BACHELOR OF COMPUTER APPLICATIONS

SEMESTER 3

DCA2201

COMPUTER NETWORKING

Unit 1

Introduction to Computer Networks

Table of Contents

1. INTRODUCTION

A group of devices connected by a communication link is known as computer networks. These devices are often called nodes. Devices can be a computer, printer or any other device capable of sending and receiving data generated by other nodes on the network. Nowadays a revolution is taking place in the fields of communications and networking. Communication and networking technologies together enable us to exchange data such as text, audio and video from the farthest point in the world.

In this unit, we are going to discuss different hardware used in networking. In the next session, we will discuss network edge, and different ways to connect computers in a network. Then we will discuss the two important reference models, TCP/IP (Transmission Control Protocol/Internet Protocol) and OSI (open System Interconnection) model.

In the last session, we will discuss about network performance and the history of networking.

1.1 Objectives

After studying this unit, you should be able to:

- *Describe different network hardware*
- *Explain network edge*
- *Describe two reference models*
- *Describe network performance*
- *Explain the history of networking*

2. NETWORK HARDWARE

A group of physical or networked devices known as "network hardware" are necessary for interaction and communication among hardware components operating on a computer network. These are specialized hardware elements that link to one another and allow a network to run smoothly and effectively.

Due to its assistance for scalability, network hardware is crucial as industries develop. Depending on the requirements of the organization, it incorporates any number of components. Hardware for networks enables successful communication, raising business standards in the process. Additionally, it encourages multiprocessing and makes resource, data, and software sharing simple.

Twisted pair or fiber cable is used as the connecting medium by network equipment, which is a component of Ethernet network protocol improvements. Examples of network hardware include routers, hubs, switches, and bridges.

Let's take a closer look at the core components of a computer network.

Modems:

- Computers can connect to the internet using a modem to connect over a phone line.
- The modem at one end transforms the digital signals from the computer into analogue signals and transmits them via a phone line.
- On the other end, it transforms the analogue signals into digital signals that a different computer can understand.

Routers:

- Two or more networks are connected by a router. The router is frequently used to link a LAN (local area network) in a house or office to the internet (WAN).
- Along with connections to link computers on the LAN, it typically includes an internet cable hooked in.
- As an alternative, a network device can have a wireless (Wi-Fi-enabled) LAN connection. Wireless access points is another name for them (WAPs).

Hubs, bridges, and switches:

Hubs, bridges, and switches are networking components that enable several devices to connect to a router and permit data transit to every device on a network. A router is a sophisticated device that has hub, bridge, and even switch functionality.

Hub:

- Data is broadcast to all networked devices by a hub.
- Because many computers might not need to receive the transmitted data, it uses a lot of bandwidth.
- A wired or wireless LAN might be used to connect the hub to a few gaming consoles for a local multiplayer game.

Bridge:

- Two different LAN networks are connected by a bridge. Before transmitting a message, it looks for the receiving device.
- This suggests that it prevents pointless data transfers in the absence of a receiving device.
- Additionally, it confirms that the recipient device has not already received the message.
- The network performs better as a whole thanks to these techniques.

Switch:

- A switch serves the same purpose as a hub or a bridge but is more powerful.
- It keeps track of the MAC addresses of network devices and only sends data packets to those that have asked for them.
- As a result, a switch becomes more effective when there is a strong demand since the latency is decreased.

Cables:

On a network, cables link the various devices together. Since cables are more secure than wireless connections nowadays and can carry more data per second while doing so, most networks use them instead of wireless connections.

Information is transmitted from a source to a receiver via a transmission medium. Transmission mediums are regulated by the physical layer, which they are located beneath. Transmission medium is another name for communication channels.

There are 2 types of transmission media:

- Guided
- Unguided

Other names for directed transmission media are bounded media and wired media. They are made up of wires or cables that transmit data. Because they serve as a physical connection between the transmitter and receiving devices, they go by the label "guided." The signal that can flow via these mediums is constrained by their physical properties. As follows:

- Secure high-speed links.
- Generally used for shorter distances.

Twisted Pair Cable:

This is the most widely used transmission medium cable. It consists of two distinct insulated conductor wires coiled around each other. Several similar pairs are usually packed together in a protective sheath.

Unshielded Twisted Pair:

Characteristics:

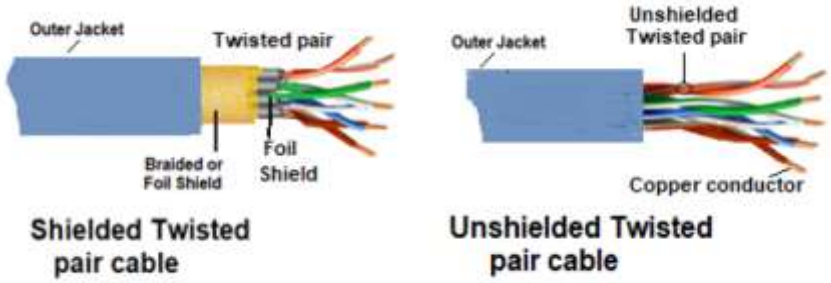
- Offers a fast connection.
- The least expensive.
- Easy to set up
- There is a chance of outside meddling.

- It performs and has a smaller capacity compared to Shielded Twisted Pair.

Shielded Twisted Pair:

Characteristics:

- Insulated twisted pair cable is not particularly expensive or inexpensive.
- It has greater attenuation.
- A higher data transmission rate is possible because to its shielding.

