**Batch: B2 Roll No.: 16014022050**

**Experiment No.: 1**

**Grade: AA / AB / BB / BC / CC / CD / DD**

**Signature of the staff in-charge with date**

Ccff

**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:**

**CO1:** Understand concept of computer communication and network model.

**Books / Journals / Websites Referred:**

1. S. Tanenbaum, “Computer Networks”, Pearson Education, Fourth Edition
2. 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.

**Study of Connecting Devices**

1. **Hub:**

In computer networks, hubs serve as central connection points within a network, allowing devices to communicate and share data. Operating at the physical layer of the OSI model, hubs transmit data signals to all connected devices, regardless of the intended recipient.

Purpose

A hub is a networking device that serves as a central connection point within a local area network (LAN). Its primary function is to receive data signals from connected devices and broadcast them to all other connected devices, regardless of the intended recipient. Hubs operate at the physical layer (Layer 1) of the OSI model, focusing on raw data transmission without any data processing or intelligence. It operates at the physical layer (Layer 1) of the OSI model and broadcasts data to all connected devices, without any intelligent forwarding.

Types of Hubs

1. Active Hub

An active hub also known as a powered hub; it requires an external power source to operate. It amplifies and regenerates incoming signals, enabling data transmission over longer distances without signal degradation. Active hubs can support a larger number of ports, making them suitable for expanding network connectivity.

1. Passive Hub

A passive hub, also referred to as an unpowered hub, does not require an external power source. It simply provides a physical connection between devices without signal amplification or regeneration. Passive hubs have limited transmission distances and can support only a smaller number of ports.

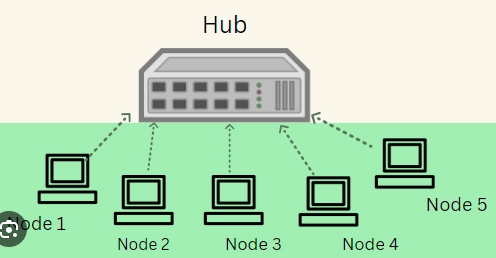
How do Hubs work?

Hubs operate by receiving data signals from connected devices and rebroadcasting them to all other devices. When a device sends data, the hub receives the signal and immediately broadcasts it to all other connected devices. This broadcast approach is known as "store-and-forward" transmission, where the hub doesn't perform any data filtering or processing.

Connectivity

* The hub receives data from one device and sends it to all other devices on the network. It does not distinguish between devices, leading to potential network congestion and inefficiencies.
* Hubs typically connect devices using Ethernet cables (RJ45) and can have multiple ports (e.g., 4, 8, 12, or 24 ports).

Diagram



Applications

* Small, Simple Networks: Hubs were used in early networking for connecting computers in small, simple LANs.
* Cost-Effective for Simple Connectivity: Suitable in non-demanding environments where network performance is not a critical factor.
* Old Equipment: Some older networking setups still use hubs, although they have mostly been replaced by switches.

1. **Repeater:**

A repeater is a device that amplifies or regenerates signals to extend the range of a network. It works at the physical layer (Layer 1) and boosts the signal strength so it can travel further without degradation.

Purpose

A repeater is a networking device that helps to amplify and regenerate signals to increase the reach of a network. Also operating at the [physical layer of the OSI model,](https://www.geeksforgeeks.org/physical-layer-in-osi-model/) repeaters help overcome distance-related limitations by strengthening the strength and quality of the signal. They are instrumental in LANs and [WANs](https://www.geeksforgeeks.org/wan-full-form/) as they minimize errors, reduce data loss, and ensure reliable delivery to specific locations. One of the primary benefits of repeaters is the error free transfer of data over longer distances. This will ensure efficient and safe communication.

Types of Repeaters

1. Analog Repeater

Analog repeaters are used to amplify only the analog signals. Analog repeaters receive the analog signal, amplifies it and then regenerates it as the output. Analog repeaters were mostly used in the older network technologies where analog signal was used.

1. Digital Repeater

Digital repeaters are the type of repeaters that does not amplify digital signal but regenerates it directly. Digital repeaters are mostly used in the modern technologies where digital signal is being used. Digital repeaters are also capable to reconstruct a distorted signal.

