DATA COMMUNICATION & COMPUTER NETWORK

UNIT -3

LAN: Local Area Network

LAN stands for Local Area Network. Through LAN, we can connect multiple computers or devices over a single network within an enclosed building like School or office so that the internet can be made accessible on those devices and also for sharing common resources.

To connect through a LAN, the Ethernet cable, wires, fibre optics cable and even Wi-Fi are commonly used. You can combine multiple numbers of laptops, printers, scanners, and other computational devices by using LAN. Once connected, you can interact through the devices and make use of the resources accordingly.

Advantages of LAN

- LAN can share data at speeds ranging from 10 Mbps to 1000 Mbps. The transmission speed of data is high in LAN networks because the range of the LAN is limited to a certain space.
- Multiple computers and devices like printers and scanners can be connected using a LAN cable.
- LAN is considered a very secure network as it can be accessed only within a specific range, and it is impossible to get connected without its ID and password if implemented.

- The ownership of the LAN network is private. It can be accessed only when the user has an authentic user ID and password.
- The user can download or upload any document over the LAN network and print any copy through the printer connected to the same LAN.
- Any software and application can also be downloaded and uploaded using LAN.
- Usually, the range of the LAN network is 0-150m, but the range of the LAN can also be extended up to 1 Km if required.
- It becomes easy for the users to keep their data secured as if someone is using LAN, then all the data get stored in one place, which is referred to as the host computer.
- The users also do not need to purchase separate printers or scanners for each computer as the LAN allows the users to share one printer with all the other computers that are connected to the same LAN, and because of this, cost reduction in purchasing hardware can be made.
- LAN enables the users to share one internet connection with all others computers or devices connected to it.
- LAN is also very cheap to use as the users can share data with other connected devices instantly and cheaply.

Disadvantages of LAN

- There is no doubt that LAN does not cost much as compared to other options available. But initially, to set up the LAN, a high cost has to be incurred by the user for its proper installation as there are some software/hardware requirements.
- The tools which are required while installing the LAN and for its proper working are somewhat costly. These tools are Ethernet cables, routers, switches, etc.
- All the connected users on a single LAN can access the files and data of other devices which are connected on the same LAN. They can also access the internet history of each device that is connected through that LAN which means that LAN does not provide privacy to its users from inside accesses.
- The range of the LAN is limited, and therefore only those who are in the range of the LAN can use it.

- As all the data of the different devices connected through LAN are stored in the server/host computer, it becomes easy for hackers to access the entire data at once, which means that there is always a risk to data privacy, including loss and misuse.
- There should be someone with a piece of proper knowledge about LAN and networking as LAN need regular maintenance. Most of the time, problems like hardware failure and failure of the system can be seen. Therefore, those who are using LAN in the office or for some other official work should keep someone as a full-time employee to fix this kind of issue instantly when required.
- The presence of any kind of virus becomes very dangerous for all the computers connected on the same LAN. If any one of the computers is affected by the virus, then there are chances that all of the other computers will also be affected by the virus.
- As all the data of the connected device are stored on one central server; therefore, in case of server failure, no files of the other connected devices can be accessed in such a situation.

