Lab 2.1

1.List two benefits of modern networks.

Increased Security and Reliability: Modern networks prioritize security features and offer redundancy, meaning they have backups in place to keep things running smoothly in case of outages. This helps ensure your data and applications are protected and accessible when you need them.

Improved Scalability and Efficiency: Modern networks are designed to handle the ever-growing demands of today's digital world. They can easily adapt to accommodate more users, devices, and applications without sacrificing performance. This allows businesses and organizations to scale their operations efficiently.

2. How are PC networks similar to older mainframe networks? How are they different?

- **Resource Sharing:** Both types of networks allow for shared resources like printers, files, and applications. Users on the network can access these resources instead of having them on individual machines.
- **Communication:** Both facilitate communication between devices. In a PC network, this could be email, file sharing, or video conferencing. Mainframe networks also enabled communication, but it might have been limited to specific business applications.
- **Centralized Management:** Both can have a central point of control. In PC networks, this could be a server or network management software. Mainframes were inherently centralized, with the mainframe itself being the central point of control.

Differences:

- **Scale and Capacity:** Mainframe networks were designed to handle a massive number of users and transactions simultaneously. Think banks processing millions of transactions daily. PC networks, while scalable, are generally meant for smaller groups or departments.
- **Processing Power:** Mainframes were (and still are) beasts in terms of raw processing power. They excel at high-volume, repetitive tasks. Modern PCs are powerful enough for everyday tasks, but wouldn't hold a candle to a mainframe in terms of sheer processing muscle.
- **Security:** Modern PC networks prioritize user authentication, access control, and firewalls to protect data. Mainframe security historically relied on physical security of the machine and limited user access. While still secure, the approach is different.
- **Accessibility:** PCs are readily available and relatively inexpensive. Mainframes are expensive, require specialized skills to manage, and are typically housed in secure data centers.
- **User Interface:** PC networks are designed for individual users with graphical interfaces. Mainframe users often interact through terminals with text-based interfaces.

3. Why is security for PC networks a concern?

- **Increased Attack Surface:** PC networks have a much larger attack surface compared to mainframes. With many devices (PCs, laptops, smartphones) and users, there are more potential entry points for attackers to exploit.
- **Human Error:** Many security breaches are caused by human error, like clicking on phishing emails or falling for social engineering attacks.
- **Complexity:** PC networks can be complex with a mix of devices, operating systems, and software. This complexity makes it harder to maintain consistent security across the network.
- **Evolving Threats:** Cybercriminals are constantly developing new malware, phishing techniques, and other attack methods. PC networks need constant vigilance and updates to stay ahead of these threats.
- **Data at Risk:** Modern PC networks often store sensitive data like financial information, personal records, and intellectual property. A security breach can lead to this data being stolen, corrupted, or held hostage by ransomware.

4.What are some of the access control methods used to protect networked information?

Authentication: This verifies a user's identity before granting access. This can be done through passwords, multi-factor authentication (MFA), biometrics (fingerprint, facial recognition), or security tokens.

Authorization: Even if a user is authenticated, authorization determines what specific resources they can access and what actions they can perform. This is often controlled through Access Control Lists (ACLs), Role-Based Access Control (RBAC), or Attribute-Based Access Control (ABAC).

Encryption: Encryption scrambles data using algorithms, making it unreadable to anyone without the decryption key. This protects sensitive information at rest (stored on a disk) and in transit (being transmitted over a network).

Firewalls: These act as a barrier between a network and the internet, filtering incoming and outgoing traffic based on security policies. They can block unauthorized access attempts and malicious traffic.

Network Segmentation: Dividing a network into smaller segments can limit the spread of a security breach. If one segment is compromised, the damage is contained and doesn't affect the entire network.

Virtual Private Networks (VPNs): VPNs create a secure tunnel over the public internet, encrypting data traffic and making it appear as if the user is directly connected to the private network.

Intrusion Detection and Prevention Systems (IDS/IPS): These systems monitor network traffic for suspicious activity and can either alert security personnel or take automated actions to block potential threats.

Data Loss Prevention (DLP): DLP solutions can identify and prevent sensitive data from being exfiltrated from the network, either intentionally or accidentally.

How would you use biometrics to improve security of a computer network?

Replacing Passwords:

- **Stronger Authentication:** Biometric factors like fingerprints, iris scans, or facial recognition are unique to each individual and more difficult to steal or replicate compared to traditional passwords. This reduces the risk of unauthorized access through stolen credentials.
- **Multi-Factor Authentication (MFA):** Biometrics can be combined with passwords or security tokens to create a layered approach to security (MFA). Even if an attacker obtains a password, they wouldn't have the necessary biometric factor to gain access.

Access Control:

- **Granular Access Control:** Biometrics can be used to grant different levels of access to network resources based on an individual's identity. This ensures that only authorized users have access to sensitive data or systems.
- **Physical Access Control:** Biometric scanners can be integrated with physical security systems to control access to buildings or server rooms, further restricting unauthorized physical entry points to the network.

Improved User Experience:

- **Convenience:** Biometric authentication can be faster and more convenient than remembering complex passwords. Users don't need to type passwords or carry tokens, simplifying the login process.
- **Reduced Risk of Credential Fatigue:** With multiple passwords for different systems, users often resort to weak or reused passwords. Biometrics eliminate this issue and can encourage stronger overall security practices.

Here are some specific examples of how biometrics can be implemented:

- **Fingerprint scanners** integrated into laptops or keyboards for user login.
- **Facial recognition systems** for access control at building entrances or ATMs.
- **Iris scanners** for high-security environments requiring even stricter authentication.

However, it's important to consider some limitations of biometrics:

- **Cost:** Implementing biometric systems can be more expensive than traditional password-based authentication.

- **Accuracy:** Biometric scanners may not be perfect and can have error rates. Factors like sensor quality or environmental conditions can affect accuracy.
- **Privacy Concerns:** Some users might be apprehensive about storing their biometric data. Security measures to protect this data are crucial.
- **Potential Workarounds:** In rare cases, sophisticated attackers might try to forge biometric data, although this is generally more difficult than compromising passwords.

In conclusion, biometrics offer a valuable layer of security for computer networks, especially when combined with other security measures. While limitations exist, biometrics can significantly enhance network security and user convenience.

Lab2.2

1.Compare the roles of network clients and network servers.