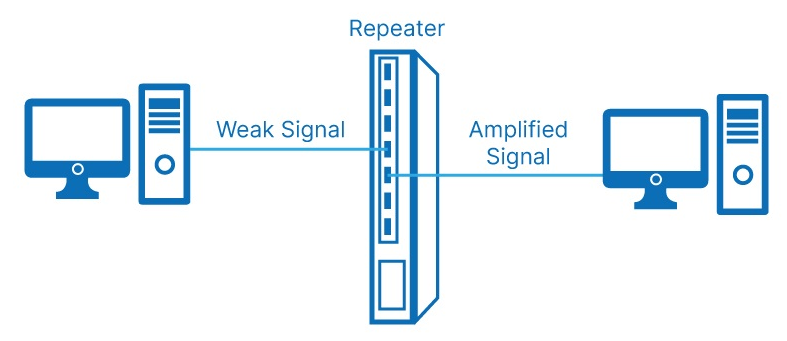
1. Wired Repeaters

Wired repeaters are used in wired Local Area Networks (LANs). Wired repeater receives the signal and repeats it. This helps to extend the network travel data without losing its strength and data.

1. Wireless Repeaters

Wireless repeaters are used in wireless Local Area Networks (LANs) and Cellular networks. A router connected in the network sends wireless signal to the repeater. Once received, repeater broadcast the signal to increase the coverage of network.

Diagram



Connectivity

* A repeater is placed between two segments of a network to extend the communication distance. It receives a weak or degraded signal, amplifies it, and then retransmits the signal to the next segment.
* It is commonly used in wireless networks to extend coverage, or in wired networks to overcome the distance limitations of cables (e.g., Ethernet, fibre optic).

Applications

* Long-Distance Communication: Used in large networks where the signal needs to be boosted over long distances, like in large office buildings or campuses.
* Wireless Networks: Extends the coverage area of Wi-Fi networks by placing repeaters to relay signals between routers and clients.
* Satellite Communications: Amplifies signals for communication between satellites and ground stations.

1. **Switch:**

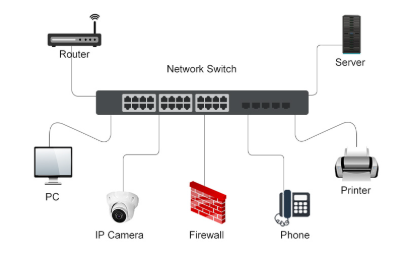
Purpose

A switch is an intelligent networking device that operates at the data link layer (Layer 2) of the OSI model. It selectively forwards data frames to the correct destination device based on MAC addresses, making it more efficient than a hub.

Connectivity

* A switch connects devices in a network by learning their MAC addresses and maintaining a MAC address table. It then forwards frames only to the specific device (or port) associated with the destination MAC address, reducing unnecessary traffic.
* Modern switches operate with multiple ports (typically 8, 16, 24, or more) and support full-duplex communication, allowing simultaneous data transmission in both directions.

Diagram



Applications

* Enterprise Networks: Used to connect computers, printers, servers, and other devices within a business or enterprise LAN.
* Segmenting Traffic: Switches are used in larger networks to divide the traffic into segments, minimizing collisions and improving performance.
* Data Centers: Switches manage high-speed data transfers between servers and storage devices.
* VoIP Networks: Switches can prioritize traffic to ensure low-latency communication for Voice over IP (VoIP) calls.

1. **Bridge:**

A network bridge is an electronic device designed to intelligently connect and filter network traffic between multiple network segments. Unlike simple repeaters that blindly forward all traffic, bridges make intelligent decisions about data transmission based on advanced MAC address learning and filtering techniques.

Purpose

A bridge is a [network device](https://www.shiksha.com/online-courses/articles/network-devices-in-computer-networks-and-its-types/) that connects multiple subnetworks to create a single network. It provides interconnection with other computer networks that use the same protocol. Through a bridge, multiple LANs can be connected to form a larger and extended LAN. This function of creating a single aggregate network from multiple network segments is called network bridging. It works in the data link layer, which is the second network layer in the [OSI model](https://www.shiksha.com/online-courses/articles/osi-model-explained/).

