Session 1: Basics of Networking

1. Binary/Hexadecimal Number System

Q1: Convert the decimal number 45 to binary.
A1: 45 in binary is **101101**.

Q2: Convert the binary number 1101 to hexadecimal.
A2: 1101 in hexadecimal is **D**.

2. Networking Terms

Q3: What is the difference between a switch and a router?
A3: A **switch** connects devices within a LAN and operates at Layer 2, forwarding data based on MAC addresses. A **router** connects different networks and operates at Layer 3, forwarding data based on IP addresses.

Q4: What is the OSI model?
A4: The **OSI model** has 7 layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application. It standardizes network communication.

3. Understanding Cable Infrastructure

Q5: What are the different types of network cables?
A5:

- **Twisted Pair (UTP/STP)** – Used in Ethernet connections.
- **Coaxial Cable** – Used in cable internet.
- **Fiber Optic** – High-speed, long-distance communication.

4. Network Operating Systems

Q6: What is a Network Operating System (NOS)?
A6: NOS is an OS designed to manage and operate network resources, such as Windows Server, Linux, or Cisco IOS.

Session 2: Network Infrastructure

1. Ports, Interfaces, and MAC Addresses

Q7: What is a MAC address?
A7: A **MAC address** is a unique hardware identifier assigned to network devices at Layer 2 of the OSI model.

Q8: What is the use of ports in networking?
A8: Ports help in identifying specific processes or services running on a device. Example: HTTP (Port 80), HTTPS (Port 443), SSH (Port 22).

2. Switches, Routers, and VLANs

Q9: What is a VLAN?
A9: A **VLAN (Virtual Local Area Network)** separates a physical network into multiple logical networks to improve security and performance.

3. Understanding Packets

Q10: What is the structure of a network packet?
A10: A network packet has three main parts:

1. **Header** – Contains source/destination addresses and protocol info.
2. **Payload** – Data being transmitted.
3. **Trailer** – Error-checking info like CRC.

Session 3: TCP/IP Protocol Framework

Q11: What is the difference between TCP and UDP?
A11:

- **TCP** is connection-oriented, reliable, and ensures ordered delivery (e.g., HTTP, FTP).
- **UDP** is connectionless, faster, and does not guarantee delivery (e.g., DNS, VoIP).

Q12: What is CIDR notation?
A12: CIDR (Classless Inter-Domain Routing) represents IP addresses with a subnet mask, e.g., 192.168.1.0/24.

Session 4: IP Subnetting & Routing

Q13: How do you subnet the IP address 192.168.1.0/24 into two subnets?
A13:

- **Subnet 1:** 192.168.1.0/25 (Subnet mask: 255.255.255.128)
- **Subnet 2:** 192.168.1.128/25 (Subnet mask: 255.255.255.128)

Q14: What is a routing table?
A14: A **routing table** contains paths for forwarding packets based on their destination IP addresses.

Session 5: Networking Tools

Q15: What command is used to check network connectivity?
A15: The `ping` command checks connectivity between two devices.

Q16: What is ARP?
A16: Address Resolution Protocol (ARP) maps IP addresses to MAC addresses.

Session 6: Packet Tracer Installation

Q17: What is Cisco Packet Tracer used for?
A17: It is a network simulation tool for designing and testing network topologies.

Session 7: Network Address Translation (NAT)

Q18: What is NAT and its types?
A18: NAT (Network Address Translation) converts private IP addresses to public IP addresses.
Types:

- **Static NAT** – One-to-one mapping.
- **Dynamic NAT** – Automatic assignment.
- **PAT (Port Address Translation)** – Multiple private IPs use a single public IP.

Session 8: VLAN

Q19: What is the difference between Access and Trunk ports?
A19:

- **Access port** – Carries traffic for one VLAN.
- **Trunk port** – Carries traffic for multiple VLANs.

Session 9: ACLs

Q20: What is an ACL?
A20: Access Control List (ACL) is a rule-based filtering system for controlling traffic.

Session 10: NTP & Port SPAN

Q21: What is NTP?
A21: Network Time Protocol (NTP) synchronizes time across devices in a network.

