Network Fundamentals

1. Network Components

A computer network is composed of different hardware and software components that allow communication between devices. The main components include:

- **End Devices: PCs, smartphones, printers.**
- **Network Infra Devices: Switches, routers, access points.**
- **Media: Cables (Ethernet, fiber optics) or wireless signals.**
- **Services and Protocols: DNS, HTTP, FTP, etc.**

2. Types of Networks

Networks can be categorized based on their size and purpose:

- **LAN (Local Area Network): Covers a small geographic area (like an office).**
- **WAN (Wide Area Network): Connects devices over large distances (e.g., the internet).**
- **MAN (Metropolitan Area Network): Spans a city or large campus.**
- **PAN (Personal Area Network): Small, close-range (like Bluetooth).**

3. Network Metrics

Performance is measured using several key metrics:

- **Speed:**
    1. **Bandwidth: Maximum data transfer rate (e.g., Mbps).**
    2. **Latency: Time taken for data to reach the destination (delay).**
    3. **Packet Loss: Data packets lost in transmission.**

- **Availability: 24 / 7.**

- **Security: confidentiality (ensures that sensitive info is accessed only by authorized individuals), integrity (guarantees the accuracy and trustworthiness of data).**

- **Quality of service: priority between apps**

- **Cost**

4. Ethernet Protocol Fundamentals

Ethernet is the most common wired LAN technology. It defines rules for how devices communicate within the same network using frames.

- **Operates at Layer 1 and 2 of the OSI model.**

- **Uses MAC addresses to identify devices.**

5. Ethernet Frames

Ethernet frames are the units of data sent over Ethernet networks. They include:

- **Destination MAC Address**
- **Source MAC Address**
- **Type/Length Field**
- **Payload: The actual data**
- **FCS (Frame Check Sequence): Error detection**

6. MAC Addresses

- **A MAC (Media Access Control) address is a unique 48-bit identifier assigned to network interfaces.**
- **Format: `00:1A:2B:3C:4D:5E`**
- **Types:**
  - **Unicast: one dest**
  - **Broadcast: all dest (ff-ff-ff-ff-ff-ff)**
  - **Multicast: Group of dest**

7. Switch Operations

Switches are essential Layer 2 devices that:

1. **Learn MAC addresses dynamically from incoming frames.**

2. **Use MAC address tables to forward frames only to the correct port.**
    - **2.1. Dest mac**
        - **2.1.1. If in mac table then forwarding**
        - **2.1.2. Else flooding**

8. IP Protocol Fundamentals

1. Purpose of IP

- **Identifying Devices: Each device gets a unique IP address.**
- **Routing Packets: It ensures data travels from the source to the destination, even across multiple networks.**
- **Connectionless Protocol: IP does not guarantee delivery. It simply tries to forward packets.**

2. Structure of an IPv4 Address

An IPv4 address has two parts:

- **Network Portion – identifies the network**
- **Host Portion – identifies the device on the network**

This division is determined by the subnet mask (e.g., `255.255.255.0`)

3. Private vs Public IP

- **Private IP: Used inside local networks. Not routable on the internet.**
- **Public IP: Routable over the internet. Assigned by ISPs.**

4. IP Packet Structure

An IP packet contains:

- **Header: Contains source/destination IPs, TTL, etc.**
- **Payload: The actual data being transmitted**

Important header fields:

- **Source IP address**
- **Destination IP address**
- **TTL (Time to Live): Limits the packet's lifespan**
- **Protocol: Indicates what transport layer protocol is used (e.g., TCP or UDP)**

5. IP vs MAC

Feature	IP Address	MAC Address
Logical Address	Yes	No (physical address)
Layer	Layer 3 (Network)	Layer 2 (Data Link)
Changeable	Yes (can be assigned)	No (burned into hardware)
Used By	Routers	Switches

8. Routing Fundamentals

What is Routing?

Routing is the process of selecting the best path for data packets to travel from a source to a destination across multiple networks.

- **Happens at Layer 3 (Network Layer) of the OSI model.**
- **It involves routers making decisions based on destination IP addresses.**

What is a Routing Table?

A routing table is a database inside a router that tells it where to forward packets based on their destination IP.

Each entry contains:

Field	Description
Destination network	**The IP network the packet is going to (e.g., `192.168.2.0/24`)**

Subnet mask / Prefix	**Defines the size of the destination network (e.g., `/24` or `255.255.255.0`)**
Next hop	**The IP address of the next router (e.g., `10.0.0.2`)**
Outgoing interface	**The router's own interface to send the packet through (e.g., `GigabitEthernet0/1`)**
Metric	**A value used to decide the best route when multiple exist — lower is better**
Route type / source	**How the route was learned:** **C = Connected** **S = Static** **D = Dynamic (e.g., RIP, OSPF, BGP)**

Static vs Dynamic Routing

Feature	Static Routing	Dynamic Routing
Route Configuration	Manually configured by the admin	Learned automatically from other routers
Updates	No automatic updates	Automatically adjusts to network changes
Complexity	Simple (good for small networks)	Scales better for large networks
CPU/Memory	Low resource usage	Requires more resources

9. Address Resolution Protocol (ARP)

ARP is a network protocol used to map an IP address (Layer 3) to a MAC address (Layer 2) within a local area network (LAN). Since Ethernet frames require MAC addresses to deliver data on the network, devices use ARP to discover the MAC address associated with a known IP address.

