UNIT 1

1. Introduction: Networks, Network types.
2. Network Models: TCP / IP protocol suite, Addressing.
3. The OSI Model.
4. Transmission Modes: Parallel Transmission and Serial Transmission.
5. Link Layer: Data Link Control (DLC): DLC Services, Data Link Layer Protocols.
6. High Level Data Link Control (HDLC).
7. Point-to-Point Protocol (PPP): Framing, Transition phases.
8. Media Access Control (MAC): Random Access: CSMA/CD, CSMA/CA.

1. Introduction

Communication is required for sharing information. When communication is local, it happens face to face, when the communication has to take place remotely distance communication is required. Data communication is basically exchange of data between devices. The main components of data communication include:

1. Data- The information that is to be shared. For example: text, audio, video and images.

2. Sender and receiver- The device that is capable of sending and receiving of messages. It could be a computer, workstation mobile devices etc.

3. Protocol- It is the set of rules that govern the data communications. It is basically an agreement between two communicating devices. In absence of a protocol, the devices are connected but they will not be able to communicate with each other.

4. Transmission Medium- The path by which the data is exchanged between the devices.

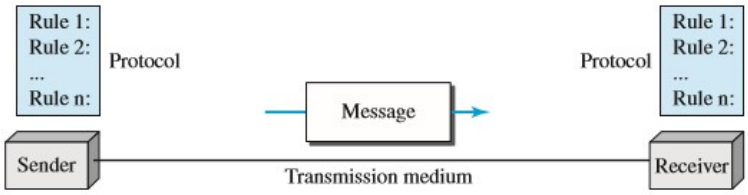


Figure 1. Components of data communications system

1.1 Networks and network types

Definition: Networks is interconnection of set of devices that are able to communicate and interact with other devices. The device could be an end node or a connecting device. The example for the former is a computer system, mobile device, laptop, desktop, security system etc and example for latter is a switch, router, gateways etc.. The devices in the network are connected using a wired or wireless connections.

1.1.1 Network Criteria

A network must be able to meet a certain number of criteria such as performance, reliability and security.

Performance can be measured in transit time and response time.

Transit time is the amount of time required for a message to travel from one device to another.

Response time is the elapsed time between an inquiry and a response.

The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software.

Performance is often evaluated by two networking metrics: throughput and delay. We often need more throughput and less delay. However, these two criteria are often contradictory. If we try to send more data to the network, we may increase throughput but we increase the delay because of traffic congestion in the network.

Reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.

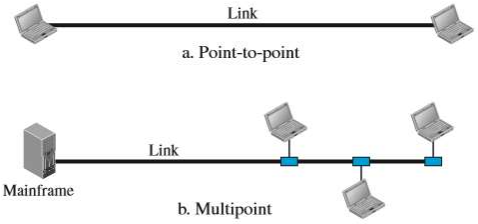
Security include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

1.1.2 Physical Structures

Network is formed by connecting various devices. These devices can be connected in:

Point to point connection: provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible.

Multipoint connection: A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link.

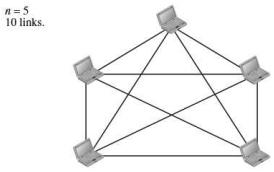


1.2 Network Topologies

The term physical topology refers to the way in which a network is laid out physically. Two or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another. There are four basic topologies possible: mesh, star, bus, and ring.

1.2.1 Mesh Topology

In a mesh topology, every device has a dedicated point-to-point link to every other device.



Properties

1. A dedicated link carries data between two devices only, thus provides high reliability.
2. A mesh topology is robust- If one link becomes unusable, it does not incapacitate the entire system.
3. Provides privacy and data security- When every message travels along a dedicated line, only the intended recipient sees it.
4. Point-to-point links make fault identification and fault isolation easy.

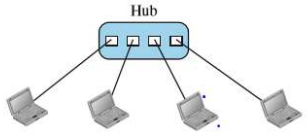
5. Requires more amount of cabling and I/O ports.
6. Hence laying down the network in mesh topology is expensive.

Applications

Used in backbone networks, for example- connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

1.2.2 Star topology

In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub.



Properties

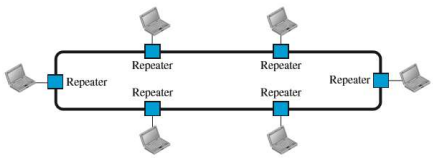
1. Does not allow direct data transfer between devices, the central controller acts as an exchange.
2. Less expensive than mesh topology and it is easy to install and reconfigure.
3. The topology is robust, if one link fails only that device/link is affected hence easy to identify faults and fault isolation.
4. Since central controller controls the entire network, if it goes down the entire network is affected.