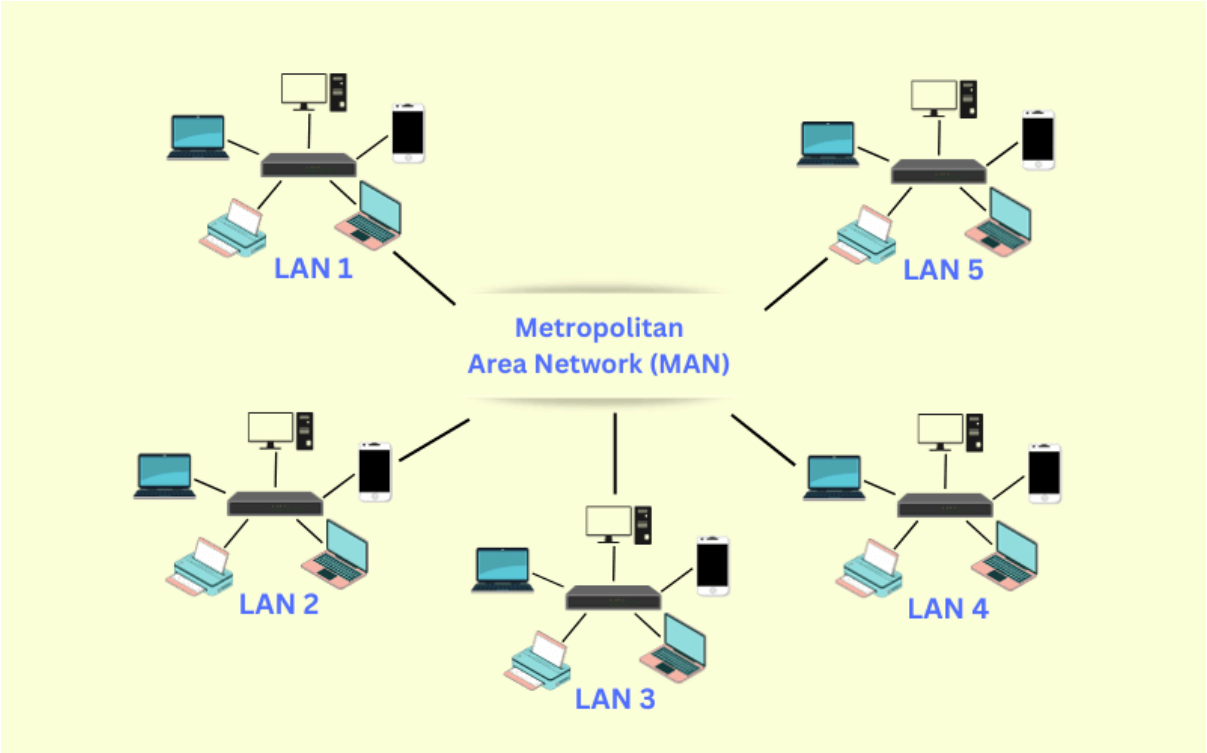
Introduction of MAN

MAN is the short form of Metropolitan Area Network, which is a computer network typically used to connect computers in a metropolitan area (large geographical area) such as a city or university. It is basically a larger version of LAN. A single private or public company mainly operates it.

It is bigger than a LAN (Local Area Network) and smaller than a WAN (Wide Area Network). It is used to expand over a larger area, such as an entire city. It covers a range of up to 50 km and uses telecommunication media within the city.

It connects various LANs using local exchange carriers such as fiber optics. For example, it may connect branch offices to head offices through metropolitan area networks within the same city. It uses local exchange carriers that facilitate connection between the branch and head offices.

The metropolitan area uses switches or hubs to establish a LAN and routers or bridges to connect to other LANs. Local Area Network consists of computers that can communicate with other Local Area Network computers with the help of a metropolitan area network that uses routers for the interconnection of multiple LANs.



It is commonly used on large companies or school campuses with multiple buildings. It serves as a high-speed network to permit the sharing of regional resources. The most common examples of MAN are cable TV networks and telephone company networks.

Metropolitan Area Network commonly uses fiber optic cables to share high-speed data between devices on different LANs.

Advantages of Metropolitan Area Network

The advantages of Metropolitan Area Networks are as follows:

- It uses technologies such as fiber optics, Ethernet, or wireless connections to provide high-speed data transmission.
- Data speeds can reach up to 1000Mbps based on the technology used in the metropolitan area networks.
- MANs cover a significant metropolitan area, making them suitable for connecting multiple locations, such as businesses, educational institutions, government offices, and data centers, within the same city or region.
- It is designed to be scalable, which means that new locations and users can be effortlessly added to the network without significant disruption.

- It can offer cost-effective solutions for high-speed connectivity. They are especially useful for businesses and institutions that require reliable and fast communications across a city.
- It allows you to send local emails fast and free.
- Users can share their Internet connection with the MAN installation.
- It has a higher level of security than WAN.
- It is less expensive to establish a connection using MAN compared to WAN.

