

Networking (CCNA Core Topics) - Interview Preparation Canvas

1. OSI Model

Concept Explanation: - 7 layers: Physical, Data Link, Network, Transport, Session, Presentation, Application - Functions: - Physical: hardware, cables, bits - Data Link: MAC addressing, error detection - Network: IP addressing, routing - Transport: TCP/UDP, flow control, segmentation - Session: manages sessions between apps - Presentation: data translation, encryption - Application: end-user services (HTTP, FTP, SMTP) - Common protocols per layer: - Physical: Ethernet, Wi-Fi - Data Link: ARP, PPP, Switches - Network: IP, ICMP, OSPF - Transport: TCP, UDP - Application: HTTP, DNS, FTP

Interview Answer: "The OSI model has 7 layers, each with specific roles. Physical handles the actual transmission of bits, Data Link ensures reliable node-to-node communication, Network manages IP addressing and routing, Transport ensures reliable delivery via TCP/UDP, Session handles sessions, Presentation formats and encrypts data, and Application provides end-user network services like HTTP and FTP."

Delivery Example: "In an interview, I would say: 'The OSI model is a conceptual framework with 7 layers that helps us understand networking. For instance, the Physical layer deals with cables and bits, Data Link ensures MAC-based delivery, Network handles IP routing, Transport manages reliable delivery with TCP or fast delivery with UDP, and so on up to Application where users interact with services like web or email.'"

2. TCP/IP Model

Concept Explanation: - Layers: Application, Transport, Internet, Network Access - Protocols: HTTP, FTP, SMTP (App), TCP/UDP (Transport), IP/ICMP (Internet), Ethernet/Wi-Fi (Network Access)

Interview Answer: "TCP/IP model has 4 layers: Application for end-user services, Transport for TCP/UDP, Internet for IP addressing and routing, and Network Access for physical transmission."

Delivery Example: "I would explain: 'TCP/IP is a 4-layer model mapping closely to OSI. Application layer handles HTTP/FTP, Transport manages TCP/UDP, Internet handles IP routing, and Network Access deals with Ethernet and Wi-Fi.'"

3. Subnetting

Concept Explanation: - Subnetting divides networks into smaller subnets. - Example: /24 network 192.168.1.0 - Divide into 4 subnets: 192.168.1.0/26, 192.168.1.64/26, 192.168.1.128/26, 192.168.1.192/26 - Each has 62 usable hosts

Interview Answer: "Subnetting a /24 into 4 subnets results in /26 networks, each with 62 usable hosts. IP ranges are 192.168.1.0-63, 64-127, 128-191, 192-255."

Delivery Example: "I would say: 'Starting with a /24 network, dividing into 4 subnets increases the subnet mask to /26. Each subnet has 62 usable hosts. For example, 192.168.1.0/26 gives usable IPs 192.168.1.1 to 192.168.1.62.'"

4. Routing Protocols

Concept Explanation: - Static: manually configured, simple, less scalable - Dynamic: automatically finds routes - OSPF: link-state, fast convergence, hierarchical, uses cost metric - EIGRP: Cisco proprietary, hybrid, fast, efficient - RIP: distance-vector, slow, max 15 hops

Interview Answer: "OSPF is a link-state protocol that builds a topology map and calculates shortest paths. It's faster and more scalable than RIP."

Delivery Example: "I would explain: 'OSPF floods link-state info, calculates shortest paths using Dijkstra, supports VLSM, and converges quickly, which makes it better than RIP for medium and large networks.'"

5. Switching (VLANs, Trunking, STP)

Concept Explanation: - VLAN: logically separates networks on a switch - Trunk: carries multiple VLANs between switches - STP: prevents loops in layer 2 networks

Interview Answer: "VLANs segment traffic, trunk ports carry multiple VLANs, and STP prevents broadcast storms."

Delivery Example: "I would say: 'We use VLANs to separate departments, trunk ports between switches carry multiple VLANs using 802.1Q tagging, and STP prevents loops that can crash the network.'"