Applications

Used in Local Area networks(LAN)

1.2.3 Ring topology

In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.



Properties

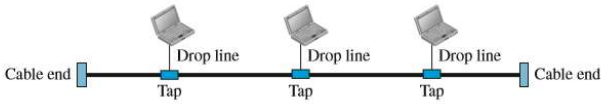
1. Relatively easy to install and reconfigure as each device is linked to only its immediate neighbours (either physically or logically)addition or deletion requires changing only two connections.
2. Signal is circulating in a ring at all times, if one device does not receive a signal within a specified period, it can issue an alarm which alerts the network operator to the problem and its location.
3. The breakage of the link may disable the entire network, this is overcome by using a dual ring or a switch capable of closing off the break.

Applications

In Local Area Networks – IBM token ring.

1.2.4 Bus topology

Provides a multipoint connection where one long cable acts as a backbone to link all the devices in a network.



The nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable. A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core.

As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.

Properties:

1. Ease of installation- Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths.
2. Installation cost is less as redundancy is eliminated.
3. Reconnection and fault isolation is difficult also signal reflection at the taps can degrade the quality of the signal.
4. A fault or break in the bus cable stops all transmission, even between devices on the same side of the problem. The damaged area reflects signals back in the direction of origin, creating noise in both directions.

1.3 Network Types

Networks can be classified based on the geographical area they cover as Local Area Networks(LAN), Wide Area Networks(WAN) and Internet.

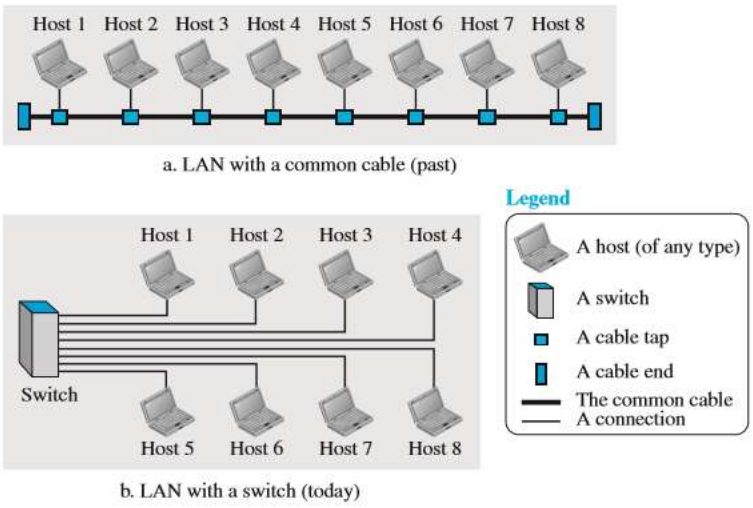
1.3.1 Local Area Networks

A local area network (LAN) is usually privately owned and connects some hosts in a single office, building, or campus. Depending on the needs of an organization, a LAN can be as simple as two PCs and a printer in someone's home office, or it can extend throughout a company and include audio and video devices.

Each host in a LAN has an identifier, an address, that uniquely defines the host in the LAN. A packet sent by a host to another host carries both the source host's and the destination host's addresses.

Nowadays, LANs use a smart connecting switch, which is able to recognize the destination address of the packet and guide the packet to its destination without sending it to all other hosts.

The switch alleviates the traffic in the LAN and allows more than one pair to communicate with each other at the same time if there is no common source and destination among them.

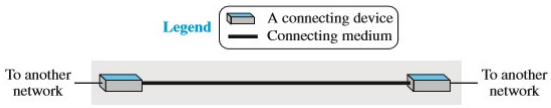


1.3.2 Wide Area Networks

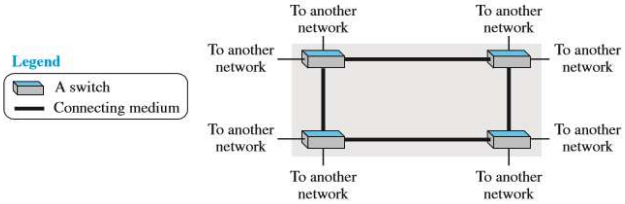
A wide area network (WAN) is also an interconnection of devices capable of communication. There are differences between LAN and a WAN- (i) A LAN is normally limited in size, spanning an office, a building, or a campus; a WAN has a wider geographical span, spanning a town, a state, a country, or even the world. (ii) A LAN interconnects hosts; a WAN interconnects connecting devices such as switches, routers, or modems. (iii) A LAN is normally privately owned by the organization that uses it; a WAN is normally created and run by communication companies and leased by an organization that uses it.

