MODULE 1: INTRODUCTION TO NETWORKING

COMPUTER NETWORK

NOTES

BY

FAIZ 🤫🫵

SOURCES

OF

NOTES:

CHATGPT,

GEEKS FOR GEEKS,

TECH KNOWLEDGE

Q.1) OSI REFERENCE MODEL

⇒

OSI stands for Open Systems Interconnection , where open stands to say non-proprietary.

It is a 7-layer architecture with each layer having specific functionality to perform.

All these 7 layers work collaboratively to transmit the data from one person to another across the globe.

The OSI reference model was developed by ISO – 'International Organization for Standardization ', in the year 1984.

The OSI model provides a theoretical foundation for understanding network communication . However, it is usually not directly implemented in its entirety in real-world networking hardware or software .

Instead, specific protocols and technologies are often designed based on the principles outlined in the OSI model to facilitate efficient data transmission and

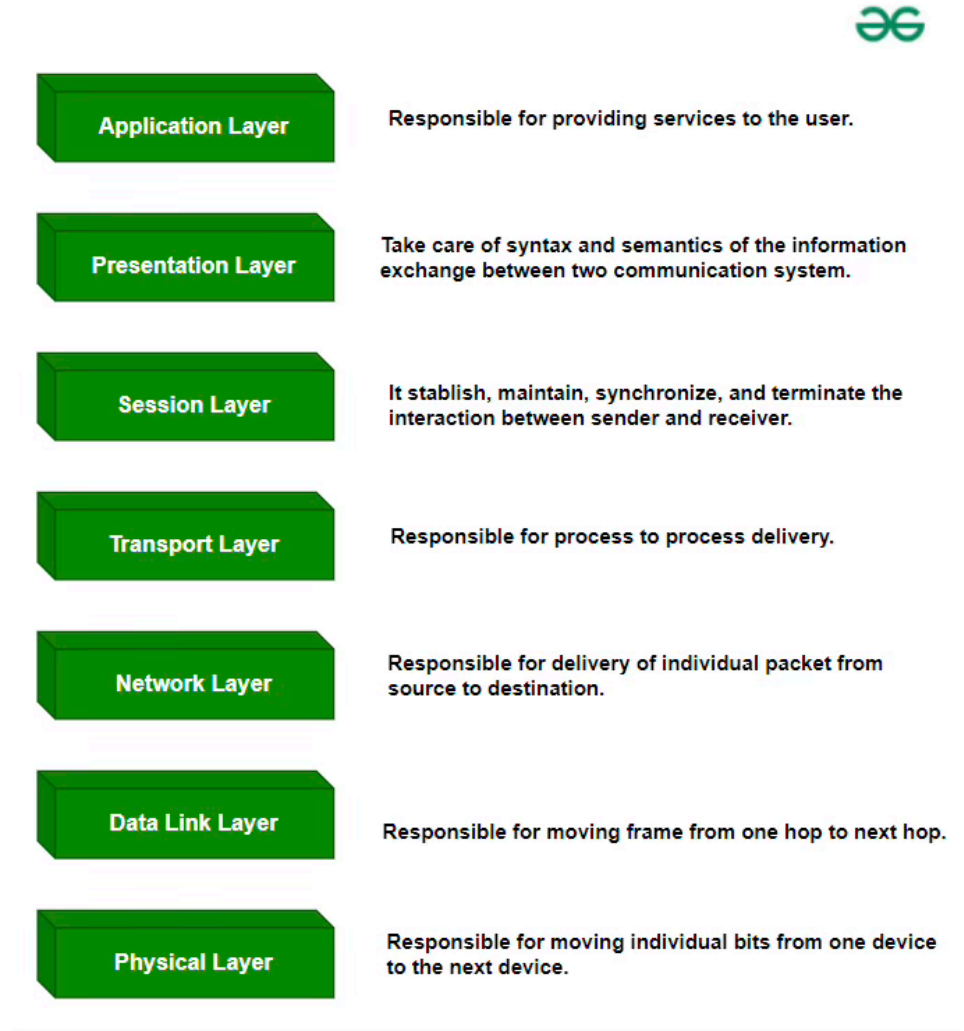
networking operations.

The OSI model, created in 1984 by ISO , is a reference framework that explains the process of transmitting data between computers.

It is divided into seven layers that work together to carry out specialised network functions , allowing for a more systematic approach to networking.

Data Flow In OSI Model

When we transfer information from one device to another, it travels through 7 layers of OSI model. First data travels down through 7 layers from the sender's end and then climbs back 7 layers on the receiver's end.



1. Physical Layer (Layer 1)

- **Function**: Deals with the physical connection between devices, including the transmission and reception of raw data bits over a communication medium (like cables, fiber optics, etc.).

- **Key Components**: Cables, switches, hubs, repeaters, electrical signals, and binary data (bits).
- **Protocols/Standards**: Ethernet, USB, Bluetooth, RS-232.