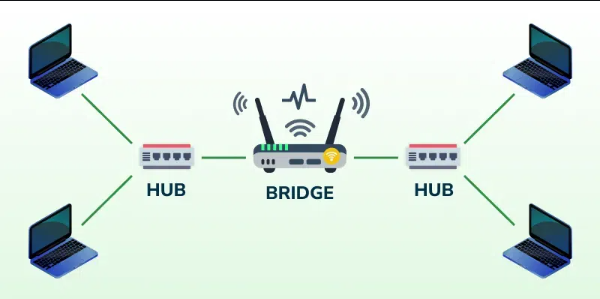
Functions of Bridges –

* Store [MAC address](https://www.shiksha.com/online-courses/articles/mac-address-format-and-types/) in the PC that is used in the network for reducing network traffic.
* Divide local area networks into multiple segments.
* Connects multiple networks to ensure communication between them.
* It connects [LAN](https://www.shiksha.com/online-courses/articles/lan-local-area-network/) segments into a single network.
* Recognizes areas where data is to be sent and on which device it will be sent.
* Maintains MAC address table to discover new segments.
* Used in load filtering of network traffic by separating it into segments or packets.

Connectivity

* A bridge receives frames from one network segment and forwards them to another, making decisions based on the MAC addresses. This helps reduce network traffic by not forwarding unnecessary frames to other segments.
* A bridge can connect different types of physical media (e.g., connecting a wireless network to a wired one), and also helps isolate collision domains, improving network performance.

Diagram



Applications

* Segmentation of Large Networks: Used to break up large, congested networks into smaller, manageable segments, improving overall performance.
* Connecting Different Media: Bridges can connect different types of network media, such as wired Ethernet and Wi-Fi.
* Improving Network Performance: Helps reduce traffic in larger networks by filtering out unnecessary traffic, reducing the risk of collisions and improving bandwidth utilization.

1. **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.

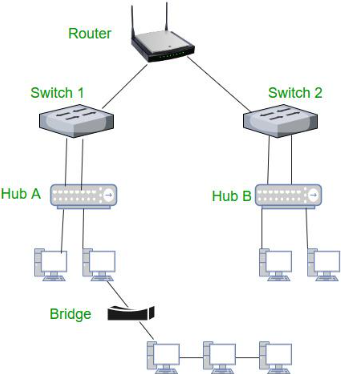
Purpose

* Connects and manages communication between multiple networks (e.g., LAN, WAN, or the Internet).
* Directs data packets to their destination using IP addressing and routing protocols.
* Ensures efficient data transfer by finding the best path between source and destination.
* Enables devices on a local network to access the internet.

Connectivity

* WAN Port: Connects to an external network, such as the internet via a modem.
* LAN Ports: Connect to local devices like computers, printers, or switches.
* Wireless Connectivity: Provides Wi-Fi access for mobile devices, laptops, and IoT devices.
* Supports protocols like TCP/IP, DHCP, and routing protocols (RIP, OSPF, BGP).

Diagram

****

****

How does router work?

A router determines the path of a data packet by analysing the destination IP address in its header and referencing a routing table, which contains rules and predefined paths to specific network locations. Using these tables, the router decides the most efficient way to transmit data to its destination.

Routing tables can be either static, where paths are manually configured, or dynamic, where they are automatically updated based on network activity. Routers connect devices to the internet through modems like cable, fibre, or DSL modems, and they typically include multiple ports to allow several devices to connect simultaneously. By managing traffic, routers ensure data is delivered efficiently while also identifying its source and destination.

For unknown destinations, routers rely on a default route, such as directing all traffic to an ISP in an office network. This process ensures smooth communication between devices and networks.

Applications

* Home Networking: Connects devices in a home network to the internet.
* Enterprise Networks: Connects and manages traffic in larger networks across multiple locations.
* ISP Networks: Used by Internet Service Providers to route data across the internet.

1. **Gateway:**

A Gateway is a network device or software that acts as a bridge between two networks with different communication protocols, enabling seamless data transfer and communication.