Q22: What is port mirroring (SPAN)?
A22: It duplicates network traffic to a specific port for monitoring.

Session 11: Wireless Basics & Wireless LANs

Q23: What is SSID?
A23: SSID (Service Set Identifier) is the name of a Wi-Fi network.

Session 12: Wireshark Installation & Packet Capturing

Q24: What is Wireshark used for?
A24: Wireshark is a network analysis tool used to capture and inspect packets.

Session 13: Dissecting TCP, UDP, IPv4, IPv6 in Wireshark

Q25: How can you filter only TCP packets in Wireshark?
A25: Use the filter `tcp`.

Session 14 & 15: GNS3 Setup & Switching Options

Q26: What is GNS3?
A26: Graphical Network Simulator 3 (GNS3) is a tool for network simulation using real device images.

Session 1: Basics of Networking

1. Binary/Hexadecimal Number System

Q1: Convert the decimal number **250** to binary.
A1: 250 in binary is **11111010**.

Q2: Convert the hexadecimal number **3F** to decimal.
A2:
3F (Hex) = ((3 \times 16^1) + (15 \times 16^0))
= ((3 \times 16) + (15 \times 1))
= **63 (Decimal)**.

Q3: What is the significance of hexadecimal notation in networking?
A3:
Hexadecimal is used in networking for **MAC addresses**, **IPv6 addresses**, and binary representations because it is more compact and human-readable.

---

2. Networking Terms

Q4: What is the difference between a hub, switch, and router?
A4:

- **Hub**: Broadcasts data to all devices; works at Layer 1.
- **Switch**: Sends data only to the intended recipient; works at Layer 2.
- **Router**: Connects different networks and makes routing decisions; works at Layer 3.

Q5: What is a default gateway?
A5: The **default gateway** is the IP address of a router that forwards traffic from a local network to other networks.

---

3. Understanding Cable Infrastructure

Q6: What is the difference between straight-through and crossover cables?
A6:

- **Straight-through cable**: Connects different devices, e.g., PC to switch.
- **Crossover cable**: Connects similar devices, e.g., PC to PC or switch to switch.

Q7: What is the max distance for a Cat5e Ethernet cable?
A7: 100 meters (328 feet).

Session 2: Network Infrastructure

1. Ports, Interfaces, and MAC Addresses

Q8: How is a MAC address structured?
A8:
A MAC address is **48 bits (6 bytes)** and is written in hexadecimal (e.g., `00:1A:2B:3C:4D:5E`).

- First **24 bits** (OUI) = Manufacturer ID.
- Last **24 bits** = Unique device ID.

Q9: What is an ephemeral port?
A9: An **ephemeral port** is a temporary port (range **1024–65535**) assigned by a system for client connections.

---

2. Switches, Routers, and VLANs

Q10: What are the types of switching in networking?
A10:

- **Store-and-Forward**: Stores full packet before forwarding (error-checking).
- **Cut-Through**: Forwards packet immediately after reading destination address.
- **Fragment-Free**: A hybrid of both.

Q11: What is the purpose of VLAN tagging?
A11: VLAN tagging (IEEE 802.1Q) is used to mark frames with VLAN information so they can be transmitted across trunk links.

---

3. Understanding Packets

Q12: What is the MTU (Maximum Transmission Unit)?
A12: MTU is the largest packet size a network interface can handle without fragmentation.

- Default MTU for Ethernet = **1500 bytes**.

Q13: What is a packet fragment?
A13: When a packet is larger than the MTU, it is divided into smaller fragments for transmission.

Session 3: TCP/IP Protocol Framework

1. IP Addresses (IPv4/IPv6)

Q14: What are the classes of IPv4 addresses?
A14:

- **Class A**: 1.0.0.0 - 126.255.255.255 (Large networks)
- **Class B**: 128.0.0.0 - 191.255.255.255 (Medium networks)
- **Class C**: 192.0.0.0 - 223.255.255.255 (Small networks)
- **Class D**: 224.0.0.0 - 239.255.255.255 (Multicast)
- **Class E**: 240.0.0.0 - 255.255.255.255 (Experimental)

Q15: What is the loopback address?
A15: 127.0.0.1 is used for testing network interfaces on a local machine.