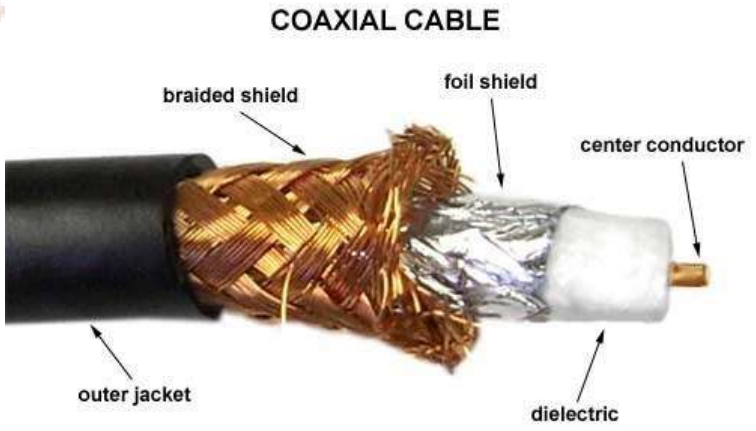


Coaxial Cable:

It has two parallel conductors, each with its own insulated protective cover, and an outer plastic covering. Baseband and broadband are the two modes of operation.

Applications:

Coaxial cables are commonly used in cable TV and analogue television networks.



Optical Fibre Cable:

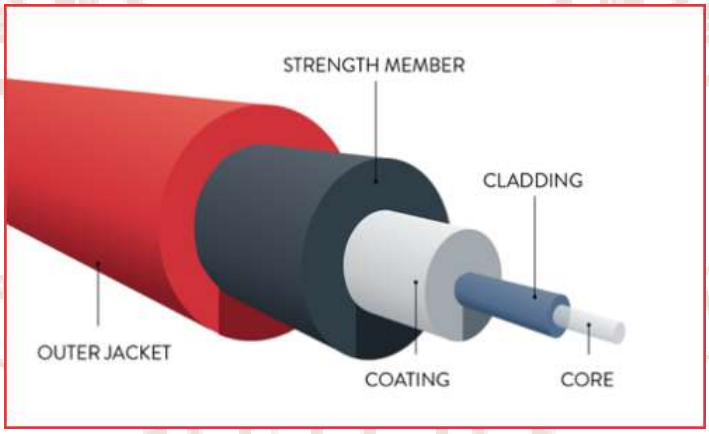
- It operates on the idea of light reflection through a glass or plastic core.
- The core is enclosed by the cladding, which is a thinner layer of glass or plastic.
- In large-volume data transport, it is useful.
- The cable may have a unidirectional or bidirectional configuration.

Optical fibre cable components:

Core: A thin strand of glass or plastic makes up the core of an optical fibre. The portion of the fibre that transmits light is called the core. The size of the core affects how much light is transmitted into the fibre.

Cladding: Glass that is layered in a concentric pattern is referred to as cladding. The cladding's main purpose is to lower the refractive index at the core-interface, which causes reflection inside the core and permits light waves to flow through the fibre.

A jacket is a particular kind of plastic protective layer. A jacket's main purpose is to keep you warm.



Unguided Transmission Media:

It is also possible to transfer electromagnetic signals without a physical medium. They are additionally referred to as wireless or unrestricted transmission media.

Unguided media have certain characteristics.

- Secure compared to directed media.
- Utilized over greater distances.

There is no generally accepted classification in to which all networks fit. Taxonomy varies based on transmission technology and scale. Broadcast links and point-to-point links are the two transmission technologies that are in widespread use. Point-to-point links connect individual pairs of machines. Multiple routes are possible in this method, and finding best path is important in point-to-point networks. Point-to-point transmission with exactly one sender and exactly one receiver is known as unicasting.

In broadcast network, communication channel is shared by all the machines on the network. Broadcast systems allow the possibility of addressing a packet to all the destinations by specifying a special code in the address field. This packet is received and processed by every machine on the network. This method of operation is called broadcasting. Few broadcast systems also support transmission to a subset of the machines, which is known as multicasting.

Another criterion for classifying networks is by scale. Distance is an important classification metric. In the following sections, we will discuss different network hardware by scale.

- **Personal Area Networks (PAN):** In this network, devices communicate over the range of persons in communication. Different components can be connected using cables or short-range wireless network called Bluetooth also available to connect these components without wires.
- **Local Area Networks (LAN):** A Local Area Network (LAN) is a private owned network that can be operated within and nearby a single building like home or office. This is widely used to connect personal computers and electronic devices to share resources. Wireless LANs are very popular nowadays. There is a standard for wireless LANs called IEEE802.11, popularly known as WiFi.
- **Metropolitan Area Networks (MAN):** A MAN (Metropolitan Area Network) covers a city. Cable television networks are the best-known example of MANs.
- **Wide Area Networks (WAN):** A WAN (Wide Area Network) covers a large area, often a country or a continent. Computers that connect together in this network are called

hosts and the network that connects these hosts is called the communication subnet or subnet. Subnet consists of transmission lines and switching elements. Transmission lines move bits between machines, and switching elements are specialized computers that connect two or more transmission lines.

- **Internetworks:** A collection of interconnected networks is called internetwork or internet. In this type of network, different and frequently incompatible networks are connected.

Self-Assessment Questions - 1

1. In a network, device connected are known as_____.
2. Point-to-point transmission with exactly one sender and one exactly one receiver is known as _____ .
3. In_____network, communication channel is shared by all the machines on the network.
4. A collection of interconnected networks is called _____ .

3. NETWORK EDGE

We are now going to explain about the components of the Internet. We begin in this section at the edge of the network and look at the components with which we are most familiar, the computers (e.g., PCs and workstations) that we use on a daily basis.

3.1 End Systems, Clients And Servers

In computer networking, Computer that connects together in the network is called **host** or **end system**. They are referred to as "hosts" because they (host) run application-level programs such as a Web browser or server program, or an e-mail program. They are also referred to as "end systems" because they sit at the "edge" of the Internet, as shown in Figure 1.1.