6. Network Devices

Concept Explanation: - Router: forwards packets between networks - Switch: connects devices in a LAN - Firewall: filters traffic - Access Point: wireless connectivity

Interview Answer: "Routers route traffic between networks, switches connect LAN devices, firewalls enforce security, and APs provide wireless access."

Delivery Example: "I would explain: 'Routers connect networks, switches handle LAN traffic efficiently, firewalls block unauthorized access, and APs let devices connect wirelessly.'"

7. NAT & PAT

Concept Explanation: - NAT: translates private to public IPs - PAT: multiple private IPs share single public IP

Interview Answer: "NAT allows private IPs to communicate externally, while PAT lets multiple devices share one public IP."

Delivery Example: "I would say: 'NAT maps private IPs to public ones, enabling internet access. PAT allows many devices to use one public IP by using port numbers.'"

8. ACLs

Concept Explanation: - Standard ACL: filter by source IP - Extended ACL: filter by source, destination, protocol

Interview Answer: "Standard ACLs control access by source IP, extended ACLs by source, destination, and protocols."

Delivery Example: "I would explain: 'A standard ACL might block a specific source network, while an extended ACL can block traffic from a source to a destination on a particular port, like HTTP.'"

9. WAN Technologies

Concept Explanation: - MPLS: fast, reliable layer 3 WAN, supports QoS - VPN: secure connection over public network - Point-to-Point: direct link between two sites

Interview Answer: "MPLS provides efficient WAN routing, VPN secures traffic over public networks, and Point-to-Point links are simple dedicated connections."

Delivery Example: "I would say: 'MPLS helps connect multiple sites with QoS, VPN secures remote access, and Point-to-Point links are basic but reliable.'"

10. Network Troubleshooting Tools

Concept Explanation: - ping: test connectivity - tracert/traceroute: path to destination - ipconfig/ifconfig: view IP config - nslookup/dig: DNS queries

Interview Answer: "ping checks connectivity, tracert shows path and hops, ipconfig displays IP details, and nslookup queries DNS."

Delivery Example: "I would say: 'To troubleshoot, I start with ping to see if the host is reachable, use tracert to check the path, ipconfig to verify local IPs, and nslookup for DNS issues.'"

Example Questions & Scenario Responses:

Q1: Difference between TCP and UDP? - TCP is connection-oriented, reliable; UDP is connectionless, faster, no guarantee of delivery. - Interview Delivery: 'TCP ensures reliable delivery using handshake and acknowledgments, while UDP is faster but doesn't guarantee packet delivery, useful for streaming.'

Q2: How does OSPF work? Advantages over RIP? - OSPF floods link-state info, builds topology map, uses Dijkstra - Faster convergence, scalable, supports VLSM - Delivery: 'OSPF floods link-state info to routers, calculates shortest paths using Dijkstra, and converges quickly. Unlike RIP, it supports larger networks and variable subnet masks.'

Q3: Subnetting /24 into 4 subnets? - Answer: /26 each, 62 usable hosts, IP ranges 0-63,64-127,128-191,192-255 - Delivery: 'Dividing /24 into 4 subnets, each subnet becomes /26, providing 62 hosts. The ranges are 192.168.1.0-63, 64-127, etc.'

Q4: Purpose of VLANs? - Segmentation, security, broadcast control - Delivery: 'VLANs separate network traffic logically, enhance security, and reduce broadcast domains.'

Q5: Configure trunk on Cisco switch? - Switch>interface fa0/1; switchport mode trunk - Delivery: 'I would enter interface config, then set switchport mode trunk to carry multiple VLANs.'

Scenario 1: Users in VLAN 10 cannot reach internet? - Check IP, gateway, ACLs, NAT, VLAN assignment - Delivery: 'I would verify the host IP and default gateway, check VLAN config on switch, ensure NAT and ACLs allow internet traffic.'

Scenario 2: Router interface down after config? - Check cables, interface status, IP config, logs - Delivery: 'I would check physical connectivity, run show ip interface brief, verify IP/subnet mask, and examine logs.'

Scenario 3: High CPU usage on switch? - Could be loops, STP recalculation, too many broadcasts - Delivery: 'I would check for loops, monitor STP status, and identify high traffic sources causing CPU spike.'