Clients:

- **Role: Request Resources:** Clients initiate requests for resources or services from servers on the network. These resources could be files, applications, data, printers, or even connections to other networks.
- **Examples:** Personal computers, laptops, smartphones, tablets, gaming consoles, smart TVs – any device that relies on a network for functionality.
- **Processing Power:** Clients typically have moderate processing power, enough to run user applications and handle basic tasks.
- **Storage:** Clients may have local storage, but often rely on servers for larger datasets or centralized storage.
- **Security:** Clients are generally less secure compared to servers. They are more vulnerable to malware and targeted attacks.

Servers:

- **Role: Provide Resources:** Servers act as the central repository for resources and services on a network. They wait for client requests and fulfill them by sending data, running applications, or managing network traffic.
- **Examples:** File servers, web servers, email servers, database servers, print servers, game servers – any computer dedicated to providing a specific service or resource to clients.
- **Processing Power:** Servers are typically much more powerful than clients, with strong processors and large amounts of RAM for handling multiple requests simultaneously.
- **Storage:** Servers often have large storage capacities to hold vast amounts of data, applications, and user files.
- **Security:** Servers are typically more secure than clients, with robust security measures in place to protect sensitive information and prevent unauthorized access.

2. How is a router used in a network?

- **Devices Send Data:** Your devices on the network, like your computer, phone, or smart speaker, initiate communication by sending data packets. These packets contain the information you want to send (an email, a video, a website request) along with an addressing system, like a digital mailing label.
- **Router Receives Data:** The router receives these data packets from the devices on your network.
- **Reading the Address:** The router then examines the destination IP address in the packet header. This IP address acts like the final destination written on a physical mail package.

- **Consulting the Routing Table:** The router maintains a routing table, which is a map of the network. This table shows the path to different destinations (other devices on your local network or networks on the internet).

- **Forwarding the Packet:** Using the IP address and the routing table, the router determines the best route to send the data packet. It then forwards the packet to the next device on the network that gets it closer to its final destination.

Routers can also perform other functions:

- **Network Address Translation (NAT):** In a home network with one public IP address, the router uses NAT to translate private IP addresses of your devices to the public IP address for internet access.
- **Security Features:** Many routers offer security features like firewalls to filter incoming and outgoing traffic and help protect your network from unauthorized access.

3. Compare the client/server, directory services, and peer-to-peer network models.

Model Purpose | Share resources and services | Organize and locate resources on a network **Components** | Clients (request resources), Servers (provide resources) | Directory server (centralized database), Clients (query and access resources) | Peers (each device acts as both client and server) **Resource Sharing** | Centralized on servers. Clients request and access resources from servers. | Facilitates resource sharing between peers directly. No central server.**Scalability** | Highly scalable. Can add more clients and servers as needed. | Moderately scalable. Adding too many clients can strain the directory server. | Limited scalability. Performance can degrade with large numbers of peers.**Security** | More secure due to centralized control and security measures on servers. | Relies on individual peer security. Can be vulnerable if a peer is compromised.**Complexity** | More complex to set up and manage due to server configuration and maintenance. | Relatively simple to set up. Requires directory server management. | Simplest to set up. No central server to manage.**Examples** | File servers, web servers, email servers, database servers | Active Directory, LDAP | File sharing networks, BitTorrent, online gaming

Here's an additional breakdown to highlight key differences:

- **Client/Server:** Imagine a library with librarians and patrons. Librarians (servers) manage the resources (books, computers) and fulfill requests from patrons (clients).
- **Directory Services:** Think of a phone book for a large company. The directory service stores information about employees (resources) and their contact details (location), making it easy to find them.
- **Peer-to-Peer:** Picture a group of friends sharing music files directly from their laptops. Each laptop acts as both a client (requesting files) and a server (providing files) to others.

In essence:

- Client/Server - Centralized model for efficient resource sharing and management.
- Directory Services - Specialized service to locate resources on a network.
- Peer-to-Peer - Decentralized model for direct resource sharing between devices.

Describe how you use your computer at home. Do you have more than one computer? Are they interconnected? Do you have an Internet Service Provider (ISP) and broadband Internet?

- **Multiple Computers:** Many homes have multiple computers, including desktops, laptops, tablets, and even smartphones. These devices can be interconnected for sharing resources and information.
- **Interconnected Devices:** Home networks are often created using Wi-Fi routers, allowing devices to connect wirelessly to the internet and share resources like printers or files.
- **Internet Service Provider (ISP):** To access the internet, most home users subscribe to an Internet Service Provider (ISP). The ISP provides the connection to the wider internet through various technologies like cable, DSL, fiber optics, or satellite.
- **Broadband Internet:** Broadband internet refers to a high-speed internet connection that allows for faster data transfer compared to dial-up connections of the past. This enables users to stream videos, download large files, and participate in online activities more efficiently.

how a home user might utilize their computer:

- **Work:** Many people use their computers for work-related tasks such as checking email, working on documents, or video conferencing.
- **Entertainment:** Computers are used for entertainment purposes like watching videos, listening to music, playing games, or browsing social media.
- **Communication:** People use computers to stay connected with friends and family through email, social media, or video chat.
- **Learning and Research:** The internet provides access to a vast amount of information, allowing users to learn new skills, research topics of interest, or read news articles.
- **Online Shopping and Banking:** Many people use their computers for online shopping, banking, and bill payments.

Lab2.3

1. Define data communications.

- **Transferring data:** The core objective is to move data from one point to another.
- **Digital format:** The information is encoded into a digital form, typically consisting of 0s and 1s, for efficient transmission.
- **Communication channels:** These are the pathways through which the data travels. Examples include cables, fiber optic lines, and wireless signals.
- **Sending and receiving:** There's a sender and a receiver involved in the communication process.

2. How have newer systems taken advantage of the merging of data communications and telecommunications?

- **Unified Communication and Collaboration:** Convergence allows for voice, video, data, and instant messaging to be integrated into a single platform. This enables features like video conferencing over the internet, seamless file sharing during calls, and unified inboxes for managing all communication channels.

- **Convergence Devices:** Smartphones are a prime example. They combine phone functionality with web browsing, email access, social media, and multimedia capabilities, all on a single device. This convergence eliminates the need for separate devices for different communication needs.

- **Mobility and Flexibility:** The convergence of data and telecom has made communication much more mobile. With internet access available almost everywhere, users can make calls, send messages, and access information from virtually any location using their smartphones, laptops, or tablets.

