EXPERIMENT-2

OBJECTIVE

To study of different type of LAN & Network Equipment's.

THEORY

Local Area Network (LAN)

We're confident that you've heard of these types of networks before – LANs are the most frequently discussed networks, one of the most common, one of the most original and one of the simplest types of networks. LANs connect groups of computers and low-voltage devices together across short distances (within a building or between a group of two or three buildings in close proximity to each other) to share information and resources. Enterprises typically manage and maintain LANs.

Using routers, LANs can connect to wide area networks (WANs, explained below) to rapidly and safely transfer data.

Metropolitan Area Network (MAN)

These types of networks are larger than LANs but smaller than WANs – and incorporate elements from both types of networks. MANs span an entire geographic area (typically a town or city, but sometimes a campus). Ownership and maintenance is handled by either a single person or company (a local council, a large company, etc.).

Wide Area Network (WAN)

Slightly more complex than a LAN, a WAN connects computers together across longer physical distances. This allows computers and low-voltage devices to be remotely connected to each other over one large network to communicate even when they're miles apart.

The Internet is the most basic example of a WAN, connecting all computers together around the world. Because of a WAN's vast reach, it is typically owned and maintained by multiple administrators or the public.

Different Networking Equipment —

Network Hub:

Network Hub is a networking device which is used to connect multiple network hosts. A network hub is also used to do data transfer. The data is transferred in terms of packets on a computer network. So when a host sends a data packet to a network hub, the hub copies the data packet to all of its ports connected to. Like this, all the ports know about the data and the port, for whom the packet is intended, claims the packet.

However, because of its working mechanism, a hub is not so secure and safe. Moreover, copying the data packets on all the interfaces or ports makes it slower and more congested which led to the use of network switch.

Network Switch:

Like a hub, a switch also works at the layer of LAN (Local Area Network) but you can say that a switch is more intelligent than a hub. While hub just does the work of data forwarding, a switch does 'filter and forwarding' which is a more intelligent way of dealing with the data packets.

So, when a packet is received at one of the interfaces of the switch, it filters the packet and sends only to the interface of the intended receiver. For this purpose, a switch also maintains a CAM (Content Addressable Memory) table and has its own system configuration and memory. CAM table is also called as forwarding table or forwarding information base (FIB).

Modem:

A Modem is somewhat a more interesting network device in our daily life. So if you have noticed around, you get an internet connection through a wire (there are different types of wires) to your house. This wire is used to carry our internet data outside to the internet world. However, our computer generates binary data or digital data in forms of 1s and 0s and on the other hand, a wire carries an analog signal and that's where a modem comes in.

A modem stands for (Modulator+Demodulator). That means it modulates and demodulates the signal between the digital data of a computer and the analog signal of a telephone line.

Network Router:

A router is a network device which is responsible for routing traffic from one to another network. These two networks could be a private company network to a public network. You

can think of a router as a traffic police who directs different network traffic to different directions.

Bridge:

If a router connects two different types of networks, then a bridge connects two subnetworks as a part of the same network. You can think of two different labs or two different floors connected by a bridge.

Repeater:

A repeater is an electronic device that amplifies the signal it receives. In other terms, you can think of repeater as a device which receives a signal and retransmits it at a higher level or higher power so that the signal can cover longer distances.

For example, inside a college campus, the hostels might be far away from the main college where the ISP line comes in. If the college authority wants to pull a wire in between the hostels and main campus, they will have to use repeaters if the distance is much because different types of cables have limitations in terms of the distances they can carry the data for.

When these network devices take a particular configurational shape on a network, their configuration gets a particular name and the whole formation is called Network topology. In certain circumstances when we add some more network devices to a network topology, its called Daisy chaining.

Figure 1: Different network equipment

EXPERIMENT-3

OBJECTIVE

Study and verification of standard Network Topologies (Star, Bus, Ring, Mesh etc.)

THEORY

Network Topologies:

LAN physical topology defines the geographical arrangement of networking devices. Topologies are driven fundamentally by two network connection types. A point-to-point connection is a direct link between two devices. For example, when you attach your computer to a printer, you have created a point-to-point link. In networking terms, most of the today's point-to-point connections are associated with modems and PSTN (Public Switched Telephone Network) communications because only two devices share point-to-point connections, it defeats the purpose of a shared network.

