Introduction to Networks

A network is a connected system of objects or people. The most common example of a network is the telephone system, which is widely known as the Public Switched Telephone Network (PSTN). The PSTN allows virtually everybody, anywhere in the world to communicate with anyone who has access to a telephone.

A computer network works similar to the PSTN. It allows users to communicate with other users on the same network by transmitting data on the medium used to connect them. A computer network, is defined as having two or more devices such as workstations, printers, or servers. These devices are linked together for the purpose of sharing information, resources, or both. Network links may be copper cables, fiber-optic cables, or wireless connections. The information and resources shared on a network can include data files, application programs, printers, modems, or other hardware devices.

Protocols

No matter what kind of computers the network uses and what software the computers are running, they must have a common language to understand each other. These common languages are called protocols, and computers use many of them during even the simplest exchanges of network data. The protocol is a set of rules that governs data communications.

Protocol elements:-

Protocols define what is communicated, how it is communicated and when it can be communicated. The key elements of any protocol are:-

1. Syntax:- It refers to the structure or format of data. In other words it expresses the way in which the data can be presented.
2. Semantics:- refers to the meaning of each section or field of the data. It defines how each section is interpreted and what action is to be taken depending on that interpretation.
3. Timing: - it defines when the data should be sent and how fast it could be sent.

Protocols' functions

Protocols usually have one or more of the following functions:-

- Packet acknowledgment : This is the transmission of a return message by the recipient to verify the receipt of a packet or packets, where the packet is the fundamental unit of data transmitted over a LAN.

- Segmentation : This is the division of a lengthy data stream into segments sufficiently small for transmission over the network inside packets.
- Flow control : This is the generation by a receiving system of messages that instruct the sending system to speed up or slow down its rate of transmission.
- Error detection : This is the inclusion of special codes in a packet that the receiving system uses to verify that the content of the packet wasn't damaged in transit.
- Error correction : This is the generation by a receiving system of messages that informs the sender that specific packets were damaged, it includes the way to repair this damage such as asking the sender to retransmit.
- Data compression : This is a mechanism for reducing the amount of data transmitted over a network by eliminating redundant information.
- Data encryption : This is a mechanism for protecting the data transmitted over a network by encrypting it using a key already known by the receiving system.
- Encapsulation : This is the process of adding control information to the front of a block of data as a header or/and to the end of a block of data as a footer. This additional data can be used for addressing, error control, synchronization or many other purposes.
- Addressing : It is the definition of the source and destination of the data. The source and the destination can be an application, a logical address, or a physical device.

Networks Classified by Geography:-

Geographically, networks can be sorted into five classes:-

1. Personal Area Networks (PAN)
2. Local Area Network (LAN)
3. Metropolitan Area Network (MAN)
4. Wide Area Network (WAN)
5. Global Area Network (GAN)

1-PAN

PAN is a network that serves a single person or a small workgroup and is characterized to limited distance, limited speed, and low volume. PANs have traditionally been used to transfer data between a laptop or PDA and a desktop PC or printer using IR or Bluetooth technologies.

2- LAN

A LAN can connect many computers in a relatively small geographical area. These areas can be in a home, an office, or a campus. A LAN is usually characterized by three primary attributes: its topology, its medium, and its protocols.

- The topology is the pattern used to connect the computers together. Examples are bus and ring topologies.
- The network medium is the actual physical connection between the networked computers.
- The protocol, as defined earlier, is the common language necessary for the networked devices to communicate,

In most cases all computers on a LAN use the same medium, topology and protocols.

LANs are often designed to do the following:

- Operate within a limited geographic area.
- Allow many users to access high-bandwidth media.
- Connect physically adjacent devices.
- Usually private owned by a person, school, company, etc.

Ethernet and WiFi networks are the most common examples on LANs.

3-MAN

It is a network designed to be extend over an entire city (usually the range of MANs extends up to 100 miles) , it may be a single network or may be consists of many interconnected LANs. MANs may be owned and operate by private company or usually a public company. FDDI and WiMax networks are good examples on MANs.

4-WAN

WAN connects devices across a large distance that often crosses the geographical boundaries of cities or states. WAN connections can use telephone lines, radio waves, or any one of many other technologies. WAN coverage can be up to 1000 miles.

For economic and technical reasons, LANs are not suitable for communications over long distances. On a LAN, the computers must coordinate their use of the network and this coordination takes time. Long distances have greater delays in communication. The computers would take more time coordinating the use

of the shared medium and less time sending data messages. In addition, the costs of providing high-speed media over long distances are much greater than in the case of LANs. For these reasons, WAN technologies differ from LANs.

WANs use point-to-point or point-to-multipoint, serial communications lines. Point-to-point lines connect only two locations, one on each side of the line. Point-to-multipoint lines connect one location on one side of the line to multiple locations on the other side. They are called serial lines because the bits of information are transmitted one after another in a series.