Hosts can be further divided into two categories: *clients* and *servers*. Informally, clients often tend to be desktop PC's or workstations, while servers are machines which provide certain services to clients. But there is a more precise meaning of a client and a server in computer networking. In the so-called *client-server model*, a client program running on one end system requests and receives information from a server running on another end system. This client-server model is undoubtedly the most common structure for Internet applications. The Web, e-mail, file transfer, remote login, new groups and many other popular applications adopt the client- server model. Since a client typically runs on one computer and the server runs on another computer, client-server Internet applications are, by *definition, distributed applications*. The client and the server interact with each other by communicating (i.e., sending each other message) over the Internet. At this level of abstraction, the routers, links and other "pieces" of the Internet serve as a "black box" that transfers messages between the distributed, communicating components of an Internet application. This is the level of abstraction depicted in Figure 1.1.

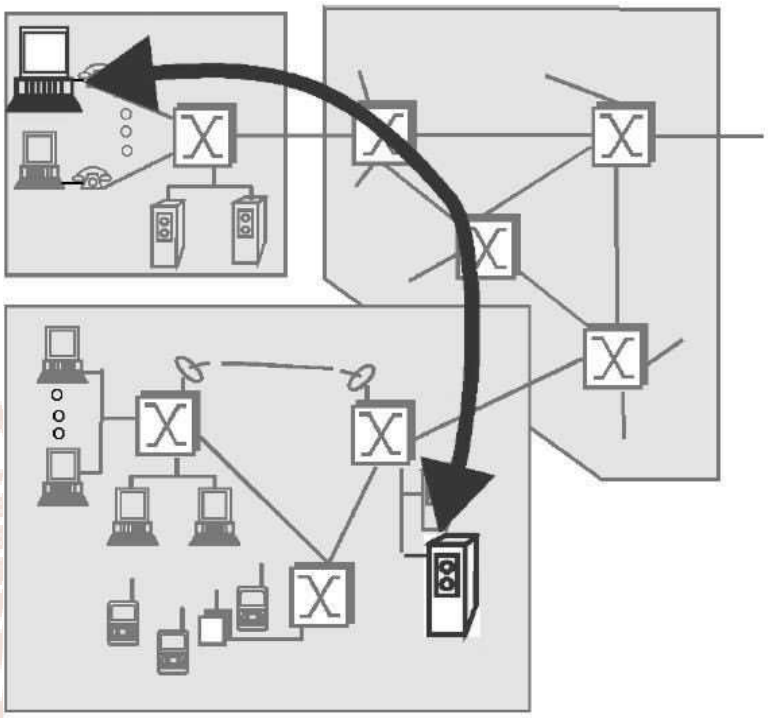


Figure 1.1: End System Interaction

3.2 Connectionless And Connection-Oriented Services

We know that end systems exchange messages with each other according to an application-level protocol in order to accomplish some tasks. The links, routers and other pieces of the Internet provide the means to transport these messages between the end system applications. The Internet, and more generally TCP/IP networks, provide two types of services to its applications; they are connectionless service and connection-oriented service. A developer creating an Internet application (e.g., an email application, a file transfer application, a Web application or an Internet phone application) must program the application to use one of these two services. These two services are explained below.

Connection-Oriented Service

When an application uses the connection-oriented service, the client and the server (residing in different end systems) send control packets to each other before sending packets with real

data (such as e-mail messages). This procedure is called handshaking. Handshaking alerts the client and server, allowing them to prepare for communicating the data packets.

Once the handshaking procedure is finished, a "connection" is said to be established between the two end systems. But the two end systems are connected only till they exchange the data packets, hence the terminology "connection-oriented" is used for this type of connection services. In particular, only the end systems themselves are aware of this connection; the packet switches (i.e., routers) within the Internet are completely unmindful to the connection. This is because a TCP connection is nothing more than allocated resources (buffers) and state variables in the end systems. The packet switches do not maintain any connection state information.

Connection oriented service offers other services such as reliable data transfer, flow control and congestion control. Reliability means an application can trust a connection to deliver all of its data without error and in proper order. Reliability can be achieved through the use of acknowledgments and retransmission. In a reliable transmission between end systems A and B, when B receives a packet from A, it sends an acknowledgment. When A receives the acknowledgment, it can make sure that the packet has been delivered. In the other way, if it hasn't received the acknowledgment, then it assumes that the packet was not received by B. Therefore, it will retransmit the packet.

Flow control is the process that manages the rate of transmission between sender and receiver such that neither side of a connection overwhelms the other side by sending too many packets too fast. Flow-control property forces the sender to reduce the rate whenever there is a risk.

Congestion control prevents the network from overloading a portion of the network. In case of congestion, packet loss can occur. To avoid this packet loss, network forces the host (end systems) to diminish the rate at which they send packets into the network during periods of congestion. End systems are alerted to the existence of severe congestion when they stop receiving acknowledgments for the packets they have sent.

Connection-oriented service comes with reliable data transfer, flow control and congestion control. These three features are the essential components of a connection-oriented service.

TCP (Transmission Control Protocol) is the name of the internet's connection-oriented service. TCP provides reliable transport, flow control and congestion control.

Connectionless Service

There is no handshaking with the Internet's connectionless service. When one side of an application wants to send packets to another side of an application, the sending application simply sends the packets. Since there is no handshaking procedure prior to the transmission of the packets, data can be delivered faster. But there are no acknowledgments either, so a source never knows for sure which packets arrive at the destination. Moreover, the service makes no provision for flow control or congestion control. The Internet's connectionless service is provided by UDP (User Datagram Protocol).