- **New Services and Applications:** The combined power of data and telecom has opened doors for innovative services. Examples include video streaming platforms, cloud storage solutions, real-time communication apps, and the Internet of Things (IoT) which allows devices to connect and share data over the internet.

- **Increased Efficiency and Cost Savings:** Convergence can streamline communication processes and reduce costs. Businesses can eliminate the need for separate phone lines and internet connections, and employees can collaborate more effectively using integrated communication tools.

- **Improved User Experience:** Newer systems offer a more user-friendly and intuitive communication experience. Features like voice commands, touchscreens, and intuitive interfaces make communication faster and more convenient.

- **Network Infrastructure:** The convergence has placed greater demands on network infrastructure. High-speed internet connections like fiber optics are crucial to support the increased data traffic and bandwidth requirements of converged services.

- **Security Concerns:** With more data flowing through a single network, security becomes even more critical. Newer systems address this by implementing robust security measures like encryption and user authentication protocols.

3. Compare the role of low-level and high-level protocols.

Low-Level Protocols

- **Function:** Low-level protocols handle the nitty-gritty of data transmission. They operate "closer to the metal" and deal with the physical characteristics of the communication channel.
- **Examples:**
  - TCP/IP (Transmission Control Protocol/Internet Protocol) suite: The foundation of the internet, it defines how data is broken down into packets, addressed, transmitted, and reassembled at the receiving end.
  - Ethernet: Governs how data travels over physical media like cables.
  - Wi-Fi standards (802.11): Define how data is transmitted wirelessly.
- **Focus:** Low-level protocols ensure reliable and efficient physical transmission of data packets across the network. They handle error detection and correction, flow control (regulating data transmission rate), and media access control (determining which device gets to transmit on a shared medium).
- **Details:** These protocols deal with technical specifications like voltage levels on a cable, data encoding methods, and packet formats. They are device-specific and not concerned with the meaning or content of the data itself.

High-Level Protocols

- **Function:** High-level protocols operate at a more abstract level. They focus on the application and user experience.
- **Examples:**
  - HTTP (Hypertext Transfer Protocol): The foundation of web communication, it defines how web browsers and servers communicate to exchange information.
  - FTP (File Transfer Protocol): Used for transferring files between computers.
  - SMTP (Simple Mail Transfer Protocol): Governs how emails are sent and received.
- **Focus:** High-level protocols define how data is presented, structured, and exchanged between applications. They ensure applications on different devices can understand each other and exchange information meaningfully.
- **Details:** These protocols focus on aspects like message formats, error handling specific to the application, and user authentication mechanisms.

Analogy:

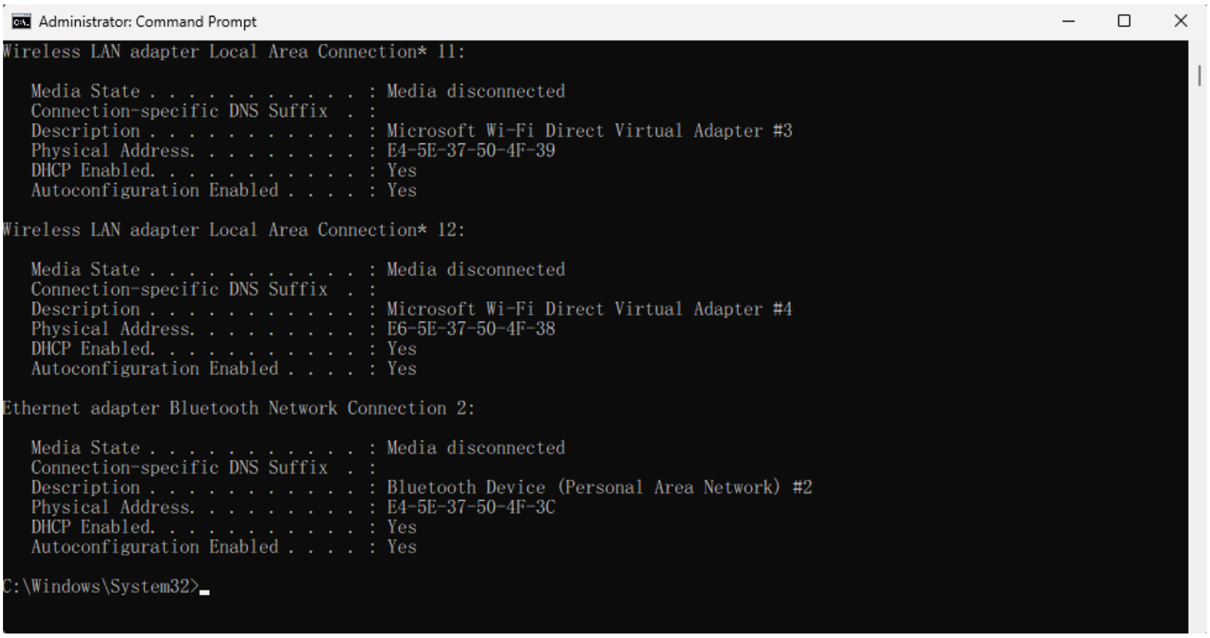
Imagine sending a package across the country.

- **Low-Level Protocols:** These are like the packing materials (boxes, tape), shipping labels (with addresses), and the delivery service (FedEx, UPS) that handles the physical transportation.
- **High-Level Protocols:** These are like the contents of the package (a birthday gift, important documents) and any specific instructions for handling (fragile, signature required).

In essence:

- Low-level protocols ensure the reliable delivery of data packets across the network.
- High-level protocols ensure the data is presented and exchanged meaningfully between applications.