Some of the common WAN technologies are analog modems, T1, T3, E1 and E3.

WANs usually:-

- Operate over large geographical area
- Owned and operated by public companies.

5- GAN

GAN provides connectivity between countries around the globe. Internet is the most obvious example on GANs where it connects a huge number of LANs, MANs, and WANs into an interconnected network.

Packet Switching and Circuit Switching:-

- ### Packet switching

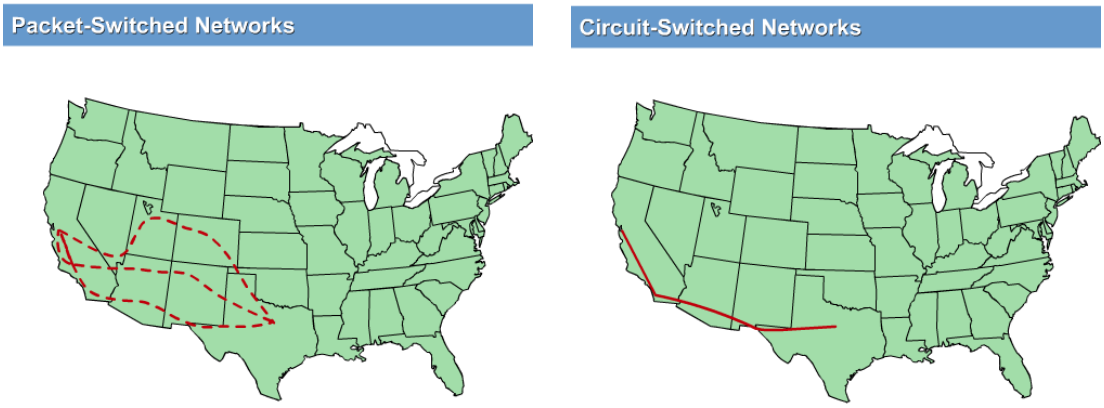
Here data is divided into packets where each individual packet of data can take a different route. With a packet-switched network, no dedicated pathway or circuit is established. Using a packet-switched network to transfer data enables each individual packet to take a different route when going from one computer to another. Although it all arrives at the same destination, it does not all travel the same path to get there. Internet traffic uses packet-switching technology

- ### Circuit switching

The alternative to a packet-switching network is a circuit-switching network, in which the two systems wanting to communicate establish a path through the network that connects them (called a circuit) before they transmit any information. That circuit remains close throughout the life of the exchange and is broken only when the two systems are finished communicating. This is an impractical solution for computers on a baseband network, because two systems connected by a circuit could take the network medium for long periods of time, preventing other systems from communicating.

If the same number is called another time from the same location the path would probably not be the same. The circuit is created by a series of switches that use currently available network paths to set up the call end-to-end. This explains why

callers can get a clear connection one day, and noise and static on another. This demonstrates that a circuit-switched connection is end-to-end or point-to-point. And a good example on circuit switching is the telephone network.



Transmission modes

A data channel, over which a signal is sent, can operate in one of three modes: simplex, half-duplex, or full-duplex.

1-Simplex

Simplex transmission is a single one-way usually baseband transmission. Simplex transmission, as the name implies, is simple. It is also called unidirectional because the signal travels in only one direction. An example of simplex transmission is the signal sent from the TV station to the home television.

2-Half-duplex

In half-duplex mode, transmission is possible in both directions but not at the same time. Thus half duplex lines are called either-way lines. An example of a half-duplex communication system is a two-way radio.

3-Full-duplex

Two systems that can communicate in both directions simultaneously are operating in full-duplex mode. The most common example of a full-duplex network is the telephone system.

Segments and backbones

When a small network begins to grow, it is possible to connect LANs together in a haphazard manner for a while. However, building a large enterprise network by connecting many LANs is a complex undertaking that requires careful planning. One of the most common designs for a network of this type is a series of segment LANs connected by a backbone LAN.