Disadvantages of Metropolitan Area Networks

The disadvantages of Metropolitan Area Networks are as follows:

- MAN requires high initial costs to set up because fiber-optic cables and other networking equipment can be expensive.
- MAN requires highly technical people to set up.
- It requires regular maintenance to provide the best performance.
- As compared to LAN, MAN is more complex to implement.
- As the geographical area in MAN increases, it is at risk of being attacked by hackers; hence, more security measures are followed to protect against intruders.
- It is hard to make the system safe from hackers.
- It becomes very difficult to manage if the size and number of LANs increase.
- Its reach is limited to a 50-kilometer area, so organizations located beyond the metropolitan area require a WAN connection.

Switches, Bridges, Routers

Switches:

- Function: Operate primarily at the data link layer (Layer 2) and sometimes at the network layer (Layer 3) of the OSI model. Switches manage data flow within a LAN by using MAC addresses to direct data packets to the correct destination port.
- Operations:

        - MAC Address Table: Maintains a table of MAC addresses and the corresponding switch ports.
        - Frame Forwarding: Uses the MAC address table to forward frames to the appropriate port.
        - VLAN Support: Can segment networks into Virtual LANs (VLANs) to enhance security and performance.
- Types:
    - Unmanaged Switches: Basic, plug-and-play, with no configuration options.
    - Managed Switches: Offer advanced features like VLANs, Quality of Service (QoS), and SNMP monitoring.
    - Layer 3 Switches: Combine switching and routing functions, allowing for inter-VLAN routing.

Bridges:

- Function: Connect multiple LAN segments, working at the data link layer to filter traffic, reduce collisions, and segment the network.
- Operations:
    - Learning: Bridges learn MAC addresses by examining the source address of incoming frames.
    - Forwarding/Filtering: Decides whether to forward or filter a frame based on the destination MAC address.
    - Spanning Tree Protocol (STP): Prevents loops in the network by creating a spanning tree that disables redundant paths.
- Types:
    - Local Bridges: Connect LAN segments within the same geographic location.
    - Remote Bridges: Connect LAN segments over long distances using WAN links.
    - Transparent Bridges: Operate without any configuration, automatically learning and filtering MAC addresses.

Routers:

- Function: Operate at the network layer (Layer 3), connecting different networks and directing data packets based on IP addresses.
- Operations:
    - Routing Table: Maintains a table of routes to different network destinations.
    - Path Selection: Uses routing algorithms to determine the best path for data packets.
    - Packet Forwarding: Forwards packets from one network to another based on routing decisions.
- Types:
    - Static Routers: Routes are manually configured by a network administrator.

- Dynamic Routers: Use routing protocols like OSPF (Open Shortest Path First), BGP (Border Gateway Protocol), and RIP (Routing Information Protocol) to dynamically update routing tables.
- Wireless Routers: Provide wireless connectivity and routing functions in home and small office networks.

The Network Layer

Function:

- The network layer (Layer 3) is responsible for logical addressing, routing, and forwarding packets across different networks. It enables devices on different networks to communicate.

Key Components:

1. Logical Addressing: Utilizes IP addresses (IPv4 or IPv6) to uniquely identify devices on a network.
2. Routing: Determines the optimal path for data to travel from source to destination using routing algorithms.
3. Packet Forwarding: Forwards packets based on the routing table entries.

Routing Algorithms:

1. Distance Vector Routing:
    - Example: RIP (Routing Information Protocol).
    - Mechanism: Routers share distance vectors with their immediate neighbors. Each vector contains the distance to every network destination.
    - Characteristics: Simple, uses hop count as a metric, limited to small networks due to a maximum hop count of 15.
2. Link State Routing:
    - Example: OSPF (Open Shortest Path First).
    - Mechanism: Routers broadcast link state advertisements (LSAs) to all other routers in the network, containing information about directly connected links and their costs.
    - Characteristics: Builds a complete map of the network topology, uses Dijkstra's algorithm to calculate the shortest path, scales well for large networks.
3. Path Vector Routing:
    - Example: BGP (Border Gateway Protocol).
    - Mechanism: Maintains the path information that gets updated dynamically as the topology of the network changes.