Purpose

* Serves as an entry/exit point for a network.
* Connects and translates data between networks with different protocols or architectures.
* Facilitates communication between a local network (LAN) and external networks (like the internet).
* Manages traffic flow and provides security features like firewalls and NAT (Network Address Translation).

Types of Gateways

1. Unidirectional Gateways

They allow data to flow in only one direction. Changes made in the source node are replicated in the destination node, but not vice versa. They can be used as archiving tools.

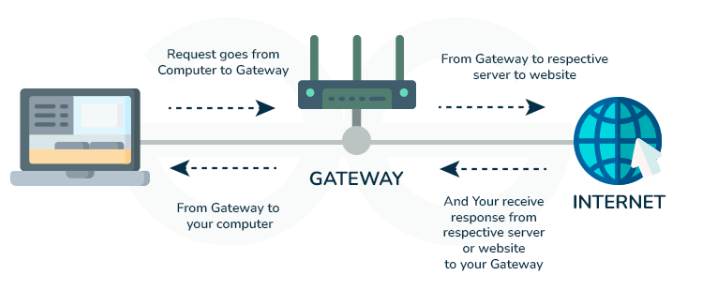
1. Bidirectional Gateways

They allow data to flow in both directions. They can be used as synchronization tools.

Connectivity

* Connects multiple networks (LAN, WAN, Internet) or devices.
* Acts as an intermediary between different protocols (e.g., IPv4 to IPv6, TCP/IP to X.25).
* Connects internal private networks to external public networks.

Diagram



1. **NIC:**

A network interface card (NIC) is a hardware component without which a computer cannot be connected over a network. It is a circuit board installed in a computer that provides a dedicated network connection to the computer. It is also called network interface controller, network adapter, or LAN adapter.

Purpose

* NIC allows both wired and wireless communications.
* NIC allows communications between computers connected via local area network (LAN) as well as communications over large-scale network through Internet Protocol (IP).
* NIC is both a physical layer and a data link layer device, i.e. it provides the necessary hardware circuitry so that the physical layer processes and some data link layer processes can run on it.

Types of NIC

1. Internal Network Cards

In internal networks cards, motherboard has a slot for the network card where it can be inserted. It requires network cables to provide network access. Internal network cards are of two types. The first type uses Peripheral Component Interconnect (PCI) connection, while the second type uses Industry Standard Architecture (ISA).

****

1. External Network Cards

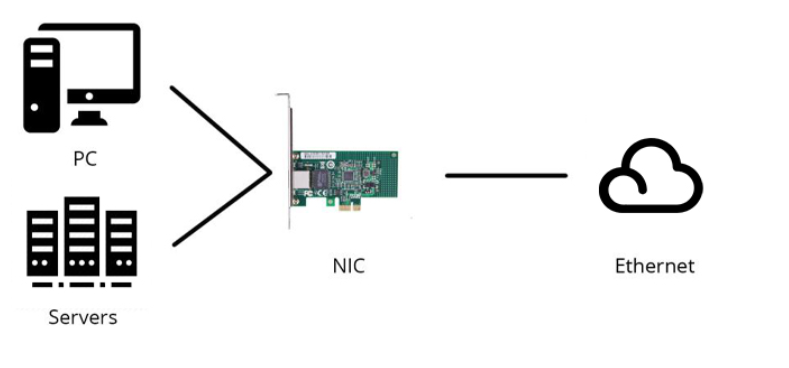
In desktops and laptops that do not have an internal NIC, external NICs are used. External network cards are of two types: Wireless and USB based. Wireless network card needs to be inserted into the motherboard; however, no network cable is required to connect to the network. They are useful while traveling or accessing a wireless signal.