2. Data Link Layer (Layer 2)

- **Function**: Provides node-to-node data transfer, error detection, and correction, ensuring that data sent from the physical layer is free of errors.
- **Sub-layers**:
  - **MAC (Media Access Control)**: Controls how devices on the network gain access to the data and permission to transmit it.
  - **LLC (Logical Link Control)**: Manages frame synchronization, flow control, and error checking.
- **Key Components**: Network interface cards (NIC), switches, bridges.
- **Protocols**: Ethernet, PPP (Point-to-Point Protocol), HDLC.

3. Network Layer (Layer 3)

- **Function**: Handles packet forwarding, including routing through different routers. It ensures that data reaches its destination, even if multiple networks are involved.
- **Key Components**: Routers, Layer 3 switches.
- **Protocols**: IP (Internet Protocol), ICMP (Internet Control Message Protocol), IPsec.

4. Transport Layer (Layer 4)

- **Function**: Ensures reliable data transmission between devices, handling flow control, error detection and correction, and re-transmissions. It can offer both connection-oriented (TCP) and connectionless (UDP) services.
- **Key Components**: Gateways, firewalls (in some cases).
- **Protocols**: TCP (Transmission Control Protocol), UDP (User Datagram Protocol).

5. Session Layer (Layer 5)

- **Function**: Manages sessions or connections between applications. It establishes, manages, and terminates connections, ensuring that data streams are properly synchronized.

- **Protocols**: PPTP (Point-to-Point Tunneling Protocol), RPC (Remote Procedure Call), SMB (Server Message Block).

6. Presentation Layer (Layer 6)

- **Function**: Translates data between the application layer and the network. It handles data encryption, decryption, compression, and conversion (e.g., from ASCII to binary).
- **Key Components**: Codecs, encryption devices.
- **Protocols**: SSL (Secure Sockets Layer), TLS (Transport Layer Security), JPEG, ASCII, MPEG.

7. Application Layer (Layer 7)

- **Function**: Provides network services directly to end-user applications. It enables software applications to communicate over the network and provides an interface for users.
- **Key Components**: Web browsers, email clients.
- **Protocols**: HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), DNS (Domain Name System).

Q.2) NETWORK TOPOLOGIES

⇒

The way of connecting the computers is called Topology

The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as Network Topology .

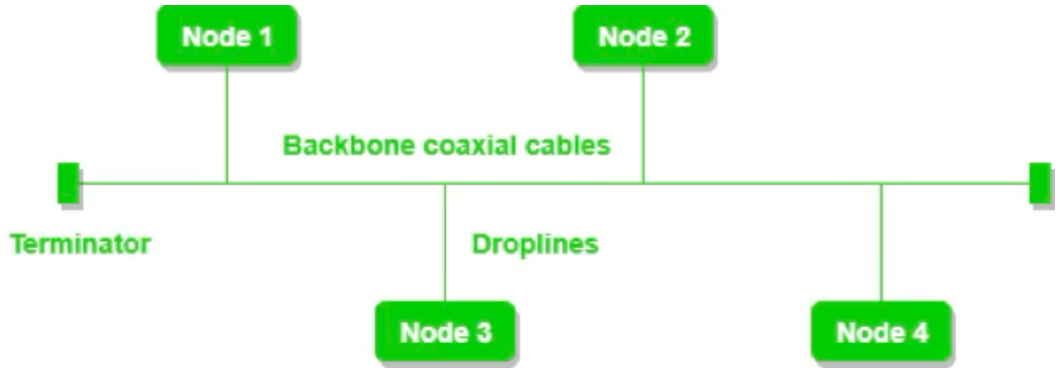
Network topology refers to the arrangement of different elements like nodes, links, or devices in a computer network.

It defines how these components are connected and interact with each other. Understanding various types of network topologies helps in designing efficient and robust networks.

Common types include bus, star, ring, mesh, logical, hybrid and tree topologies, each with its own advantages and disadvantages.

1. Bus Topology

- **Structure**: All devices are connected to a single central cable (known as the bus or backbone). Data sent by any device is broadcast to all devices in the network, but only the intended recipient accepts and processes the data.



- **Advantages**:
  - Simple to install and requires less cable than other topologies.
  - Cost-effective for small networks.
- **Disadvantages**:
  - Difficult to troubleshoot and expand.
  - Performance decreases as more devices are added.
  - A failure in the central cable can bring down the entire network.
- **Use Cases**: Small networks, typically used in legacy systems or in simple setups like small LANs.

2. Ring Topology

- **Structure**: Devices are connected in a circular loop. Each device has exactly two neighbors for communication, and data travels in one direction (or sometimes both in dual-ring setups).

- **Advantages**:
  - Easy to install and manage.
  - Good for networks where data travels in predictable patterns.
- **Disadvantages**:
  - A failure in one device or cable can disrupt the entire network.
  - Troubleshooting can be difficult, as the entire ring might need to be examined to find the fault.
- **Use Cases**: Historically used in token-ring networks, though it's now less common in modern systems.

