255.255.0 (/24) means the first 24 bits identify the network.

Q14 What is subnetting and why is it used?

Subnetting is the process of dividing a larger IP network into smaller subnetworks (subnets). Benefits include:

- Improved performance by reducing broadcast domains
- Better security through traffic isolation
- More efficient IP address allocation
- Simplified network management for large organizations

Q15 What is CIDR (Classless Inter-Domain Routing)?

CIDR replaces the rigid old class-based IP addressing with a flexible variable-length subnet mask (VLSM) approach.

IP addresses use a prefix notation- e.g., 192.168.1.0/24 where /24 means 24 bits are the network portion. CIDR enables more efficient allocation of IP address space and reduces routing table size.

Q16 What is NAT (Network Address Translation)?

NAT translates private IP addresses within a local network to a single public IP for internet communication.

This allows multiple devices on a private network to share one public IP, conserves IPv4 address space, and hides the internal network structure for added security. Commonly implemented on routers.

Q17 What is a VLAN?

A VLAN (Virtual LAN) logically groups network devices to communicate as if they are on the same physical network, regardless of actual location.

VLANs segment networks into smaller broadcast domains, improving performance, security, and manageability. Devices in different VLANs need a Layer 3 switch or router to communicate.

Q18 How does a firewall work?

A firewall is a security system that monitors and controls network traffic based on pre-configured rules.

It acts as a barrier between a trusted internal network and an untrusted external network (the internet), blocking or permitting traffic based on IP addresses, ports, and protocols.

Q19 What is the difference between static and dynamic routing?

- **Static routing:** Routes manually configured by an administrator. Simple but requires manual updates when topology changes. Best for small, stable networks.
- **Dynamic routing:** Uses routing protocols (RIP, OSPF, BGP) to automatically learn and update routes in real-time. More complex but highly scalable and resilient for large networks.

Q20 What is RIP (Routing Information Protocol)?

RIP is a distance-vector routing protocol that uses hop count (maximum 15 hops) as its metric.

It broadcasts its full routing table to neighbors every 30 seconds. Best for small to medium networks. The 15-hop limit makes it unsuitable for large deployments.

Q21 What is OSPF (Open Shortest Path First)?

OSPF is a link-state routing protocol that calculates the shortest path using Dijkstra's algorithm based on network topology and link costs.

Scalable and efficient, OSPF is suitable for large enterprise networks. It only sends updates when topology changes occur, significantly reducing unnecessary bandwidth usage.

Q22 What is BGP (Border Gateway Protocol)?

BGP is the standardized exterior gateway protocol that exchanges routing information between autonomous systems (AS) on the internet.

BGP makes routing decisions based on path attributes, network policies, and administrator-defined rules. It is the core protocol that powers the global internet routing system.

Q23 What is SDN (Software Defined Networking)?

SDN decouples the network control plane from the data forwarding plane, centralizing intelligence in a software-based controller.

This enables programmatic, dynamic network configuration- improving automation, flexibility, and scalability compared to traditional hardware-centric network management.

Q24 What is Wi-Fi 6 (802.11ax)?

Wi-Fi 6 is the sixth-generation Wi-Fi standard, designed to improve performance in dense environments with many connected devices.

- OFDMA: Allows multiple devices to share a channel simultaneously
- MU-MIMO: Supports more concurrent device connections
- Target Wake Time (TWT): Improves battery efficiency for IoT devices

Wi-Fi 6 delivers faster speeds and greater capacity than Wi-Fi 5 (802.11ac).

Q25 What is the difference between bandwidth and throughput?

- Bandwidth: Maximum theoretical data transfer capacity of a link (e.g., 1 Gbps). It is the 'pipe size.'
- Throughput: Actual data successfully delivered in practice, accounting for packet loss, latency, and protocol overhead.

Throughput is always equal to or lower than bandwidth in real-world conditions.

Q26 What is QoS (Quality of Service)?

QoS is a set of techniques that prioritize specific network traffic types to guarantee reliable performance for critical applications.

