Pratiksha Patel

Module 2 CS- Fundamental of Operating Systems & Networks

1. Difference between hardware and software.

Ans:

Hardware is the physical part of a computer that you can see and touch, like the keyboard, monitor, mouse, and CPU.

Software is a set of instructions or programs that tell the hardware what to do, like Windows, apps, or games.

- **Hardware = body**
- **Software = brain**

Aspect	Hardware	Software
Definition	The physical parts of a computer that you can touch.	The programs or instructions that tell the computer what to do.
Examples	Keyboard, mouse, monitor, CPU, printer	Windows, apps, games, web browsers
Tangibility	Tangible (you can see and touch it)	Intangible (cannot touch, only use)
Function	Performs tasks physically (processes data, input/output)	Provides instructions for hardware to perform tasks
Durability	Can wear out or get damaged physically	Can get corrupted or outdated
Dependency	Works alone but needs software to be useful	Cannot work alone; needs hardware to run

2. Define IP address range and private address range.

Ans:

IP Address Range

An **IP address range** means the set of all possible IP addresses that can be used.

- Example for **IPv4**: from 0.0.0.0 to 255.255.255.255
- Example for **IPv6**: from 0000:0000:0000:0000:0000:0000:0000:0000 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Private Address Range

A **private IP address range** is a special part of the IP range that is used **inside local networks (home, office, school)**. They are **not routable on the internet**.

For **IPv4**, the private ranges are:

- 10.0.0.0 → 10.255.255.255
- 172.16.0.0 → 172.31.255.255
- 192.168.0.0 → 192.168.255.255

Example: your WiFi might give you 192.168.1.5 at home.

- **IP address range** = all possible IP addresses.
- **Private address range** = reserved part of IPs used only in local/private networks.

3. Explain Network protocol and Port number.

Ans:

A **network protocol** is like a **set of rules** that computers follow to talk to each other over a network.

- Example: Just like humans use English or Hindi to communicate, computers use protocols.
- Common protocols:
  - **HTTP** → used for browsing websites
  - **FTP** → used for file transfer
  - **SMTP** → used for sending emails

Port Number

A **port number** is like a **door** on a computer that allows data to enter or leave for a specific service.

- Example: Think of an apartment building (computer) → each flat has a number (port).
- Common port numbers:
  - **80** → for HTTP (websites)
  - **443** → for HTTPS (secure websites)
  - **25** → for sending emails (SMTP)

- **Protocol = language/rules** for communication.
- **Port number = door number** that decides which service or app will handle the data.

Port Numbers List:

- **20, 21** → FTP (File Transfer Protocol)
- **22** → SSH (Secure Shell)
- **23** → Telnet
- **25** → SMTP (Email sending)
- **53** → DNS (Domain Name System)
- **67, 68** → DHCP (IP address assignment)
- **80** → HTTP (Websites)
- **110** → POP3 (Email receiving)
- **143** → IMAP (Email receiving)
- **161** → SNMP (Network management)
- **389** → LDAP (Directory services)
- **443** → HTTPS (Secure websites)
- **445** → SMB (File sharing in Windows)
- **3389** → RDP (Remote Desktop Protocol)

Web → 80 (HTTP), 443 (HTTPS)

Email → 25 (SMTP), 110 (POP3), 143 (IMAP)

Remote access → 22 (SSH), 23 (Telnet), 3389 (RDP)

4. Explain Types of Network Devices

Ans:

1. **Router** 🛣️

- Connects different networks together (like your home network to the internet).
- Chooses the best path for data to travel.

2. **Switch** 🔀

- Connects multiple computers/devices inside the same network (like in an office).
- Sends data only to the device it's meant for (faster than a hub).

3. **Hub** 📡

- Old/basic device that connects computers in a network.
- Sends data to **all devices** (less secure, slower).

4. **Access Point (AP)** 📶

- Provides **Wi-Fi** so devices can connect wirelessly.
- Works with a router or switch to expand the network.

5. **Modem** 🌐

- Connects your network to the **Internet Service Provider (ISP)**.
- Converts signals (digital ↔ analog).

6. **Firewall** 🔒

- Protects the network by filtering traffic.
- Blocks suspicious or unauthorized access.

