I think the brain is essentially a computer and consciousness is like a computer program. It will cease to run when the computer is turned off. Theoretically, it could be recreated on a neural network, but that would be very difficult, as it would require all one's memories.

Stephen Hawking

1

Introduction to Computer Network

1.1 Introduction

History

1. 18^{th} Century - Era of mechanical system; Industrial Revolution.
2. 19^{th} Century - Age of steam engine.
3. 20^{th} Century - Age of Technology.
    - Installation of world wide telephone network.
    - Invention of radio and television.
    - Growth in computer industry
    - Launching of communication satellites.
    - Internet
4. 21^{th} Century - Age of Information.
    - Unprecedented growth in sophisticated information processing system.

1.1.1 Computer Network

- Computer network is a large number of separate computers that are interconnected to exchange data and information.

- Two computers are said to be interconnected if they are able to exchange information.
- The connection can be made through wired or wireless transmission media.
- Networks come in many sizes, shapes and forms.
- In computer network, users directly interact with the actual machine to invoke the data exchange and the system do not attempt to make the computers or machines to act coherently.
- An example of a network is the Internet, which connects millions of people all over the world.

1.1.2 Network Criteria

A network must be able to meet a certain number of criteria, which are *performance, reliability, and security.*

Performance

Performance can be measured in many ways, including 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 ad 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, this two criteria are often contradictory.

Reliability

A 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

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

1.2 Characteristic of a Computer Network

- Share resources from one computer to another.
- Create files and store them in one computer, access those files from the other

computer(s) connected over the network.

- Connect a printer, scanner, or a fax machine to one computer within the network and let other computers of the network use the machines available over the network.

1.3 Advantages of Computer Network

- Resource sharing such as printers and storage devices
- Exchange of information by means of e-Mails and FTP
- Information sharing by using Web or Internet
- Interaction with other users using dynamic web pages
- IP phones
- Video conferences
- Parallel computing
- Instant messaging

1.4 Drawbacks of Computer Network

- Server failure affects all other client.
- Initial set-up cost is very high.
- The efficiency of a network is very dependent on the skill of the system manger.
- As network traffic increases on the network the performance decreases unless it is properly designed.
- If network stops working then it may not be possible to access hardware and software resources.

1.5 Uses of Computer Network

1.5.1 Business Application

Most company have a large number of computers . They are connected to distribute information throughout the company, though some computer may work in isolation.
The issues in business applications are:

1.5.1.1 Resource Sharing

- The purpose is to make all programs, equipments, and especially data available to anyone on the network without regard to the physical location of the resource or the

user.

- Example: sharing printer to a group of people. A network printer is often cheaper, faster, and easier to maintain than a larger collection of individual printers.

1.5.1.2 Sharing Information

- Companies small or large are vitally dependent on computerized information.
- Most companies have customer records, product information, inventories, financial statements, tax information, and much more on-line.
- It allows the people to access relevant information and documents instantly on company database.
- Networks called Virtual Private Networks (VPN) may be used to join the individual networks at different sites into one extended network.

1.5.1.3 E-commerce

- A third goal of many companies is doing business electronically, especially with customers and suppliers. This new model is called **e-commerce (electronic commerce)** and it has grown rapidly in recent years.

Tag	Full name	Example
B2C	Business-to-consumer	Ordering books online
B2B	Business-to-business	Car manufacturer ordering tires from supplier
G2C	Government-to-consumer	Government distributing tax forms electronically
C2C	Consumer-to-consumer	Auctioning second-hand products online
P2P	Peer-to-peer	Music sharing

Figure 1.1: Some forms of e-commerce

1.5.2 Home Applications

- Internet access provides home users with connectivity to remote computers; home user can access information, communicate with other people, and buy products and services with e-commerce.
- Access to remote information can be inform of surfing the world wide web for information (i.e. online news, online digital library) or just for entertainment (listening to, looking at, and creating music, photos, and videos, playing games online).
- Person-to-Person communication: e.g. Email, instant messaging

- Multi-person messaging: e.g. twitter service.
- **ubiquitous computing**, in which computing is embedded into everyday life; many homes are already wired with security systems that include door and window sensors, and many more sensors that can be folded in to a smart home monitor, such as energy consumption, smoke detector that could call the fire department etc.
- Devices such as television that plug into the wall can use **power-line network** to send information throughout the house over the wire that carry electricity.