Types of WAN

1. Point to point WAN: A point-to-point WAN is a network that connects two communicating devices through a transmission media (cable or air).

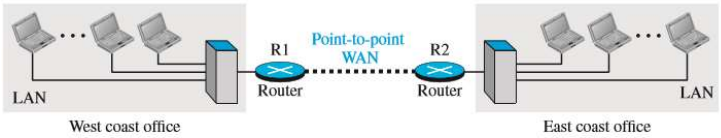


2. Switched WAN: A switched WAN is a network with more than two ends. A switched WAN is used in the backbone of global communication today. It is a combination of several point-to-point WANs that are connected by switches.



1.3.3 Internetwork

LANs and WANs are interconnected to form a internetwork also called as internet. The interconnection may be point to point or switched.



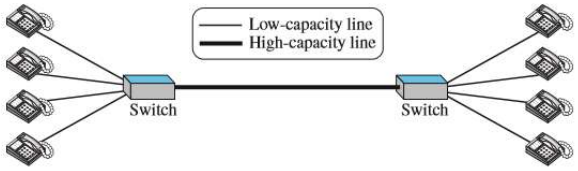
Two networks are connected via a point to point WAN(this forms a private internet or internet) between two offices of an organization to make the communication possible.

Switching

An internet is a switched network in which a switch connects at least two links together. A switch needs to forward data from a network to another network when required. The two most common types of switched networks are circuit-switched and packet-switched networks.

Circuit switched network

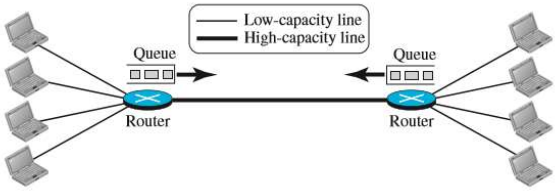
In a circuit-switched network, a dedicated connection, called a circuit, is always available between the two end systems; the switch can only make it active or inactive. Such a network is used in telephone system where in a dedicated line exists between two ends.



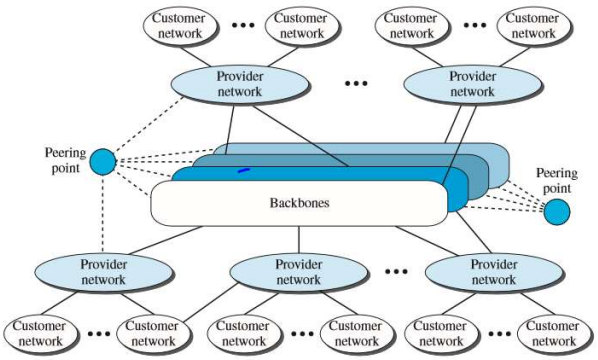
The network is efficient when it is working and is used in full capacity, however it is most of the time it is inefficient as it is working partially.

Packet switched network.

In a computer network, the communication between the two ends is done in blocks of data called packets. The switches function for both storing and forwarding because a packet is an independent entity that can be stored and sent later.



A router in a packet-switched network has a queue that can store and forward the packet, hence it is efficient than circuit switched network with some delay of packets.



The figure shows the Internet as several backbones, provider networks, and customer networks.

- At the top level, the backbones are large networks owned by some communication companies such as Sprint, Verizon (MCI), AT&T, and NTT. The backbone networks are connected through some complex switching systems, called peering points.
- At the second level, there are smaller networks, called provider networks, that use the services of the backbones for a fee. The provider networks are connected to backbones and sometimes to other provider networks.
- The customer networks are networks at the edge of the Internet that actually use the services provided by the Internet. They pay fees to provider networks for receiving services.
- Backbones and provider networks are also called Internet Service Providers (ISPs).
- The backbones are often referred to as international ISPs; the provider networks are often referred to as national or regional ISPs.

1.4 Accessing the network

To access any part of the internet the user has to become a part of it, this can happen using any of the following access methods:

1. Using telephone networks- Since the telephone system is connected to Internet, if the user owns the telephone service he can access the network using Digital Subscriber Line (DSL). DSL supports both data and voice communication.

2. Using Cable networks- More and more residents over the last two decades have begun using cable TV services instead of antennas to receive TV broadcasting. It provides a higher speed connection, but the speed varies depending on the number of neighbours that use the same cable.

3. Using Wireless Networks - Wireless connectivity has recently become increasingly popular. A household or a small business can use a combination of wireless and wired connections to access the Internet. With the growing wireless WAN access, a household or a small business can be connected to the Internet through a wireless WAN.

4. Direct connection to network- A large organization or a large corporation can itself become a local ISP and be connected to the Internet. This can be done if the organization or the corporation leases a high-speed WAN from a carrier provider and connects itself to a regional ISP. For example, a large university with several campuses can create an internetwork and then connect the internetwork to the Internet.