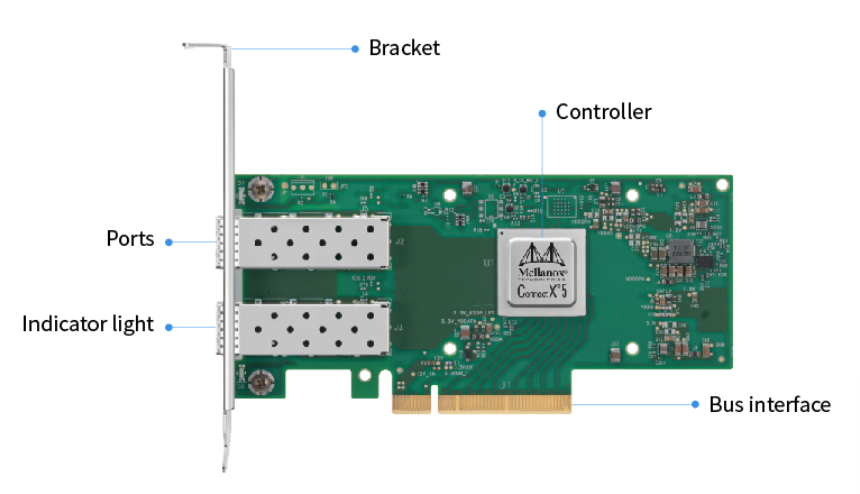
****

Connectivity

* Wired NIC: Connects via an Ethernet cable to a router, switch, or modem.
* Wireless NIC: Uses Wi-Fi to connect to wireless access points.
* Supports different communication protocols like Ethernet, Wi-Fi, or Fibre Channel.
* Operates on network layers (Layer 2: Data Link, Layer 1: Physical Layer).

Diagram

****

****

The network card has the following 6 components –

* Controller: The central component of the NIC, responsible for processing data transmission.
* Boot ROM Slot: Allows diskless workstations to boot via the network, enhancing security and reducing costs.
* Interface Port: Connects to the network using an Ethernet cable or transceiver to transfer data signals.
* Bus Interface: Plugs into an expansion slot to link the NIC with the computer's motherboard.
* LED Indicators: Show the network card's connection and activity status, providing users with an understanding of its operation.
* Bracket: Comes in standard and compact sizes for securing the NIC within the expansion slot.

Applications

* Used in computers, servers, printers, and IoT devices for network communication.
* Enables internet browsing, file sharing, remote access, and cloud computing.
* Crucial for online gaming, video streaming, and VoIP services.

**Study of Transmission Media**

The below information is given for reference purpose only; you need to replace this with the information you have searched.

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.

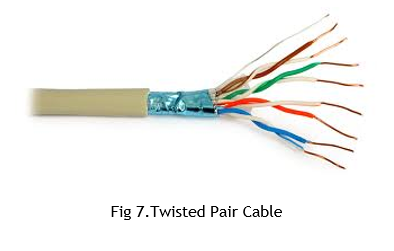
UTP cables are found in many Ethernet networks and telephone systems. For indoor telephone applications, UTP is often grouped into sets of 25 pairs according to a standard 25-pair color code originally developed by AT&T Corporation. A typical subset of these colors (white/blue, blue/white, white/orange, orange/white) shows up in most UTP cables. The cables are typically made with copper wires measured at 22 or 24 American Wire Gauge (AWG),[3] 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 fibre and coaxial cable.

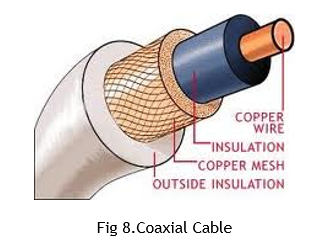
UTP is also finding increasing use in video applications, primarily in security cameras. Many cameras include a UTP output with screw terminals; UTP cable bandwidth has improved to match the baseband of television signals. As UTP is a balanced transmission line, a balun is needed to connect to unbalanced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



1. **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.

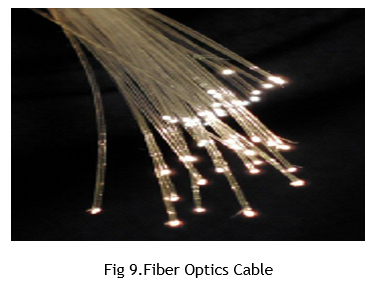
Coaxial cable is called "coaxial" because it includes one physical channel that carries the signal surrounded (after a layer of insulation) by another concentric physical channel, both running along the same axis. The outer channel serves as a ground. Many of these cables or pairs of coaxial tubes can be placed in a single outer sheathing and, with repeaters, can carry information for a great distance.