1.5.3 Mobile Users

- Mobile computers, such as laptop and handheld computers, are one of the most fastest-growing segments of the computer industry.
- People often use their mobile devices to read and send mail, tweet, watch movies, download music, play games, or simply surf web for information whenever they want from anywhere on land, sea or in the air, provided connectivity to the Internet is available through wireless hotspots, which is based on 802.11 standard, or through cellular network.
- One of the key application of wireless is mobile phone, which is mostly used for text messaging (i.e. Short Message Service).
- Another promising driver of mobile is smart phones, which combines aspects of mobile phones and mobile computers. Equipped with different sensors such as GPS (Global Positioning System), NFC (Near Field Communication), mobile phones are used to know the locations, pay the bills, know health issues, m-commerce etc.

1.5.4 Social Issues

- Computer networks, like the printing press 500 years ago, allow ordinary citizens to distribute and view content in ways that were not previously possible.
- Social networks, message boards, content sharing sites, and a host of other applications allow people to share views with like-minded individuals thorough text, photographs, video clips, live show etc.

1.6 Transmission Technology/Types of Connection

- A network is two or more devices connected through link. A link is a communications pathway that transfers data from one device to another.
- Broadly speaking, there are two type of transmission technology: point-to-point link and Broadcast link.

1.6.1 Point-to-Point Link

- A point-to-point link provides dedicated link between two devices.
- Point-to-point connection are connection between two devices through cable, microwave or satellite link, connection between the remote control and the television's control system etc.
- Point-to-point transmission with exactly one sender and exactly one receiver is sometimes called **unicasting**.

1.6.2 Broadcast Link

- In multipoint network, the communication channel is shared by all the machines on the network; packets sent by the any machine are received by all the others. An address field within each packet specifies the intended recipient.
Upon receiving a packet, a machine checks the address field. If the packet is intended for the receiving machine, that machine processes the packet; otherwise ignore it.
- Example: wireless network
- If the packet is intended for the machines in the network, the mode is **broadcasting**; while if it is intended for some particular subset of network, it is known as **multicasting**.

1.7 Network Types Based on Scale

Based on the geographical area(i.e. scale or distance) the encompass, computer network can be:

1. Personal Area Network (PAN)
2. Local Area Network (LAN)
3. Metroplitan Area Network (MAN)
4. Wide Area Network (WAN)

1.7.1 Personal Area Network

- The smallest and most basic type of network.
- Made up of wireless router, computers, phones, printers, Bluetooth, etc., and revolves around one person in building.
- Network meant for one person i.e. PAN let devices communicate over the range of a person i.e. less than 2 meters. - Example: wireless network connecting a computer with its mouse, keyboard, and printer; Bluetooth network connecting phone with headset;

Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

Figure 1.2: Classification of interconnected processors by scale.

RFID on smartcards and library books etc.
- A completely different kind of PAN is formed when an embedded medical device such as a pacemaker, insulin pump, or hearing aid talks to a user-operated remote control.

1.7.2 Local Area Network

- A LAN is a privately owned network that operates within and nearby a single building like a home, office or factory.
- LANs are used to connect personal computers and electronics to let them share resources (e.g., printers) and exchange information.
- LANs when used by companies is called **enterprise networks**.
- Nodes are connected by wire or wireless.
- The standard for the wireless LANs is called IEEE 802.11 (**WiFi**).
- The standard for the wired LANs, built from point-to-point line, is IEEE 802.3 and popularly called as **Ethernet**.
- It has higher speed data transfer rate maximum up to 10 Gbps.
- It is highly secured network and it has least error rate than others.
- One large physical LAN can divided into smaller logical LANs, usinb Virtal LAN (VLAN)

1.7.3 Metropolitan Area Network

- A Metropolitan Area Network (MAN) covers a city.
- Examples: cable television network available in cities, IEEE 802.16 Standard WiMAX, connection of a large number of LAN etc..

