TRAINING DAY 12 REPORT

Understand Computer Networking

Today, I learn some important concepts

Network

A **network** refers to a collection of **interconnected devices** (like computers, servers, switches, routers, and other hardware) that can **communicate and share resources** (such as files, internet access, or printers) with each other.

Computer Networking

Computer networking is the practice of **connecting two or more computing devices** (such as computers, servers, smartphones, and other hardware) so that they can **communicate, exchange data, and share resources** like files, internet connections, printers, and applications. Computer networking is the process of linking computers and other devices to share information and resources.

Computer Networking Functionalities

Mandatory

1. Error Control

Purpose:

Ensures that **data is delivered accurately** and **without corruption**.

How it works:

- Uses **checksums** to detect errors in transmitted segments.
- If an error is detected, the receiver can request a **retransmission**.
- Protocols like **TCP** implement error control by **acknowledgments (ACKs)** and **timeouts**.

Example: If a data packet is lost or damaged during transmission, TCP retransmits it.

2. Flow Control

Purpose:

Prevents the **sender from overwhelming the receiver** with too much data too fast.

How it works:

- Uses a mechanism like **sliding window** to control how much data can be sent before needing an acknowledgment.
- Ensures that the receiver has enough buffer space to process the data.

Example: If a sender sends data too fast, the receiver may drop it. Flow control prevents this.

---

3. Multiplexing

Purpose:

Allows **multiple applications or processes** to send data over the **same network connection**.

How it works:

- The transport layer uses **port numbers** to distinguish between different processes.
- Multiple streams (like browser and email) can be handled over one network link.

Example: You can browse the web (HTTP) and receive email (SMTP) at the same time using the same internet connection.

---

4. Demultiplexing

Purpose:

Delivers the received data to the **correct application or process** on the receiving device.

How it works:

- The receiver uses **destination port numbers** to determine which application should get the data.

Example: TCP delivers web data (port 80 or 443) to the browser and mail data (port 25 or 587) to the mail client.

Optional

1. Encryption

> **Encryption in networking** is the process of encoding data so that it can only be accessed or understood by someone with the correct **decryption key**.

How Encryption Works:

1. **Sender** encrypts the data using an **encryption algorithm** and a **key**.
2. The encrypted data (cipher text) is sent over the network.
3. **Receiver** uses a **decryption key** to turn the cipher text back into readable **plain text**.

2. Compression

Compression is a technique used to **reduce the size of data** so it can be **transmitted faster** over a network and **consume less bandwidth**.

Purpose of Compression:

- Reduce file size
- Speed up data transmission
- Minimize bandwidth usage
- Save storage and memory

How It Works:

1. **Before transmission**, the sender compresses the data using a **compression algorithm**.
2. The **compressed data** is transmitted over the network.
3. **Receiver** decompresses the data back to its original form.

Advantages of Computer Networking

1. Resource Sharing

- Share hardware like printers, scanners, and internet connections.
- Share software and files without the need for duplication.

Example: One printer can serve multiple computers in an office.

2. Data Sharing and Communication

- Easy exchange of information between users through emails, messaging, file transfers, and video conferencing.

Example: Teams can collaborate using chat apps like Slack or Microsoft Teams.

3. Centralized Data Management

- Store data on centralized servers for easy access, backup, and security.

Example: All employee data is stored and accessed from a central HR server.

---

4. Internet Access and Sharing

- A single internet connection can be shared across multiple devices.

Example: Wi-Fi routers at home allow many devices to connect to the internet.

5. Improved Communication Speed

- Real-time communication and file transfer improve productivity.

Example: Instant sharing of documents over the network rather than using USB drives.

6. Cost Efficiency

- Reduces the cost of hardware (e.g., shared printers), and software licenses when shared.

Example: A company can buy one licensed copy of software and share it over the network.

7. Scalability

- Easy to add new users or devices to the network without major changes.

