Network Layer in Computer Networks

Key Viva Exam Questions to Prepare

For a network layer viva exam, I recommend focusing on these questions:

1. What are the key activities of the Network Layer? (Fundamental concept)
2. What is the difference between routing and forwarding? (Core concept distinction)
3. Compare and contrast static vs. dynamic routing (Practical implementation knowledge)
4. Explain distance vector vs. link state routing protocols (Core routing concepts)
5. What is NAT and how does it work? (Critical for modern networks)
6. Describe IP addressing classes and CIDR (Basic addressing knowledge)
7. Compare virtual circuit and datagram networks (Foundational concept)
8. How do routers handle congestion? (Network performance)
9. What is subnetting and why is it used? (Practical networking skill)
10. Explain how shortest path algorithms work (Algorithm understanding)
11. Compare RIP, OSPF, and EIGRP routing protocols (Protocol knowledge)
12. Is IP connection-oriented or connectionless and why? (Basic protocol characteristic)

These questions cover the fundamentals of network layer operation, routing protocols, addressing concepts, and practical implementations that demonstrate both theoretical and practical knowledge.

1. Activities of Network Layer

The Network Layer's primary activities include:

- Logical addressing (IP addressing)
- Routing of packets between networks
- Path determination for data packets
- Packet forwarding
- Fragmentation and reassembly of packets
- Error handling and diagnostics
- Quality of Service (QoS) management
- Congestion control

2. Routing

Routing is the process of selecting optimal paths through a network for forwarding data packets from source to destination. It involves:

- Path determination based on network topology and routing algorithms
- Making forwarding decisions based on destination addresses
- Using routing tables to store path information

- Adapting to network changes and failures

3. Major Network Layer Activities

The two major activities of the Network Layer are:

1. **Forwarding**: Moving packets from input to appropriate output ports (local decision)
2. **Routing**: Determining the end-to-end paths that packets take through the network (global decision)

4. Network Layer Device

The primary device that operates at the network layer is the **router**. Routers:

- Connect different networks together
- Make forwarding decisions based on IP addresses
- Maintain routing tables
- Implement routing protocols
- Perform packet filtering and traffic management

5. Difference between Routing and Forwarding

Routing	Forwarding
Global process determining end-to-end paths	Local process of moving packets from input to output ports
Creates and maintains routing tables	Uses routing tables to make decisions
Can be complex and computationally intensive	Simple lookup and decision process
Handles network topology and changes	Handles individual packets
Occurs periodically or when topology changes	Occurs for every packet

6. Virtual Circuit Network

A virtual circuit network establishes a predetermined path between sender and receiver before data transmission begins:

- Connection-oriented approach
- Resources are allocated during circuit setup
- All packets follow the same path
- Each packet carries a virtual circuit identifier (VCI) instead of destination address
- Examples: ATM, Frame Relay

7. Datagram Network

A datagram network treats each packet independently:

- Connectionless approach
- No predefined path established

- Each packet carries complete addressing information
- Packets may take different routes to the same destination
- Router makes independent forwarding decisions for each packet
- Example: IP networks

8. Difference between Virtual Circuit and Datagram Network

Virtual Circuit Network	Datagram Network
Connection-oriented	Connectionless
Fixed path for all packets	Independent path for each packet
Circuit setup required	No setup phase
Packets identified by circuit ID	Packets contain full destination address
Guaranteed in-order delivery	No order guarantees
Better for stable traffic	Better for bursty traffic
Higher setup overhead	No setup overhead
Lower per-packet overhead	Higher per-packet overhead

9. Static vs. Dynamic Routing

Static Routing	Dynamic Routing
Manually configured by network administrator	Automatically learned through routing protocols
No adaptation to network changes	Adapts to changing network conditions
No bandwidth consumption for routing updates	Consumes bandwidth for routing updates
Better security (routes are fixed)	More vulnerable to routing attacks
Suitable for small, simple networks	Suitable for large, complex networks
No CPU overhead	Requires CPU resources to run routing algorithms

Which is better? Dynamic routing is generally better for medium to large networks because it adapts to changes automatically and requires less manual intervention. Static routing is better for very small networks or special cases where precise control is needed.

10. Adaptive Routing

Adaptive routing changes routing decisions based on current network conditions:

- Adjusts to topology changes (link failures, congestion)
- Uses metrics like delay, bandwidth, load to make decisions
- Examples include OSPF, EIGRP, and BGP
- Can respond to both short-term and long-term network changes
- Typically uses dynamic algorithms that exchange information between routers

11. Non-Adaptive Routing

Non-adaptive routing doesn't change based on network conditions:

- Routes are fixed or change only when manually reconfigured

- Doesn't respond to congestion or failures
- Examples include static routing and flooding
- Simpler to implement but less resilient
- Decision based on fixed topology, regardless of current conditions

12. Shortest Path Routing Algorithm

Shortest path algorithms find the lowest-cost path between source and destination:

Dijkstra's Algorithm (commonly used):

1. Start with source node, assign 0 cost to it, infinite cost to all others
2. Mark source node as "current"
3. For each neighbor of current node, calculate tentative distance
4. If tentative distance is less than known distance, update the distance
5. Mark current node as "visited"
6. Select unvisited node with lowest distance as new "current"
7. Repeat steps 3-6 until destination is reached or all nodes are visited

