Experiment No.: 1

Title: Study of Network devices: Hubs/Repeaters, Switches, Bridges, and Routers.

Roll No.: _________ *Batch:* __________

Date of Performance: _________________

Date of Assessment: ___________________

Particulars	Marks
Attendance (05)	
Journal (05)	
Performance (05)	
Understanding (05)	
Total (20)	
Signature of Staff Member	

Experiment No. 1

Title: Study of Network devices: Hubs/Repeaters, Switches, Bridges, Routers.

Aim: To understand the functions, characteristics, and differences of key network devices: Hubs/Repeaters, Switches, Bridges, and Routers and to analyze their roles in building and managing computer networks.

Prerequisite:

- Basic knowledge of computer networks and the OSI model.
- Understanding of IP addressing and subnetting.
- Familiarity with network topologies and types of network cables.
- Ability to use basic networking commands (e.g., ping, ipconfig).
- Availability of network devices like hubs, switches, bridges, routers, and connecting cables.

Objectives:

1. Define and describe the basic concepts of Hubs, Repeaters, Switches, Bridges, and Routers.
2. Working principles of each network device and how they facilitate data transmission.
3. Identify appropriate use cases and scenarios where each device is most effective.

Theory:

A computer network is made up of various devices, such as the hub, repeater, modem, switch, computer devices, etc. Each device plays a vital role in networking. Repeaters are used to extend the network and provide security, strength, and no data loss.

What is a Repeater?

A repeater is a networking device that helps to regenerate signals to increase the reach of a network. Also operating at the physical layer of the OSI model, 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. One of the primary benefits of repeaters is the error free transfer of data over longer distances. This will ensure efficient and safe communication.

Features of Repeaters:

- 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.
- Use of Repeaters reduces error and loss of data.
- Using repeater can add complexity in the network.

Working of Repeaters:

- Initially the source system transmits the signals. This source systems can be a mobile phone, laptop or radio.
- This transmitted signal from the source system travels in air if it's wireless network or through the cable if it is wired network. As the signal goes away from the source its strength gets weak.
- The signal received to the repeater is not the actual signal sent by source system but a weak signal. Therefore, repeater amplifies this weak signal to get it strengthen.
- The strengthen signal is now being sent from the repeater to its destination. This signal is stronger and can travel at longer distance. In short, it extends the network without losing the quality of signal.
- Repeaters are therefore used in various wireless technologies such as Wi-Fi and wired technologies such as ethernet.

What is HUB?

A hub is a multi-port repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, the collision domain of all hosts connected through hub remains one. Hub does not have any routing table to store the data of ports and map destination addresses., the routing table is used to send/broadcast information across all the ports.

How Does a Network Hub Work?

A hub is a multiport device, which has multiple ports in a device and shares the data to multiple ports altogether. A hub acts as a dumb switch that does not know, which data needs to be forwarded where so it broadcasts or sends the data to each port.

Suppose there are five ports in a hub A, B, C, D, and E. Consider A wants to send any data frame, or let's say A is acting as a sender, so the hub will forward the data transmitted by A to B, C, D, E.

\Now, at the same time B also wants to send the data then data received from A and B will collide and can cause data loss. In this situation, the data gets destroyed, and the hosts send a jam signal to all the hosts informing them about the collision, and each sender needs to wait for a certain amount of time.

Types of Network Hubs:

Networks hubs are classified into three types:

1. **Active Hub:** They have a power supply for regenerating, and amplifying the signals. When a port sends weak signaled data, the hub regenerates the signal and strengthens it, then send it further to all other ports. Active hubs are expensive in costs as compared to passive hubs.
2. **Passive Hub:** Passive hubs are simply used to connect signals from different network cables as they do not have any computerized element. They simply connect the wires of different devices in the star topology.
3. **Intelligent Hub:** Intelligent hubs as the name suggests are smarter than active and passive hubs. The intelligent hub comprises a special monitoring unit named a Management Information Base (MIB). This is software that helps in analyzing and troubleshooting network problems. It can monitor the traffic of the network and the configuration of a port.

Features of Hubs:

- 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.
- 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.

What is Switch?

Switches in computer networks are devices that connect multiple devices (like computers, and printers) within a network. They manage data traffic efficiently by directing data only to the devices that need it, enhancing network performance. Unlike hubs, switches operate at the data link layer (Layer 2) of the OSI model, making decisions based on MAC addresses. They are crucial for creating reliable and fast local area networks (LANs).

Switches are the connectivity points of an Ethernet network. These are small devices that can receive data from multiple input ports and send it to the specific output port that takes data to its intended destination in the network.