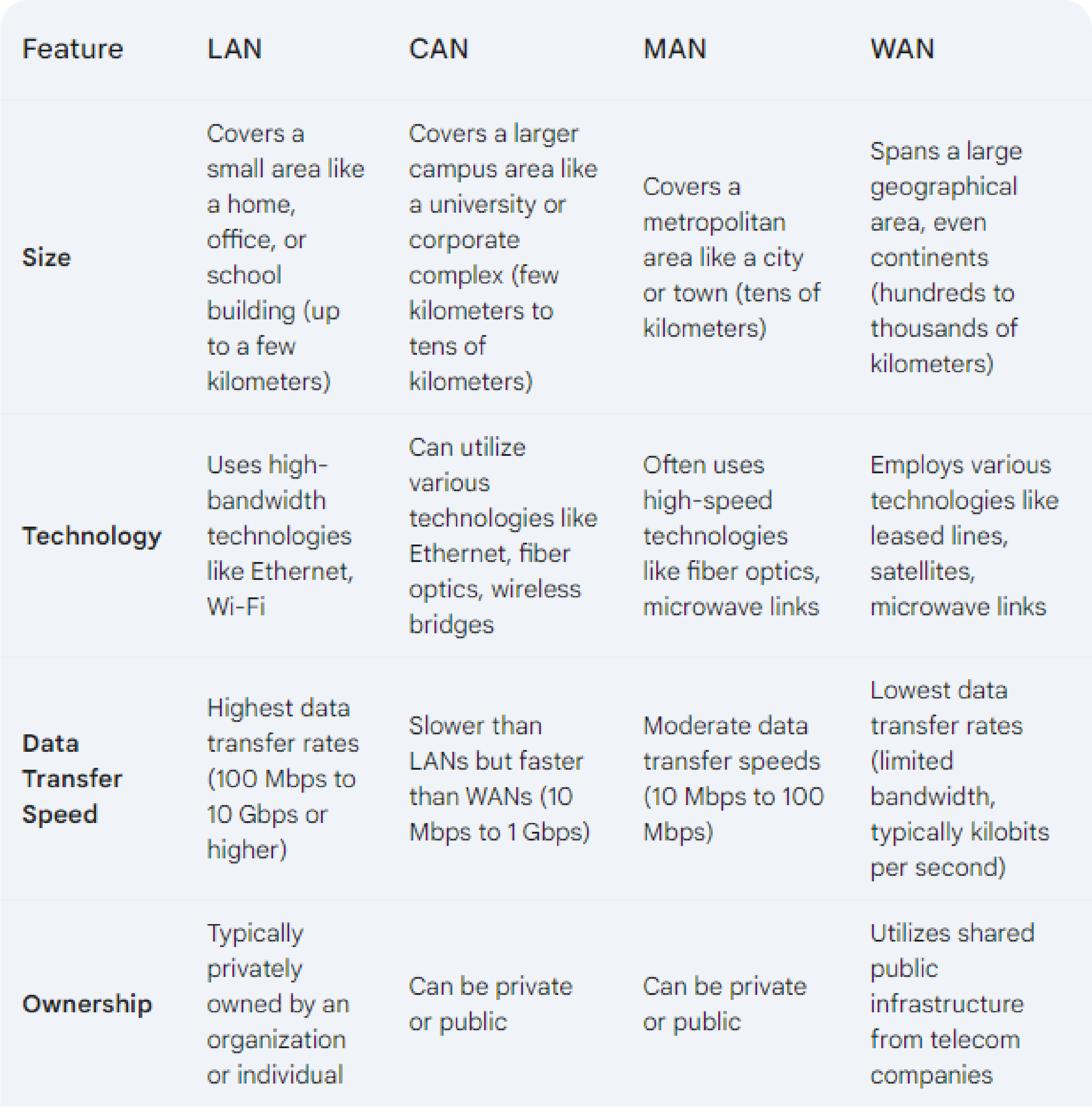
Why do you think Microsoft abandoned its
original network communications protocols of NetBEUI in favor of the
TCP/IP protocol suite?



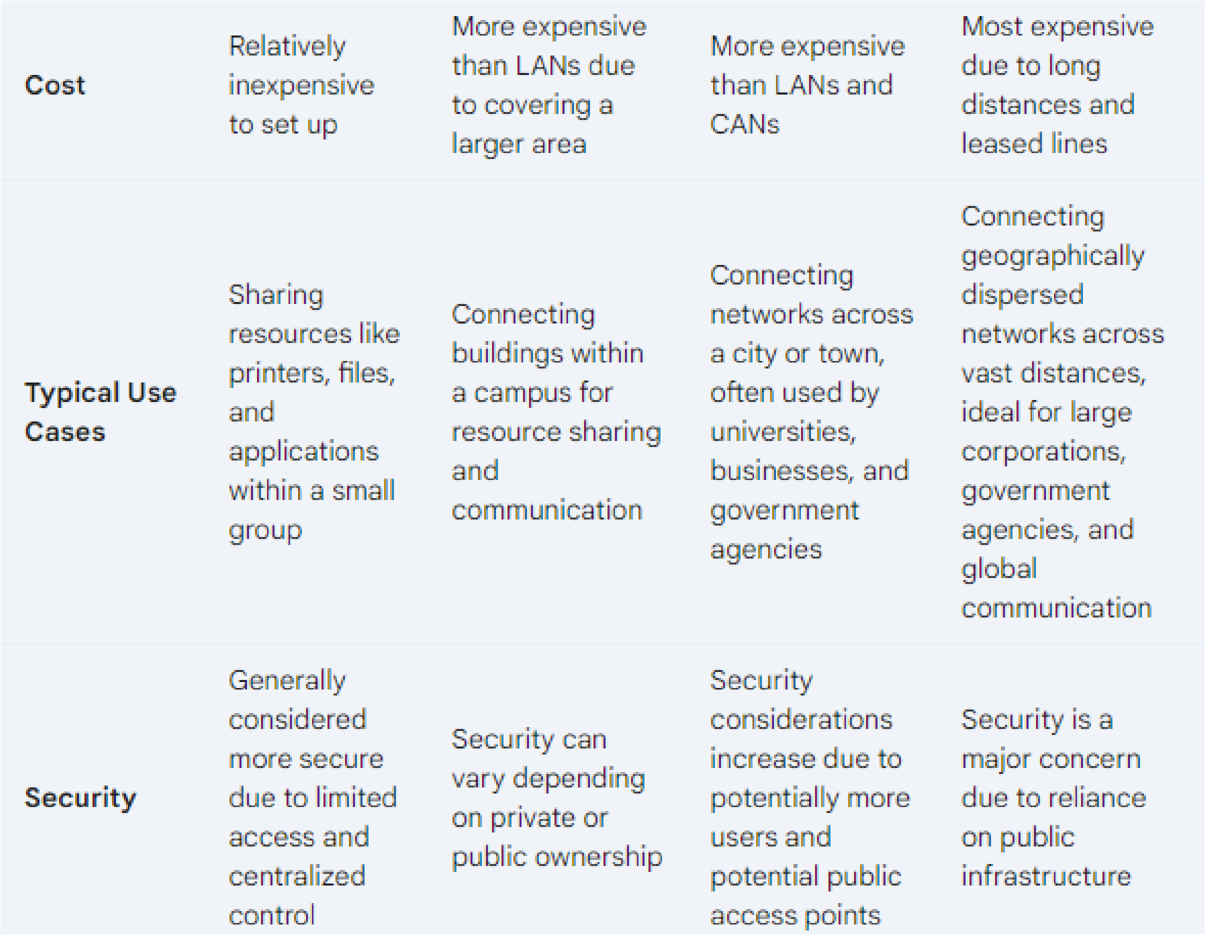
```
Wireless LAN adapter Local Area Connection* 11:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
   Physical Address. . . . . . . . . : E4-5E-37-50-4F-39
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 12:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #4
   Physical Address. . . . . . . . . : E6-5E-37-50-4F-38
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Bluetooth Network Connection 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network) #2
   Physical Address. . . . . . . . . : E4-5E-37-50-4F-3C
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

C:\Windows\System32>
```