3. Star Topology

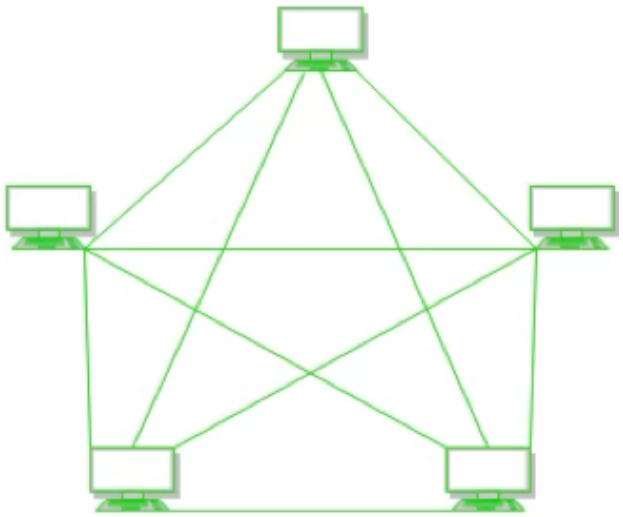
- **Structure**: All devices are connected to a central hub or switch. Data from any device passes through the central hub before being forwarded to the destination device.

Star topology

- **Advantages**:
  - Easy to install and manage.
  - If one device or connection fails, the rest of the network remains unaffected.
  - Centralized management via the hub/switch.
- **Disadvantages**:
  - If the central hub fails, the entire network goes down.
  - Requires more cabling than bus or ring topologies.
- **Use Cases**: Widely used in modern LAN setups, home networks, and office networks.

4. Mesh Topology

- **Structure**: Every device is connected to every other device in the network, either fully or partially.
  - **Full Mesh**: Every node is connected to every other node.
  - **Partial Mesh**: Some nodes are connected to multiple nodes, but not all.

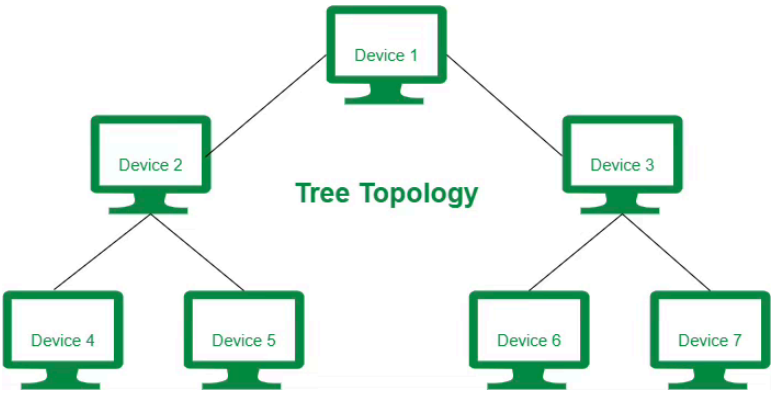


- **Advantages**:
  - High redundancy and reliability. If one link fails, data can take another path.
  - Excellent fault tolerance.

- **Disadvantages**:
  - Expensive due to the amount of cabling required.
  - Complex to install and manage.
- **Use Cases**: Used in mission-critical networks, WANs, and large-scale wireless networks where reliability is paramount.

5. Tree Topology

- **Structure**: A combination of bus and star topologies. It has a root node, and all other nodes are connected to it in a hierarchical manner, forming a tree-like structure.



- **Advantages**:
  - Allows for easy expansion of the network.
  - Hierarchical management is possible, suitable for large networks.
- **Disadvantages**:
  - If the backbone (trunk) fails, large portions of the network can go down.
  - More complex and expensive to install than star or bus topologies.
- **Use Cases**: Used in large organizational networks that need to be segmented into different branches or departments.

6. Logical Topology

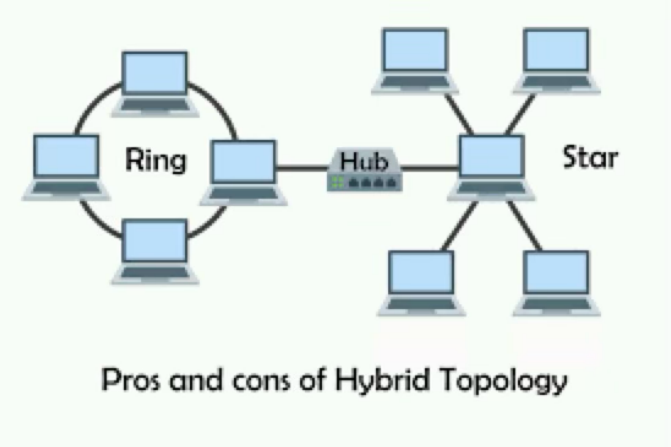
- **Definition**: Describes the way data travels through a network rather than the physical layout. It can differ from the physical topology.
- **Examples**:

- **Logical Bus**: Data flows along a single path, even if the network's physical layout is different (e.g., a physical star may operate logically as a bus).
- **Logical Ring**: Data flows in a circular pattern, regardless of the physical topology.

- **Use Cases**: Used to understand how data is transmitted in complex networks like virtual networks, VPNs, and wireless systems.

7. Hybrid Topology

- **Structure**: A combination of two or more different topologies, such as a mix of star, bus, mesh, etc. The combination aims to leverage the advantages of each topology while minimizing their drawbacks.