13. Flooding

Flooding is a simple routing technique where:

- Each incoming packet is sent out on every outgoing link except the one it arrived on
- Ensures packet reaches destination if a path exists
- Highly redundant (generates many duplicate packets)
- Used in military networks for reliability
- Modified with sequence numbers or hop counts to prevent infinite looping
- Useful for broadcasting and discovering network routes

14. Distance Vector Routing

Distance Vector Routing is based on the Bellman-Ford algorithm:

- Each router maintains a table (vector) of distances to all destinations
- Routers exchange these vectors with direct neighbors
- Updates are periodic or triggered by topology changes
- Each router updates its table based on information from neighbors
- Suffers from "count to infinity" problem during failures
- Examples: RIP (Routing Information Protocol)
- Metric: Hop count (RIP limits to 15 hops)

15. Link State Routing

Link State Routing creates a complete map of the network:

- Each router discovers its neighbors and link costs
- This information is flooded throughout the network

- Each router builds identical database of network topology
- Dijkstra's algorithm is used to calculate shortest paths
- Faster convergence than distance vector
- Examples: OSPF (Open Shortest Path First)
- Metric: Cost based on bandwidth

RIP, OSPF, EIGRP Routing Protocols & Their Distance Metrics

Protocol	Type	Metric	Administrative Distance	Features
RIP	Distance Vector	Hop count (max 15)	120	Simple, limited scalability
OSPF	Link State	Cost (inversely proportional to bandwidth)	110	Hierarchical, fast convergence
EIGRP	Advanced Distance Vector	Composite metric (bandwidth, delay, reliability, load)	90	Cisco proprietary, fast convergence

16. Congestion and Control

Congestion occurs when too many packets are present in a network, causing:

- Packet delays and losses
- Throughput degradation
- Resource (buffer, bandwidth) exhaustion

Congestion Control Methods:

- **Traffic shaping**: Regulating packet flow rate
- **Admission control**: Limiting new connections
- **Load shedding**: Selectively dropping packets
- **Quality of Service (QoS)**: Prioritizing critical traffic
- **Explicit Congestion Notification (ECN)**: Network signals congestion to endpoints
- **Congestion window adjustment**: TCP slows down transmission rate

17. Jitter and Control

Jitter is the variation in packet delay (latency) over time, causing:

- Degraded quality for real-time applications (VoIP, video)
- Buffer underruns or overruns
- Irregular data reception

Jitter Control Methods:

- **Jitter buffers**: Store packets temporarily to smooth playback
- **Quality of Service (QoS)**: Prioritize time-sensitive traffic

- **Traffic shaping**: Regulate packet flow to ensure consistent timing
- **Packet scheduling**: Service disciplines like Weighted Fair Queueing
- **Constant bit rate services**: Reserve network capacity

18. NAT (Network Address Translation)

NAT translates private IP addresses to public IP addresses:

Why NAT is used:

- Conserves public IPv4 addresses
- Provides basic security by hiding internal network structure
- Enables multiple devices to share one public IP address
- Facilitates connecting private networks to the Internet

How NAT works:

1. Internal device sends packet to external destination
2. NAT router replaces source IP (private) with its public IP
3. NAT router records this translation in a table
4. Response packets arrive at NAT's public IP
5. NAT router looks up translation table
6. NAT replaces destination IP with internal private IP
7. Packet is forwarded to internal device

19. IP Address Class Ranges

Class	First Octet Range	First Bits	Network Bits	Host Bits	Default Subnet Mask
A	1-126	0	8	24	255.0.0.0
B	128-191	10	16	16	255.255.0.0
C	192-223	110	24	8	255.255.255.0

Note: 127.x.x.x is reserved for loopback addressing.

20. Selecting Network Class

Network class selection depends on:

- Number of required host addresses
- Number of required subnets
- Organization size and growth projections
- Address allocation policies

Guidelines:

- Class A: Very large organizations (16,777,214 hosts)
- Class B: Medium to large organizations (65,534 hosts)
- Class C: Small organizations (254 hosts)

- Modern networks typically use CIDR (Classless Inter-Domain Routing) rather than strict classes

21. Loopback Address

A loopback address is a special IP address (127.0.0.1 in IPv4) that directs traffic back to the originating device:

- Used to test local network software
- Represents "this machine" to applications
- Not physically transmitted on any network
- Any address in 127.0.0.0/8 range functions as loopback in IPv4
- In IPv6, ::1 is the loopback address

22. Subnet and Subnet Mask

Subnet is a logical subdivision of an IP network:

- Divides a large network into smaller, manageable segments
- Improves performance by reducing broadcast domain size
- Enhances security by isolating network segments
- Simplifies management and troubleshooting

Subnet Mask is a 32-bit value that:

- Separates the network portion from the host portion of an IP address
- 1s indicate network/subnet bits, 0s indicate host bits
- Example: 255.255.255.0 (or /24 in CIDR notation) means first 24 bits are network/subnet
- Used in logical AND operation with IP address to determine subnet

23. IP Connection Type

IP (Internet Protocol) is **connectionless**:

- No connection establishment before data transfer
- Each packet is routed independently
- No guaranteed delivery or packet order
- No session state maintained
- Relies on higher protocols (like TCP) for connection-oriented services