- Characteristics: Used for routing between autonomous systems (AS), important for the global Internet routing.

Congestion Control Algorithms

Overview:
Congestion control algorithms manage network congestion by controlling the rate at which data is sent to ensure efficient network operation and prevent packet loss.

Key Algorithms:

1. TCP Congestion Control:
    - Slow Start: Begins transmission with a small congestion window, increasing it exponentially until a packet loss occurs or a threshold is reached.
    - Congestion Avoidance: After the threshold is reached, increases the congestion window size linearly.
    - Fast Retransmit: Detects packet loss through duplicate ACKs (acknowledgments) and retransmits the lost packet without waiting for a timeout.
    - Fast Recovery: Temporarily reduces the congestion window size after a packet loss, then gradually increases it to probe the network capacity.
2. Active Queue Management (AQM):
    - Random Early Detection (RED): Monitors the average queue size and drops incoming packets probabilistically to signal the sender to slow down before the queue becomes full.
    - Explicit Congestion Notification (ECN): Uses a marking mechanism instead of dropping packets to indicate congestion.

The Transport Layer

Function:

- The transport layer (Layer 4) is responsible for providing end-to-end communication, error recovery, flow control, and ensuring complete data transfer between devices.

Protocols:

1. TCP (Transmission Control Protocol):
    - Connection-Oriented: Establishes a connection before data transfer, ensuring reliable communication.
    - Error Recovery: Uses checksums and acknowledgments to detect and recover from errors.

- Flow Control: Uses the sliding window mechanism to manage data flow between sender and receiver.
- Congestion Control: Implements various algorithms to control the rate of data transmission based on network conditions.

2. UDP (User Datagram Protocol):
    - Connectionless: Does not establish a connection, providing a faster, less reliable service.
    - Low Overhead: Suitable for applications requiring speed over reliability, like video streaming and online gaming.
    - No Built-in Error Recovery or Flow Control: Relies on the application layer for these functions if needed.

The Presentation Layer

Function:

- The presentation layer (Layer 6) is responsible for translating data between the application layer and the network, ensuring data is in a usable format. It handles data encryption, decryption, compression, and translation.

Key Responsibilities:

1. Data Translation: Converts data from one format to another, ensuring interoperability between different systems (e.g., translating between ASCII and EBCDIC).
2. Encryption/Decryption: Secures data by converting it into a coded format for transmission and back into a readable format upon reception.
3. Compression: Reduces the size of data to optimize transmission speed and bandwidth usage.

The Session Layer

Function:

- The session layer (Layer 5) manages sessions between applications. It establishes, maintains, and terminates sessions, ensuring structured data exchange.

Key Responsibilities:

1. Session Management: Controls the dialog between devices, managing the establishment, maintenance, and termination of sessions.
2. Synchronization: Inserts synchronization points (checkpoints) in the data stream, allowing for recovery and resumption of data transfer in case of failures.

3. Dialog Control: Manages the direction of data flow (e.g., full-duplex or half-duplex) and ensures proper sequencing and timing.

The Application Layer

Function:

- The application layer (Layer 7) provides network services directly to user applications. It interfaces with the lower layers to facilitate communication and provides various protocols for different types of network services.

Key Services:

1. Network Services: Includes protocols and services such as:
    - HTTP (HyperText Transfer Protocol): Used for web browsing.
    - FTP (File Transfer Protocol): Used for transferring files between computers.
    - SMTP (Simple Mail Transfer Protocol): Used for email transmission.
    - DNS (Domain Name System): Translates domain names into IP addresses.
2. User Interface: Provides the necessary protocols and interfaces for user applications to communicate over the network, ensuring that applications can request and receive network services seamlessly.