2. Network Models

A networking model is also called as a networking architecture or a network blueprint refers to a comprehensive set of documents. Individually, each document describes one small function required for a network; collectively, these documents define everything that should happen for a computer network to work. Some documents define a protocol, which is a set of logical rules that devices must follow to communicate. Other documents define some physical requirements for networking. For example, a document could define the voltage and current levels used on a particular cable when transmitting data.

Protocol is defined as set of that both sender and receiver and intermediate nodes need to follow to be able to communicate effectively.

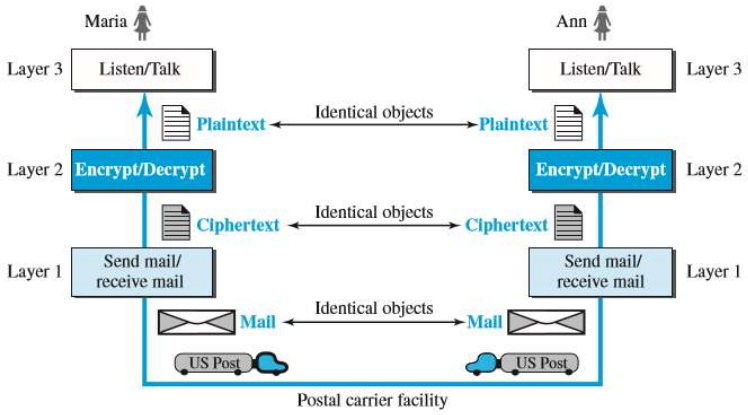
With simple communication only one protocol is sufficient, when communication is complex the task is divided between different layers and a protocol is required at every layer. This is called protocol layering.

For example- Simple communication

Assume Mr. X and Mr.Y are neighbors with a lot of common ideas. Communication between them takes place in one layer, face to face, in the same language.

Set of rules needs to be followed. First, X and Y know that they should greet each other when they meet. Second, they know that they should confine their vocabulary to the level of their friendship. Third, each party knows that she should refrain from speaking when the other party is speaking. Fourth, each party knows that the conversation should be a dialog, not a monolog: both should have the opportunity to talk about the issue. Fifth, they should exchange some nice words when they leave.

Complex Communication



Mr. X and Mr. Y move to different places, and they decide to continue their conversation using regular mail through the post office. However, they do not want their ideas to be revealed by other people if the letters are intercepted. They agree on an encryption/decryption technique. The sender of the letter encrypts it to make it unreadable by an intruder; the receiver of the letter decrypts it to get the original letter. The communication between X and Y takes place in three layers. Let us assume that X sends the first letter to Y. X talks to the machine at the third layer as though the machine is Y and is listening to her. The third layer machine listens to what X says and creates the plaintext (a letter in English), which is passed to the second layer machine. The second layer machine takes the plaintext, encrypts it, and creates the ciphertext, which is passed to the first layer machine. The first layer machine, presumably a robot, takes the ciphertext, puts it in an envelope, adds the sender and receiver addresses, and mails it.

Protocol layering enables us to divide a complex task into several smaller and simpler tasks also we can separate the services from the implementation- A layer needs to be able to receive a set of services from the lower layer and to give the services to the upper layer; we don't care about how the layer is implemented.

2.1 Principles of Protocol Layering

First principle

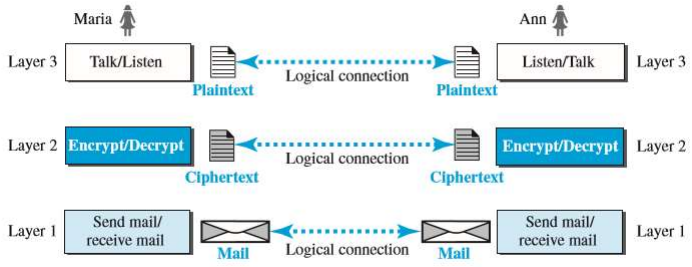
For a bidirectional communication each layer is required to perform opposite tasks, one in each direction.

Second Principle

The two objects under each layer at both sites should be identical.

2.2 Logical connection

This means that there is a layer-to-layer communication. Mr. X and Mr. Y think that there is a logical (imaginary) connection at each layer through which they can send the object created from that layer.