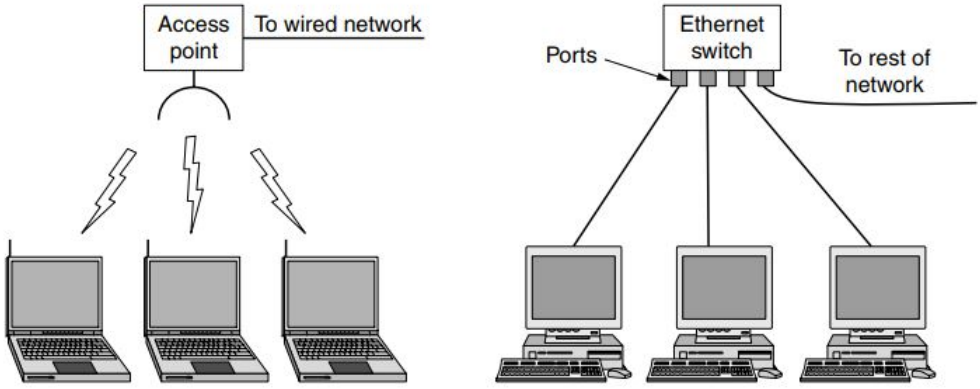

Figure 1.3: Wireless and wired LANs.

- When this type of network is specifically designed for a college campus, it is sometimes referred to as a campus area network, or CAN.

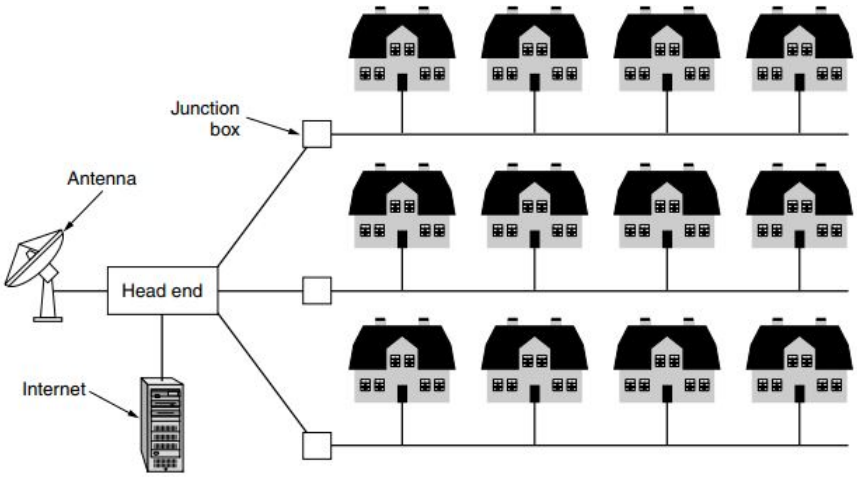

Figure 1.4: A MAN based on cable TV.

1.7.4 Wide Area Network

- WAN spans a large geographical area, often a country or continent.
- In most WANs, the subnet consists of two distinct components: transmission lines and switching elements.
- **Transmission lines** moves bits between machines through copper wires, optical fiber, or even radio links.
- Most companies do not have transmission lines lying about, so they lease the lines from a telecommunication company.
- Transmission lines can be dedicated link, or virtual link using virtual private network (VPN).

- **Switching element**s, or just **switches**, are networking devices that connect two or more transmission lines.
- So, WAN consists of a number of interconnected switching nodes(switches, routers, gateway etc.) which routes the transmitted data from source through node to node until they reach their destination.
- Transmission of data rates = 20 Kbps to 8 Mbps
- Error rate = 10^{-5} to 10^{-7}