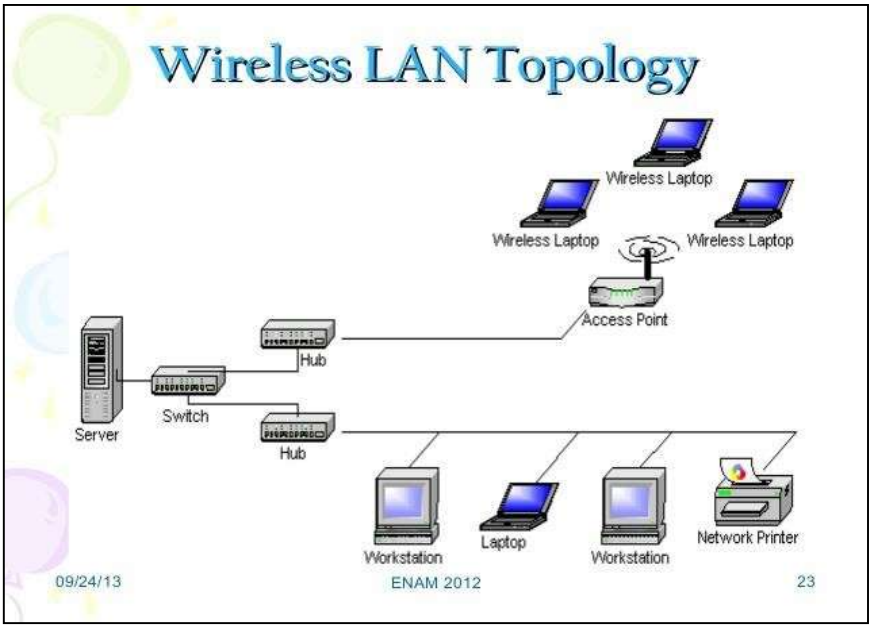


Figure 2: Pictorial Description of LAN Topology

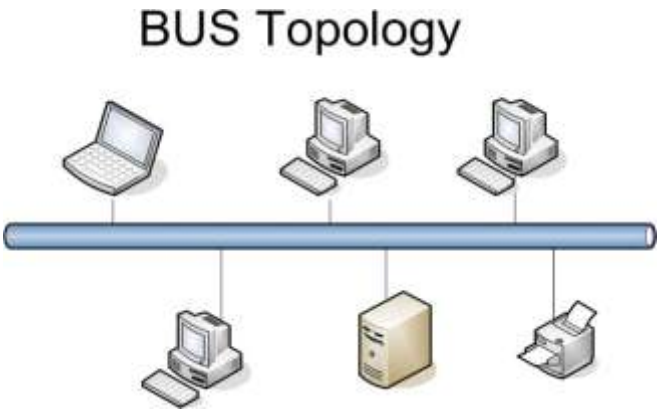
The major topologies of LAN are:

Bus Topology:

The physical bus topology is the simplest and most widely used of the network designs. It consists of one continuous length of cabling (trunk) and a terminating resistor (terminator) at

each end. The data communications message travels along the bus in both directions until it is picked up by a workstation or server NIC.

If the message is missed or not recognized, it reaches the end of the cabling and dissipates at the terminator. All nodes in the bus topology have equal access to the trunk no discriminating here. This is accomplished using short drop cables or direct T-connectors.
This design is easy to install because the backbone trunk traverses the LAN as one cable segment. This minimizes the amount of transmission media required. Also, the number of devices and length of the trunk can be easily expanded. Advantages of Bus Topology: It uses established standards and it is relatively easy to install.



Advantages of Bus Topology:

- It uses established standards and it is relatively easy to install.
- It requires fewer media than other topologies.

Disadvantages of Bus Topology:

- The bus networks are difficult to reconfigure, especially when the acceptable number of connections or maximum distances have been reached.
- They are also difficult to troubleshoot because everything happens on a single media segment. This can have dangerous consequences because any break in the cabling brings the network to its knees.