Most of the more familiar Internet applications use TCP, the Internet's connection-oriented service. These applications include Telnet (remote login), SMTP (for electronic mail), FTP (for file transfer), and HTTP (for the Web). Nevertheless, UDP, the Internet's connectionless service, is used by many applications, including many of the emerging multimedia applications, such as Internet phone, audio-on demand, and video conferencing.

Criteria	Connection-Oriented	Connection-Less
Connection	Prior connection needs to be established.	No prior connection is established.
Resource Allocation	Resources need to be allocated.	No prior allocation of resource is required.
Reliability	It ensures reliable transfer of data.	Reliability is not guaranteed as it is a best effort service.
Congestion	Congestion is not at all possible.	Congestion can occur likely.
Transfer mode	It can be implemented either using Circuit Switching or VCs.	It is implemented using Packet Switching.
Retransmission	It is possible to retransmit the lost data bits.	It is not possible.
Suitability	It is suitable for long and steady communication.	It is suitable for bursty transmissions.
Signaling	Connection is established through process of signaling.	There is no concept of signaling.
Packet travel	In this packets travel to their destination node in a sequential manner.	In this packets reach the destination in a random manner.
Delay	There is more delay in transfer of information, but once connection established faster delivery.	There is no delay due absence of connection establishment phase.

Self-Assessment Questions - 2

5. Hosts can be further divided into two categories, they are _____ and_____ .
6. Two types of services provided by a TCP/IP network is known as service _____ and service_____.
7. Most of the more familiar Internet applications use _____ , the Internet's connection-oriented service.

4. REFERENCE MODELS

In this section, we will discuss two important network architectures: the OSI (Open System Interconnection) reference model and TCP/IP (Transmission Control Protocol/Internet Protocol) reference model. In the case of OSI model, the protocol associated with the OSI model are not used any more, but the model itself is quite general and still valid and features of each layer are still very important. In the case of TCP/IP model, the protocols are widely used, but the model itself is not much use.

4.1 OSI Reference Model

The OSI Model is based on the protocol developed by ISO (International Standards Organization) as the first step towards international standardization of the protocols used in the various layers. This model deals with connecting open systems, so it is called ISO OSI (Open Systems Interconnection). OSI model has seven layers, each layer is created when a different abstraction is needed, and each layer has well-defined function. The OSI model is shown in figure 1.2. In the following section, we will explain the seven layers of OSI model.

1. **The Physical Layer**

   This layer is concerned with the transmission of raw bits over a communication channel. This layer coordinates the functions required to carry a bit stream over a physical medium. So, it deals with the hardware, such as electrical and mechanical specifications of the interface and transmission medium.

2. **Data Link Layer**

   This layer transforms a raw transmission facility into a reliable link. In the data link layer, the sender breaks up the input data into data frames and transmits the frames sequentially. It makes the physical layer appear error-free to the higher layers like network layer. Other functions of data link layer include framing, error control, flow control, addressing and access control.

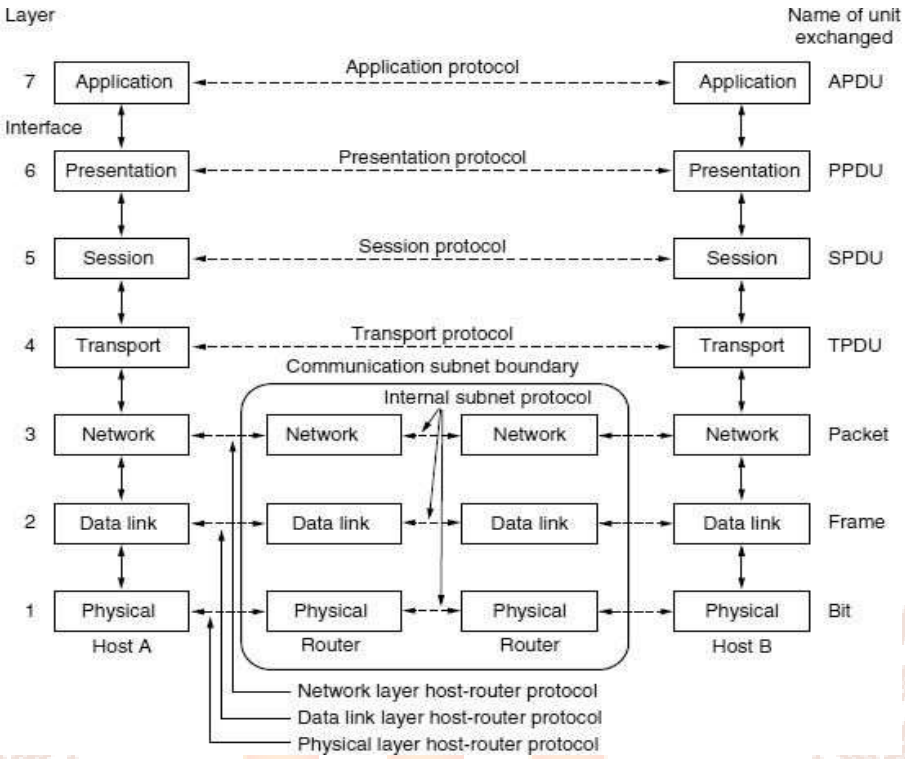


Figure 1.2: The OSI reference model

3. Network Layer

Source- to destination delivery of packets is carried out by this layer. Network layer controls the operation of the subnet. Main responsibility of network layer is the routing of packets to the destination. If too many packets are there in the subnet at the same time, a condition called congestion occurs and this will cause packet loss. Congestion control is another responsibility of the network layer. Logical addressing in a heterogeneous network is another responsibility of network layer.

4. Transport Layer

The transport layer is responsible for process-to-process delivery of the message. This layer is a true end to end layer and carries data from source to destination. The error-free point-to-point channel is the most popular type of transport connection. Other transport services like transporting isolated messages with no guarantee about the order of delivery, and broadcasting of messages to multiple destinations also exist.

