

**Experiment No. 1**

| **TITLE:**  Study of Networking devices (Hub, router, Gateway, Switch etc.) and Transmission Media |
| --- |

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**AIM:** To study different Networking devices and transmission media used in day to day networks.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Expected Outcome of Experiment:**

**CO:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Books/ Journals/ Websites referred:**

1. A. S. Tanenbaum, “Computer Networks”, Pearson Education, Fourth Edition
2. B. A. Forouzan, “Data Communications and Networking”, TMH, Fourth Edition

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Pre Lab/ Prior Concepts:** Basics of LAN and Connecting devices

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**New Concepts to be learned:** Layer wise connecting devices

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Stepwise-Procedure:**

.

**Study of Connecting Devices**

Networking Devices in CN:

1. Hubs:  
   A hub is a basic networking device that connects multiple computers in a local area network (LAN). It operates at the physical layer of the OSI model, meaning it doesn't perform any filtering or data processing. When data arrives at one of its ports, the hub simply broadcasts it to all other ports, regardless of the destination. This can lead to network inefficiencies and collisions, as all devices share the same bandwidth. Hubs are largely obsolete today, having been replaced by more intelligent devices like switches.

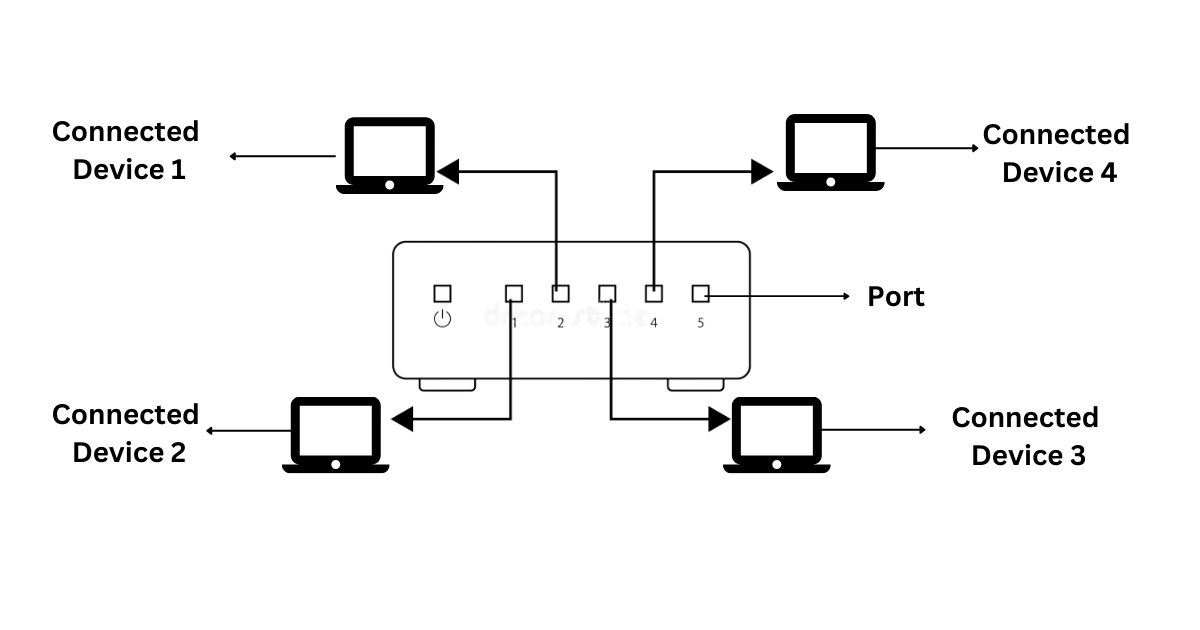
Types of Hub :

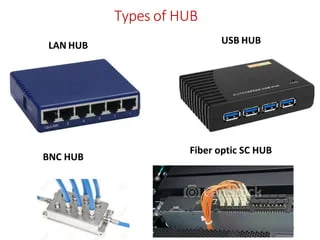
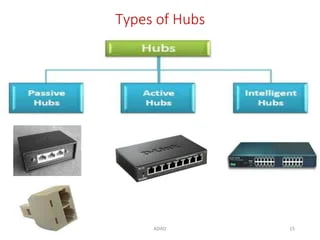
* Active Hub
* Passive Hub
* Intelligent Hub

One significant drawback of hubs is their lack of intelligence in data handling. They do not filter traffic or manage any form of data routing. This leads to a high probability of data collisions, particularly in larger networks where multiple devices may try to communicate simultaneously. As a result, network performance can degrade due to the increased number of collision domains, which necessitate retransmissions of data packets.

