Batch: A1	**Roll No.: 16010123012**
Experiment / assignment / tutorial No.: 01	
Grade: AA / AB / BB / BC / CC / CD /DD	
Signature of the Staff In-charge with date	

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

1. **Switch**

   The Switch is a network device that is used to segment the networks into different subnetworks called subnets or LAN segments. It is responsible for filtering and forwarding the packets between LAN segments based on MAC address. Switches have many ports, and when data arrives at any port, the destination address is examined first and some checks are also done and then it is processed to the devices. Different types of communication are supported here like unicast, multicast, and broadcast communication.

   Functionality –

   - It performs error checking before forwarding data
   - It transfers the data only to the device that has been addressed
   - Packet-switching techniques are used to transfer data packets from source to destination

   Specifications –

   Switches typically support Ethernet standards like 10/100/1000 Mbps and use MAC

addresses to forward data. They come in various sizes, from small home switches with a few ports to large enterprise switches with dozens or hundreds of ports.

Layer –
Switches operate mainly at the Data Link Layer (Layer 2) of the OSI model, though some advanced switches can also work at Layer 3 (Network Layer) to handle routing functions

Pros –

- **Dedicated Bandwidth -** Switches provide dedicated bandwidth to each connected device, meaning that when one device transmits data, it doesn't affect the bandwidth available to other devices on the network. This leads to faster and more efficient data transmission
- **Improved Security -** Switches can isolate traffic between different ports, preventing unauthorized access to data intended for other devices
- **Enhanced Scalability -** Switches can handle more devices and accommodate network growth more effectively than hubs
- **Smart Packet Handling -** Switches can intelligently forward data packets only to the intended recipient, reducing unnecessary traffic and collisions
- **Full-Duplex Communication -** Switches enable full-duplex communication, allowing devices to send and receive data simultaneously, maximizing bandwidth utilization

Cons –

- **Higher Cost -** Switches are generally more expensive than hubs, especially managed switches with advanced features
- **Complexity -** Configuring and managing managed switches can be more complex, requiring technical expertise
- **Broadcast Traffic Issues -** While switches reduce broadcast traffic compared to hubs, it can still be an issue if not properly managed, potentially leading to broadcast storms if not handled carefully
- **Vulnerability to Attacks -** Switches can be vulnerable to security attacks like IP spoofing and Ethernet frame capturing if not properly configured and secured
- **Hardware Dependency -** Older switches may not support newer networking protocols and technologies, requiring hardware upgrades

2. **Router**
A Router is a networking device that forwards data packets between computer networks. One or more packet-switched networks or subnetworks can be connected using a router. By sending data packets to their intended IP addresses, it manages traffic between different networks and permits several devices to share an Internet connection.

Functionality –

- **Forwarding -** The router receives the packets from its input ports, checks its header, performs some basic functions like checking checksum, and then looks up to the routing table to find the appropriate output port to dump the packets onto, and forwards the packets onto that output port
- **Network Address Translation (NAT):** Routers use NAT to translate between different IP address ranges. This allows devices on a private network to access the internet using a single public IP address
- **Security:** Routers can be configured with firewalls and other security features to protect the network from unauthorized access, malware, and other threats
- **Quality of Service (QoS):** Routers can prioritize network traffic based on the type of data being transmitted. This ensures that critical applications and services receive adequate bandwidth and are not affected by lower-priority traffic
- **Virtual Private Network (VPN) connectivity:** Routers can be configured to allow remote users to connect securely to the network using a VPN
- **Bandwidth management:** Routers can be used to manage network bandwidth by controlling the amount of data that is allowed to flow through the network. This can prevent network congestion and ensure that critical applications and services receive adequate bandwidth

Specifications –

Routers support various protocols such as IPv4 and IPv6, and often include Wi-Fi capabilities. They come in models suited for home use or large enterprise networks

Layer –

Routers operate mainly at the Network Layer (Layer 3) of the OSI model, using IP addresses to route data between different networks

Pros –

- **Easier Connection -** Sharing a single network connection among numerous machines is the main advantage of router. This enables numerous people to connect to the internet, boosting total productivity.
- **Security -** Installing a router is the first step in securing a network connection. Because using a modem to connect directly to the internet exposes your computer to several security risks. So that the environment is somewhat secure, routers can be utilized as an intermediary between two networks. While not a firewall or antivirus replacement.
- **NAT Usage -** Routers use Network Address Translation (NAT) to map multiple private IP addresses into one public IP address. This allows for a better Internet connection and information flow between all devices connected to the network.