Lab 2.4

1 Compare characteristics of LANs, CANs, MANs, and WANs



Feature	LAN	CAN	MAN	WAN
Size	Covers a small area like a home, office, or school building (up to a few kilometers)	Covers a larger campus area like a university or corporate complex (few kilometers to tens of kilometers)	Covers a metropolitan area like a city or town (tens of kilometers)	Spans a large geographical area, even continents (hundreds to thousands of kilometers)
Technology	Uses high-bandwidth technologies like Ethernet, Wi-Fi	Can utilize various technologies like Ethernet, fiber optics, wireless bridges	Often uses high-speed technologies like fiber optics, microwave links	Employs various technologies like leased lines, satellites, microwave links
Data Transfer Speed	Highest data transfer rates (100 Mbps to 10 Gbps or higher)	Slower than LANs but faster than WANs (10 Mbps to 1 Gbps)	Moderate data transfer speeds (10 Mbps to 100 Mbps)	Lowest data transfer rates (limited bandwidth, typically kilobits per second)
Ownership	Typically privately owned by an organization or individual	Can be private or public	Can be private or public	Utilizes shared public infrastructure from telecom companies



Cost	Relatively inexpensive to set up	More expensive than LANs due to covering a larger area	More expensive than LANs and CANs	Most expensive due to long distances and leased lines
Typical Use Cases	Sharing resources like printers, files, and applications within a small group	Connecting buildings within a campus for resource sharing and communication	Connecting networks across a city or town, often used by universities, businesses, and government agencies	Connecting geographically dispersed networks across vast distances, ideal for large corporations, government agencies, and global communication
Security	Generally considered more secure due to limited access and centralized control	Security can vary depending on private or public ownership	Security considerations increase due to potentially more users and potential public access points	Security is a major concern due to reliance on public infrastructure

- **LAN:** Think of a small local community where everyone knows each other and shares resources easily.
- **CAN:** Imagine a university campus where different buildings are connected for students and faculty to access resources across departments.
- **MAN:** Picture a city with a network connecting various institutions like government offices, libraries, and businesses.
- **WAN:** Consider a global company with offices in different countries, all connected to share information and resources seamlessly.

2. How are intranets and extranets similar? How are they different?

- **Internal Networks:** Both intranets and extranets are private networks designed for a specific group of users. They are not accessible to the general public like the internet.
- **Controlled Access:** Access to both intranets and extranets is controlled by the organization. Users need proper authentication (usernames, passwords) to log in.
- **Purpose:** Both intranets and extranets aim to facilitate communication, collaboration, and information sharing within a controlled environment.

Differences:

- **Target Users:**
    - **Intranet:** Exclusively for internal users like employees of a company or organization.
    - **Extranet:** For authorized external users in addition to internal users. This could include partners, vendors, customers, or suppliers.
- **Content:**
    - **Intranet:** Contains internal information and resources relevant to employees, such as company policies, training materials, employee directories, and communication platforms.
    - **Extranet:** May contain a mix of internal and external information. External users might have access to specific resources relevant to the business relationship, like product catalogs, order tracking systems, or collaboration tools for joint projects.
- **Security:**
    - **Intranet:** Security is typically focused on preventing unauthorized internal access and protecting sensitive company information.
    - **Extranet:** Security is more stringent as it grants access to external users. There might be additional access controls and restrictions on what external users can see or do on the extranet.

Here's an analogy to understand the difference:

- **Intranet:** Imagine a company building. Employees have badges to enter and access common areas. There might be restricted areas only accessible to authorized personnel.
- **Extranet:** Picture a secure wing within the company building. It requires additional access control for authorized external partners to collaborate on specific projects while keeping some areas restricted to employees only.

In essence:

- Intranets are for internal communication and collaboration within an organization.
- Extranets extend access to authorized external users to collaborate and share specific information..

Can you identify any of these network types in your university?
Describe it and explain how it fits into one of these models.

Network Types:

1. **Campus Area Network (CAN):** This is highly likely to be the core network of your university. A CAN interconnects all the buildings and departments within the university campus, creating a single, large network. It follows the **Campus Area Network (CAN) model**.