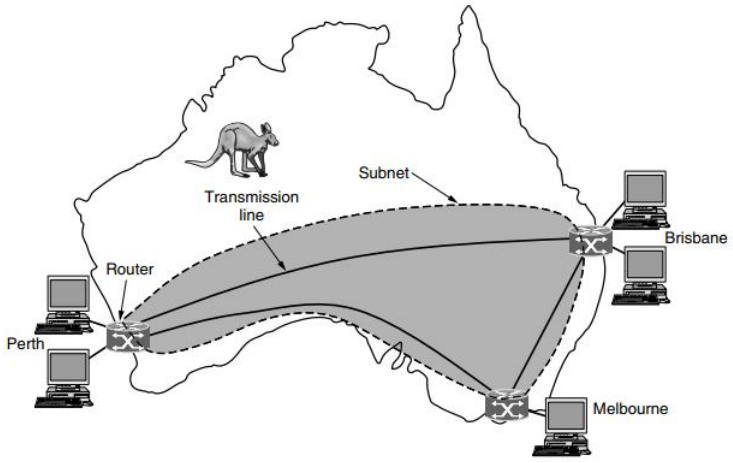

Figure 1.5: WAN that connects three branches in Australia.

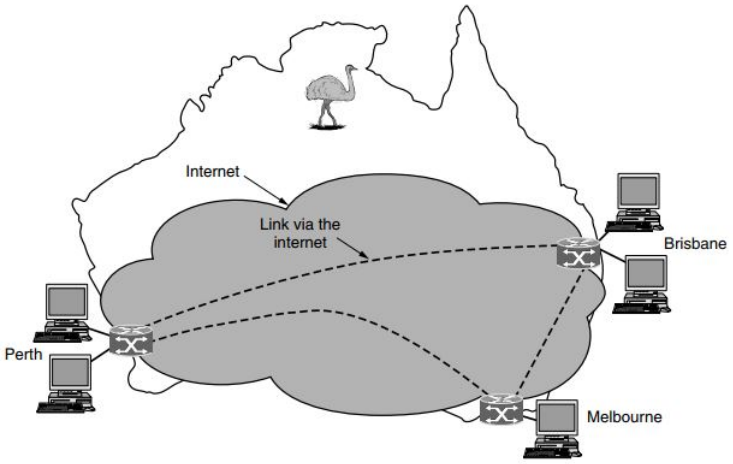

Figure 1.6: WAN using virtual private network.

WANs are designed to do the following:

- Operate over a large and geographically separated area.
- Allow users to have real-time communication capabilities with other user.
- Provide full-time remote resources connected to local services.
- Provide e-mail, Internet, file transfer, and e-commerce services.

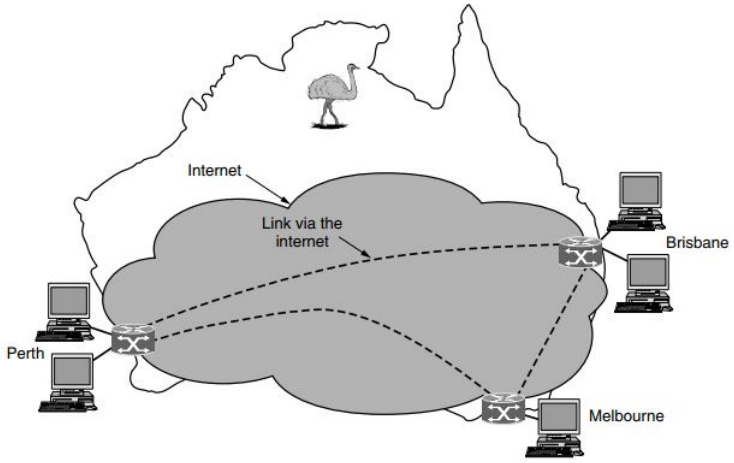

Figure 1.7: WAN using an ISP network.

WAN Technology:

1. Point-to-Point WANS
    - Modems
    - Digital Subscriber Line (DSL) Technology (Types: ADSL, SDDL, HDSL, VDSL)
    - Hybrid Fiber-Coaxial (HFC) Network
    - T Lines (T-1 line, T-3 line)
    - SONET (Synchronous Optical Network)
    - PPPoE (PPP over Ethernet)
2. Switched WAN
    - X.25
    - Frame Relay
    - ATM (Asynchronous Transfer Mode)

1.8 Network Topology

- Topology is the physical layout of network or simply it is the geometric arrangement of the computers in the network.
- The term topology refers to the way a network is laid out, either physically or logically.
- Physical topologies describe how the cables are connected. Logical topologies describe how the network message travel.