- **Supports Dynamic Routing -** The router employs dynamic routing strategies to aid in network communication. The internet work's optimum path is chosen through dynamic routing.
- **Filtering of Packets -** Switching between packets and filtering packets are two more router services. A collection of filtering rules are used by routers to filter the network.

Cons –

- **Slower -** Routers analyze multiple layers of information, from the physical layer to the network layer, which slows down connections. The same issue can also be encountered when multiple devices are connected to these network devices
- **High Cost -** They are more expensive than some other tools for systems administration. This includes security, extension, and the focal point. As a result, routers are typically not the greatest option for issues.
- **Need for configuration -** The router must be properly configured to work properly. In general, the more complex the intended use, the more configuration is required. This requires professional installation, which can add to the cost of buying a router.
- **Quality Issues -** The time transitions are not always accurate. Even yet, some modern devices use the 2.4GHz band, which is frequently deactivated. These kinds of separations are frequently possible for those who live in apartments and condominiums.
- **Bandwidth shortages -** Dynamic routing techniques used by routers to support connections tend to cause network overhead, consuming a lot of bandwidth. This leads to a bandwidth shortage that significantly slows down the internet connection between connected devices

3. **Gateway**

A gateway is a network connectivity device that connects two different configuration networks. Gateways are also known as protocol converters, because they play an important role in converting protocols supported by traffic on different networks. As a result, it allows smooth communication between two networks. It works as the entry-exit point for a network because all traffic that passes across the networks must pass through the gateway.

Functionality –

- A gateway is situated at a network edge and manages all data that enters or exits the network.
- Gateways made the transmission more feasible as it queued up all the data and divided it into small packets of data rather than sending it bulk.
- Gateways provide security within the network.

Specifications –
Gateways support multiple protocols and can handle various types of data conversion, often customized for specific network environments or applications.

Layer –
Gateways operate at multiple layers of the OSI model, depending on the function, but typically work at the higher layers (Layer 4 and above) to translate between protocols.

Pros –

- Gateway helps in connecting two different network.
- Gateway is used to filters and does not allow anything that can harm to the network.
- Gateway is worked as the protocol converter.
- Gateway is the highly secure device that provides security from external attacks.

Cons –

- Gateway causes time delay since the conversion of data according to the network requires time.
- Failure of the gateway might lead to the failure of connection with other networks.
- The implementation of Gateway is very complex and it is not cost efficient.

4. **Repeater**
A repeater is a networking device that helps to regenerate signals to increase the reach of a network. Repeaters help overcome distance-related limitations by strengthening the strength and quality of the signal. They are instrumental in LANs and WANs as they minimize errors, reduce data loss, and ensure reliable delivery to specific locations

Functionality –

- Repeater can regenerate the signal without modifying it.
- Repeaters can be used in analog signals and digital signals.
- Repeaters can extend the range of networks.
- Dynamic networking is supported by repeater.
- Use of Repeaters reduces error and loss of data.
- Power is required for working of repeaters.
- Using repeater can add complexity in the network.

Specifications –
Repeaters work at the physical layer and support standard signal types like Ethernet or fiber optics, depending on the network medium.

Layer –
Repeaters operate at the Physical Layer (Layer 1) of the OSI model, focusing purely on signal transmission.

Pros –

- **Better Performance of Network -** Repeaters provide with better performance of network because they do not always depend on processing overheads at the time.
- **Cost Effective -** Repeaters are more cost effective as compared to other network devices therefore they are cost effective.
- **Extends the network -** Repeaters provides with an advantage to extend the available network for transmission of data.
- **No Physical barriers -** Using physical devices can led to some barrier while transmission of signals. With the help of wireless repeaters such issues are resolved.
- **Enhanced Signals -** When computer devices and routers are connected in a network over long distance it weakens the strength of signals. While using repeaters it improves the strength of signals even over long distances.

Cons –

- **Network Traffic -** Repeaters do not have features to segment the network traffic. Therefore repeaters do lack with the property to congestion.
- **Network Segmentation -** As repeaters do not have feature to segment the network traffic repeaters cannot create a separate traffic from one cable to another.
- **Limited number of repeaters -** Use of limited number of repeaters is supported by the network. If more number of repeaters are used that the specified one, it can even create collision of packets and increase the noise.
- **Collision Domain -** The information is passed from various domains repeater is not able to separate the devices.

5. **Hub**

A hub is a hardware device used at the physical layer to connect multiple devices in the network. Hubs are widely used to connect LANs. A hub has multiple ports. Unlike a switch, a hub cannot filter the data, i.e. it cannot identify the destination of the packet, so it broadcasts or sends the message to each port.