It enables administrators to allocate bandwidth, control latency, and manage packet loss for applications like VoIP, video conferencing, and streaming — even during network congestion.

Q27 What is a VPN and how does it work?

A VPN (Virtual Private Network) creates a secure, encrypted tunnel over a less secure network like the internet.

It allows remote users or offices to access private network resources as if directly connected. VPNs protect sensitive data, enable secure remote work, and can bypass geo-restrictions.

Q28 What is SSH and how does it differ from TELNET?

- TELNET: Remote access protocol that transmits all data including credentials in plain text- highly vulnerable to eavesdropping.
- SSH (Secure Shell): Provides encrypted, authenticated remote system access. Protects against interception and tampering.

SSH is always preferred. TELNET should never be used in any security-conscious environment.

Q29 What is ICMP and what is it used for?

ICMP (Internet Control Message Protocol) allows network devices to send error messages and operational information.

- ping: Uses ICMP Echo Request/Reply to test reachability and measure round-trip time
- traceroute: Uses ICMP TTL expiry messages to map the network path to a destination

ICMP is essential for network diagnostics and troubleshooting.

Q30 What is SNMP?

SNMP (Simple Network Management Protocol) is used to monitor and manage network devices such as routers, switches, and servers.

Administrators use SNMP to collect device status, performance metrics, and configuration data. It uses a Management Information Base (MIB) to organize device information and supports both polling and trap-based alerts.

Fresher Tip: Always explain not just what something is, but how it works and why it matters. Interviewers value clear reasoning over memorized definitions. Use analogies: 'DNS is like the internet's phone book.'

Networking Interview Questions for Intermediate Level (INTERMEDIATE LEVEL · 2–5 YEARS)

Q31 What is a DDoS attack?

A DDoS (Distributed Denial-of-Service) attack floods a target with massive traffic from multiple compromised systems (a botnet), overwhelming its resources.

The goal is to make the service unavailable to legitimate users. DDoS attacks cause service disruption, financial losses, and reputational damage.

Q32 How do you prevent DDoS attacks?

Effective DDoS prevention requires a multi-layered strategy:

- Traffic Filtering: Use firewalls and IDS/IPS to identify and block malicious traffic
- Rate Limiting: Cap requests per IP address to prevent flooding
- CDN (Content Delivery Network): Absorb and distribute traffic across global servers
- DDoS Mitigation Services: Use cloud-based traffic scrubbing services
- Over-provisioning: Maintain spare bandwidth and capacity for unexpected spikes

Q33 What is the difference between IDS and IPS?

- IDS (Intrusion Detection System): Passively monitors traffic, detects threats, and alerts administrators. Takes no automated action.
- IPS (Intrusion Prevention System): Actively detects AND blocks threats by dropping malicious packets, terminating connections, or quarantining systems.

IDS is passive (detect only); IPS is active (detect and block).

Q34 What is ARP poisoning?

ARP poisoning is an attack where an attacker sends forged ARP replies to associate their MAC address with a legitimate device's IP address.

This redirects traffic through the attacker's machine, enabling man-in-the-middle attacks, data interception, and traffic manipulation. Mitigated using Dynamic ARP Inspection (DAI).

Q35 What is MAC flooding?

MAC flooding overwhelms a switch's MAC address table by sending thousands of fake MAC addresses.

When the table is full, the switch broadcasts all traffic to every port like a hub, allowing an attacker to sniff sensitive data. Prevented using port security configurations on the switch.

Q36 What is VLAN hopping?

VLAN hopping allows an attacker to send packets to VLANs they are not authorized to access by exploiting switch misconfigurations or double-tagging vulnerabilities.

Prevention: Disable unused trunk ports, use dedicated native VLANs, implement VLAN Access Control Lists (VACLs), and enable BPDU Guard on edge ports.

Q37 What is a man-in-the-middle (MITM) attack?

A MITM attack occurs when an attacker secretly intercepts and potentially alters communication between two parties who believe they are communicating directly.