Main responsibility of transport layer is to accept data from higher layers break it into smaller units and pass that into lower (network) layer.

5. **Session Layer**

   Dialog control, token management and synchronization are the main responsibilities of session layer. Dialog control is keeping track of whose turn it is to transmit. Token management prevents two hosts from attempting the same critical operation simultaneously. Synchronization means check pointing long transmissions to allow them to pick up from where they left off in the event of a crash and subsequent recovery.

6. **Presentation Layer**

   The presentation layer deals with the syntax and semantics of information transformed. Data structures should be defined in an abstract way in order to allow computers with different internal data representation to communicate. The presentation layer manages these abstract data structures and allows higher-level data structures to be defined and exchanged.

7. **Application Layer**

   The application layer contains a variety of protocols that are commonly needed by users. One widely used application protocol is HTTP (Hyper Text Transfer Protocol), which is the basis for the World Wide Web. When a browser wants a Web page, it sends the name of the page it wants to the server hosting the page using HTTP. The server then sends the page back. Other application protocols are used for file transfer, electronic mail, and network news.

4.2 TCP/IP Reference Model

The TCP/IP (Transmission Control Protocol/Internet Protocol) has become the standard method of interconnecting hosts, networks, and the Internet. The TCP/IP protocol suite is so named for two of its most important protocols: Transmission Control Protocol (TCP) and Internet Protocol (IP). Main aim of TCP/IP is to build an interconnection of networks known

as internet that provides global communication over heterogeneous physical networks. TCP/IP provides standardized abstraction of the communication mechanisms provided by each type of physical network.

TCP/IP model is also modelled in layers. This layered representation leads to the term protocol stack, which refers to the stack of layers in the protocol suite. Each layer provides services to the layer directly above it and makes use of services provided by the layer directly below it. The TCP/IP model is shown in figure 1.3.

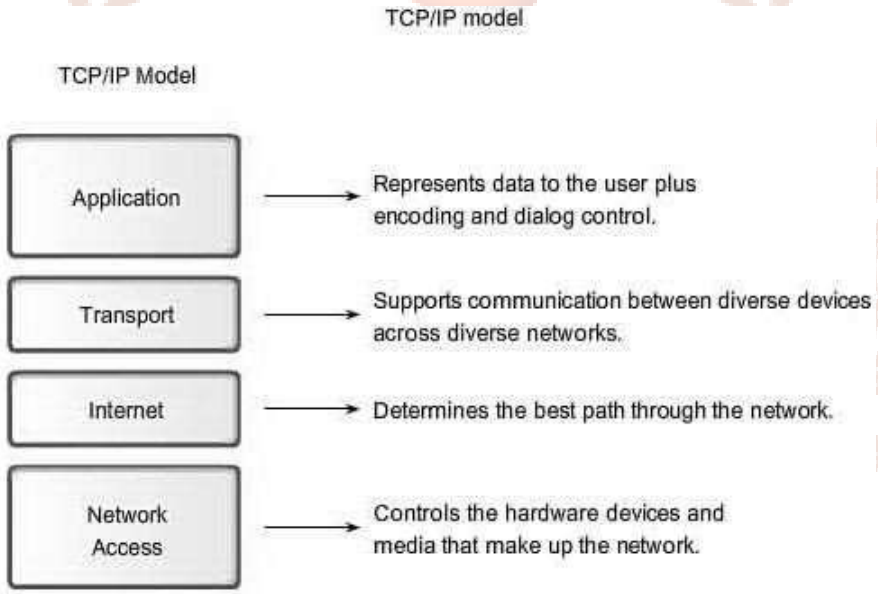


Figure 1.3: TCP/IP Model

Both OSI and TCP/IP reference model is shown in figure 1.4, for comparison.

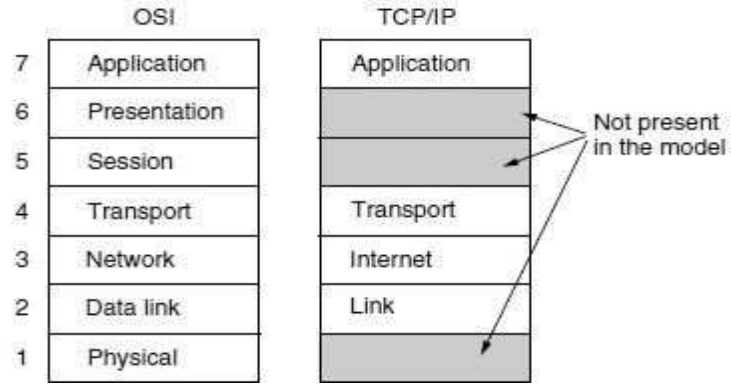


Figure 1.4: Comparison of OSI and TCP/IP reference model

The four layers are explained below:

1. **Link Layer (Network Interface Layer)**

   The lowest layer in the model, the link layer describes what links such as serial lines and classic Ethernet must do to meet the needs of this connectionless internet layer. Link layer is also called network interface layer or the data-link layer. This act as an interface to the actual network hardware that is the interface between hosts and transmission links.

2. **Internet Layer**

   The Internet layer is the backbone that holds the whole architecture together. It allows the hosts to inject packets into any network and have them travel independently to the destination. Internet layer defines a packet format and protocol called IP (Internet Protocol) and a companion protocol called ICMP (Internet Control Message Protocol) that helps it function. The job of the internet layer is to deliver IP packets. Packet routing and congestion control are managed by internet layer.

