Topic 4A: Compare Network Types

Local Area Network:

Local Area Network (LAN) is a group of computers and devices connected to share resources, such as printers, files, and internet access, within a specific area. Think of it like the network in your home, office, or school, where all the computers are connected, allowing them to communicate. A LAN can cover a small area like one floor of a building, an entire building, or even multiple nearby buildings like a school campus. Essentially, if all the devices are within about **1 or 2 kilometers (roughly 1 mile)** of each other, it's considered a LAN. The organization using the LAN usually **owns** and manages the cabling and devices that make it work.

Most LANs today are built using standards called **802.3 Ethernet**, which are defined by an organization called the IEEE (Institute of Electrical and Electronics Engineers). These standards determine how data is sent and received in the network and are described using terms like **xBASE-Y**, where:

- **x** refers to the data speed.
- **Y** refers to the type of cable.

For example:

1. **100BASE-T**: This standard means data moves at **100 Mbps** (Fast Ethernet) using copper twisted-pair cables, similar to phone wires.
2. **1000BASE-T**: This standard is called **Gigabit Ethernet**, and it's faster, transferring data at **1000 Mbps (1 Gbps)** over copper cables. It's the most common choice for LANs today because it's fast and reliable.
3. **10GBASE-T**: This is an even faster standard, transferring data at **10 Gbps**, but it's usually used in high-performance setups, like data centers.

Cabling Types: Copper vs. Fiber Optic

LANs use two main types of cabling to send data:

1. **Copper Cables**: These use electrical signals to send information. They are affordable and commonly used in most LANs.
2. **Fiber Optic Cables**: These use pulses of light to send data, making them faster and more reliable over longer distances, but they are more expensive. Fiber is often used in larger buildings or campuses that require high-speed connections.

Wireless Local Area Networks (WLANs):

A **Wireless Local Area Network (WLAN)** is like a regular LAN but without the cables. Instead of using physical wires, it uses **radio signals** and **antennas** to send and receive data. This makes it more flexible and convenient, especially in environments where running cables isn't practical, like homes, offices, or public spaces like coffee shops and airports. Imagine you're at home streaming a movie on your laptop over Wi-Fi while your sibling is using a desktop computer connected via Ethernet. Both devices are part of the same network, but the laptop uses a wireless connection, while the desktop uses a wired one. This setup shows how Wi-Fi and Ethernet can work together in the same network.

Most WLANs follow the **IEEE 802.11** standards, commonly known by their brand name, **Wi-Fi**. These standards define how wireless devices communicate with each other and with the network. Wi-Fi complements Ethernet, so both wired and wireless devices can coexist and communicate within the same local network.

Wide Area Networks (WAN):

A **Wide Area Network (WAN)** connects multiple Local Area Networks (LANs) across different geographic locations, enabling them to communicate as a single system. Unlike a LAN, which operates within a single building or campus, a WAN spans larger areas, often between cities, countries, or even continents. Imagine a company with a head office in New York and branch offices in Los Angeles, London, and Tokyo. Each office has its own LAN for internal communication. To connect these offices and allow them to share data, the company sets up a WAN. This enables employees in different locations to access the same files and systems as if they were in the same building.

The Internet is the largest example of a WAN—a global network connecting millions of private, public, academic, and government networks. Companies and individuals access the Internet through **Internet Service Providers (ISPs)**, which facilitate communication between local networks and the broader Internet.

Metropolitan Area Networks (MANs):

A **Metropolitan Area Network (MAN)** is a type of network designed to cover a geographic area the size of a city or a large town. It sits between a **Local Area Network (LAN)**, which operates within a single site, and a **Wide Area Network (WAN)**, which connects networks across distant locations. A MAN is typically larger than a LAN but smaller than a WAN, making it ideal for connecting multiple networks within the same metropolitan area.

Imagine a university with multiple campuses spread across a city. Each campus has its own LAN, but the university wants all campuses to communicate as part of a unified network. They set up a MAN to connect these LANs, enabling resource sharing, centralized administration, and seamless communication between campuses.

SOHO and Enterprise Networks:

Networking needs differ significantly between small offices/home offices (SOHO) and larger enterprises, so the design and components of these networks vary to meet specific requirements.

A **Small Office/Home Office (SOHO) network** is a simpler setup designed for smaller businesses or home offices. It often uses a single device, like a **SOHO router**, which combines multiple functions:

- Provides LAN (Local Area Network) connectivity for client devices (computers, printers, etc.).
- Offers Internet connectivity.
- Sometimes includes wireless access points for Wi-Fi.

Example: Imagine a small law firm with a few employees. They use a SOHO router to connect their computers, share a printer, and access the Internet. All the network tasks—such as routing, wireless connectivity, and Internet sharing—are handled by this one device.