Common techniques: ARP poisoning, DNS spoofing, SSL stripping. The attacker can eavesdrop on sensitive data, inject malicious content, or impersonate one party to the other.

Q38 What is the AAA framework?

AAA (Authentication, Authorization, Accounting) is a security framework for controlling network access:

- Authentication: Verifies who the user or device is
- Authorization: Defines what resources the authenticated user can access
- Accounting: Logs user activity — bandwidth usage, session times, and access history

Implemented via RADIUS or TACACS+ servers in enterprise environments.

Q39 What is the difference between RADIUS and TACACS+?

- RADIUS: Standard protocol, uses UDP, encrypts only the password. Widely supported across vendors. Used in wireless and VPN authentication.
- TACACS+: Cisco-proprietary, uses TCP, encrypts the ENTIRE packet. Provides more granular per-command authorization control.

TACACS+ offers better security and flexibility; RADIUS has broader multi-vendor support.

Q40 What is Kerberos?

Kerberos is a network authentication protocol that uses secret-key cryptography and tickets to authenticate users without transmitting passwords over the network.

It provides mutual authentication (both client and server verify each other), preventing eavesdropping and replay attacks. Kerberos is the default authentication protocol in Microsoft Active Directory environments.

Q41 What is 802.1X authentication?

802.1X is a port-based network access control (PNAC) standard that requires devices to authenticate before being granted network access.

The device connects ➔ presents credentials to the switch/WAP ➔ an authentication server (usually RADIUS) verifies them ➔ access is granted or denied. Prevents unauthorized devices from joining the network.

Q42 What is Single Sign-On (SSO)?

SSO is an authentication mechanism that allows users to log in once and access multiple applications and services without re-entering credentials.

It improves user experience, reduces password fatigue, and centralizes access management. Common SSO protocols include SAML 2.0, OAuth 2.0, and OpenID Connect.

Q43 What is PoE (Power over Ethernet)?

PoE allows standard Ethernet cables to carry electrical power along with network data to connected devices.

- 802.3af (PoE): Up to 15.4W per port — IP phones, basic cameras
- 802.3at (PoE+): Up to 30W — PTZ cameras, dual-band APs
- 802.3bt (PoE++): Up to 90W — high-power devices, laptops

Eliminates separate power supplies, simplifies installation, and reduces cabling costs.

Q44 What is the difference between a crossover and straight-through cable?

- Straight-through: Same wiring on both ends. Connects different device types: PC to switch, switch to router.
- Crossover: Transmit and receive wires swapped. Connects similar devices directly: PC to PC, switch to switch.

Modern devices with Auto-MDI/MDIX auto-detect cable type, making crossover cables largely obsolete.

Q45 What is the difference between T1 and E1 lines?

- T1: North American standard. 1.544 Mbps over 24 channels (64 Kbps each). Used for dedicated voice/data in North America.
- E1: European standard. 2.048 Mbps over 32 channels (64 Kbps each). Used in Europe, Asia, and Latin America.

Both are dedicated leased lines providing guaranteed, symmetrical bandwidth.

Q46 What is MPLS?

MPLS (Multiprotocol Label Switching) routes data using short path labels rather than complex IP address lookups at each hop.

Benefits: High throughput, QoS support, traffic engineering, and support for multiple protocols. Used in carrier and enterprise backbone networks to efficiently carry voice, video, and data with predictable latency.

Q47 What is IPSec?

IPSec is a suite of protocols that secures IP communications by authenticating and encrypting every IP packet in a session.

- AH (Authentication Header): Provides authentication and integrity — no encryption
- ESP (Encapsulating Security Payload): Provides encryption, authentication, and integrity
- IKE (Internet Key Exchange): Negotiates security associations and manages cryptographic keys

IPSec is the most common protocol for building secure site-to-site VPN tunnels.

Security Tip: When discussing network attacks in interviews, always follow up with prevention techniques. Mention tools like port security, Dynamic ARP Inspection (DAI), and DHCP snooping to show you think like a defender.