In terms of network topology, hubs are often used in star topologies where each device is connected to a central hub. While this setup can simplify network management and troubleshooting, it also means that the hub becomes a single point of failure. If the hub fails, all connected devices lose network connectivity.

Despite their simplicity and cost-effectiveness, hubs have largely been replaced by more sophisticated devices like switches and routers in modern networks. These advanced devices provide better traffic management, reduced collisions, and improved overall network performance. However, hubs are still occasionally used in specific scenarios where their limitations are not a significant concern, such as small home networks or simple office setups.



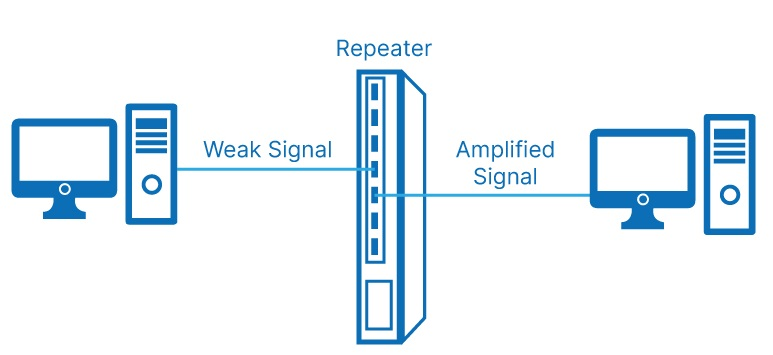
1. Repeaters  
   A repeater is a device used in networking to extend the reach of a network by amplifying and regenerating signals. It operates at the physical layer of the OSI model. When a signal travels over a long distance, it can weaken and degrade. A repeater takes the weak signal, amplifies it, and retransmits it at its original strength. This makes repeaters essential for maintaining the quality of signal transmission over long distances, especially in wired networks.It is a 2-port device.

When data is transmitted over a network, the signal gradually degrades due to attenuation, which is the loss of signal strength as it travels through a medium. This degradation can lead to errors in data transmission, making it difficult or impossible for the receiving device to correctly interpret the signal. A repeater addresses this issue by capturing the weakened signal before it becomes too degraded, regenerating it to its original strength and quality, and then sending the restored signal onward.

Repeaters do not analyze the data they retransmit; they simply amplify the electrical signal. This simplicity allows them to function with minimal latency, making them suitable for real-time applications that require consistent signal strength over long distances.

Types of Repeaters

* Ethernet Repeaters: Used in wired networks to extend the length of Ethernet cables beyond the standard maximum (typically 100 meters for Cat5e/Cat6 cables). Ethernet repeaters regenerate the signal, allowing network segments to be connected over greater distances.
* Optical Repeaters: Utilized in fiber optic networks, optical repeaters amplify the light signals used for high-speed data transmission. These repeaters are essential for long-distance fiber optic communication, such as transcontinental data links.
* Wireless Repeaters: Also known as range extenders, these devices receive wireless signals from a Wi-Fi router or access point and retransmit them to cover areas with weak or no signal. Wireless repeaters are commonly used in homes and offices to improve Wi-Fi coverage and eliminate dead zones.
* Satellite Repeaters: Used in satellite communication, these repeaters receive signals from one location on Earth, amplify them, and then transmit them to another location via satellite. They are critical for global communication networks, including television broadcasts and internet services.



1. NIC  
   A Network Interface Card (NIC) is a hardware component that enables a computer or other device to connect to a network. It operates at both the physical and data link layers of the OSI model. Each NIC has a unique MAC address, which it uses to communicate over the network. NICs can be used in both wired and wireless networks, providing the necessary interface for devices to transmit and receive data. Without a NIC, a device would be unable to participate in network communications.