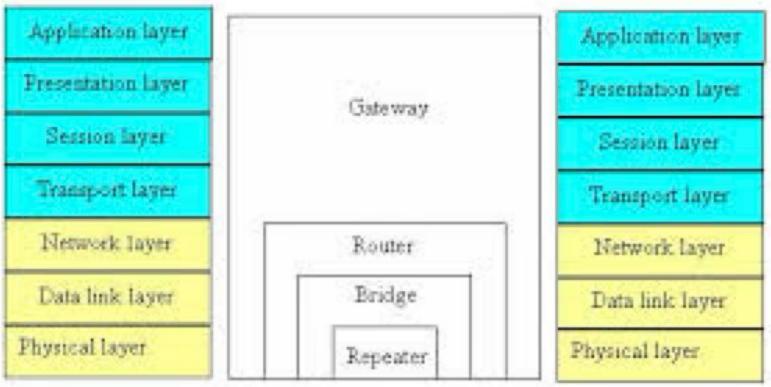


- **Advantages**:
  - Flexible and scalable, as it allows you to tailor the topology to specific needs.
  - Improved fault tolerance by combining redundancy methods from different topologies.
- **Disadvantages**:
  - Complex design and implementation.
  - More expensive due to varied technologies used.
- **Use Cases**: Large enterprises, WANs, or networks with specific needs like combining a star topology in one section with a mesh in another for redundancy.

Each topology serves different purposes, and the choice depends on factors such as the size of the network, budget, reliability, and future scalability.

Q.3) WRITE A NOTE ON INTERCONNECTING / NETWORKING DEVICES

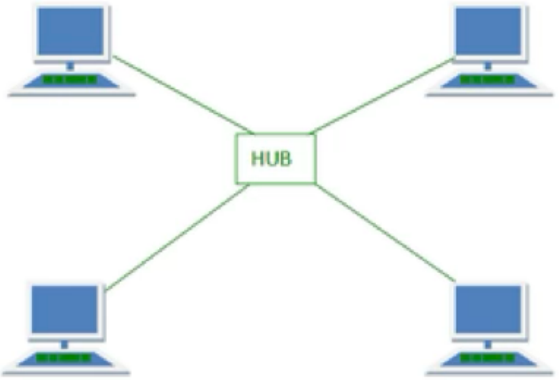
⇒



Interconnecting devices are hardware components that allow multiple computers, servers, or network devices to communicate with each other within a network. They play a crucial role in directing data traffic, ensuring proper communication, and maintaining the integrity and performance of the network. Below are the most common interconnecting devices used in networking:

1. Hub

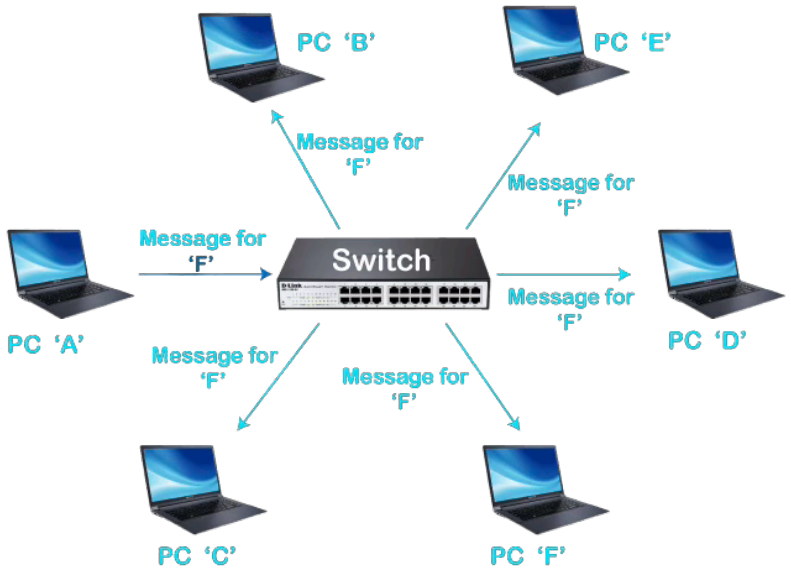
- **Function**: A basic device that connects multiple devices in a network. It works at the **Physical Layer (Layer 1)** of the OSI model and transmits data to all connected devices.
- **Operation**: When a device sends data to the hub, the hub duplicates the data and sends it to all other connected devices, regardless of the intended recipient.



- **Advantages**:
  - Simple and inexpensive.
  - Useful for small networks.
- **Disadvantages**:
  - Inefficient, as it sends data to all devices, which leads to network congestion.
  - No filtering or intelligent data handling.
- **Use Cases**: Small and basic network setups, though it is largely obsolete due to its inefficiency.