Session 4: IP Subnetting & Routing

Q16: What is the subnet mask for a /26 network?
A16: 255.255.255.192

- **/26** means 64 hosts per subnet.

Q17: What is a routing metric?
A17: A routing metric determines the best path based on **hop count, bandwidth, latency, and reliability**.

Session 5: Networking Tools

Q18: What is the difference between nslookup and dig?
A18:

- **nslookup**: Simple DNS query tool (Windows & Linux).
- **dig**: More advanced DNS tool (Linux).

Q19: What does `traceroute` do?
A19: Shows the path packets take from source to destination.

Session 6: Packet Tracer Installation

Q20: What are the advantages of using Cisco Packet Tracer?
A20:

- Simulates real-world network scenarios.
- No physical hardware needed.
- Free for Cisco Networking Academy students.

Session 7: Network Address Translation (NAT)

Q21: What is the difference between SNAT and DNAT?
A21:

- **SNAT (Source NAT)**: Changes the source IP address.
- **DNAT (Destination NAT)**: Changes the destination IP address.

Session 8: VLAN

Q22: What is Inter-VLAN Routing?
A22: Inter-VLAN Routing allows communication between VLANs using a router or Layer 3 switch.

Session 9: ACLs

Q23: What are standard and extended ACLs?
A23:

- **Standard ACL**: Filters by source IP.
- **Extended ACL**: Filters by source, destination, and protocols.

Session 10: NTP & Port SPAN

Q24: Why is NTP important in networks?
A24: Synchronizes time across all network devices for logs, security, and troubleshooting.

Session 11: Wireless Basics

Q25: What is WPA3?
A25: WPA3 is the latest Wi-Fi security protocol with stronger encryption than WPA2.

Session 12: Wireshark & Packet Capturing

Q26: What does a TCP three-way handshake look like in Wireshark?
A26:

1. **SYN** → Client requests connection.
2. **SYN-ACK** → Server acknowledges.
3. **ACK** → Connection established.

Session 13: Packet Dissection

Q27: How do you filter UDP packets in Wireshark?
A27: Use filter: `udp`.

Session 14 & 15: GNS3

Q28: What is the advantage of using GNS3 over Packet Tracer?
A28:

- Supports real Cisco images.
- Provides advanced network simulation.
- Used for CCNA/CCNP/CCIE labs.

Session 1: Basics of Networking

1. Binary/Hexadecimal Number System

Q1: Convert **11110011** (binary) to decimal.
A1: (1 \times 2^7 + 1 \times 2^6 + 1 \times 2^5 + 1 \times 2^4 + 0 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 1 \times 2^0)
= **243 (Decimal)**.

Q2: What is **10101100** in hexadecimal?
A2: AC (Hex).

Session 2: Network Infrastructure

2. Ports, Interfaces, and MAC Addresses

Q3: How do you find the MAC address of a system?
A3:

- **Windows:** Run `ipconfig /all` in CMD.
- **Linux/macOS:** Use `ifconfig -a` or `ip link show`.

Q4: What is the difference between public and private IP addresses?
A4:

- **Public IP:** Used to communicate over the internet. Assigned by ISPs.
- **Private IP:** Used within local networks. Cannot be routed to the internet.

Session 3: TCP/IP Protocol Framework

1. TCP vs. UDP

Q5: Name three protocols that use UDP.
A5:

1. **DNS** (Port 53)
2. **DHCP** (Port 67, 68)
3. **SNMP** (Port 161)

Q6: Why does DNS use UDP instead of TCP?
A6: UDP is faster and has lower overhead, making it ideal for quick DNS queries.

Session 4: IP Subnetting & Routing

Q7: How many usable hosts are in a **/27 subnet**?
A7:

- **Subnet Mask:** 255.255.255.224
- **Hosts:** (2^{(32-27)} - 2 = 30) usable hosts.

Q8: What is the purpose of a **default route**?
A8: The **default route (0.0.0.0/0)** is used when no specific route is found in the routing table.

Session 5: Networking Tools

1. DNS, DHCP, ARP

Q9: What is the purpose of ARP?
A9: Address Resolution Protocol (ARP) resolves an **IP address** to a **MAC address**.