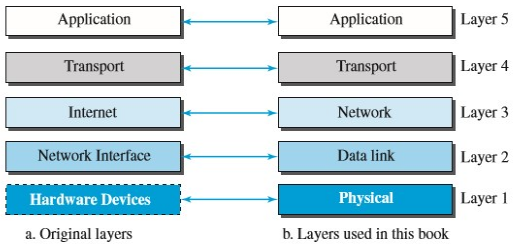


2.3 TCP/IP Protocol suite

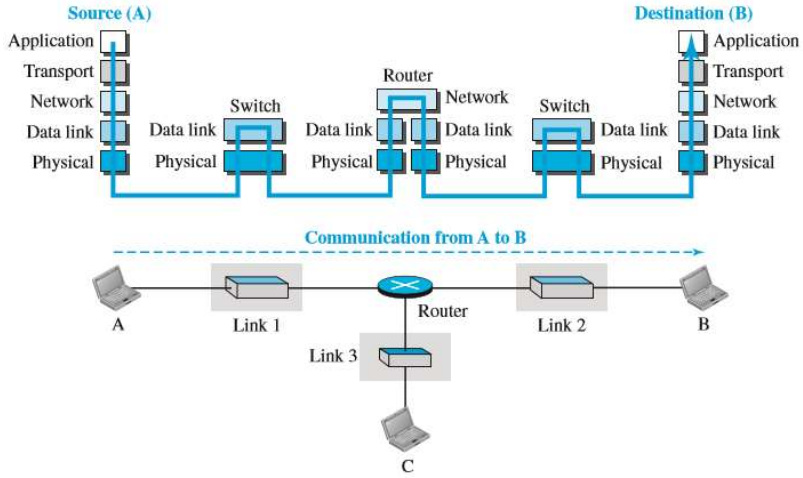
TCP/IP is a protocol suite (a set of protocols organized in different layers) used in the Internet today. It is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality. The term hierarchical means that each upper level protocol is supported by the services provided by one or more lower level protocols. The original TCP/IP protocol suite was defined as four software layers built upon the hardware. Today, however, TCP/IP is thought of as a five-layer model.

2.4 Layers in TCP/IP model

The model has five layers- Application, transport, network, datalink and physical layers. Figure below shows the original layers and the layers used in the book.



To understand the operation of the model consider the communication between the devices A and B in the internet.



- There are five communicating devices in this communication: source host (computer A), the link-layer switch in link 1, the router, the link-layer switch in link 2, and the destination host (computer B).
- Each device is involved with a set of layers depending on the role of the device in the internet.
- The two hosts are involved in all five layers; the source host needs to create a message in the application layer and send it down the layers so that it is physically sent to the destination host.
- The destination host needs to receive the communication at the physical layer and then deliver it through the other layers to the application layer.

Note

- The router is involved in only three layers, there is no transport or application layer in a router as long as the router is used only for routing.
- A link-layer switch in a link two layers has two layers data-link and physical.

2.5 Functionalities of layers in TCP/IP suite

1. Physical layer- This layer is the lowest layer in the OSI model. It helps in the transmission of data between two machines that are communicating through a physical medium, which can be optical fibres, copper wire or wireless etc. The following are the main functions of the physical layer:

Hardware Specification: The details of the physical cables, network interface cards, wireless radios, etc are a part of this layer.

Encoding and Signalling: How are the bits encoded in the medium is also decided by this layer. For example, on the copper wire medium, we can use different voltage levels for a certain time interval to represent '0' and '1'. We may use +5mV for 1nsec to represent '1' and -5mV for 1nsec to represent '0'. All the issues of modulation is dealt with in this layer. Eg, we may use Binary phase shift keying for the representation of '1' and '0' rather than using different voltage levels if we have to transfer in RF waves.

Data Transmission and Reception: The transfer of each bit of data is the responsibility of this layer. This layer assures the transmission of each bit with a high probability. The transmission of the bits is not completely reliable as their is no error correction in this layer.

Topology and Network Design: The network design is the integral part of the physical layer. Which part of the network is the router going to be placed, where the switches will be used, where we will put the hubs, how many machines is each switch going to handle, what server is going to be placed where, and many such concerns are to be taken care of by the physical layer. The various kinds of topologies that we decide to use may be ring, bus, star or a hybrid of these topologies depending on our requirements.

Data Link Layer

This layer provides reliable transmission of a packet by using the services of the physical layer which transmits bits over the medium in an unreliable fashion. This layer is concerned with :

- Framing : Breaking input data into frames (typically a few hundred bytes) and caring about the frame boundaries and the size of each frame.
- Acknowledgment : Sent by the receiving end to inform the source that the frame was received without any error.
- Sequence Numbering : To acknowledge which frame was received.
- Error Detection : The frames may be damaged, lost or duplicated leading to errors.The error control is on link to link basis.
- Retransmission : The packet is retransmitted if the source fails to receive acknowledgment.
- Flow Control : Necessary for a fast transmitter to keep pace with a slow receiver.