1. **Optical Fiber:**

Fiber-optic communication is a method of transmitting information from one place to another by sending pulses of light through an optical fibre. The light forms an electromagnetic carrier wave that is modulated to carry information. First developed in the 1970s, fibre-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 fibres have largely replaced copper wire communications in core networks in the developed world.

The process of communicating using fibre-optics involves the following basic steps: Creating the optical signal involving the use of a transmitter, relaying the signal along the fibre, ensuring that the signal does not become too distorted or weak, receiving the optical signal, and converting it into an electrical signal.

****

**Conclusion:**

Researched and studied different types of transmission media and connecting devices such as Hub, Repeater, Switch, Bridge, Router, Gateway and NIC.

**Post Lab Questions:**

1. **Compare Hub, Switch, Bridge and Gateway and specify the use in different cases.**

**Hub**

Functionality:

A hub is a basic networking device that connects multiple computers in a LAN (Local Area Network). It operates at the Physical Layer (Layer 1) of the OSI model. A hub simply receives data from one device and broadcasts it to all connected devices. It does not perform any filtering or processing of the data; everything it receives is forwarded to all other ports, making it inefficient for large networks.

Use Cases:

* Small, simple networks (e.g., home or small office networks).
* Legacy systems: Older networks before switches became more common.
* Short-range applications: Used when cost is a major factor and the network size is small.

Disadvantages:

* Broadcasting: All data is sent to all connected devices, which can cause collisions and network congestion.
* Security: Lack of filtering allows unauthorized devices to receive data.

**Switch**

Functionality:

A switch operates at the Data Link Layer (Layer 2) of the OSI model. It is more intelligent than a hub. A switch receives data and forwards it only to the device (MAC address) that the data is intended for, based on its MAC address table. It reduces network congestion and increases efficiency by managing data flow more effectively.

Use Cases:

* Medium to large networks: Most modern networks use switches instead of hubs.
* Enterprise-level networks: Suitable for offices, data centres, and large networks where high-speed and low-latency communication are important.
* Improved security and performance: Reduces the chance of collisions and unauthorized data interception by using a point-to-point connection.

Disadvantages:

* Cost: More expensive than hubs.
* Limited to Layer 2: A switch typically doesn't perform IP routing or protocol translation.

**Bridge**

Functionality:

A bridge operates at the Data Link Layer (Layer 2) as well and is used to connect two separate network segments. It filters traffic based on MAC addresses and only forwards data between segments if necessary, reducing network traffic and collisions. It is often used to divide a large network into smaller, more manageable segments.

Use Cases:

* Segmentation of networks: Helps reduce traffic on a large LAN by dividing it into smaller segments.
* Connecting networks with similar technologies: Can be used to connect two networks that use the same protocol but are physically separated.

Disadvantages:

* Limited scalability: A bridge works best for smaller networks and cannot handle more complex scenarios like inter-network communication.
* Slower performance compared to routers: It is not as efficient for large-scale or complex networks.

**Gateway**

Functionality:

A gateway operates at the Network Layer (Layer 3) or above in the OSI model. It is used to connect different networks that use different communication protocols. Gateways perform protocol translation, allowing systems with different communication methods or data formats to communicate with each other. They are often used to connect a LAN to a wider network, such as the internet.

Use Cases:

* Interconnecting different networks: Used when you need to connect networks using different protocols (e.g., a local network to the internet or connecting two networks using different communication protocols).
* Internet connectivity: Often used to connect a LAN to an external network (e.g., router acting as a gateway to the internet).
* Protocol conversion: Translating between protocols such as TCP/IP and older or proprietary network protocols.

Disadvantages:

* Complex configuration: Gateways often require more setup compared to simpler devices like switches and hubs.
* Performance impact: They can introduce delays due to the need to translate between protocols.

1. **Which of the following device is used to connect two systems, especially if the systems use different protocols?**
2. **Hub**
3. **Bridge**
4. **Gateway**
5. **Repeater**
6. **None of the above**
7. **Frames from one LAN can be transmitted to another LAN via the device**
8. **Router**
9. **Bridge**
10. **Repeater**
11. **Modem**