Functionality –

- It supports half-duplex transmission
- It works with shared bandwidth and broadcasting.
- The hub can provide a high data transmission rate to different devices.

- It can detect collisions in the network and send the jamming signal to each port.
- Hub does not support Virtual LAN(VLAN) and spanning tree protocol.
- It is unable to filter the data and hence transmit or broadcast it to each port.
- It cannot find the best route/ shortest path to send any data, which makes it an inefficient device.

Specifications –
Hubs support basic Ethernet speeds (like 10 Mbps or 100 Mbps) and come with varying numbers of ports, usually between 4 and 24.

Layer –
Hubs operate at the Physical Layer (Layer 1) of the OSI model, dealing only with raw data transmission without any processing.

Pros –

- **Connectivity** - The primary function of the hub is to permit clients to attach to a network in order that they will share and have conversations. For this purpose, hubs use network protocol analyzer.
- **Performance** - Hub is understood for having very less number of performance impacts on the network. This is often because it operates using a broadcast model which rarely affects the network.
- **Cost** - Comparing to switches, hubs are really inexpensive.
- **Device Support** - Hubs can connect different types of media all at once with a central hub.
- **Area Coverage -** Area coverage of a network is restricted to a certain distance. Hub extends the space of the network such communication is formed easy.

Cons –

- **Collision Domain** - The function of the collision domain and again transfer of packet does not affect actually it increases more chances of collision in between domains.
- **Full-Duplex Mode** - Hubs cannot communicate fully duplex mode, it can only operate in half-duplex mode. Half-duplex mode, in essence, means data are often transmitted just one occasion at a given time. Therefore, the hub must constantly switch its modes.
- **Specification** - Hubs cannot support networks that are large like a token ring.
- **Network Traffic** - As the attachment was received in the packet so it cannot reduce traffic.
- **Bandwidth Wastage** - Hubs cannot provide dedicated bandwidth for every device, it is to share them. When sending large pieces of information all the

bandwidths are going to be occupied by the two computers leaving other computers with slow network.

6. **Bridge**
A bridge in a computer network is a device used to connect multiple LANs together with a larger Local Area Network (LAN). The mechanism of network aggregation is known as bridging. There are three types of bridges in computer networks -

- **Transparent Bridge:** Transparent bridges are invisible to other devices on the network. This bridge doesn't reconfigure the network on the addition or deletion of any station. The prime function of the transparent bridge is to block or forward the data according to the MAC address.
- **Source Routing Bridge:** Source routing bridges were developed and designed by IBM specifically for token ring networks. The frame's entire route is embedded with the data frames by the source station to perform the routing operation so that once the frame is forwarded it must follow a specific defined path/route.
- **Translational Bridge:** Translational bridges convert the received data from one networking system to another. Or it is used to communicate or transmit data between two different types of networking systems. Like if we are sending data from a token ring to an Ethernet cable, the translational cable will be used to connect both the networking system and transmit data.

Functionality –

- The bridge is used to divide LANs into multiple segments.
- To control the traffic in the network.
- It can interconnect two LANs with a similar protocols.
- It can filter the data based on destination/MAC address.

Specifications –

Bridges operate using MAC addresses and support Ethernet standards, typically managing traffic between LAN segments.

Layer –

Bridges operate at the Data Link Layer (Layer 2) of the OSI model

Pros –

- Bridges can be used as a network extension like they can connect two network topologies together.
- It has a separate collision domain, which results in increased bandwidth.
- It can create a buffer when different MAC protocols are there for different segments.
- Highly reliable and maintainable. The network can be divided into multiple LAN segments.
- Simple installation, no requirement of any extra hardware or software except the bridge itself.
- Protocol transparency is higher as compared to other protocols.

Cons –

- Expensive as compared to hubs and repeaters.
- Slow in speed.
- Poor performance as additional processing is required to view the MAC address of the device on the network.
- As the traffic received is in bulk or is broadcasted traffic, individual filtering of data is not possible.
- During the broadcasting of data, the network has high broadcast traffic and broadcast storms can be formed.

7. **NIC**

NIC stands for Network Interface Card. NIC is additionally called Ethernet or physical or network card. NIC is one of the major and imperative components of associating a gadget with the network. Each gadget that must be associated with a network must have a network interface card. Even the switches comprise of NIC in arrange to associate to the systems. It is the foremost essential network component without which you cannot interface any gadget to a network.

Functionality –

- Enables communication between a device and the network.
- Converts data from the device into signals for transmission over the network.
- Receives incoming data from the network and translates it for the device.
- Handles both wired (Ethernet) and wireless (Wi-Fi) connections, depending on the type.