Network Layer

Its basic functions are routing and congestion control.

Routing: This deals with determining how packets will be routed (transferred) from source to destination.

Congestion Control: A router can be connected to 4-5 networks. If all the networks send packet at the same time with maximum rate possible then the router may not be able to handle all the packets and may drop some/all packets. In this context the dropping of the packets should be minimized and the source whose packet was dropped should be informed. The control of such congestion is also a function of the network layer. Other issues related with this layer are transmitting time, delays, jittering.

Internetworking: Internetworks are multiple networks that are connected in such a way that they act as one large network, connecting multiple office or department networks. Internetworks are connected by networking hardware such as routers, switches, and bridges .Internetworking is a solution born of three networking problems: isolated LANs, duplication of resources, and the lack of a centralized network

management system. With connected LANs, companies no longer have to duplicate programs or resources on each network. This in turn gives way to managing the network from one central location instead of trying to manage each separate LAN. We should be able to transmit any packet from one network to any other network even if they follow different protocols or use different addressing modes.

Network Layer does not guarantee that the packet will reach its intended destination. There are no reliability guarantees.

Transport Layer

Its functions are :

Multiplexing / Demultiplexing : Normally the transport layer will create distinct network connection for each transport connection required by the session layer. The transport layer may either create multiple network connections (to improve throughput) or it may multiplex several transport connections onto the same network connection (because creating and maintaining networks may be expensive). In the latter case, demultiplexing will be required at the receiving end. A point to note here is that communication is always carried out between two processes and not between two machines. This is also known as process-to-process communication.

Fragmentation and Re-assembly : The data accepted by the transport layer from the session layer is split up into smaller units (fragmentation) if needed and then passed to the network layer. Correspondingly, the data provided by the network layer to the transport layer on the receiving side is re-assembled.

Types of service : The transport layer also decides the type of service that should be provided to the session layer. The service may be perfectly reliable, or may be reliable within certain tolerances or may not be reliable at all. The message may or may not be received in the order in which it was sent. The decision regarding the type of service to be provided is taken at the time when the connection is established.

Error Control : If reliable service is provided then error detection and error recovery operations are also performed. It provides error control mechanism on end to end basis.

Flow Control : A fast host cannot keep pace with a slow one. Hence, this is a mechanism to regulate the flow of information.

Connection Establishment / Release : The transport layer also establishes and releases the connection across the network. This requires some sort of naming mechanism so that a process on one machine can indicate with whom it wants to communicate.

Session Layer

It deals with the concept of Sessions i.e. when a user logins to a remote server he should be authenticated before getting access to the files and application programs. Another job of session layer is to establish and maintain sessions. If during the transfer of data between two machines the session breaks down, it is the session layer which re-establishes the connection. It also ensures that the data transfer starts from where it breaks keeping it transparent to the end user. E.g. In case of a session with a database server, this layer introduces check points at various places so that in case the onnection is broken and reestablished, the transition running on the database is not lost even if the user has not committed. This activity is called Synchronization. Another function of this layer is Dialogue Control which determines whose turn is it to speak in a session. It is useful in video conferencing.

Presentation Layer

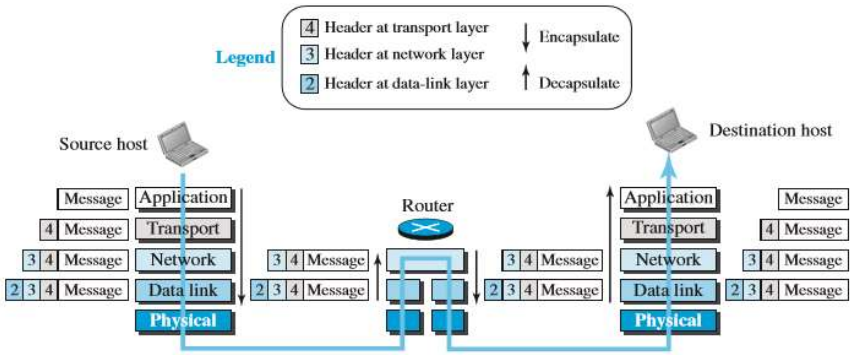
This layer is concerned with the syntax and semantics of the information transmitted. In order to make it possible for computers with different data representations to communicate data structures to be exchanged can be defined in abstract way alongwith standard encoding. It also manages these abstract data structres and allows higher level of data structres to be defined an exchange. It encodes the data in standard agreed way(network format). Suppose there are two machines A and B one follows 'Big Endian' and other 'Little Endian' for data representation. This layer ensures that the data transmitted by one gets converted in the form compatibale to othe machine. This layer is concerned with the syntax and semantics of the information transmitted.In order to make it possible for computers with different data representations to communicate data structures to be exchanged canbe defined in abstract way alongwith standard encoding. It also manages these abstract data structres and allows higher level of data structres to be defined an exchange. Other functions include compression, encryption etc.