Type of Network Topology

1. Bus Topology
2. Star Topology
3. Ring Topology
4. Mesh Topology
5. Tree Topology
6. Hybrid Topology

1.8.0.1 Bus Topology

-it is simplest physical topology, in which all device are connected to the single shared common line, called backbone.
- Cable is terminated at both the ends.
- Break in the cable will bring the network to a halt.
- The message is transmitted from one host to another though the broadcast mechanism; computer whose address matches the destination address, receives the packet.
- CSMA/CD is used as media access protocol to ensure only one host transmit at a time.

Factors affecting performance:

- Break in the cable or loss of termination will stop network traffic.
- More computers, the longer the wait, slower the network.
- Simple to install, difficult to troubleshoot.

Advantages:

- It is simple and easy to setup ad extend the network.
- It is inexpensive topology because it requires less amount of cable and no networking devices.
- It any computer in the network downs, then it does not affect other computers.
- It is more flexible because we can easily connect and disconnect any number of computers in the bus.

Disadvantages:

- Data traffic is very high in bus, so there may be chances of data collision.
- The length of bus should be small otherwise the performance of the network goes down.
- If there is problem is bus, then the entire network goes down.
- It is very difficult to find out the fault in the bus i.e. difficult for troubleshoot.

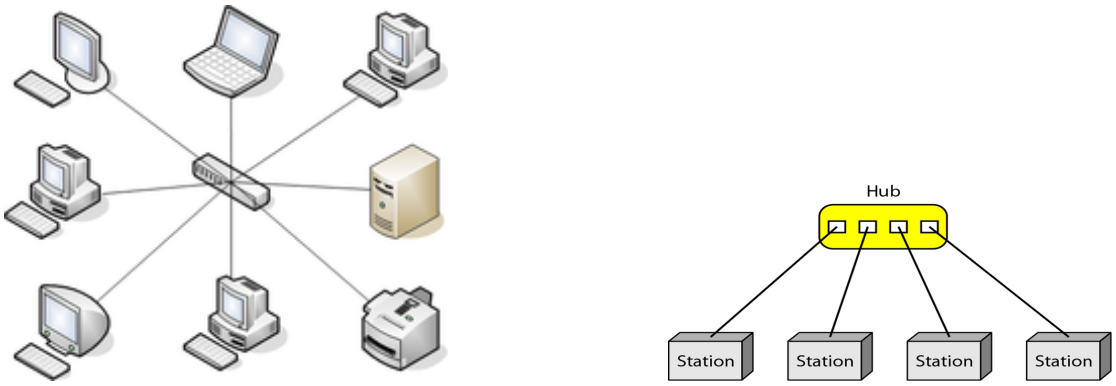

Figure 1.8: Star Topology Illustration.

1.8.0.2 Star Topology

- In star topology, all the hosts are connected to the central device called **hub** or **switch**.
- In order to transmit the data between the two hosts, all the data must pass through this device, which may also regenerate/amplify the data signal so that it can travel longer distances. Also,a computer can send the broadcast message to all the hosts connected to the hub.
- A hub can be active or passive. An active hub regenerates the electrical signal and sends it to all the computers connected to it. This type of hub is also called an multiport repeater. A passive hub only act as connector point and doesn't amplify or regenerate the signal. This type of hub doesn't require power to run.
- It requires more cable than bus.
- Failure of a cable or computer affects only that computer.
- Failure of a hub affects the whole segment.

Advantages:

- simple, reliable and easy to setup and re-configure.
- Flexible to connect new computer and remove existing computer.
- Easy to find out the faults.
- Problem in one computer only affect that; the network won't get down.

Disadvantages:

- Requires large amount of cables.
- Expensive to use.
- Problem in central device cause the network failure.
- Data traffic is high, so can occur data collision.
- Performance depends on capacity of central device.

1.8.0.3 Ring Topology

- In the ring topology, the hosts are connected in the form of ring, which acts as a common shared channel. Each host is connected to two other hosts.
- The network consists of a set of repeaters joined by point-to-point link in closed loop.
- The data circulate around the ring in one direction. (clockwise or anticlockwise) using broadcast mechanism.
- Used token passing protocol which ensures that the only host which is in possession of token (a special message) can transmit the message on the channel.
- This topology is found in peer-to-peer network.