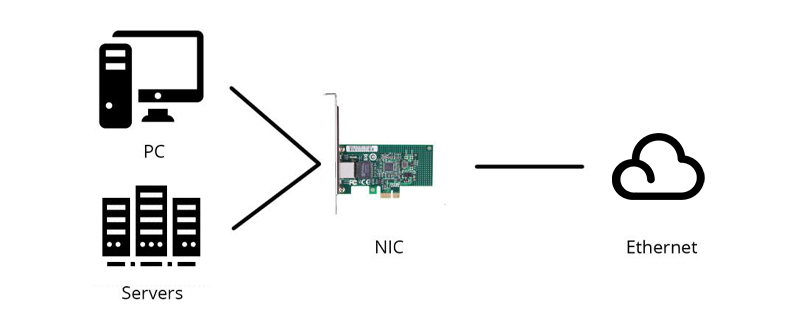
NIC key components:

* Controller: The main processor of the NIC, responsible for managing data transmission and reception. It processes network protocols, handles data buffering, and manages data flow between the computer's system bus and the network.
* Transceiver: This component handles the physical signaling to and from the network medium. In wired NICs, it is responsible for converting digital data to electrical signals and vice versa. In wireless NICs, the transceiver converts digital data to radio signals and vice versa.
* MAC Address: Each NIC has a unique Media Access Control (MAC) address, a 48-bit identifier assigned by the manufacturer. The MAC address is used to identify the device on the network and ensure proper delivery of data packets.
* Interface: The physical connection point between the NIC and the network medium. For wired NICs, this is usually an Ethernet port (RJ-45). For wireless NICs, it includes an antenna and radio interface for Wi-Fi connectivity.
* Memory: NICs often include onboard memory for buffering incoming and outgoing data packets, ensuring smooth data transmission even when the host system is busy.

Types of NICs

* Ethernet NICs: The most common type, used for wired network connections. They support various Ethernet standards, such as Fast Ethernet (100 Mbps), Gigabit Ethernet (1 Gbps), and 10 Gigabit Ethernet (10 Gbps).
* Wireless NICs: These provide Wi-Fi connectivity, supporting various wireless standards like 802.11a/b/g/n/ac/ax. Wireless NICs are commonly found in laptops, tablets, and smartphones, allowing devices to connect to wireless networks.
* Fiber NICs: Used for high-speed network connections over optical fiber. They are common in data centers and enterprise environments where high bandwidth and long-distance connectivity are required.
* Virtual NICs: Software-based NICs used in virtualized environments. They enable virtual machines to connect to virtual or physical networks, simulating the functions of a physical NIC.

NICs play a crucial role in network performance and reliability. They handle the critical task of framing and addressing data packets, ensuring that data is correctly formatted for transmission and accurately delivered to the intended recipient. High-quality NICs can enhance network throughput, reduce latency, and support advanced features like offloading CPU tasks related to network processing, improving overall system performance.



1. Switch  
   A switch is an advanced networking device that connects multiple devices within a network and uses MAC addresses to forward data to the correct destination. Operating primarily at the data link layer, switches are more efficient than hubs because they only send data to the specific device it is intended for, rather than broadcasting it to all ports. This reduces collisions and improves bandwidth usage. Some switches also operate at the network layer, providing additional routing functions. Switches are a staple in modern local area networks (LANs) due to their ability to manage data traffic efficiently.  
     
   Types of Switch:

* Unmanaged switches
* Managed switches
* Smart switches
* Layer 2 switches
* Layer 3 switches
* PoE switches
* Gigabit switches
* Rack-mounted switches
* Desktop switches
* Modular switches