Application Layer

The seventh layer contains the application protocols with which the user gains access to the network. The choice of which specific protocols and their associated functions are to be used at the application level is up to the individual user. Thus the boundary between the presentation layer and the application layer represents a separation of the protocols imposed by the network designers from those being selected and implemented by the network users. For example commonly used protocols are HTTP(for web browsing), FTP(for file transfer) etc.

2.6 Encapsulation and Decapsulation

One of the important concepts in protocol layering in the Internet is encapsulation/ decapsulation.



Encapsulation at the Source Host

At the application layer, the data to be exchanged is referred to as a message.

1. A message normally does not contain any header or trailer, but if it does, we refer to the whole as the message. The message is passed to the transport layer.
2. The transport layer takes the message as the payload, the load that the transport layer should take care of. It adds the transport layer header to the payload, which contains the identifiers of the source and destination application programs that want to communicate plus some more information that is needed for the end-toend delivery of the message, such as information needed for flow, error control, or congestion control. The result is the transport-layer packet, which is called the segment (in TCP) and the user datagram (in UDP). The transport layer then passes the packet to the network layer.
3. The network layer takes the transport-layer packet as data or payload and adds its own header to the payload. The header contains the addresses of the source and destination hosts and some

more information used for error checking of the header, fragmentation information, and so on. The result is the network-layer packet, called a datagram. The network layer then passes the packet to the data-link layer.

4. The data-link layer takes the network-layer packet as data or payload and adds its own header, which contains the link-layer addresses of the host or the next hop (the router). The result is the link-layer packet, which is called a frame. The frame is passed to the physical layer for transmission.

Decapsulation and Encapsulation at the Router

At the router both decapsulation and encapsulation take place because the router is connected to two or more links.

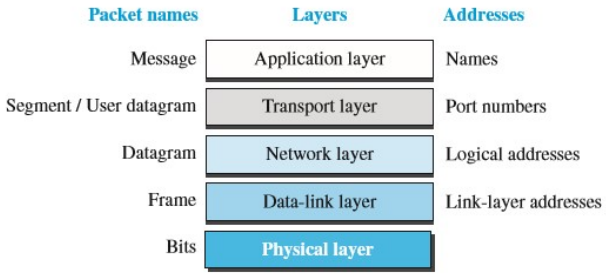
1. After the set of bits are delivered to the data-link layer, this layer decapsulates the datagram from the frame and passes it to the network layer.
2. The network layer only inspects the source and destination addresses in the datagram header and consults its forwarding table to find the next hop to which the datagram is to be delivered. The contents of the datagram should not be changed by the network layer in the router unless there is a need to fragment the datagram if it is too big to be passed through the next link. The datagram is then passed to the data-link layer of the next link.
3. The data-link layer of the next link encapsulates the datagram in a frame and passes it to the physical layer for transmission.

Decapsulation at the Destination Host

At the destination host, each layer only decapsulates the packet received, removes the payload, and delivers the payload to the next-higher layer protocol until the message reaches the application layer. It is necessary to say that decapsulation in the host involves error checking.

2.7 Addressing

Any communication that involves two parties needs two addresses: source address and destination address. There is a relationship between the layer, the address used in that layer, and the packet name at that layer.



Link layer/ Physical addresses: every interface (NIC) of a communicating device usually has a unique physical address, that helps in uniquely identifying and communicating with the interface at the physical and data link layers. These physical addresses are used in the data link layer frame headers, for carrying frames between neighbouring nodes belonging to the same network. If the underlying interface is Ethernet, then the physical layer address is termed as a MAC address and it consists of 6 bytes. The address is written in hexadecimal format. For example: 0A:12:34:45:55:67.

IP addresses used at the network layer (layer 3), to uniquely identify interfaces of communicating nodes globally. IP version 4 (IPV4) have 4 byte IP addresses in the form A.B.C.D and IP version 6 (IPV6) have 16 byte IP addresses. Each communicating node on the Internet MUST have at least one unique public IP address, in order to successfully communicate on the Internet. IP addresses, unlike physical addresses, have end to end significance. An IP packet containing application layer data is carried end to end across the network, from the source node to a remote destination node, using mainly the destination IP address. Examples of IPV4 addresses are 10.0.0.1, 144.224.1.34 etc.

Port Addresses: Used at transport layer and used to identify various processes in the host machine. Theses are 16 bit numbers, written as decimal numbers.