2. Switch

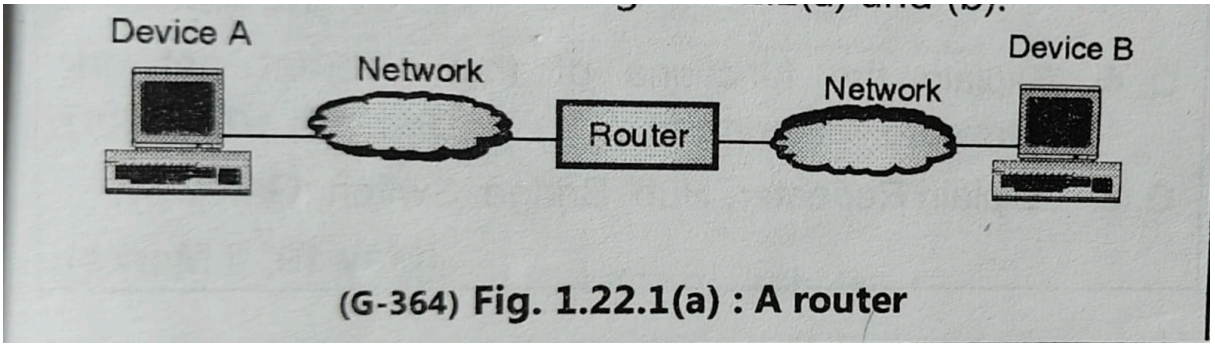
- **Function**: Operates at the **Data Link Layer (Layer 2)** and connects devices within a local area network (LAN). Unlike hubs, switches use MAC addresses to forward data only to the intended recipient.
- **Operation**: When a device sends data, the switch reads the MAC address of the recipient and sends the data only to the appropriate port where the recipient is connected.



- **Advantages**:
  - Reduces unnecessary data transmission and network congestion.
  - More efficient than hubs.
  - Supports VLANs (Virtual Local Area Networks) for segmenting the network.
- **Disadvantages**:
  - More expensive than hubs.
- **Use Cases**: Widely used in home and office LANs for efficient device interconnection.

3. Router

- **Function**: Operates at the **Network Layer (Layer 3)** and is responsible for forwarding data packets between different networks, typically connecting a local network to the internet or other networks.
- **Operation**: A router examines the destination IP address in a packet and determines the best path to route the packet toward its destination, often across multiple networks.

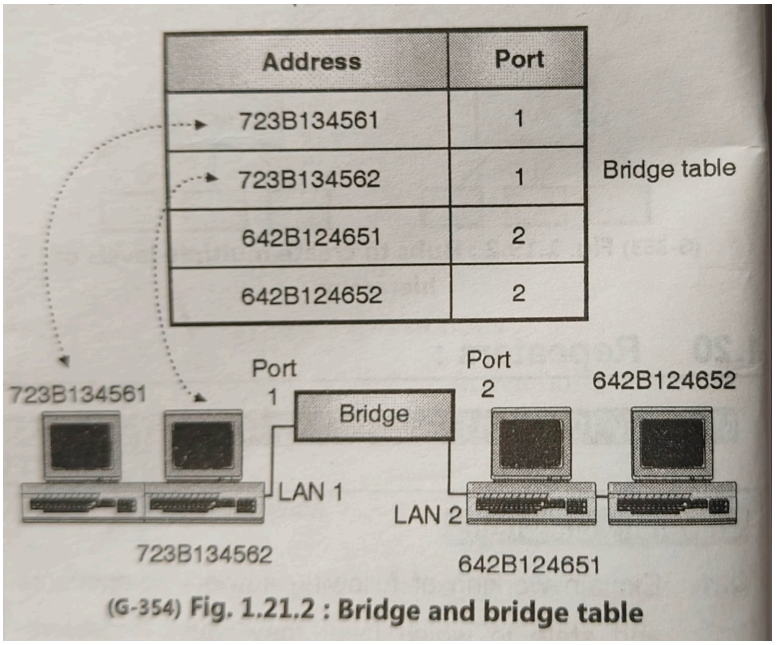


(G-364) **Fig. 1.22.1(a) : A router**

- **Advantages**:
  - Provides network segmentation and connects different networks (LAN to LAN, LAN to WAN).
  - Can assign IP addresses using DHCP.
  - Can implement security policies and firewall features.
- **Disadvantages**:
  - More expensive and complex than switches.
- **Use Cases**: Connecting home or office networks to the internet, WAN setups, or networks requiring segmentation.

4. Bridge

- **Function**: Operates at the **Data Link Layer (Layer 2)** and is used to connect two separate LAN segments to form a single network.
- **Operation**: A bridge analyzes the MAC addresses of incoming traffic to determine whether the data should be forwarded to another network segment.

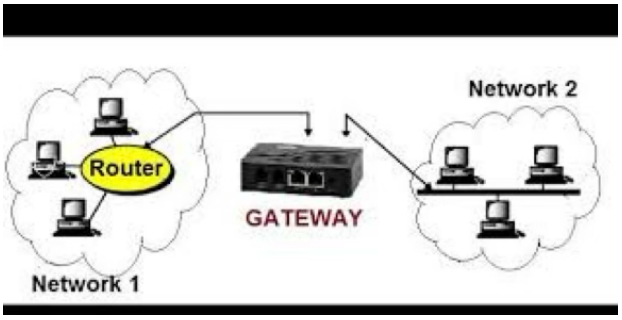


(G-354) Fig. 1.21.2 : Bridge and bridge table

- **Advantages**:
  - Reduces network traffic by filtering and forwarding data based on MAC addresses.
  - Connects different network types (e.g., wireless and wired).
- **Disadvantages**:
  - Can become a bottleneck in large networks.
- **Use Cases**: Connecting different segments of a LAN or integrating wireless and wired networks.