Characteristics of a Switch:

Before we dive into different types of switches, let's understand some key features of a switch:

- In a switch, two important things to know are its "poles" and "throws." A pole is where an electrical contact is made, and a throw is how many different contacts each pole can connect to. The number of poles and throws tells you how the switch works and what it can connect to in a circuit.

- In switches, you often find two standard types: Single, which has one contact point or one connection, and Double, which has two contact points or two connections. These terms describe how switches are built and what they can do in electronic devices.
- If a switch has more than two poles or throws, we usually just state the number directly. For
- example, a switch with three poles and six throws is called a "3P6T" switch.
- Momentary switches, like push buttons, make contact only while they are pressed. They're used for brief actions or as long as you hold the button.
- Latched switches, on the other hand, maintain their contact position until they are switched to the other position.

Types of Switches in Computer Network:

There are different types of switches in a network. These are:

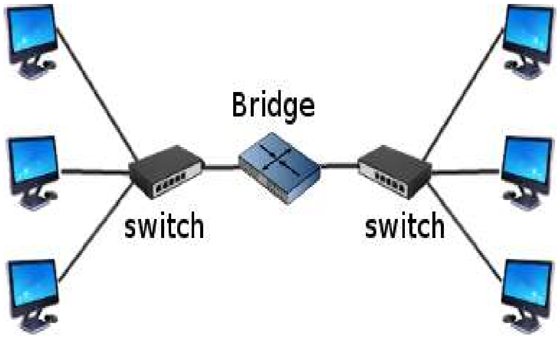
- Mechanical Switches
- Electronic Switches
- Managed Switches
- Unmanaged Switches
- Layer 2 Switches
- Layer 3 Switches

What is Bridge?

A Bridges is a network device that connects and filters traffic between two or more network segments (like LANs or subnets). It operates at the data link layer (Layer 2) of the OSI model. It helps reduce network traffic by only forwarding data between segments when necessary, improving overall network performance. Bridges are relatively easy to configure and focuses on MAC addresses.

Types of Bridges:

- **Transparent Bridge**: Automatically connects and filters traffic between network segments without requiring configuration.
- **Source Routing Bridge**: Used in networks where the sender defines the data path, common in Token Ring networks.
- **Translational Bridge**: Connects different types of



networks (e.g., Ethernet to Token Ring).

- **Wireless Bridge**: Connects two networks wirelessly over long distances, typically in remote locations.

Advantages of a Bridge:

- Traffic Segmentation: Reduces network traffic by dividing a large network into smaller segments.
- Improves Performance: Helps in isolating collision domains, which reduces packet collisions.
- Filtering: It filters data based on MAC addresses and only passes relevant information between segments.
- Security: Provides basic security by preventing unnecessary traffic between different segments.
- Broadcast Control: Reduces broadcast traffic in large networks.

Disadvantages of a Bridge:

- Slower Speeds: Bridges can introduce delays as they filter and forward data.
- Limited Scalability: Not suitable for large-scale networks as the traffic filtering becomes inefficient.
- Requires Configuration: May need manual configuration and management to work effectively.
- Cost: More expensive than repeaters and simpler devices.

What is a 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.

How Does Router Work?

- A router determines a packet's future path by examining the destination IP address of the header and comparing it to the routing database. The list of routing tables outlines how to send the data to a specific network location. They use a set of rules to determine the most effective way to transmit the data to the specified IP address.

- To enable communication between other devices and the internet, routers utilize a modem, such as a cable, fiber, or DSL modem. Most routers include many ports that can connect a variety of devices to the internet simultaneously. In order to decide where to deliver data and where traffic is coming from, it needs routing tables.

- A routing table primarily specifies the router's default path. As a result, it might not determine the optimum path to forward the data for a particular packet. For instance, the office router directs all networks to its internet service provider through a single default channel.
- Static and dynamic tables come in two varieties in the router. The dynamic routing tables are automatically updated by dynamic routers based on network activity, whereas the static routing tables are configured manually.

Functions of Router

The router performs below major functions:

1. **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.
2. **Routing:** Routing is the process by which the router ascertains what is the best path for the packet to reach the destination, It maintains a routing table that is made using different algorithms by the router only.
3. **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.
4. **Security:** Routers can be configured with firewalls and other security features to protect the network from unauthorized access, malware, and other threats.
5. **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.
6. **Virtual Private Network (VPN) connectivity:** Routers can be configured to allow remote users to connect securely to the network using a VPN.

Conclusion:

____

____

____

____