Ring Topology

As its name implies, the physical ring topology is a circular loop of point-to-point links. Each device connects directly or indirectly to the ring through an interface device or drop cable.

Messages travel around the ring from node to node in very organized manner. Each workstation checks the messages for a matching destination address.

If the address doesn't match, the node simply regenerates the message and sends it on its way. If the address matches, the node accepts the message and sends a reply to the originating sender. Initially, ring topologies are moderately simple to install; however, they require more media than bus systems because the loop must be closed. Once your ring has been installed, it's a bit more difficult to reconfigure. Ring segments must be divided or replaced every time they are changed. Moreover, any break in the loop can affect all devices on the network.

Advantages of Ring Topology:

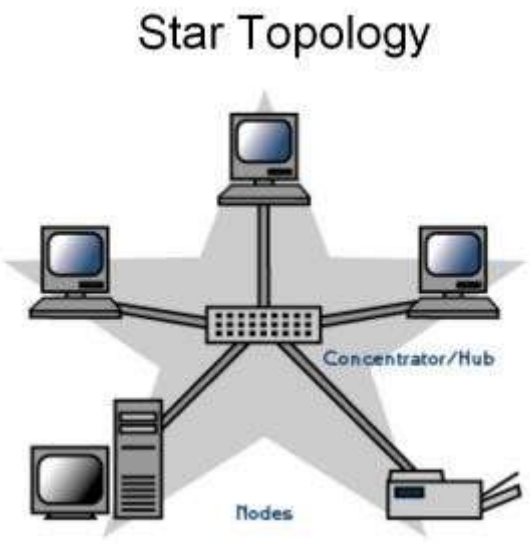
- They are very easy to troubleshoot because each device incorporates a repeater.
- A special internal feature called becoming, allows the troubled workstation to identify them quickly.

Disadvantages of Ring Topology:

- It is considerably difficult to install and reconfigure ring topology.
- Media failure on unidirectional or single loop causes complete network failure.

Star Topology:

The Physical star topology uses a central controlling hub with dedicated legs pointing in all directions like points of a star. Each network devices has a dedicated point-to-point link to the central hub. This strategy prevents troublesome collisions and keeps the line of communication open and free of traffic.



Star topologies are somewhat difficult to install because each device gets its own dedicated segment. Obviously, they require a great deal of cabling. This design provides an excellent platform for reconfiguration and troubleshooting. Changes to the network are as simple as plugging another segment into the hub. In addition, a break in the LAN is easy to isolate and doesn't affect the rest of the network.

Advantages of Star Topology:

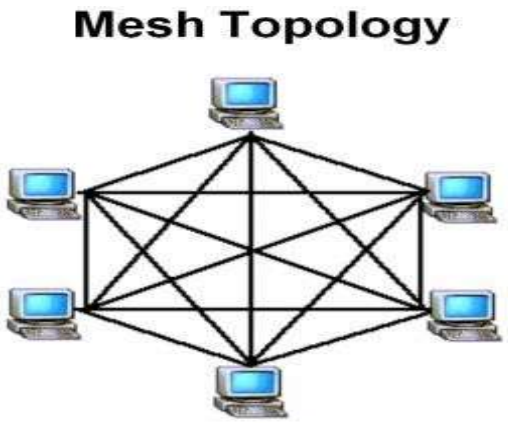
- Relatively easy to configure.
- Easy to troubleshoot.
- Media faults are automatically isolated to the failed segment.

Disadvantages of Star Topology:

- Requires more cable than most topologies.
- Moderately difficult to install.

Mesh Topology

The mesh topology is the only true point-to-point design. It uses a dedicated link between every device on the network. This design is not very practical because of its excessive waste of transmission media. This topology is difficult to install and reconfigure.



Moreover, as the number of devices increases geometrically, the speed of communication also becomes slow. ATM (Asynchronous Transfer Mode) and switched Hubs are the example of high-speed Mesh implementation.

Advantages of Mesh Topology:

- Easy to troubleshoot because each link is independent of all others.
- You can easily identify faults and isolate the affected links.
- Because of the high number of redundant paths, multiple links can fail before the failure affects any network device.

Disadvantages of Mesh Topology:

It is difficult to install and reconfigure especially as the number of devices increases.