7. **Gateway** 🌍

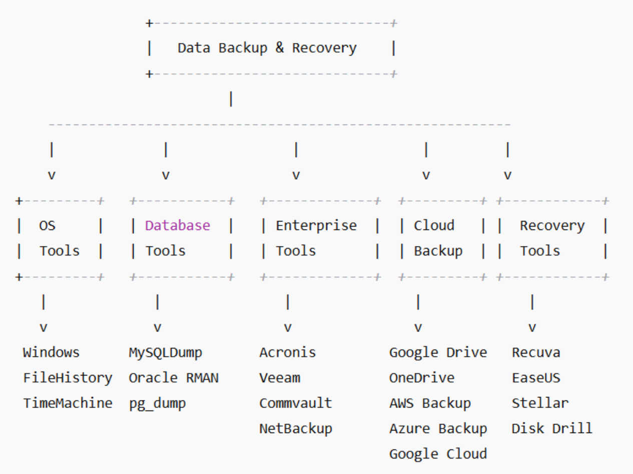
- Acts as an entry/exit point between two networks that use **different protocols**.
- Example: translating between IPv4 and IPv6 networks.

☑ In short:

- **Router** → connects networks
- **Switch** → connects devices
- **Hub** → connects devices but slower
- **Access Point** → gives Wi-Fi
- **Modem** → connects to ISP/Internet
- **Firewall** → provides security
- **Gateway** → connects networks with different rules

5. Which Tools use for Data Backup and Recovery

Ans:



```
                +-----------------------------+
                |   Data Backup & Recovery    |
                +-----------------------------+
                          |
    ----------------------------------------------------------
    |             |                |              |          |
    v             v                v              v          v
+---------+   +------------+  +--------------+ +----------+ +------------+
|  OS     |   | Database   |  | Enterprise   | | Cloud    | |  Recovery  |
|  Tools  |   | Tools      |  | Tools        | | Backup   | |  Tools     |
+---------+   +------------+  +--------------+ +----------+ +------------+
   |             |               |               |             |
   v             v               v               v             v
 Windows      MySQLDump       Acronis         Google Drive   Recuva
 FileHistory  Oracle RMAN     Veeam           OneDrive       EaseUS
 TimeMachine  pg_dump         Commvault       AWS Backup     Stellar
                              NetBackup       Azure Backup   Disk Drill
                                              Google Cloud
```

1. Built-in Operating System Tools

These are the tools that come **pre-installed** in your computer's OS.

- **Windows Backup & Restore** → lets you create a copy of your files or even the whole system.
- **File History (Windows 10/11)** → automatically saves versions of your files (like Documents, Pictures).
- **Time Machine (Mac)** → creates full backups of your Mac system to an external drive.

👉 **Best for**: Home users and small offices.

2. Database Backup Tools

Databases need special tools to keep records safe.

- **MySQLDump** → used to back up MySQL databases into text files.
- **Oracle RMAN (Recovery Manager)** → powerful backup & recovery for Oracle databases.
- **pg_dump** → backup tool for PostgreSQL databases.

👉 **Best for**: IT admins, companies using large databases.

3. Enterprise Backup Software

Big organizations use these because they handle **huge data**.

- **Acronis Cyber Protect** → backup + cybersecurity in one.
- **Veeam Backup & Replication** → popular for virtual machines, cloud, and servers.
- **Commvault** → advanced enterprise backup with automation.
- **Veritas NetBackup** → handles backup for large-scale businesses.

👉 **Best for**: Companies with servers, big data centers.

4. Cloud Backup Services

These save your files **online (cloud)** so you can recover them anywhere.

- **Google Drive, OneDrive, Dropbox** → simple cloud storage + backup.
- **AWS Backup (Amazon)** → automatic cloud backup for Amazon services.
- **Microsoft Azure Backup** → protects cloud + on-premises data.
- **Google Cloud Backup & DR** → disaster recovery with cloud.

👉 **Best for**: People who want to access data anywhere, organizations using cloud.

5. Data Recovery Tools

Used when data is **deleted, corrupted, or lost**.