Networking Interview Questions for Experienced Professionals (EXPERIENCED LEVEL · 5+ YEARS)

Q48 What is the difference between SAN, NAS, and DAS?

- **SAN (Storage Area Network):** High-speed network providing block-level storage access. Multiple servers share storage. Used for performance-critical workloads in data centers.
- **NAS (Network Attached Storage):** File-level storage accessed over standard network protocols (NFS, SMB). Easy to manage, ideal for file sharing and collaboration.
- **DAS (Direct Attached Storage):** Storage physically connected to a single server. Fast but not shareable across the network. Best for dedicated, single-server applications.

Q49 What is iSCSI?

iSCSI (Internet Small Computer Systems Interface) encapsulates SCSI storage commands inside IP packets, enabling block-level storage access over standard Ethernet networks.

It allows organizations to build SANs using existing IP infrastructure rather than dedicated Fibre Channel hardware — reducing cost while maintaining enterprise-grade storage performance and access over long distances.

Q50 What is Fibre Channel?

Fibre Channel is a high-speed networking technology (up to 128 Gbps) primarily used in SANs to connect servers to shared storage.

It provides low-latency, lossless data transfer over fiber optic or copper cables. Fibre Channel is the preferred choice for mission-critical storage in enterprise data centers due to its exceptional reliability and performance.

Q51 What is DHCP snooping?

DHCP snooping is a switch-level security feature that validates DHCP messages and filters untrusted DHCP traffic to prevent rogue DHCP servers from assigning incorrect IP addresses.

It builds a trusted binding table mapping legitimate MAC addresses to their IP assignments, switch port, and VLAN. Protects against DHCP starvation attacks and unauthorized IP assignment.

Q52 What is the difference between SSL and TLS?

SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are cryptographic protocols that encrypt data transmitted over a network.

- SSL: The original protocol — now fully deprecated due to security vulnerabilities
- TLS: Modern successor to SSL (current version: TLS 1.3) — widely used for HTTPS, email, and VPNs

Both provide confidentiality, integrity, and authentication. Only TLS should be used today.

Q53 What is the difference between symmetric and asymmetric encryption?

- Symmetric: Uses the SAME key for both encryption and decryption. Fast and efficient for large data. Challenge: securely distributing the shared key. Examples: AES, DES, 3DES.
- Asymmetric: Uses a PUBLIC key to encrypt and a PRIVATE key to decrypt. Slower but eliminates the key-sharing problem. Supports digital signatures. Examples: RSA, ECC.

In practice, TLS uses asymmetric encryption to exchange a symmetric session key, then uses symmetric encryption for the actual data transfer — combining the strengths of both.

Q54 What is AES and why is it the preferred encryption standard?

AES (Advanced Encryption Standard) is the gold-standard symmetric encryption algorithm, adopted by NIST in 2001 to replace DES.

- Supports key sizes: 128-bit, 192-bit, and 256-bit
- AES-256 is considered computationally infeasible to brute-force
- Used in: VPNs, disk encryption, HTTPS, wireless security (WPA2/WPA3), and file encryption

AES is fast in both hardware and software, making it the universal encryption standard worldwide.

Q55 What is the difference between DES, 3DES, and AES?

- DES: 56-bit key. Now considered insecure and vulnerable to brute-force. Fully deprecated.
- 3DES: Applies DES three times with different keys (112 or 168-bit effective strength). More secure than DES but significantly slower. Currently being phased out.
- AES: 128/192/256-bit keys. Fast, secure, and the current global standard. Completely replaces both DES and 3DES.

Q56 What is hashing and how does it differ from encryption?

Hashing converts data of any size into a fixed-length string (hash value). It is a one-way function- the original data cannot be recovered from the hash.

- Used for: verifying data integrity, secure password storage, digital signatures
- Key difference: Encryption is two-way (encrypt/decrypt); hashing is one-way (irreversible)
- Common algorithms: MD5 (deprecated), SHA-1 (deprecated), SHA-256 (current standard), SHA-3

Example: When you log in, the stored hash of your password is compared to the hash of what you typed- the plain password is never stored.