5. Gateway

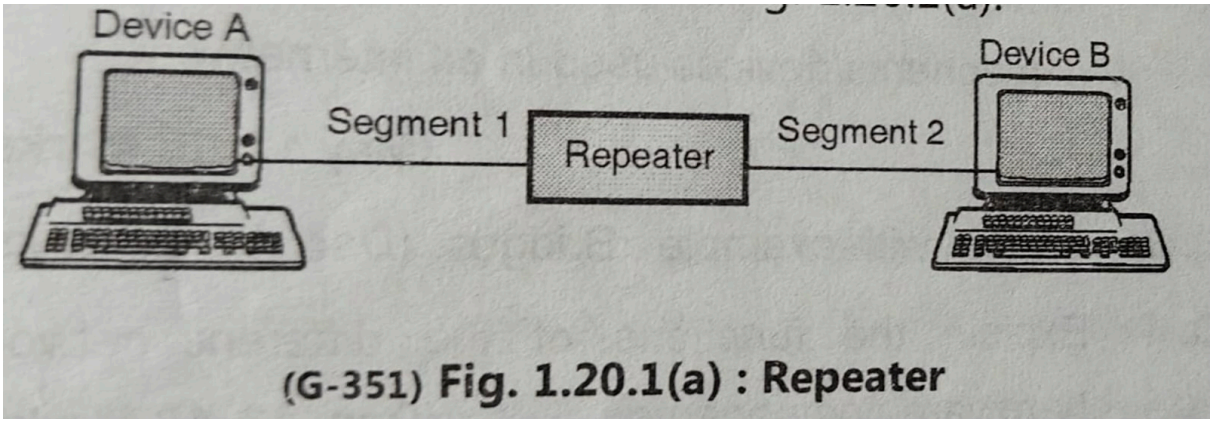
- **Function**: Operates at multiple layers of the OSI model (often starting at Layer 4 and higher) and serves as a **translator** between different networks that use different protocols. It can connect dissimilar networks, such as LANs and the internet, or different network architectures.
- **Operation**: A gateway can perform protocol conversion, data format translation, or network address translation (NAT), allowing devices on different networks to communicate.



- **Advantages**:
  - Enables communication between networks using different protocols.
  - Can incorporate security functions like firewalls.
- **Disadvantages**:
  - More complex and often more expensive.
- **Use Cases**: Internet gateways, VoIP (Voice over IP) gateways, and other protocol conversions.

6. Repeater

- **Function**: A device that amplifies or regenerates signals to extend the distance over which data can travel in a network. It operates at the **Physical Layer (Layer 1)**.
- **Operation**: A repeater receives a weak signal, amplifies it, and retransmits it, ensuring the data can travel over longer distances without degradation.

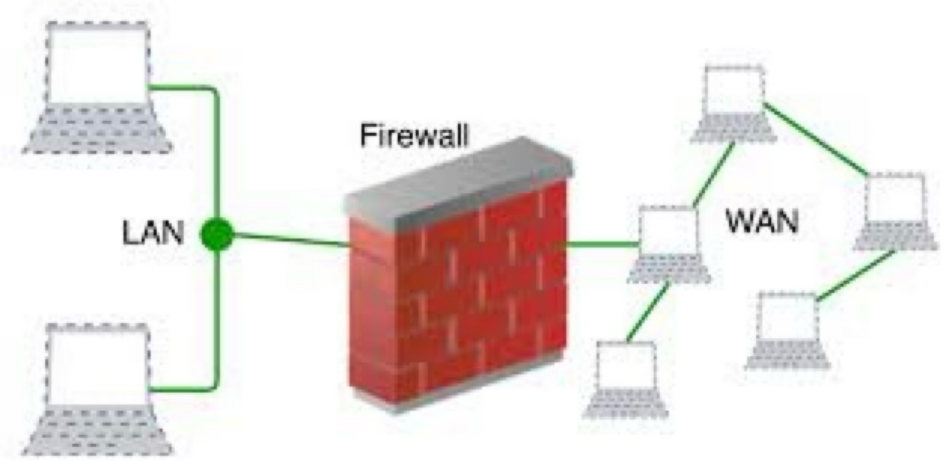


- **Advantages**:
  - Extends the range of a network.
  - Simple to install and operate.

- **Disadvantages**:
  - Only regenerates signals; does not filter or manage traffic.
- **Use Cases**: Used in long-distance networking or to extend wireless network coverage.

7. Firewall

- **Function**: A security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It operates at multiple layers of the OSI model (typically starting at Layer 3).
- **Operation**: Firewalls examine the data packets and either allow or block them based on defined security rules, protecting the network from unauthorized access or cyber-attacks.