3. **Transport Layer**

   Transport layer is the layer above internet layer. Two transport protocols have been defined here. The first one is TCP (Transmission Control Protocol), which is a reliable connection-oriented protocol that allows a byte stream originating on one machine to be delivered without error on any other machine in the internet. The second one is UDP (User Datagram Protocol), which is an unreliable connectionless protocol. This is widely used for applications in which prompt delivery is more important than accurate delivery like transmitting speech or video.

4. **Application Layer**

   On top of the transport layer, TCP/IP has an application layer. This layer contains all the higher-level protocols. This includes virtual terminal (TELNET), file transfer (FTP), electronic mail (SMTP), Domain Name System (DNS), for mapping host names onto their network addresses, HTTP, the protocol for fetching pages on the World Wide Web,

and RTP, the protocol for delivering real-time media such as voice or movies and many other.

Self-Assessment Questions - 3

8. The _____ model is based on the protocol developed by ISO.
9. How many layers are there for OSI Reference model?
   (a) 4
   (b) 7
   (c) 3
   (d) 6
10. Which layer is concerned with the transmission of raw bits over a communication channel?
   (a) Physical layer
   (b) Data link
   (c) Network
   (d) Transport
11. 1Source- to destination delivery of packets is carried out by _____ Layer.
12. Which layer deals with the syntax and semantics of information transformed?
   (a) Physical
   (b) Network
   (c) Presentation
   (d) Application
13. The _____ layer contains a variety of protocols that are commonly needed by users.
14. The TCP/IP protocol suite contains two protocols known as _____ and _____ .

5. NETWORK PERFORMANCE

Performance of a network is measured in two fundamental ways. Bandwidth (also known as throughput) and latency (also known as delay). The bandwidth of a network is given by the number of bits that can be transmitted over the network in a certain period of time. For instance, a network might have a bandwidth of 10 million bits/second (Mbps), meaning that it is able to deliver 10 million bits every second. It is sometimes useful to think of bandwidth in terms of how long it takes to transmit each bit of data. On a10-Mbps network, for example, it takes 0.1 microseconds (μs) to transmit each bit.

When talking about the bandwidth of the network as a whole, it can be more precise, focusing, for example, on the bandwidth of a single physical link or of a logical process-to-process channel. At the physical level, bandwidth is constantly improving, with no end in sight. Intuitively, if you think of a second of time as a distance you could measure with a ruler and bandwidth as how many bits fit in that distance, then you can think of each bit as a pulse of some width. For example, each bit on a 1-Mbps link is 1 μs wide, while each bit on a 2-Mbps link is 0.5 μs wide, as illustrated in Figure 1.5.

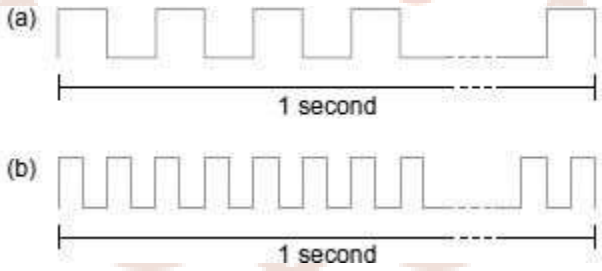


Figure 1.5: Bits transmitted at a particular bandwidth can be regarded as having some width: (a) bits transmitted at 1 Mbps (each bit is 1 μs wide; (b) bits transmitted at 2 Mbps (each bit is 0.5 μs wide).

The more advanced the transmitting and receiving technology, the narrower each bit can become and, thus, the higher the bandwidth. For logical process-to-process channels, bandwidth is also influenced by other factors, including how many times the software that implements the channel has to handle, and possibly transform, each bit of data.

The second performance metric is latency which corresponds to how long it takes a message to travel from one end of a network to the other. There are many situations in which it is more important to know how long it takes to send a message from one end of a network to the other and back, rather than the one-way latency. We call this the round-trip time (RTT) of the network.

Latency has three components. First is the speed-of-light propagation delay. If the distance between two points is known, we can calculate the speed-of light latency, although we have to take care, because light travels across different media at different speeds: It travels at 3.0×108 m/s in a vacuum, 2.3×108 m/s in a copper cable, and 2.0×108 m/s in an optical fiber. Second, there is the amount of time it takes to transmit a unit of data. This is

a function of the network bandwidth and the size of the packet in which the data is carried. Third, there may be queuing delays inside the network, since packet switches generally need to store packets for some time before forwarding them on an outbound link. So total latency can be defined as

Latency = Propagation + Transmit + Queue

Propagation = Distance / Speedlight

Transmit = Size/Bandwidth

Where Distance is the length of the wire over which the data will travel, Speedlight is the effective speed of light over that wire, size is the size of the packet, and Bandwidth is the bandwidth at which the packet is transmitted. If the message contains only one bit and we are talking about a single link, then the Transmit and Queue terms are not relevant, and latency corresponds to the propagation delay only.

Bandwidth and latency combine to define the performance characteristics of a given link or channel. However, their relative importance depends on the application. For some applications, latency dominates bandwidth. For example, a client that sends a 1-byte message to a server and receives a 1-byte message in return is latency bound. In contrast, consider a digital library program that is being asked to fetch a 25-megabyte (MB) image –

the more bandwidth that is available, the faster it will be able to return the image to the user. Here, the bandwidth of the channel dominates performance.

Delay × Bandwidth Product

It is also useful to talk about the product of these two metrics, often called the *delay ×bandwidth product*. Intuitively, if we think of a channel between a pair of processes as a hollow pipe (see Figure 1.6), where the latency corresponds to the length of the pipe and the bandwidth gives the diameter of the pipe, then the delay × bandwidth product gives the volume of the pipe

– the maximum number of bits that could be in transit through the pipe at any given instant.