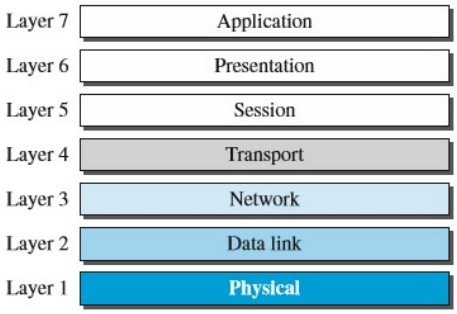
Application addressing: Specific addresses or domain addresses. For example: www.rvce.edu.in.

2.8 The OSI Model

The International Organization for Standardization (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the late 1970s.

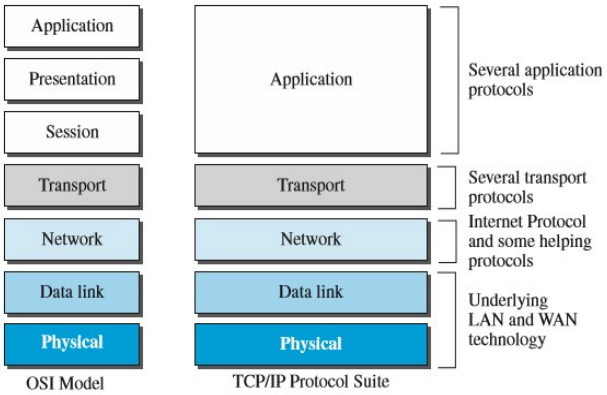
An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture. The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software. The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable. The OSI model was intended to be the basis for the creation of the protocols in the OSI stack.

The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems. It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network



OSI vs TCP model

When we compare the two models, we find that two layers, session and presentation, are missing from the TCP/IP protocol suite. These two layers were not added to the TCP/IP protocol suite after the publication of the OSI model. The application layer in the suite is usually considered to be the combination of three layers in the OSI model.

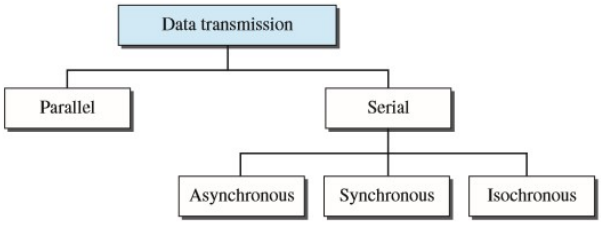


Lack of OSI models success:

- The OSI model appeared after the TCP/IP protocol suite- OSI was completed when TCP/IP was fully in place and a lot of time and money had been spent on the suite; changing it would cost a lot.
- Some layers in the OSI model were never fully defined. For example, although the services provided by the presentation and the session layers were listed in the document, actual protocols for these two layers were not fully defined.
- Third, when OSI was implemented by an organization in a different application, it did not show a high enough level of performance when compared to TCP/IP.

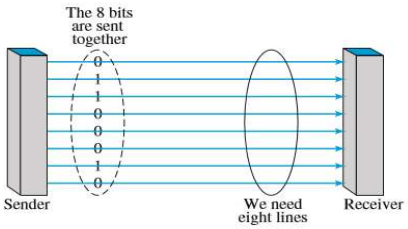
3. Transmission Modes

Transmission of data from one device to another either serially or parallel. In parallel mode, multiple bits are sent with each clock tick. In serial mode, 1 bit is sent with each clock tick. While there is only one way to send parallel data, there are three subclasses of serial transmission: asynchronous, synchronous, and isochronous.



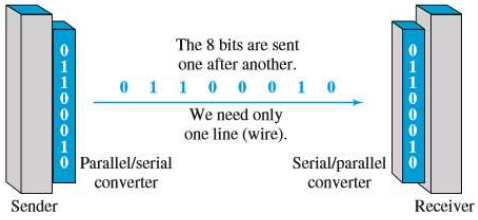
Parallel Transmission

- Binary data, consisting of 1s and 0s, may be organized into groups of n bits each, sending these n data bits at a time is called parallel transmission.
- Uses n wires to send n bits at one time. That way each bit has its own wire, and all n bits of one group can be transmitted with each clock tick from one device to another.
- Typically, the eight wires are bundled in a cable with a connector at each end.
- Parallel transmission can increase the transfer speed by a factor of n over serial transmission.
- Requires n communication lines (wires in the example) just to transmit the data stream. Because of this it is expensive and limited to short distances.



Serial transmission

In serial transmission one bit follows another, so we need only one communication channel rather than n to transmit data between two communicating devices.



Reduces the cost of transmission over parallel by roughly a factor of n. Serial transmission occurs in one of three ways: asynchronous, synchronous, and isochronous.