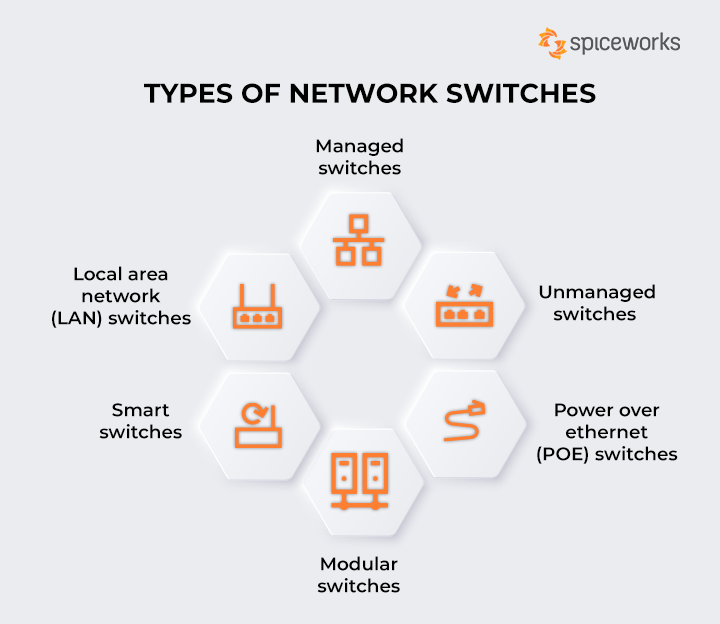
Switches maintain a MAC address table, also known as a CAM (Content Addressable Memory) table, which maps each device's MAC address to the corresponding switch port. When a data packet arrives at a switch, it examines the packet's destination MAC address and looks it up in the MAC address table. If the address is found, the switch forwards the packet only to the port associated with that address. If the address is not found, the switch broadcasts the packet to all ports, similar to a hub, but this occurs only until the address is learned and added to the table.

One of the key advantages of switches is their ability to create separate collision domains for each connected device, thereby minimizing the likelihood of data collisions. This feature, along with full-duplex communication capabilities, allows switches to handle a higher volume of network traffic more efficiently than hubs. Additionally, switches support VLAN (Virtual LAN) configurations, which enable network segmentation and improved security by isolating specific groups of devices within the same physical switch.

Advanced switches, often referred to as managed switches, provide additional functionalities such as Quality of Service (QoS) settings, link aggregation, and network monitoring. These features are essential for optimizing network performance, prioritizing critical data traffic, and ensuring reliable connectivity in complex network environments.

In summary, switches are integral to modern networking due to their efficiency in managing data traffic, reducing collisions, and supporting advanced network features. They have largely replaced hubs in both small and large network deployments, offering superior performance and scalability.





1. Bridge  
   A bridge is a device that connects and filters traffic between two or more network segments, operating at the data link layer of the OSI model. Unlike a hub, a bridge can inspect incoming data packets and decide whether to forward or discard them based on their MAC addresses. This reduces the amount of traffic on each segment and helps manage data flow more efficiently. Bridges can also be used to divide a large network into smaller, more manageable sections, enhancing overall network performance.

Types of Bridges :

* Transparent Bridges
* Source Routing Bridges

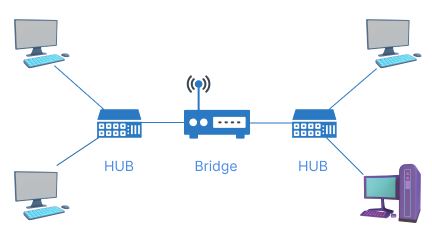
The primary function of a bridge is to connect two or more network segments, allowing data to pass between them while maintaining separation to reduce traffic load. When a bridge receives a data packet, it examines the packet's destination MAC address and determines whether the destination device resides on the same segment as the source. If it does, the bridge discards the packet to prevent unnecessary traffic. If the destination is on a different segment, the bridge forwards the packet to that segment.

Bridges maintain a MAC address table that maps device addresses to specific network segments. This table is built dynamically as the bridge learns the addresses of devices on the network by monitoring traffic. Over time, the bridge becomes more efficient in directing data to the appropriate segments, reducing broadcast traffic and collisions.

There are different types of bridges, including transparent bridges, source routing bridges, and translational bridges. Transparent bridges are the most common type, operating without requiring any configuration changes to the devices on the network. Source routing bridges, used primarily in Token Ring networks, rely on the source device to specify the path the data should take. Translational bridges connect networks using different protocols, such as Ethernet and Token Ring, facilitating communication between them.