Example: Adding a new computer to a Wi-Fi network takes seconds.

8. Security and Access Control

- Centralized control over user access and data permissions.

Example: Only authorized users can access sensitive files on a network.

9. Remote Access

- Users can access network resources from anywhere using VPN or remote desktop tools.

Example: Employees working from home can access files on the office server.

10. Backup and Recovery

- Centralized backup systems make data recovery easier and safer.

Example: Automated backups from all computers to a central server.

Disadvantages of Computer Networking

1. Security Risks

- Networks are vulnerable to **hacking, malware, and data breaches** if not properly secured.

Example: A virus entering one computer can spread across the whole network.

2. Cost of Setup and Maintenance

- Initial setup (hardware, software, cabling, etc.) and ongoing maintenance can be **expensive**.

Example: Setting up a secure enterprise network requires routers, switches, servers, and skilled IT staff.

3. Network Failure

- If the **central server or router fails**, it can **disrupt the entire network**.

Example: In a school, if the server goes down, students may lose access to online resources.

4. Complexity

- Managing a large network requires **technical knowledge** and **skilled personnel**.

Example: Configuring firewalls, IP addresses, and user permissions can be complex in large systems.

5. Virus and Malware Spread

- Malicious software can **quickly spread** across networked systems.

Example: A single infected file shared over a network can affect many computers.

6. Data Privacy Concerns

- Without proper security measures, **unauthorized users may access sensitive information**.

Example: Employees accessing confidential HR files due to weak permission settings.

7. Dependence on Network

- Users become **highly dependent** on the network. If it's slow or fails, productivity drops.

Example: Slow internet can delay file uploads, video calls, or cloud-based work.

8. Bandwidth Limitations

- Too many users or high data use can **slow down the network** performance.

Example: During peak hours, streaming or downloading can become slow in a shared network.

9. Unauthorized Access

- If not properly secured, users may **gain access to restricted areas or files**.

Example: A student accessing exam papers stored on a school server.

Networking Devices

- **Router:**
  A device that connects two or more different networks and directs data packets between them.
- **Switch:**
  A device that connects multiple devices within the same network and forwards data only to the intended recipient.
- **Hub:**
  A basic networking device that connects multiple devices in a network but sends incoming data to all connected devices.
- **Modem:**
  A device that converts digital data from a computer into signals suitable for a communication line (and vice versa), enabling internet access.
- **Access Point (AP):**
  A device that allows wireless devices to connect to a wired network.
- **Network Interface Card (NIC):**
  Hardware inside a device that allows it to connect to a network.
- **Repeater:**
  A device that amplifies or regenerates signals to extend the transmission distance.
- **Gateway:**
  A device that connects networks using different protocols and translates data between them.
- **Firewall:**
  A security device that monitors and controls incoming and outgoing network traffic based on security rules.

Types of Computer Networking

1. LAN (Local Area Network)

- **Definition:** A network that connects computers and devices in a small, localized area such as a home, office, or building.
- **Coverage:** Typically up to a few kilometers.
- **Speed:** High speed (usually 100 Mbps to 10 Gbps).
- **Ownership:** Usually privately owned.
- **Example:** Office network, home Wi-Fi network.

2. MAN (Metropolitan Area Network)

- **Definition:** A network that covers a larger geographic area than LAN, such as a city or a campus, connecting multiple LANs.
- **Coverage:** Up to 50 kilometers or more.
- **Speed:** Moderate to high speed.
- **Ownership:** Can be owned by a single organization or a service provider.
- **Example:** City-wide Wi-Fi, university campus network.

3. WAN (Wide Area Network)

- **Definition:** A network that covers a very large geographic area, connecting multiple LANs and MANs over long distances.
- **Coverage:** Can span countries or continents.
- **Speed:** Varies; generally slower than LAN but improving.
- **Ownership:** Usually owned and managed by multiple organizations or service providers.
- **Example:** The Internet, corporate networks linking branch offices worldwide.