Specifications –

NICs operate using MAC addresses and support various network protocols, including Ethernet and Wi-Fi standards. They can be configured for different speeds such as 10/100 Mbps, 1 Gbps, or higher.

Layer –

NICs operate at both the Physical Layer (Layer 1) and Data Link Layer (Layer 2) of the OSI model.

Pros –

- The communication speed utilizing the Web is high ordinarily in Gigabytes.
- Highly dependable connection.
- Many peripheral gadgets can be associated with utilizing numerous ports of NIC cards.
- Bulk information can be shared among numerous clients.

Cons –

- Badly arranged in case of wired cable NIC, because it isn't versatile like a remote router.

- The arrangement ought to be appropriate for superior communication.
- Data is unsecured.

Study of Transmission Media

1. Twisted pair cable

In balanced pair operation, the two wires carry equal and opposite signals and the destination detects the difference between the two. This is known as differential mode transmission. Noise sources introduce signals into the wires by coupling of electric or magnetic fields and tend to couple to both wires equally. The noise thus produces a common-mode signal which is cancelled at the receiver when the difference signal is taken.

This method starts to fail when the noise source is close to the signal wires; the closer wire will couple with the noise more strongly and the common-mode rejection of the receiver will fail to eliminate it. This problem is especially apparent in telecommunication cables where pairs in the same cable lie next to each other for many miles. One pair can induce crosstalk in another and it is additive along the length of the cable. Twisting the pairs counters this effect as on each half twist the wire nearest to the noise-source is exchanged.

Provided the interfering source remains uniform or nearly so, over the distance of a single twist, the induced noise will remain common-mode. Differential signalling also reduces electromagnetic radiation from the cable, along with the associated attenuation allowing for greater distance between exchanges.

The twist rate (also called pitch of the twist, usually defined in twists per meter) makes up part of the specification for a given type of cable. Where nearby pairs have equal twist rates, the same conductors of the different pairs may repeatedly lie next to each other, partially undoing the benefits of differential mode. For this reason it is commonly specified that, at least for cables containing small numbers of pairs, the twist rates must differ.

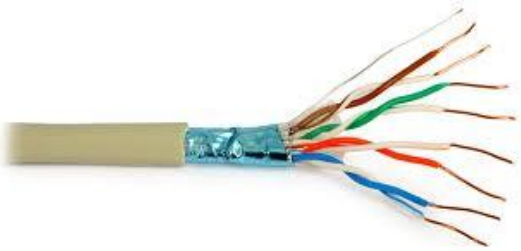
UTP cables are found in many Ethernet networks and telephone systems. For indoor telephone applications, UTP is often grouped into sets of 25 pairs according to a standard 25-pair color code originally developed by AT&T Corporation. A typical subset of these colors (white/blue, blue/white, white/orange, orange/white) shows up in most UTP cables. The cables are typically made with copper wires measured at 22 or 24 American Wire Gauge with the colored insulation typically made from an insulator such as polyurethane and the total package covered in a polyurethane jacket.

For urban outdoor telephone cables containing hundreds or thousands of pairs, the cable is divided into smaller but identical bundles. Each bundle consists of twisted pairs that have different twist rates. The bundles are in turn twisted together to make up the cable. Pairs having the same twist rate within the cable can still experience some degree of crosstalk. Wire pairs are selected carefully to minimize crosstalk within a large cable.

Unshielded twisted pair cable with different twist rates UTP cable is also the most common cable used in computer networking. Modern Ethernet, the most common data networking standard, can use UTP cables. Twisted pair cabling is often used in data networks for short and medium length connections because of its relatively lower costs compared to optical fiber

and coaxial cable.

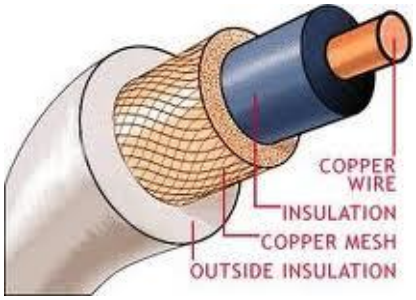
UTP is also finding increasing use in video applications, primarily in security cameras. Many cameras include a UTP output with screw terminals; UTP cable bandwidth has improved to match the baseband of television signals. As UTP is a balanced transmission line, a balun is needed to connect to unbalanced equipment, for example any using BNC connectors and designed for coaxial cable.