Bridges have been largely superseded by switches in modern networks due to the latter's superior performance and additional features. However, bridges are still used in specific scenarios where their simplicity and cost-effectiveness are advantageous. They provide a basic level of traffic management and can be useful in smaller or less complex network environments.

In summary, bridges play a crucial role in segmenting networks, reducing traffic, and improving performance. While they have been largely replaced by more advanced devices like switches, bridges remain a valuable tool in certain networking contexts.

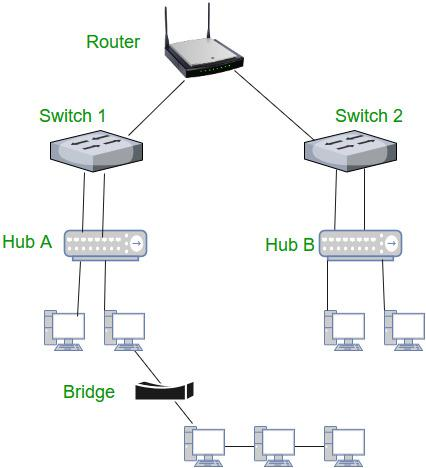


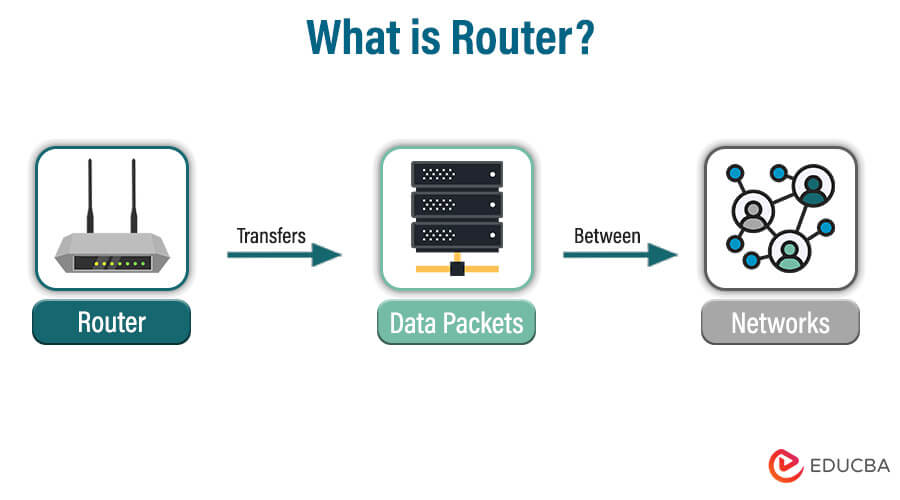
1. Router  
   A router is a critical device in networking that connects multiple networks and directs data packets between them. It operates at the network layer of the OSI model. Routers use IP addresses to determine the best path for forwarding data to its destination. They maintain routing tables to manage these paths and can connect different types of networks, including LANs, WANs, and the internet. Routers are essential for directing internet traffic, enabling communication between different network segments, and ensuring data reaches its intended destination efficiently.

Routers are essential for connecting disparate networks, such as linking a local area network (LAN) to a wide area network (WAN) or the internet. They play a pivotal role in both small and large-scale networks, facilitating communication between devices across various network segments. Routers also support advanced features such as Network Address Translation (NAT), which allows multiple devices on a private network to share a single public IP address, and Dynamic Host Configuration Protocol (DHCP), which automatically assigns IP addresses to devices on a network.

One of the key functions of a router is to maintain routing tables, which store information about network paths and their associated metrics. Routers use these tables to determine the most efficient route for data packets, considering factors such as hop count, bandwidth, and latency. Routing protocols, such as OSPF (Open Shortest Path First) and BGP (Border Gateway Protocol), enable routers to dynamically update their routing tables and adapt to changes in the network topology.