Q10: What is the difference between `ipconfig` and `ifconfig`?
A10:

- `ipconfig` **(Windows)** – Shows IP, DNS, and gateway details.
- `ifconfig` **(Linux/macOS)** – Displays network configurations.

Session 6: Packet Tracer Installation

Q11: How do you create a simple network in Cisco Packet Tracer?
A11:

1. Drag and drop **routers/switches/PCs**.
2. Connect devices using **Ethernet or Serial cables**.
3. Assign **IP addresses** and configure **routing** if needed.

Session 7: Network Address Translation (NAT)

Q12: What are the benefits of NAT?
A12:

- Conserves **public IP addresses**.
- Provides **security** by hiding internal IPs.
- Enables multiple devices to share a **single public IP**.

Q13: What is the main disadvantage of NAT?
A13: NAT can cause issues with applications that rely on end-to-end connectivity, like **VoIP and P2P services**.

Session 8: VLAN

Q14: How do VLANs improve network security?
A14:

- **Isolate traffic** between different groups of devices.
- Reduce **broadcast domain** size.
- Prevent **unauthorized access** between VLANs.

Session 9: ACLs (Access Control Lists)

Q15: How do you block all HTTP traffic using an ACL?
A15:

```
access-list 100 deny tcp any any eq 80
access-list 100 permit ip any any
```

This denies **port 80 (HTTP)** but allows all other traffic.

Session 10: NTP & Port SPAN

Q16: What happens if devices in a network have incorrect time settings?
A16:

- Log timestamps will be incorrect.
- Authentication failures in Kerberos-based systems.
- Issues with **certificate validity**.

Q17: How do you configure an NTP server in Cisco?
A17:

```
ntp server <NTP-IP>
clock timezone IST +5 30
```

This syncs time from an external NTP server.

Session 11: Wireless Basics

Q18: What is the difference between **2.4GHz and 5GHz Wi-Fi**?
A18:

- **2.4GHz**: Longer range, but **slower speed**. More interference.
- **5GHz**: Shorter range, but **higher speed**.

Q19: What is the purpose of a wireless **repeater**?
A19: A **wireless repeater** extends Wi-Fi coverage by rebroadcasting the signal.

Session 12: Wireshark Installation & Packet Capturing

Q20: How do you capture packets on a specific interface in Wireshark?
A20:

1. Open **Wireshark**.
2. Select the network **interface** (e.g., Ethernet or Wi-Fi).
3. Click **"Start Capture"**.

Q21: How do you filter **only HTTP packets** in Wireshark?
A21: Use the filter:

```
http
```

Session 13: Dissecting TCP, UDP, IPv4, IPv6 Packets

Q22: What is the **Time to Live (TTL)** field in an IP packet?
A22: TTL prevents infinite looping of packets by decreasing the **value by 1** at each hop. If TTL = 0, the packet is **discarded**.

Session 14: GNS3 Setup & Preferences

Q23: How is GNS3 different from Packet Tracer?
A23:

- **GNS3** runs **real Cisco/Juniper images**.
- **Packet Tracer** is a **simulation tool** with limited real-world commands.

Q24: What is the main requirement for running GNS3?
A24: A **good CPU and RAM** because GNS3 runs virtualized network devices.

Session 15: GNS3 Switching Options

Q25: How do you add a Cisco router to GNS3?
A25:

1. Download a **Cisco IOS image**.
2. Import it into **GNS3 Appliance Manager**.
3. Assign it to a **project topology**.

Q26: What is the advantage of using **GNS3 appliances**?
A26: GNS3 appliances allow **pre-configured Cisco and Juniper images** for easier setup and testing.

Bonus: General Networking Concepts

Q27: What is the difference between Layer 2 and Layer 3 switches?
A27:

- **Layer 2 switch**: Works only with **MAC addresses**.
- **Layer 3 switch**: Can perform **routing using IP addresses**.

Q28: What is an example of a **Layer 4 protocol**?
A28:

- **TCP** (Transmission Control Protocol)
- **UDP** (User Datagram Protocol)