- **Advantages**:
  - Provides critical security by filtering network traffic.
  - Can be customized to protect different parts of the network.
- **Disadvantages**:
  - May introduce latency due to packet filtering.
- **Use Cases**: Used in both small and large networks to prevent unauthorized access and secure sensitive information.

DIFFERENCE BETWEEN THESE ALL

University Questions

Q. 1 Differentiate between Hub and Switch.

(Dec. 09, Dec. 10, 6 Marks)

Sr. No.	Para-meter	Hub	Bridge	Switch	Router	Gate-ways
1.	Layer in OSI model	Physical	Physical and datalink	Datalink	Network	Seven layers
2.	Operation	Organises the cables and relays signals to other media segments	Regeneration, checks MAC address	Switch is a multiport bridge to connect devices or segments in a LAN	Connects two or more networks	Provides translation services between in-compatible networks
3.	Types	Passive, Active and Intelligent	Transparent and Routing	Two layer and Three layer	Distance vector and Link state	–
4.	Cost	Low cost	Very expensive	Expensive	Low cost	Costly

Q.4) DIFFERENCE BETWEEN CONNECTIONLESS VS CONNECTION ORIENTED SERVICE

⇒

Feature	Connectionless Service	Connection-Oriented Service
Establishment of Connection	No prior connection setup is required between sender and receiver.	Requires a connection to be established before data transfer.
Protocol Examples	UDP (User Datagram Protocol), IP (Internet Protocol)	TCP (Transmission Control Protocol), ATM (Asynchronous Transfer Mode)
Reliability	Less reliable, as there's no guarantee of data delivery or order.	Highly reliable; ensures data is delivered in the correct order.
Acknowledgment	No acknowledgment of received data packets.	Acknowledgment of data receipt is provided by the receiver.
Overhead	Lower overhead, as no connection setup or termination is needed.	Higher overhead due to connection setup, maintenance, and teardown.
Data Integrity	No inherent error checking or correction.	Error checking and correction are included.
Transmission Mode	Packets are sent independently and can take different routes.	Data is sent in a sequenced, organized manner, often as a continuous stream.
Suitable for	Applications that need fast, lightweight communication (e.g., streaming, gaming).	Applications requiring reliable data delivery (e.g., file transfer, email).
Speed	Faster, as there's no need for connection setup or teardown.	Slower due to the additional connection management steps.
Flow Control	No flow control mechanism; packets may be dropped in case of congestion.	Flow control is used to prevent overwhelming the receiver.
Congestion Control	No built-in congestion control.	Congestion control mechanisms ensure efficient data flow.
Order of Packets	Packets may arrive out of order.	Ensures that packets arrive in the correct order.
Use Cases	Real-time applications (e.g., VoIP, live video streams).	Applications requiring reliable data transmission (e.g., web browsing, file downloads).

Q.5) DESIGN ISSUES IN OSI MODEL

➔

The **OSI (Open Systems Interconnection) model** provides a layered framework for network communication, which standardizes how different networking protocols and devices interact. However, each layer of the OSI model has its own **design issues** that need to be addressed for efficient and reliable

communication. Here's an overview of the primary design issues at each layer of the OSI model:

1. Physical Layer (Layer 1)

- **Design Issues**:
  - **Signal Encoding**: How to convert data into electrical, optical, or radio signals for transmission.
  - **Data Rate Control**: Ensuring that the rate of data transmission is suitable for both the sender and the receiver.
  - **Physical Medium**: Choosing the appropriate transmission medium (e.g., cables, fiber optics, radio waves) based on factors like distance, bandwidth, and cost.
  - **Bit Synchronization**: Ensuring that sender and receiver are synchronized to avoid data corruption.
  - **Topology**: Determining the physical layout of the network (e.g., bus, star, ring).
  - **Transmission Mode**: Choosing between simplex, half-duplex, or full-duplex transmission modes.
  - **Noise and Interference**: Managing external factors that can distort signals, such as electromagnetic interference.

2. Data Link Layer (Layer 2)

- **Design Issues**:
  - **Framing**: How to divide the data into manageable units (frames) with proper synchronization.
  - **Error Detection and Correction**: Mechanisms to detect and correct errors that occur during data transmission, such as parity checks and CRC (Cyclic Redundancy Check).
  - **Flow Control**: Preventing the sender from overwhelming the receiver with too much data at once (e.g., using protocols like Stop-and-Wait or Sliding Window).
  - **Addressing**: Assigning physical (MAC) addresses to ensure data reaches the correct device on the local network.

- **Access Control**: Managing how multiple devices share the same communication medium without collisions (e.g., using protocols like CSMA/CD in Ethernet).
- **Link Establishment and Termination**: Ensuring that the link is established before data transfer and properly terminated afterward.

3. Network Layer (Layer 3)

- **Design Issues**:
  - **Routing**: Determining the best path for data to travel across multiple networks, considering factors like shortest path, cost, and congestion.
  - **Logical Addressing**: Assigning unique IP addresses to devices to identify them across different networks.
  - **Packet Forwarding**: Moving packets from one network to another, ensuring they reach their destination.
  - **Congestion Control**: Managing traffic to avoid overloading the network, which can cause packet loss or delays.
  - **Fragmentation and Reassembly**: Dividing large packets into smaller ones to match the data link layer's frame size and reassembling them at the destination.
  - **Error Handling**: Handling routing errors such as unreachable destinations or network failures.