Q57 What is PKI (Public Key Infrastructure)?

PKI is a framework of roles, policies, and technologies that manages digital certificates and public-key encryption for secure communications.

Key components:

- Certificate Authority (CA): Issues and digitally signs certificates
- Registration Authority (RA): Verifies identity before the CA issues a certificate
- Digital Certificate: Binds a public key to an entity's verified identity
- CRL (Certificate Revocation List): Lists certificates that have been revoked

PKI underpins HTTPS, email signing, VPN authentication, and code signing.

Q58 What is SHA-256 and where is it used?

SHA-256 (Secure Hash Algorithm 256-bit) is a cryptographic hash function that produces a 256-bit (32-byte) fixed-length output regardless of input size.

It is part of the SHA-2 family and widely used for:

- SSL/TLS certificate digital signatures
- File and data integrity verification
- Blockchain and cryptocurrency (Bitcoin uses SHA-256 for mining)
- Password hashing (with salting) in secure authentication systems

SHA-256 is considered cryptographically secure and collision-resistant.

Q59 What is the difference between a site-to-site and client-to-site VPN?

- Site-to-site VPN: Connects two entire networks via encrypted tunnels between VPN gateways. All users at both sites benefit transparently — no individual VPN client required. Used to connect branch offices to HQ.
- Client-to-site VPN: Allows individual remote users to connect to a private network using a VPN client on their device. Ideal for remote workers needing secure access from anywhere in the world.

Q60 What is WPA3 and why is it better than WPA2?

WPA3 (Wi-Fi Protected Access 3) is the latest Wi-Fi security protocol, designed to address vulnerabilities in WPA2.

- SAE (Simultaneous Authentication of Equals): Replaces PSK handshake, resistant to offline dictionary attacks
- Forward Secrecy: Protects past sessions even if the key is later compromised
- 192-bit encryption: For enterprise environments requiring stronger protection
- Enhanced Open: Protects users on open public Wi-Fi networks using opportunistic encryption

WPA3 is mandatory for Wi-Fi 6 (802.11ax) certified devices.

Expert Tip: At the senior level, discuss trade-offs- not just definitions. For encryption, address performance vs. security. For storage, explain when to use SAN vs. NAS based on workload type and latency requirements.

Quick Reference: Key Networking Protocols

Protocol	Full Name	Layer / Type	Key Use
DNS	Domain Name System	App (L7)	Resolves domain names to IPs
DHCP	Dynamic Host Config Protocol	App (L7)	Auto IP address assignment
ARP	Address Resolution Protocol	Data Link (L2)	Maps IP to MAC address
ICMP	Internet Control Message Prot.	Network (L3)	Ping, traceroute, error msgs
TCP	Transmission Control Protocol	Transport (L4)	Reliable, ordered delivery
UDP	User Datagram Protocol	Transport (L4)	Fast, connectionless delivery

OSPF	Open Shortest Path First	Routing	Link-state interior routing
BGP	Border Gateway Protocol	Routing	Inter-AS internet routing
IPSec	Internet Protocol Security	Network (L3)	VPN encryption & auth
TLS/SSL	Transport Layer Security	Session (L5)	HTTPS, encrypted comms
SSH	Secure Shell	App (L7)	Encrypted remote access
SNMP	Simple Network Mgmt Protocol	App (L7)	Network device monitoring
RADIUS	Remote Auth Dial-In User Svc	AAA	Centralized auth (UDP)
TACACS+	Terminal Access Controller +	AAA	Centralized auth (TCP)
AES	Advanced Encryption Standard	Encryption	Symmetric data encryption
SHA-256	Secure Hash Algorithm 256	Hashing	Data integrity, certificates
NAT	Network Address Translation	Network (L3)	Private to public IP mapping
VLAN	Virtual Local Area Network	Data Link (L2)	Network segmentation
MPLS	Multiprotocol Label Switching	WAN	High-perf label routing

Standardize and scale your Networking hiring with this checklist. [Talk to our experts today](#).

End of Guide