Twisted Pair

2. Coaxial cable

Coaxial cable is the kind of copper cable used by cable TV companies between the community antenna and user homes and businesses. Coaxial cable is sometimes used by telephone companies from their central office to the telephone poles near users. It is also widely installed for use in business and corporation Ethernet and other types of local area network. Coaxial cable is called "coaxial" because it includes one physical channel that carries the signal surrounded (after a layer of insulation) by another concentric physical channel, both running along the same axis. The outer channel serves as a ground. Many of these cables or pairs of coaxial tubes can be placed in a single outer sheathing and, with repeaters, can carry information for a great distance.

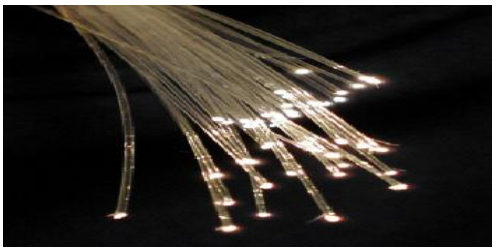


Coaxial Cable

Optical Fiber

Fiber-optic communication is a method of transmitting information from one place to another by sending pulses of light through an optical fiber. The light forms an electromagnetic carrier wave that is modulated to carry information. First developed in the 1970s, fiber-optic communication systems have revolutionized the telecommunications industry and have played a major role in the advent of the Information Age. Because of its advantages over

electrical transmission, optical fibers have largely replaced copper wire communications in core networks in the developed world.
The process of communicating using fiber-optics involves the following basic steps: Creating the optical signal involving the use of a transmitter, relaying the signal along the fiber, ensuring that the signal does not become too distorted or weak, receiving the optical signal, and converting it into an electrical signal.



Fiber Optics Cable

Summary

Computer networks use various devices and transmission media to enable efficient communication. Switches (Layer 2) segment networks into LANs and forward data using MAC addresses, supporting unicast, multicast, and broadcast. Routers (Layer 3) direct packets between networks using IP addresses and offer features like NAT. Gateways translate protocols across different networks and operate at higher OSI layers. Repeaters (Layer 1) regenerate weak signals to extend network range, while hubs (also Layer 1) simply broadcast data to all ports, causing collisions. Bridges (Layer 2) connect and filter traffic between LAN segments, and NICs (Layer 1 & 2) enable device-level network access. For transmission, twisted pair cables (e.g., UTP) are common for short-range communication, coaxial cables offer better shielding, and optical fibers provide high-speed, long-distance data transfer using light. These components together ensure smooth and scalable network performance.

CONCLUSION:

I have successfully completed the experiment on the study of networking devices and transmission media. Through this experiment, I learned about the functionality, specifications, pros, and cons of various networking components such as switches, routers, gateways, repeaters, hubs, bridges, and NICs. This experiment enhanced my understanding of how devices and media work together to establish reliable computer networks in real-world scenarios.

Post Lab Questions

1. **Compare Hub, switch, bridge, and gateway and specify the use in different cases.**
   A hub is a basic networking device that operates at the physical layer (Layer 1) of the OSI model. It simply receives data on one port and broadcasts it to all other ports without any form of filtering or traffic management. Hubs do not have the ability to learn MAC addresses, making them inefficient and prone to collisions,

especially in larger networks. They are mostly obsolete and were traditionally used in small, simple LANs where minimal traffic management was needed. A switch, on the other hand, functions at the data link layer (Layer 2) and is more intelligent than a hub. It maintains a MAC address table and forwards data only to the specific port associated with the destination MAC address. This reduces network congestion and improves speed and efficiency. Switches are widely used in modern LANs to connect multiple devices with full-duplex communication and minimal collisions. A bridge also operates at the data link layer and is used to connect and filter traffic between two or more network segments. Like a switch, it uses MAC addresses to forward or block data. Bridges help in segmenting networks to reduce traffic and extend LANs. However, they typically support fewer ports than switches and are used in simpler scenarios or legacy systems. A gateway is the most advanced of the four, functioning at the network layer (Layer 3) or higher. It is used to connect networks that use different protocols or architectures, such as connecting a local network to the internet. Unlike switches or bridges, gateways can perform protocol conversion (e.g., from IPv4 to IPv6) and are essential for enabling communication between dissimilar systems. They are commonly used in scenarios like internet access, email services, and cloud connectivity.
In summary, hubs are basic and outdated, switches are fast and efficient for LANs, bridges segment and extend networks, and gateways connect entirely different networks or protocols.

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

3. **Frames from one LAN can be transmitted to another LAN via the device**
   A. Router
   B. Bridge
   C. Repeater
   D. Modem