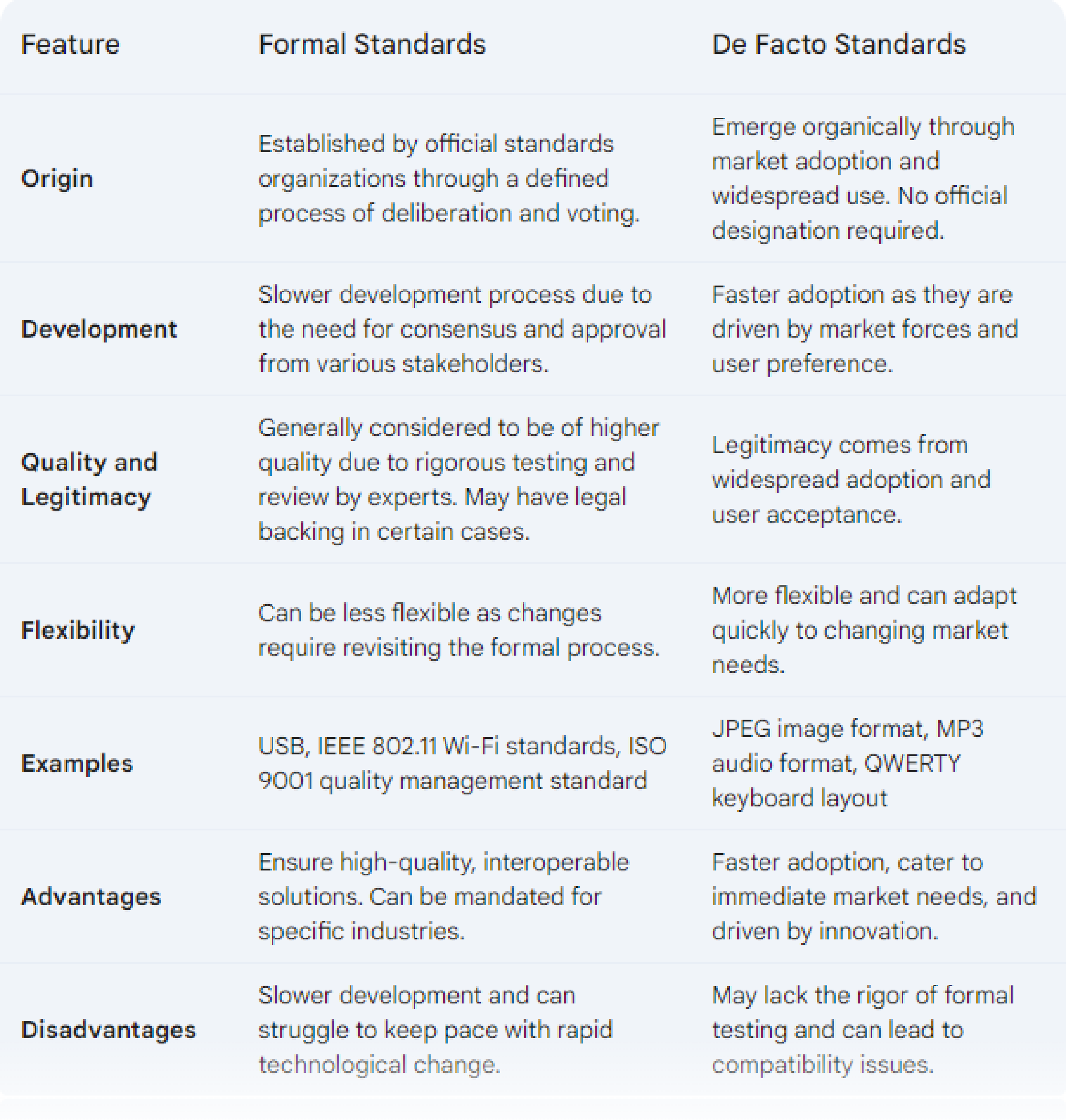
2. **Local Area Networks (LANs):** Within each department or building, there might be smaller LANs connecting computers, printers, and other devices specific to that department. These LANs would connect to the central CAN. They follow the **Local Area Network (LAN) model**.
3. **Wireless Local Area Networks (WLANs):** Many universities likely offer Wi-Fi access across campus. This would be a WLAN built on top of the existing wired LANs or CAN. It follows the **Wireless Local Area Network (WLAN) model**.
4. **Metropolitan Area Network (MAN) (Less Likely):** This is less common in a university setting, but if your university is spread across a large geographical area or consists of multiple campuses in close proximity, a MAN might connect these separate locations. It follows the **Metropolitan Area Network (MAN) model**.

How these Networks Fit into the Models:

- **CAN Model:** The CAN model describes a network spanning a limited geographical area, typically a university campus. It interconnects multiple LANs within the campus, providing a centralized infrastructure for all departments and buildings to communicate and share resources.
- **LAN Model:** The LAN model describes a network connecting devices in a limited area, like a single building or department. University departments likely have their own LANs for their specific needs, and these LANs connect to the central CAN for broader network access.
- **WLAN Model:** The WLAN model describes a wireless network built on top of an existing wired LAN. Universities likely offer Wi-Fi access using a WLAN that connects to the wired LAN infrastructure, allowing students, faculty, and staff to connect wirelessly to the network.
- **MAN Model:** The MAN model describes a network spanning a larger geographical area than a LAN but smaller than a Wide Area Network (WAN). While less common in universities, a MAN could be used if a university has multiple campuses in close proximity that need to be interconnected.

Lab 2.5

1.Compare formal and de facto standards.



Feature	Formal Standards	De Facto Standards
Origin	Established by official standards organizations through a defined process of deliberation and voting.	Emerge organically through market adoption and widespread use. No official designation required.
Development	Slower development process due to the need for consensus and approval from various stakeholders.	Faster adoption as they are driven by market forces and user preference.
Quality and Legitimacy	Generally considered to be of higher quality due to rigorous testing and review by experts. May have legal backing in certain cases.	Legitimacy comes from widespread adoption and user acceptance.
Flexibility	Can be less flexible as changes require revisiting the formal process.	More flexible and can adapt quickly to changing market needs.
Examples	USB, IEEE 802.11 Wi-Fi standards, ISO 9001 quality management standard	JPEG image format, MP3 audio format, QWERTY keyboard layout
Advantages	Ensure high-quality, interoperable solutions. Can be mandated for specific industries.	Faster adoption, cater to immediate market needs, and driven by innovation.
Disadvantages	Slower development and can struggle to keep pace with rapid technological change.	May lack the rigor of formal testing and can lead to compatibility issues.

2. Why are standards important to an industry segment like networking?

- **Interoperability:** Standards ensure that devices and software from different vendors can communicate and work together seamlessly. Imagine if every company had its own unique way of connecting to a network - it would be chaos! Standards create a common language that allows devices to understand each other and exchange data efficiently.
- **Scalability and Growth:** Standards enable networks to grow and adapt to new technologies. As new devices and applications emerge, they can integrate smoothly into existing networks if they adhere to established standards. This fosters a flexible and scalable network environment.

- **Reduced Costs:** Standards help to reduce development and manufacturing costs for networking equipment. Companies don't need to create custom solutions for each situation, and economies of scale come into play when everyone is using the same basic protocols and technologies.
- **Improved Performance:** Standards help to optimize network performance by defining efficient data transmission methods and error correction mechanisms. This ensures reliable and consistent data flow across the network.
- **Security:** Many networking standards incorporate security features like encryption and authentication protocols. This helps to protect data from unauthorized access and ensure the integrity of communication.
- **Innovation:** Standards can foster innovation by providing a stable foundation for new technologies. Developers can focus on creating new features and functionalities without having to worry about compatibility issues.
- **Fair Competition:** Standards create a level playing field for all vendors in the networking industry. Companies compete on the basis of features, performance, and price, rather than on proprietary technologies that lock in customers.