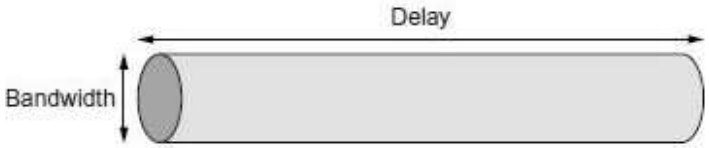


Figure 1.6: Network as a Pipe

The delay × bandwidth product is important to know when constructing high- performance networks because it corresponds to how many bits the sender must transmit before the first bit arrives at the receiver. If the sender is expecting the receiver to somehow signal that bits are starting to arrive, and it takes channel latency for this signal to propagate back to the sender, then the sender can send up one RTT × bandwidth worth of data before hearing from the receiver that transmission is proper.

6. HISTORY OF NETWORKING

The beginning of computer networking was in the early 1960s. At that time, the telephone network was the dominant communication network. Telephone networks use circuit switching to transmit information from a sender to receiver which is a suitable choice to transmit voice at a constant rate between sender and receiver. The following section discusses a brief history of computer networking and internet.

6.1 Development Of Packet Switching 1961-72

The boom of computers in the early 1960's generates the need to connect computers together so that they could be shared among geographically distributed users. Packet switching was developed for this purpose. It is developed by Leonard Kleinrock. This became an efficient and robust alternative to circuit switching. Using queuing theory, Kleinrock's work elegantly demonstrated the effectiveness of the packet-switching approach for burst traffic sources. During this time, Leonard Kleinrock was a graduate student at MIT. At the same time, two other groups were also developing the notion of packet switching. One among them is Paul Baran at the Rand Institute, had investigated the use of packet switching for secure voice over military networks. Same time, Donald Davies and Roger Scantlebury at the National Physical Laboratory in England, were also developing their ideas on packet switching.

Two colleagues of Kleinrock's at MIT .C. R. Licklider [DEC 1990] and Lawrence Roberts, went on to lead the computer science program at the Advanced Projects Research Agency (ARPA) in the United States. And there, Roberts published an overall plan for the so-called ARPAnet, which is the first packet-switched computer network and a direct ancestor of today's Internet. In 1972, the first public demonstration of ARPAnet was given by Robert Kahn at the International Conference on Computer Communications. ARPAnet had grown to approximately 15 nodes by 1972. In 1972, the first e-mail program was written by Ray Tomlinson. Also, the first host-to-host protocol between ARPAnet end systems known as the Network Control Protocol (NCP) was completed.

6.2 Networks and Internetworking 1972-80

Initially, ARPAnet was a single, closed network. Additional packet switching networks other than ARPAnet came into being in the early to mid-1970s. They are: ALOHA net, which is a satellite network linking together universities on the Hawaiian Islands; Telnet, a BBN commercial packet- switching network based on ARPAnet technology; Tymnet; and Transpac, a French packet-switching network.

In 1973, Robert Metcalfe's PhD thesis laid out the principle of Ethernet, which would later lead to a huge growth in so-called Local Area Networks (LANs) that operated over a small distance based on the Ethernet protocol. Creation of a network of network was done by Vinton Cerf and Robert Kahn by pioneering work on interconnecting networks. The term "internetting" was used to describe this work. The principles that Kahn formulated for creating a so-called "open network architecture" are the foundation on which today's Internet is built.

The principles that serve as the foundation of today's internet is: autonomy (which means network should be able to operate on its own), internetworks. By end of 1970's, three key internet protocols that exist today such as TCP, UDP and IP. In Hawaii, Norman Abramson was developing ALOHAnet which is a packet-based radio network that allowed multiple remote sites on the Hawaiian Islands to communicate with each other. ALOHA protocol was the first multiple access protocol that allowed geographically distributed users to share a single broadcast communication medium.

In addition to the DARPA internetworking efforts and the Aloha/Ethernet multiple access networks, a number of companies were developing their own proprietary network architectures. In 1975, Digital Equipment Corporation (Digital) released the first version of the DECnet, which allows two PDP-11 minicomputers to communicate with each other. Substantial parts of the OSI protocol suite being based on ideas initiated in DECnet. In the 1970's, other players were Xerox (with the XNS architecture) and IBM (with the SNA architecture). In the start of 1980's another technology was developed, which contributed to the development of the ATM (Asynchronous Transfer Mode) which is a connection-oriented architecture based on the use of fixed size packets, known as cells.

6.3 Rapid Growth Of Networks 1980-90

1980's would be a time of rapid growth of the Internet. By the end of 1970, around 200 hosts were connected to the ARPAnet. By the end of 1980's, the number of hosts connected to the public Internet would reach 100,000. Growth of networks in early 1980's resulted from the creation of computer networks linking universities together. Two more networks were established in this time, they are BITnet which provided email and file transfers among several universities in the Northeast, and CSNET (Computer Science NETwork)

was formed to link together university researchers without access to ARPAnet. To provide access to NSF- sponsored supercomputing centers, another network named NSFNET was created in 1986. This network had an initial backbone speed of 56Kbps, and it would be running at 1.5 Mbps by the end of the decade, and would be serving as a primary backbone linking together regional networks.

In the late 1980's TCP protocol would be modified by adding important extensions to implement host-based congestion control. In the 1980's, the Domain Name System which is used to map a human –readable host name and its IP address was also developed.

6.4 The Internet Explosion 1990s

In the 1990's, ARPAnet, which is the ancestor of the internet ceased to exist. MILNET and the Defense Data Network had grown in the 1980's to carry most of the US Department of Defense related traffic and NSFNET had begun to serve as a backbone network connecting regional networks in the United States and national networks overseas. Also, in the 1990's, the world (www.world.std.com) became the first public dialup Internet Service Provider (ISP). NSFNET came up with restrictions on use of NSFNET for commercial purposes in 1991 and is decommissioned in 1995 with Internet backbone traffic being carried by commercial Internet Service Providers.