Enterprise networks support larger organizations, such as corporations or universities, with many employees and devices. These networks are more complex and reliable, separating functions across multiple dedicated devices. Key features include:

1. **Work Areas**: Client computers and printers connect to the network using cables or Wi-Fi access points (APs).
2. **Server Rooms**: Network servers are kept separate from client devices for better security and efficiency.
3. **Switches**: **Workgroup switches** connect devices in each work area to **core/distribution switches**, which handle data flow between different parts of the network.
4. **Firewalls and Routers**: These appliances secure the network by filtering traffic and connecting the private LAN to the public Internet.

Example: A university campus with thousands of students and staff uses an enterprise network. Each building has its own switches and wireless access points, connecting devices to a central core switch. Firewalls protect the network while allowing secure Internet access for users and external visitors.

Security in Enterprise Networks

Enterprise networks implement additional layers of security to protect sensitive data:

- **Screened Subnets**: Areas where Internet services are separated from the private LAN, ensuring external and internal traffic are strictly filtered and monitored.
- **VPNs**: Virtual Private Networks enable secure connections between branch offices and remote employees.

Example: A retail company connects its branches across cities using VPNs, allowing employees in one location to securely access the head office servers.

Understanding Datacenters and Storage Area Networks (SANs):

Modern networks differentiate between two primary roles for computers: **servers** and **clients**. Servers are dedicated to running applications and hosting shared resources, while clients are the computers that end users use to access those resources and perform work.

Datacenters

A **datacenter** is a specialized facility dedicated to housing server resources for large organizations. Unlike a simple server room, a datacenter is designed for high-demand environments and includes:

- **Dedicated Networking**: High-speed, reliable connectivity for servers.
- **Power Management**: Backup power sources like generators and UPS (Uninterruptible Power Supplies) to ensure continuous operation.
- **Climate Control**: Temperature and humidity controls to prevent overheating and hardware failures.
- **Physical Security**: Restricted access, often using biometric scans or key cards, to protect sensitive data.

Real-Life Example: A large e-commerce company like Amazon operates massive datacenters to ensure their website and applications run smoothly 24/7, even during peak shopping seasons.

Storage Area Networks (SANs)

A **Storage Area Network (SAN)** is a specialized network that provides a shared pool of storage devices for servers. Instead of each server relying on its own local disk storage, the SAN allows multiple servers to access a centralized, flexible, and reliable storage system.

Key Features of SANs:

1. **Server Access Only**: SANs are isolated from the main network and are not accessible by client devices like PCs or laptops. Only servers, such as those running databases or critical applications, connect to the SAN.
2. **Flexible and Reliable**: Centralized storage allows for easy scaling and better redundancy. For example, if a server fails, its data remains safe on the SAN.
3. **Connectivity Technologies**:
    - **Fiber Channel**: A high-speed connection method for SANs.
    - **iSCSI (Internet SCSI)**: Allows data to be transmitted over standard IP networks.

Real-Life Example: A hospital with multiple servers running patient record databases uses a SAN to ensure all servers can securely access and store large volumes of data. If one server needs more storage, it can be allocated dynamically without interrupting other services.

Understanding Personal Area Networks (PANs):

A **Personal Area Network (PAN)** is a small network designed for short-range, wireless communication between devices within a few meters of each other. It is used to connect personal devices, making it easy to share data and resources. PANs connect devices like smartphones, tablets, and laptops to peripherals such as printers, headsets,

and speakers. For example, when you pair your wireless earbuds with your smartphone to listen to music, you're using a PAN. Smartwatches and fitness trackers connect to smartphones via PANs to sync data like notifications or fitness stats.

PANs commonly use wireless technologies such as:

- **Bluetooth**: The most widely used technology for PANs, ideal for short-range communication.
- **Infrared**: Used for connecting remote controls to TVs or projectors.
- **Wi-Fi Direct**: Allows devices to connect without requiring a traditional Wi-Fi network.

Some Questions:

A network uses an IEEE 802.11 standard to establish connections. What type of network is this?

- **Answer**: This is a **Wireless Local Area Network (WLAN)**. IEEE 802.11 is the standard for Wi-Fi, which is used for wireless connectivity in local networks.

What type of network has no specific geographical restrictions?

- **Answer**: This is a **Wide Area Network (WAN)**. WANs, like the Internet, span large areas and have no geographical limitations, connecting devices and networks worldwide.

A network uses Fiber Channel adapters to implement connections. What type of network is this?

- **Answer**: This is a **Storage Area Network (SAN)**. Fiber Channel is a high-speed connectivity technology commonly used in SANs to connect servers to centralized storage devices.