Routers can be categorized into different types based on their functionality and deployment context. Home routers, often combined with modems, provide internet connectivity and basic network management for residential users. Enterprise routers, used in business environments, offer enhanced performance, security features, and support for complex routing protocols. Core routers, deployed within the backbone of large networks, handle massive amounts of data traffic and





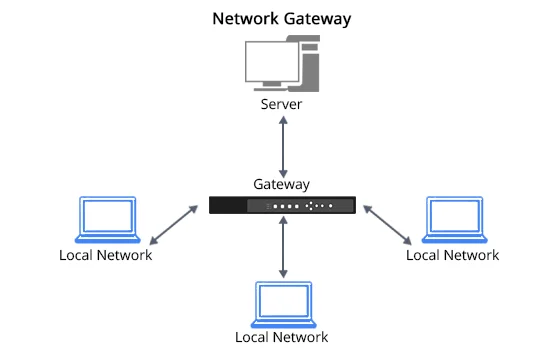
1. Gateway  
   A gateway is a network device that serves as a bridge between different networks, often using different protocols. It operates across multiple layers of the OSI model, typically up to the application layer. Gateways are essential for translating data from one protocol to another, allowing communication between disparate systems. For example, a gateway can connect a local network to the internet, translating internal network protocols to those used on the internet. Gateways are crucial for enabling interoperability and connectivity in complex, heterogeneous networks.

One of the primary roles of a gateway is protocol conversion. For instance, a gateway can translate data from one protocol, such as IPX/SPX used in legacy Novell networks, to another protocol, such as TCP/IP used in modern internet communications. This capability is essential for ensuring compatibility and seamless data exchange between different network systems.

Gateways are often implemented in complex network environments where multiple types of networks need to interconnect. For example, in an enterprise setting, a gateway might connect a corporate intranet to the internet, ensuring secure and controlled access to external resources. Similarly, gateways can connect different communication systems, such as linking VoIP (Voice over Internet Protocol) networks with traditional PSTN (Public Switched Telephone Network) systems.

In addition to protocol conversion, gateways often perform various other functions, including data compression, encryption, and traffic management. They can act as firewalls, providing security by filtering and blocking malicious traffic, and as proxy servers, enhancing privacy and performance by caching frequently accessed data and anonymizing user requests.

Gateways can be hardware devices, software applications, or a combination of both. Hardware gateways are standalone devices with dedicated processing capabilities, while software gateways are applications running on general-purpose servers. Some modern routers and firewalls also include gateway functionalities, offering an integrated solution for routing, security, and protocol conversion.

  
  
  
  
**Study of Transmission Media**

**1. Twisted pair cable**Twisted pair cables consist of insulated copper wire pairs twisted together, reducing electromagnetic interference (EMI) and crosstalk. They are commonly used in Ethernet and telephone systems, effective for short to medium distances. They are also used in video applications like security cameras.

Function:

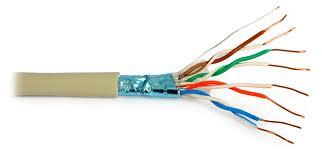
Transmits data via twisted pairs of insulated copper wires. The twisting reduces electromagnetic interference (EMI) and crosstalk by ensuring differential mode transmission, where equal and opposite signals enhance noise rejection.

Uses:

Common in Ethernet networks, telephone systems, and video applications like security cameras. Effective for short to medium distances and cost-effective.

Key Points:

* Differential Mode Transmission: Enhances noise rejection.
* Twisting: Reduces crosstalk and EMI.
* Cost-Effective: Suitable for budget-friendly applications.
* Varied Twist Rates: Helps prevent interference in multi-pair cables.



**2. Coaxial cable**Coaxial cables have a central conductor surrounded by insulation, a conductive shield, and an outer layer, minimizing signal loss and interference. They are used for cable TV, internet connections, and some business networks, providing reliable performance over longer distances compared to twisted pair cables.

Function:

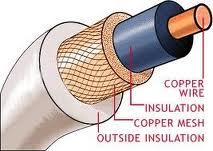
Transmits data through a central conductor encased in insulation, a conductive shield, and an outer insulating layer. This design reduces signal loss and external interference, maintaining signal integrity over longer distances.

Uses:

Used for cable TV, internet connections, and business networks. Suitable for long-distance transmission.

Key Points:

* Concentric Design: Minimizes signal loss and interference.
* Shielding: Protects against external noise.
* Long-Distance: Effective for transmitting over extended distances.
* Versatile Applications: Used in both residential and commercial setups.