3. List the major standards organizations relating to data communications, networking, and the Internet.

- **International Organization for Standardization (ISO)**:

International Organization for Standardization (ISO) logo

- A global federation of national standards bodies from over 160 countries.
- Develops a wide range of standards, including some for data communication and networking, such as the Open Systems Interconnection (OSI) model, a conceptual framework for network communications.

- **International Telecommunication Union Telecommunication Standardization Sector (ITU-T)**:

International Telecommunication Union Telecommunication Standardization Sector (ITUT) logo

- A specialized agency of the United Nations (UN) that focuses on information and communication technologies (ICTs).
- Develops technical standards for telecommunications and networking, including protocols for voice, data, and image communication.

- **Institute of Electrical and Electronics Engineers (IEEE)**:

Institute of Electrical and Electronics Engineers (IEEE) logo

- A world's largest professional association for the advancement of technology.

  - Develops a wide range of standards, including many for data communication and networking, such as Ethernet and Wi-Fi technologies.

- **Internet Engineering Task Force (IETF)**:

Internet Engineering Task Force (IETF) logo

  - A large, open, international community of network designers, operators, vendors, and researchers.
  - Develops and promotes technical standards for the Internet, such as the TCP/IP protocol suite, which is the foundation of the internet.

- **Internet Corporation for Assigned Names and Numbers (ICANN)**:

Internet Corporation for Assigned Names and Numbers (ICANN) logo

  - A non-profit organization responsible for coordinating the Domain Name System (DNS) for the Internet.
  - Assigns domain names and IP addresses to ensure they are unique and don't conflict.

The 802.11n wireless standard has been used for
some time now. Is it a de facto standard, a draft standard, or has it been
ratified as a formal standard?

The 802.11n wireless standard is a **formal standard**. It was ratified in October 2009 by the Institute of Electrical and Electronics Engineers (IEEE).

While 802.11n technology preceded the formal ratification and may have been in use in draft form, the final ratification in 2009 solidified it as a formal standard.

Lab2.6

1.List and describe the seven OSI model layers.

The OSI (Open Systems Interconnection) model is a conceptual framework that defines seven layers for network communication. It acts as a universal language for understanding how data travels across networks, regardless of the specific technologies used. Here's a breakdown of the seven layers, from the physical layer (bottom) to the application layer (top):

Layer 1: Physical Layer

- **Function:** The physical layer establishes the physical connection between network devices. It defines the electrical, mechanical, and procedural specifications for transmitting and receiving raw data bits over a physical medium like cables or wireless signals.
- **Examples:** Cables (coaxial, fiber optic), connectors (RJ-45), wireless standards (802.11 Wi-Fi)

Layer 2: Data Link Layer

- **Function:** The data link layer packages raw data bits into frames, adds error detection and correction mechanisms, and controls access to the physical media. It ensures reliable and error-free data transmission between physically connected devices on a network segment.
- **Examples:** Ethernet protocols (like 802.3), Media Access Control (MAC) addresses

Layer 3: Network Layer

- **Function:** The network layer handles routing data packets across networks. It determines the most efficient path for packets to reach their destination, performs logical addressing (IP addresses), and forwards packets to the appropriate network devices.
- **Examples:** Internet Protocol (IP), routing protocols

Layer 4: Transport Layer

- **Function:** The transport layer provides reliable data delivery services between applications on different devices. It breaks down messages from upper layers into segments, ensures in-order delivery, and handles flow control to prevent data overload.
- **Examples:** Transmission Control Protocol (TCP), User Datagram Protocol (UDP)

Layer 5: Session Layer

- **Function:** The session layer establishes, manages, and terminates sessions between communicating applications. It allows applications to exchange control information and synchronize communication.
- **Examples:** Session Initiation Protocol (SIP)

Layer 6: Presentation Layer

- **Function:** The presentation layer focuses on data presentation. It handles data formatting, encryption, decryption, and compression. This layer ensures that data is presented in a way that the receiving application can understand.
- **Examples:** Encryption algorithms, image/video compression formats

Layer 7: Application Layer

- **Function:** The application layer provides network services directly to user applications. It defines protocols for various applications like web browsing (HTTP), file transfer (FTP), email (SMTP), and video conferencing.
- **Examples:** HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol)

Analogy: Think of sending a package across the country.

- **Layer 1:** The physical box, packing tape, and shipping label.
- **Layer 2:** Addressing the package and ensuring it gets picked up by the delivery service.
- **Layer 3:** The shipping company determining the most efficient route to get the package to its destination city.
- **Layer 4:** The delivery service tracking the package and ensuring it arrives in one piece.
- **Layer 5:** Coordinating with the recipient to schedule a delivery time.
- **Layer 6:** Ensuring the contents of the package are in a format the recipient understands (e.g., fragile items are properly wrapped).
- **Layer 7:** The actual contents of the package being delivered (a gift, important documents).

2. List and describe common IEEE Physical layer standards.

- **IEEE 802.3 Ethernet:** This is a family of standards that define the physical and data link layer specifications for wired Ethernet networks. It encompasses various technologies for different data transfer speeds and media types. Some common examples include:
  - **10BASE-T (10 Mbps Ethernet):** Uses twisted-pair cabling for up to 10 Mbps data rates.
  - **100BASE-TX (Fast Ethernet):** Utilizes twisted-pair cabling for speeds of up to 100 Mbps.