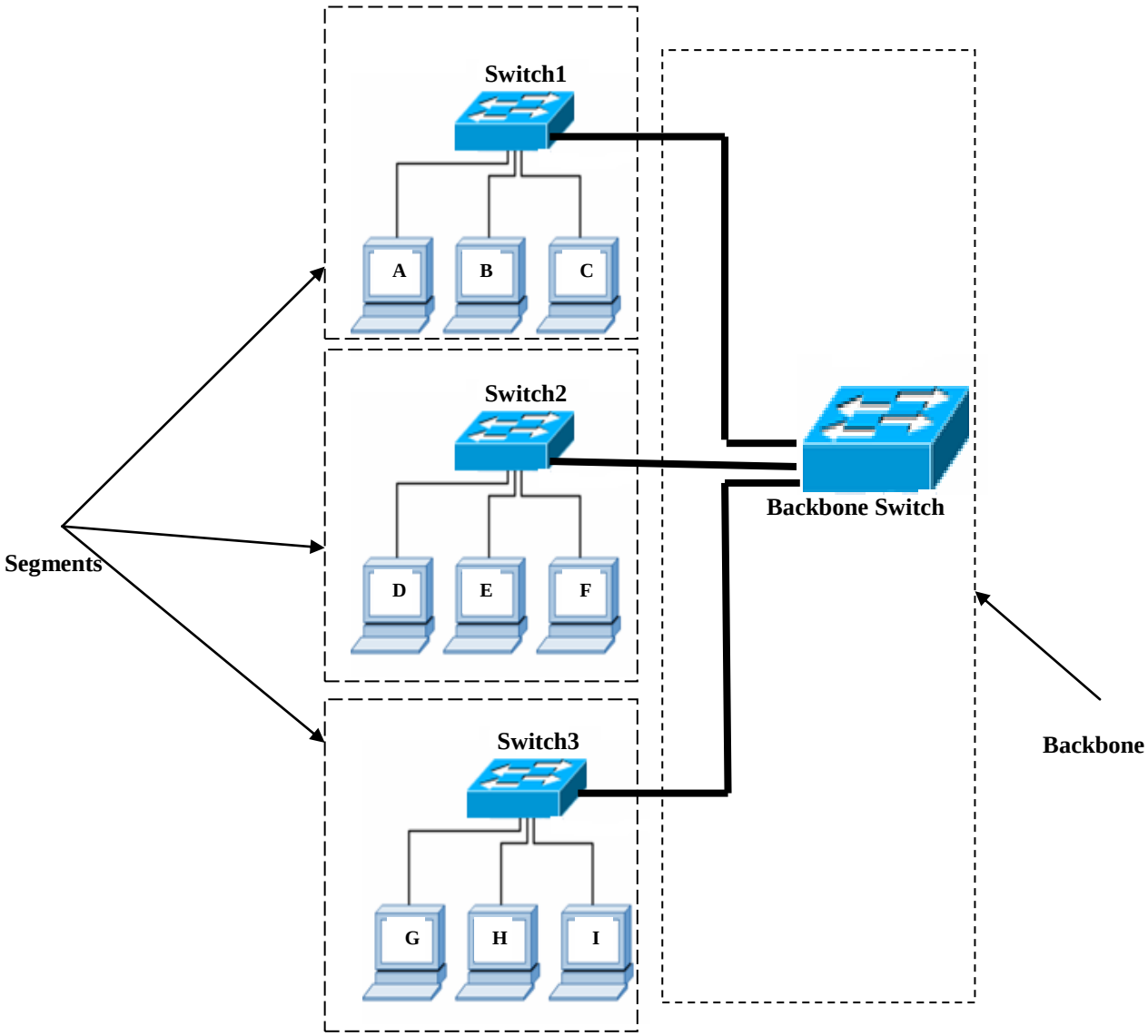
- **Segment**

The term segment refers to a LAN composed of user workstations and other end-user devices, such as servers, printers, IP phones, etc.

▪ Backbone

The backbone exists primarily as a conduit that enables the segments to communicate with each other. One common configuration for an office building with multiple floors calls for a horizontal segment connecting all of the workstations on each floor and a backbone running vertically from the top of the building to the bottom, connecting all of the segments. Such a configuration is illustrated in the following figure.

In many cases, the backbone network runs at a higher speed than the segments and may also use a different type of network medium. First, the backbone by definition must carry all of the internetwork traffic generated by all of the segments, and a faster protocol can prevent the backbone from becoming a bottleneck. Second, the backbone may have to span a much longer distance than the segments.



Client/Server vs. Peer-to-Peer Networks

Network elements can interact with each other on a network in different ways and fulfill different roles. There are two primary networking architectures used to define this interaction especially in LANs, called client/server and peer-to-peer

▪ Client/Server

On a client/server network, certain computers act as servers and others act as clients.

- A server is simply a computer (or more precisely, an application running on a computer) that provides a service to other computers.
- A client is a computer that avails itself of the services provided by servers.

Some of the most important advantages of client/server networks are

- Centralized management.
- Centralized backup and maintenance.
- Easy access to information and resources.
- Higher security.

While the main drawbacks in client server networks are:

- High cost.
- They introduce a single point of failure.
- Need more trained and expert staff to administrate and maintain.