****

**3. Optical Fiber**Optical fiber cables transmit data as light pulses through glass or plastic fibers, offering high bandwidth and low signal degradation over long distances. They are used in core telecommunications networks and high-speed internet, providing superior performance and capacity compared to copper cables.

Function:

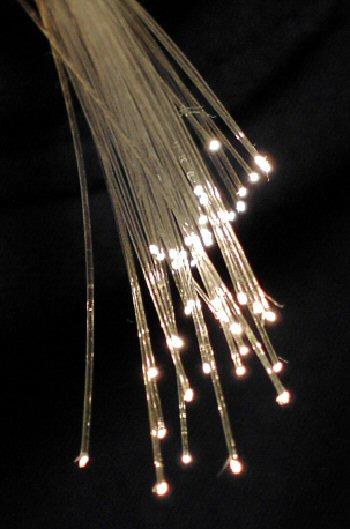
Transmits data as light pulses through glass or plastic fibers, offering high bandwidth and low signal degradation. Light pulses are modulated to carry data and converted back to electrical signals at the receiver.

Uses:

Ideal for core telecommunications networks and high-speed internet connections. Preferred for long-distance and high-capacity transmission.

Key Points:

* High Bandwidth: Supports large amounts of data.
* Low Signal Degradation: Minimal loss over long distances.
* Long-Distance Transmission: Effective for extensive network spans.
* Modern Technology: Replaces copper cables in high-capacity networks.



**Summary**

The features of the connecting devices and transmission media can be explained in brief as follows:

* Connecting Devices: Connecting devices are hardware components that facilitate the transfer of data between different devices or network segments. They include routers, switches, hubs, and network interface cards, each serving specific functions to manage and direct data traffic, ensure efficient communication, and connect various parts of a network.
* Transmission Media: Transmission media are the physical pathways used to transmit data from one point to another.They include twisted pair cable, coaxial cable, optical fibre. Each type of transmission media is chosen based on requirements like distance, bandwidth, and susceptibility to interference, with optical fiber generally preferred for high-performance and long-distance communications.

**CONCLUSION:**

Learned about Connecting devices an transmission media.

**Post Lab Questions**

1. Compare Hub, switch, bridge, and gateway and specify the use in different cases.
2. Which of the following device is used to connect two systems, especially if the systems use different protocols?

A. hub

B. bridge

C. gateway

D. repeater

E. None of the above

1. Frames from one LAN can be transmitted to another LAN via the device

A. Router

B. Bridge

C. Repeater

D. Modem

**ANSWERS:**

1.

* Hub:
* A hub is a basic networking device that connects multiple devices in a network, operating at the physical layer (Layer 1) of the OSI model. It broadcasts incoming data packets to all connected devices.
* Suitable for simple networks or small office environments where network traffic is minimal. It's rarely used in modern networks due to its inefficiency and inability to manage network traffic effectively.
* No intelligence or management capabilities; all devices share the same bandwidth, which can lead to network congestion and collisions.
* Switch:
* A switch operates at the data link layer (Layer 2) and sometimes at the network layer (Layer 3). It intelligently forwards data packets to specific devices based on their MAC addresses, reducing unnecessary traffic.
* Commonly used in local area networks (LANs) to efficiently manage and direct network traffic. It helps in creating smaller collision domains and improves overall network performance.
* While it improves efficiency over hubs, it doesn't connect different types of networks or handle routing between subnets.
* Bridge:
* A bridge operates at the data link layer (Layer 2) and is used to connect and filter traffic between two or more network segments, making them act as a single network. It helps in reducing traffic on each segment by only forwarding relevant data.
* Useful for segmenting large networks to reduce traffic and improve performance. It can also connect different network segments within the same protocol.
* Cannot handle routing between different network segments or address network layers beyond Layer 2.
* Gateway:
* A gateway operates at multiple layers of the OSI model and acts as a protocol converter between different network architectures or protocols. It enables communication between networks that use different protocols.
* Ideal for connecting disparate networks, such as connecting a network using TCP/IP with one using IPX/SPX, or interfacing between different types of networks (e.g., connecting a LAN to the Internet).
* Can be complex and require configuration to handle different protocols and network architectures.

2. C) Gateway

3. B) Bridge