The release of the World Wide Web (WWW) was the main event in the 1990s. The World Wide Web brought the Internet into the homes and businesses of millions and millions of people worldwide. The WWW was invented at CERN by Tim Berners-Lee in 1989-1991. The four key components of the WWW are HTML, HTTP, a Web server and a browser. Berners-

Lee and his associates developed initial versions of these four components. About 200 Web servers were in operation in the end of 1992.

In 1993, Marc Andreesen developed a web browser with GUI interface, which is known as Mosaic for X and in 1994 formed Mosaic Communications, which later became Netscape Communications Corporation. Microsoft move into the Web business in a big way in 1996. There were two-million Web servers in operation in 1999.

6.5 Recent Development

In computer networking, more innovations are taking place at a rapid pace. Advancement has been made on all areas including deployment of new applications, content distribution, Internet telephony, higher transmission speeds in LANs and faster routers. Three developments require special attention, they are: a growth of high-speed access networking, security and P2P networking.

Increasing penetration of broadband residential internet access via cable modem and DSL is providing the platform for new multimedia applications, including streaming high-quality video on demand and high-quality interactive video conferencing. Increasing presence of high-speed public Wi-Fi networks and medium-speed internet access of cellular telephony networks are not only making possible to remain constantly connected, but also enabling an exciting new set of location-specific services.

After the series of denial-of-service attacks on webservers in the late 1990's, network security has become important. These attacks resulted in the development of intrusion detection systems to provide early warning of an attack, use of firewalls to filter out unwanted traffic and use of IP trace back to pinpoint the origin of attacks.

A P2P networking application exploits the resources in user's computers like storage, content, CPU cycles and human presence. KaZaA is the most popular P2P file-sharing system. Its network typically has more than 4 million connected end systems and its traffic constitutes 20 to 50 percent of all internet traffic.

Self-Assessment Questions - 4

15. _____ and _____ are the two matrices to measure the performance of a network.
16. The beginning of computer networking was in _____ .
17. In the 1980's, the _____ which is used to map a human –readable host name and its IP address was developed.

7. SUMMARY

Let us recapitulate the important concepts discussed in this unit:

- A group of devices connected by a communication link is known as a computer network.
- Broadcast links and point-to-point links are the two transmission technologies that are in widespread use.
- Point-to-point transmission with exactly one sender and one exactly one receiver is known as unicasting.
- Computers that connect together in this network is called hosts or end systems.
- Two important network architectures are the OSI reference model and TCP/IP reference model.
- The OSI model deals with connecting open systems, so it is called OSI (Open Systems Interconnection).
- The TCP/IP (Transmission Control Protocol/Internet Protocol) has become the standard method of interconnecting hosts, networks, and the Internet.
- The TCP/IP protocol suite is so named for two of its most important protocols: Transmission Control Protocol (TCP) and Internet Protocol (IP).
- Performance of a network is measured in two fundamental ways. Bandwidth and latency.
- The release of the World Wide Web (WWW) was the main event in the 1990's.
- The WWW was invented at CERN by Tim Berners-Lee in 1989-1991.

8. TERMINAL QUESTIONS

1. Describe briefly on Network edge.
2. Explain OSI reference model.
3. List and explain four layers of TCP/IP model with suitable diagram.
4. Describe the history of networking.

9. ANSWERS

Self-Assessment Questions

1. Nodes
2. Unicasting
3. Broadcasting
4. Internetwork or Internet
5. Clients, servers
6. Connection less, connection oriented
7. TCP
8. OSI 9. (b) 7
9. Physical layer
10. Network
11. (c)Presentation
12. Application
13. TCP,IP
14. Bandwidth, Latency
15. 1960
16. Domain Name System

Terminal Questions

1. In computer networking, Computers that connect together in this network is called hosts or end systems. They are referred to as "hosts" because they host (run) application-level programs such as a Web browser or server program, or an e-mail program. (Refer section 3 for more details).
2. The OSI Model is based on the protocol developed by ISO (International Standards Organization) as the first step towards international standardization of the protocols used in the various layers. This model deals with connecting open systems, so it is called ISO OSI (Open Systems Interconnection). (Refer to section 4.1 for more details).
3. The four layers of TCP model are, link layer, Internet layer, Transport layer and Application layer. (Refer section 4.2 for more details).

4. The beginning of computer networking was in the early 1960s. At that time, the telephone network was the dominant communication network. Telephone networks use circuit switching to transmit information from a sender to receiver which is a suitable choice to transmit voice at a constant rate between sender and receiver. (Refer section 1.6 for more details).

References:

- Andrew S. Tanenbaum, David J. Wetherall, *"Computer Networks*," Fifth edition.
- Larry L. Peterson, Bruce S. Davie, "*Computer Networks- a Systems Approach*," Fifth edition.
- James F. Kurose, Keith W.Ross, "*Computer Networking-A top-down approach*," Sixth edition.
- Behrouz A. Forouzan, Sophia Chung Fegan, "*Data Communication and Networking*," Fourth edition.
- William Stallings, "*Computer Networking with Internet Protocols and Technology*," Third edition.
- https://www.ques10.com/p/9498/compare-connection-oriented-connection-less-servic/
- https://instrumentationapplication.com/what-is-a-twisted-pair-cable/
- https://www.indiamart.com/proddetail/finolex-coaxial-cable-13401967188.html

https://www.ofsoptics.com/optical-fiber-coatings/

https://data-flair.training/blogs/transmission-media-in-computer-network/#:~:text=A%20transmission%20medium%20is%20a,another%20name%20for%20transmission%20medium.