- **Recuva** → simple tool to recover deleted files in Windows.
- **EaseUS Data Recovery Wizard** → user-friendly tool for recovering lost data.
- **Stellar Data Recovery** → powerful tool for recovering data from damaged drives.
- **Disk Drill** → works on both Windows and Mac.

👉 **Best for**: Accidentally deleted files, damaged drives, quick recovery.

☑ **In short:**

- **OS tools** → for personal system backups
- **Database tools** → for database backups
- **Enterprise tools** → for large organizations
- **Cloud tools** → for online backup
- **Recovery tools** → for restoring lost files

6. Explain HTTP and HTTPS Protocols

Ans:

🌐 HTTP (HyperText Transfer Protocol)

- A **protocol (set of rules)** used for transferring web pages on the internet.
- When you open a website like http://example.com, it uses HTTP.
- **Not secure** → Data is sent as plain text, so hackers can intercept it.
- Works on **Port 80**.

👉 Example: If you log in on an HTTP website, your username and password can be seen by attackers.

🔒 HTTPS (HyperText Transfer Protocol Secure)

- It is **HTTP + Security** (uses **SSL/TLS encryption**).
- When you open a website like https://example.com, it uses HTTPS.
- **Secure** → Data is encrypted, so even if intercepted, hackers cannot read it.
- Works on **Port 443**.

👉 Example: Online banking, shopping, and any site that requires login should use HTTPS.

Easy Difference:

- **HTTP** = normal web browsing, not secure
- **HTTPS** = secure web browsing, encrypted (safe for sensitive data)

7. What is SSL and TLS Security?

Ans:

SSL (Secure Sockets Layer)

- SSL is a **security protocol** that encrypts data sent between a **web browser and a server**.
- Ensures that sensitive data (like passwords, credit card numbers) cannot be read by hackers.
- Old version of web security, now mostly replaced by TLS.
- Works with **HTTPS** websites.

TLS (Transport Layer Security)

- TLS is the **improved version of SSL**.
- Provides **stronger encryption** and better security than SSL.
- Ensures:
  1. **Encryption** → Data cannot be read by outsiders
  2. **Authentication** → You are communicating with the correct server
  3. **Data Integrity** → Data cannot be modified during transmission
- Also used by **HTTPS websites, email servers, and messaging apps**.

☑ **Easy:**

- **SSL = Old version of secure communication**
- **TLS = Modern, stronger version of SSL**
- Both are used to make websites and online communication **secure**.

8. Explain the MAC ADDRESS

Ans:

What is MAC Address?

MAC (Media Access Control) Address is a **unique identifier** assigned to a network device.

- Every network interface card (NIC) in a computer, phone, router, or any network device has a MAC address.
- It helps **devices identify each other in a local network (LAN)**.

Format of MAC Address

- A MAC address is **12 hexadecimal digits** (0–9 and A–F).
- Usually written as:
  - 00:1A:2B:3C:4D:5E or
  - 00-1A-2B-3C-4D-5E
- The **first half** identifies the manufacturer (OUI – Organizationally Unique Identifier).
- The **second half** identifies the device (unique to that manufacturer).

Characteristics of MAC Address

1. **Unique** → No two devices have the same MAC address on the same network.
2. **Permanent / Hardware Address** → Usually burned into the network card by the manufacturer.
3. **Used at Layer 2** → Works in the **Data Link Layer** of the OSI model.
4. **Device Identification** → Helps switches and routers send data to the right device.

MAC vs IP Address

MAC Address	IP Address
Physical address of the device	Logical address that can change
Permanent (usually)	Can change when moving between networks
Used in local network (LAN)	Used for communication over Internet
Works at Data Link Layer (Layer 2)	Works at Network Layer (Layer 3)

Uses of MAC Address

1. **Network Security** → Can restrict access to a network by allowing only certain MAC addresses.
2. **Device Identification** → Switches use MAC to deliver data to the correct device.
3. **Troubleshooting** → Helps network admins identify devices on a network.
4. **ARP (Address Resolution Protocol)** → MAC is used to find the physical device corresponding to an IP address.

☑ Easy:

- **MAC = Physical ID of device on network**
- **IP = Address that changes when device moves between networks**