How ARP Works:

1. **When a device wants to send data to another device on the same network, it first checks its ARP table (also called the ARP cache) to see if it already knows the MAC address of the destination IP.**

2. **If the MAC address is not found, the device sends out a broadcast ARP request to the network. This request asks:**

   "Who has IP address X.X.X.X? Tell me your MAC address."

3. **The device with the matching IP responds with an ARP reply, which includes its MAC address.**

4. **The sender receives the MAC address and stores it in its ARP table for future use, then sends the data using that MAC address.**

ARP Table:

The ARP table is a local cache that stores mappings of IP addresses to MAC addresses. It helps avoid sending ARP requests repeatedly for the same IP.

Example entry:

IP Address	MAC Address
192.168.1.20	00:1A:2B:3C:4D:5E

10. What is TCP (Transmission Control Protocol)?

TCP is a connection-oriented, reliable transport protocol used to deliver data between devices in a network. It operates at Layer 4 (Transport Layer) of the OSI model and works on top of the IP protocol.

Key Features:

- **Connection-oriented: Establishes a session before data transfer (3-way handshake)**
- **Reliable: Ensures data is delivered correctly and in order**
- **Error checking: Uses acknowledgments and retransmissions**
- **Flow control: Manages data rate between sender and receiver**
- **Segmented data: Splits large data into smaller units called segments**

---

2. TCP Header Structure

Each TCP segment has a header that includes:

Field	Description
Source Port	Port number of sender
Destination Port	Port number of receiver
Sequence Number	Position of the segment in the stream
Acknowledgment No.	Confirms receipt of data
Flags (SYN, ACK, etc.)	Used for control (connection setup/teardown)
Window Size	Flow control info
Checksum	Error detection

---

3. The TCP 3-Way Handshake

To establish a connection, TCP uses this 3-step process:

1. **SYN: Client sends a synchronization request**
2. **SYN-ACK: Server acknowledges and replies with its own sync**
3. **ACK: Client confirms → Connection established**

This handshake ensures both sides are ready and synchronized.

---

4. TCP vs UDP

Feature	TCP	UDP
Type	Connection-oriented	Connectionless
Reliability	Yes (acknowledgments, checks)	No
Speed	Slower	Faster
Use cases	Web, email, file transfer	Streaming, VoIP, DNS (often)

---

5. What are Ports?

A port is a logical number that helps identify specific services or applications on a device.

- **IP address = identifies the device**
- **Port number = identifies the application/service**

For example:

- **IP =** `192.168.1.10`

- **Port = `80` → means HTTP web service**

TCP and UDP use 16-bit port numbers, ranging from 0 to 65535

---

6. Port Ranges

Port Range	Name	Use
0 – 1023	Well-known ports	Reserved for core services
1024 – 49151	Registered ports	Used by user applications
49152 – 65535	Dynamic/private	Temporary (ephemeral) use

11-VLAN Fundamentals (Virtual Local Area Network)

1. What is a VLAN?

A VLAN (Virtual LAN) is a logical separation of a physical network into multiple virtual networks.

> **Even if all devices are connected to the same physical switch, a VLAN keeps their traffic separate — as if they're on different switches.**

---

2. Why Use VLANs?

- **Segmentation: Divide a network by department, function.**
- **Security: Prevent users in one VLAN from accessing devices in another.**
- **Traffic Reduction: Limits broadcast traffic to within each VLAN.**
- **Flexibility: Devices in the same VLAN don't need to be in the same physical location.**

3. How VLANs Work

- **Switch ports are assigned to VLANs.**
- **Devices in different VLANs can't communicate directly — unless a router or Layer 3 switch is used.**
- **VLAN tags (802.1Q) are used in Ethernet frames to identify VLAN membership.**

---

4. VLAN Tagging (802.1Q)

- **The IEEE 802.1Q standard adds a VLAN tag to Ethernet frames.**
- **VLAN tag is inserted between the Source MAC and EtherType fields.**
- **This allows switches to know which VLAN a frame belongs to.**

5. VLAN Types

Type	Description

Access VLAN	**Assigned to switch ports connected to end devices (e.g., PCs)**
Trunk VLAN	**Carries multiple VLANs over a single link (between switches/routers)**
Native VLAN	**The VLAN that goes untagged on a trunk link (default = VLAN 1)**