    - **1000BASE-T (Gigabit Ethernet):** Achieves Gigabit speeds (1 Gbps) over twisted-pair cables.
    - **10GBASE-T (10 Gigabit Ethernet):** Supports 10 Gbps data rates on twisted-pair cabling for shorter distances.
- **IEEE 802.11 Wi-Fi:** This family of standards defines the physical and data link layer specifications for wireless local area networks (WLANs). Different versions offer varying ranges, speeds, and security features. Some notable examples include:
    - **802.11a:** Operates in the 5 GHz band, offering high speeds (up to 54 Mbps) but with limited range.
    - **802.11b:** Operates in the 2.4 GHz band, providing good range but lower speeds (up to 11 Mbps) due to more congestion.
    - **802.11g:** Also uses the 2.4 GHz band but offers faster speeds (up to 54 Mbps) compared to 802.11b.
    - **802.11n (Wi-Fi 4):** Employs multiple antennas (MIMO) technology for increased speed (up to 300 Mbps) and range on the 2.4 GHz and 5 GHz bands.
    - **802.11ac (Wi-Fi 5):** Leverages wider channels and higher modulation techniques to achieve Gigabit speeds (up to 1.3 Gbps) on the 5 GHz band.
    - **802.11ax (Wi-Fi 6):** Introduces features like improved efficiency and capacity handling for multiple devices on the 2.4 GHz and 5 GHz bands, with speeds reaching multiple Gigabits per second (Gbps).
- **IEEE 802.5 Token Ring:** This standard defines a wired networking technology that uses a token-passing mechanism for media access control. It's less common today compared to Ethernet.

These are just a few examples, and the IEEE has developed many other physical layer standards for various applications, including:

- **IEEE 10BASE-FL (10 Mbps Ethernet):** Uses fiber optic cabling for longer distances and higher immunity to interference.
- **IEEE 100BASE-FX (Fast Ethernet):** Achieves Fast Ethernet speeds (100 Mbps) over fiber optic cables.
- **IEEE 802.3bz (2.5GBASE-T and 5GBASE-T):** Supports data rates of 2.5 Gbps and 5 Gbps over twisted-pair cabling for shorter distances.

What is a practical application of Half-duplex communications and why would it be used?

- **Walkie-Talkies:** The classic example! Walkie-talkies use a push-to-talk (PTT) button that activates half-duplex mode. Only one person can speak at a time, and the listener needs to wait for their turn to respond by pressing the PTT button. This avoids audio conflicts and wasted bandwidth.
- **Radio Communication Systems:** Two-way radios used by police, firefighters, security personnel, or construction crews often operate in half-

duplex mode. Similar to walkie-talkies, users take turns transmitting messages to minimize interference and ensure clear communication.

- **Satellite Communication:** Due to the vast distances involved in satellite communication, half-duplex mode can be used to optimize bandwidth usage. Data transmission can be prioritized in one direction at a time, depending on the need.
- **Simple Sensors and Devices:** Some sensors or data loggers might communicate using half-duplex mode. They may periodically transmit data readings or receive configuration updates, but don't require constant two-way communication.

Advantages of Half-Duplex Communication:

- **Simpler and Less Expensive:** Half-duplex devices are generally simpler to design and manufacture compared to full-duplex devices. This translates to lower costs for both the equipment and the communication infrastructure.
- **Efficient Bandwidth Usage:** Since only one device transmits at a time, half-duplex mode is more efficient in situations where constant two-way data flow is not critical. This is especially beneficial in scenarios with limited bandwidth, like radio communication or satellite links.
- **Reduced Complexity:** The system doesn't need complex algorithms to manage simultaneous data flows in both directions. This makes it suitable for simpler devices and applications.

However, half-duplex communication also has limitations:

- **Potential Delays:** There can be a slight delay in communication as users need to wait for their turn to transmit. This might not be ideal for applications requiring real-time interaction.
- **Lower Overall Throughput:** Compared to full-duplex mode, the total data exchange capacity is lower because only one device transmits at a time.

Lab 2.7

1. Compare the OSI, TCP/IP (or DoD), and Internet models.

OSI Model

- **Function:** A conceptual framework with seven layers that define network communication functionalities. It provides a universal language for understanding how data travels across networks.
- **Focus:** Describes the theoretical ideal for network communication, ensuring interoperability between different systems.
- **Not a strict implementation:** It doesn't define specific protocols, but rather the general functions each layer should perform.
- **Layers:** Physical, Data Link, Network, Transport, Session, Presentation, Application

TCP/IP Model (DoD Model)

- **Function:** A four-layer model that defines the actual protocols used in the internet. It's the foundation for internet communication.
- **Focus:** Practical implementation for internetworking, with specific protocols associated with each layer.
- **Widely adopted:** The dominant model used for internet communication today.
- **Layers:** Network Access, Internet, Transport, Application

Internet Model

- **Subset of TCP/IP Model:** Focuses on the core internetworking functionalities defined in the lower three layers (Network Access, Internet, Transport) of the TCP/IP model.
- **Focus:** Describes the internet itself, how data packets are routed and delivered across interconnected networks.

2. How are Internet layers organized into groups?

- **Network Access and Internet Layers (Group 1):**

  - **Focus:** These layers handle data addressing, routing, and packet delivery across networks. They establish the foundation for internetworking.
  - **Layers:**
    - **Network Access Layer:** Deals with the physical transmission of data packets over a network medium (Ethernet, Wi-Fi). Protocols like Ethernet or Wi-Fi reside here.

    - **Internet Layer:** Defines how data packets are addressed (IP addresses) and routed across interconnected networks. The core protocol here is the Internet Protocol (IP).

- **Transport and Application Layers (Group 2):**

  - **Focus:** These layers handle how applications exchange data and provide user-oriented services. They build upon the foundation laid by the lower layers.
  - **Layers:**
    - **Transport Layer:** Provides reliable data transfer services between applications on different devices. Key protocols include Transmission Control Protocol (TCP) for reliable, in-order delivery and User Datagram Protocol (UDP) for connectionless data transfer.
    - **Application Layer:** Defines protocols for various applications like web browsing (HTTP), file transfer (FTP), email (SMTP), and video conferencing. This layer is closest to the user and interacts with application programs.

analogy:

- Imagine a postal service delivering a package.
  - Group 1 (Network Access & Internet Layers) is like getting the package to the post office (Network Access) and then the postal system efficiently routing it to the destination city (Internet Layer).
  - Group 2 (Transport & Application Layers) is like ensuring the package contents are intact during delivery (Transport Layer) and finally getting it delivered to the recipient (Application Layer).

Why do you have both connection-oriented
and connectionless transmissions at the transport layer? Can you think of
an example of connectionless protocol use? Why is it used in this example?

- Both connection-oriented (TCP) and connectionless (UDP) protocols have their uses depending on the communication needs.
- TCP provides reliable, in-order delivery for critical data exchange.
- UDP offers faster transmission and is suitable for real-time applications where speed is a priority and some data loss is acceptable.