4. Transport Layer (Layer 4)

- **Design Issues**:
  - **Reliable Data Transfer**: Ensuring that data is delivered without errors, in the correct sequence, and without duplication (e.g., using protocols like TCP).
  - **Flow Control**: Managing the amount of data sent to ensure that the sender does not overwhelm the receiver's buffer.
  - **Error Detection and Correction**: Detecting errors in the segments of data and taking steps to correct them.
  - **Segmentation and Reassembly**: Dividing large messages into smaller segments for transmission and reassembling them at the receiver's end.

- **Multiplexing**: Allowing multiple applications to use the same network connection by assigning port numbers.
- **Connection Management**: Establishing, maintaining, and terminating connections (e.g., connection-oriented services like TCP).

5. Session Layer (Layer 5)

- **Design Issues**:
  - **Session Establishment and Termination**: Ensuring that communication sessions are properly established and gracefully terminated between applications.
  - **Synchronization**: Implementing checkpoints during long data transfers so that in case of a failure, communication can resume from the last checkpoint.
  - **Dialog Control**: Managing whether communication between applications is full-duplex (both parties can send simultaneously) or half-duplex (taking turns).
  - **Session Recovery**: Handling disruptions in the session and ensuring that communication can be resumed.

6. Presentation Layer (Layer 6)

- **Design Issues**:
  - **Data Translation**: Converting data between the formats used by the application layer and the format needed for transmission (e.g., encoding data from ASCII to binary).
  - **Data Compression**: Reducing the size of data to optimize bandwidth usage and improve transmission speed.
  - **Encryption/Decryption**: Implementing data encryption to ensure confidentiality and data integrity, and decrypting it at the destination.
  - **Character Encoding**: Handling different character sets (e.g., UTF-8, ASCII) and ensuring proper data representation.

7. Application Layer (Layer 7)

- **Design Issues**:
  - **Application Services**: Providing network-related services like email, file transfers, and remote login, ensuring they are designed to meet user

requirements.

- **User Interface**: Designing user-friendly interfaces for applications to interact with the network.
- **Resource Sharing**: Managing access to resources like files, databases, and printers over the network.
- **Security**: Implementing authentication, authorization, and encryption to ensure secure data communication at the application level.
- **Protocol Design**: Defining standard protocols for communication between different applications, such as HTTP, FTP, SMTP, and DNS.

Q.6) DIFFERENCE BETWEEN LAN, MAN & WAN

Feature	LAN (Local Area Network)	MAN (Metropolitan Area Network)	WAN (Wide Area Network)
Geographical Area	Covers a small geographical area like a room, building, or campus.	Covers a larger area, typically a city or town.	Covers a large geographical area, often across cities, countries, or continents.
Size	Smallest network in terms of area covered (usually up to a few kilometers).	Intermediate in size, usually covering several kilometers to tens of kilometers.	Largest network, spanning hundreds or thousands of kilometers.
Ownership	Typically owned and managed by a single organization (e.g., home, school, or office).	May be owned by a single organization or shared by several entities (e.g., government, ISPs).	Often owned by telecom companies or ISPs; users lease or subscribe to access services.
Data Transfer Speed	High-speed (commonly up to 1 Gbps or more).	Moderate speed (typically less than LAN but higher than WAN, ranging from 100 Mbps to several Gbps).	Lower speed compared to LAN and MAN (can range from 56 Kbps to several hundred Mbps, depending on technology used).
Cost	Low setup and maintenance costs.	Moderate cost, depending on the distance covered and the infrastructure used.	High cost due to long-distance infrastructure, such as leased lines, satellite links, etc.
Propagation Delay	Very low propagation delay due to short distances.	Moderate propagation delay.	High propagation delay due to the large distances data must travel.
Technology Used	Ethernet, Wi-Fi, Token Ring.	Fiber optics, wireless (microwave links), or leased lines.	MPLS, Frame Relay, ATM, satellite, leased lines, and internet backbone technologies.
Bandwidth	Higher bandwidth, offering fast data transmission rates.	Lower bandwidth than LAN, but higher than WAN.	Typically lower bandwidth due to the longer distances and infrastructure used.
Congestion	Less congestion since fewer devices are connected within a limited space.	Moderate congestion depending on the number of users and data traffic.	More congestion due to the large number of users and data traveling over vast distances.
Reliability	Very reliable due to smaller size and controlled environment.	Moderately reliable, though affected by larger distances and external factors.	Less reliable due to the large distances and multiple network providers involved.
Examples	Office network, home Wi-Fi, school network.	Network across a city, such as connecting multiple branches of a university or a large business.	The internet, international corporate networks, global business networks.
Use Cases	Used for connecting computers and devices within homes, offices, and small organizations.	Used for connecting networks within a city, such as connecting government offices or regional company branches.	Used for connecting networks across cities, countries, or continents, often for multinational businesses.