▪ Peer-to-peer

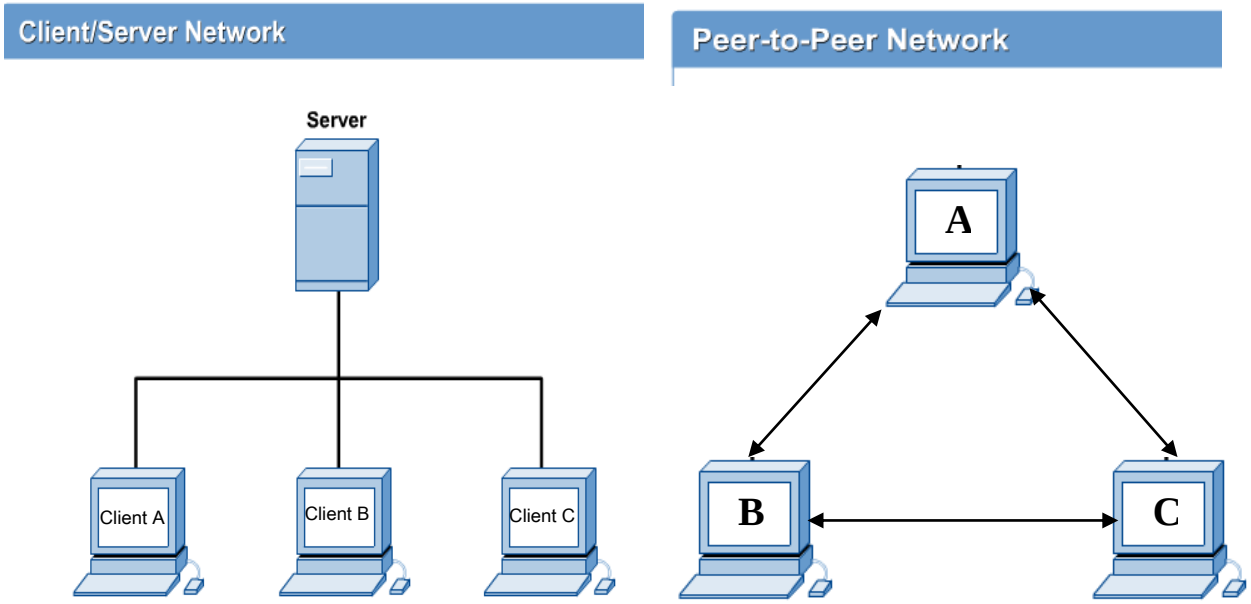
On a peer-to-peer network, every computer is an equal and functions as both a client and a server. This means that any computer can share its resources with the network and access the shared resources on other computers. Peer-to-peer networks are generally limited to 10 or 15 nodes or fewer on a single LAN, because each system has to maintain its own user accounts and other security settings.

Main features of peer-to-peer networks are

- Easy to install.
- Low cost.

While the main drawbacks are

- No centralized backup.
- Difficult to manage where there is no centralized management.
- Limited scalability.
- Less secure than client/server networks



Data transfer can be measured in three ways:

- Digital Bandwidth
- Throughput
- Goodput

▪ Digital Bandwidth

Bandwidth is the measure of how much information can flow from one place to another in a given amount of time. There are two common uses of the word bandwidth: one deals with analog signals, and the other with digital signals. Here we will work with digital bandwidth, calling it bandwidth for simplicity. Digital bandwidth is measured in terms of bits / sec.

The practical bandwidth of a network is determined by a combination of factors: the properties of the physical media and the technologies chosen for signaling and detecting network signals.

▪ Throughput

Throughput refers to actual, measured bandwidth at a specific time. Unfortunately, for many reasons, the throughput is often far less than the maximum possible digital bandwidth of the medium that is being used. Some of the main factors that determine throughput and bandwidth include the following:-

- Networking devices and medium.
- Type of data being transferred
- Topology
- Number of users
- User's computer
- Server computer

Goodput:-

A third measurement has been created to measure the transfer of usable data. That measure is known as goodput. Goodput is the measure of usable data transferred over a given period of time, and is therefore the measure that is of most interest to network users.

Unlike throughput, which measures the transfer of bits and not the transfer of usable data, goodput accounts for bits devoted to protocol overhead. Goodput is throughput minus traffic overhead for establishing sessions, acknowledgements, and encapsulation.

As an example, consider two hosts on a LAN transferring a file. The bandwidth of the LAN is 100 Mbps. Due to the sharing and media overhead the throughput between the computers is only 60 Mbps. With the overhead of the encapsulation process of the TCP/IP stack, the actual rate of the data received by the destination computer, goodput, is only 40Mbps.

▪ Transfer time calculation

It is usually observed that the time needed to transfer an amount of data over a network medium is more than the time theoretically allowed by the medium or the communication protocol, this indeed is due to the fact that you always use the throughput transfer rate not the digital bandwidth of the channel. The following equations roughly estimate the transfer time

$$T = S / BW$$

$$t = S / P$$

T : theoretical transfer time in seconds

t : actual transfer time in seconds

S: file or data size in bits

BW: digital BW of the channel in bits/seconds

P: actual throughput at the moment of transfer