Advantages:

- Simple and inexpensive.
- Less chance of data collision due to unidirectional data flow.
- Each computer has equal rights to access the channel to send the message.
- Performed better than bus topology for small size network.

Disadvantages:

- Not flexible for adding or removing new nodes; disturbs the network.
- Not suitable for large network(not more than 10 nodes).
- Problem in any computer or cable cause the whole network down.
- Difficult to troubleshoot.

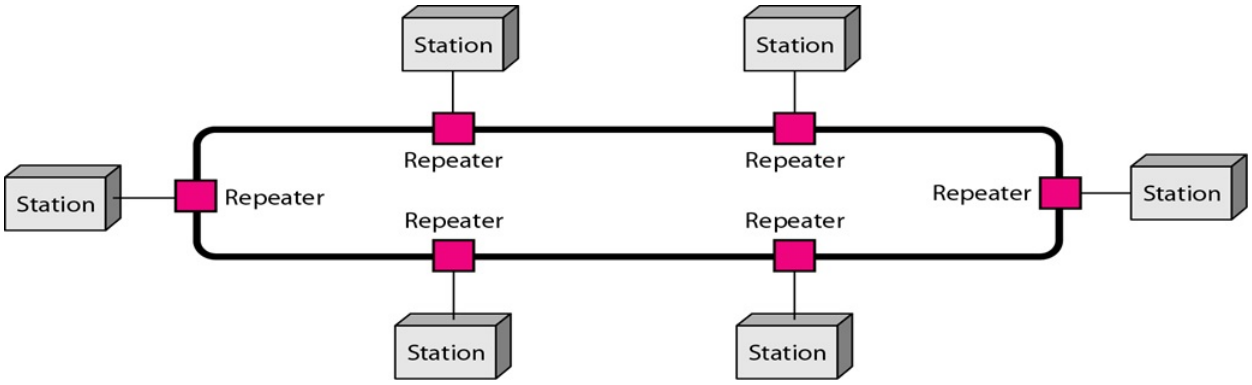

Figure 1.9: Ring topology.

1.8.0.4 Mesh Topology

- In mesh topology, each host is connected to each other through a separate point-to-point links for redundancy and fault tolerance.
- For a fully meshed topology, n hosts required *n(n-1)/2* links. - Used in WANs to connect critical internetwork.

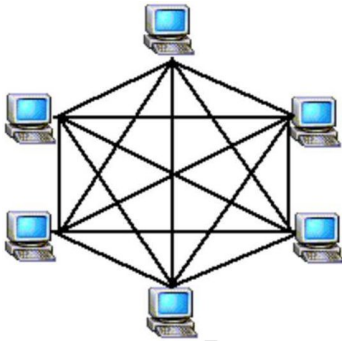

Figure 1.10: Mesh topology.

Advantages:

- Faster and robust type of topology.
- Fault tolerant, failure in one link does not affect the data transmission, as there are multiple connection between any two nodes.
- Less amount of data traffic due to multiple paths.

Disadvantages:

- Complex and expensive as highly cabled.
- Difficult in finding errors.
- Installation and configuration is difficult.
- Not flexible for adding or removing nodes.

1.8.0.5 Tree Topology

- Also known as Hierarchical topology.
- This topology imitates as extended star topology and inherits properties of bus topology.
- This topology divides the network into multiple levels. There are generally three tiers, viz access-layer (the lower most layer), the distribute layer (the middle layer), and the core layer (the upper or root layer).
- The tree topology is useful in cases where a star or bus cannot be implemented individually. It is most-suited in networking multiple departments of a university or corporation, where each unit (star segment) functions separately, and is also connected with the main node.

Advantages:

- It is easy to manage and maintain network as peer our needs because of many sub networks or units.
- Easy to find the fault nodes or hubs in the network.
- Make easier to isolate and assign priorities into different level of units.
- It is flexible so we can add and remove any number of nodes.

Disadvantages:

- The failure of root node cause the

failure of entire network.

- It is expensive because of large amount of cables and network devices - hub or switch.
- The data traffic is high at root node so there are may be chance of data collision.

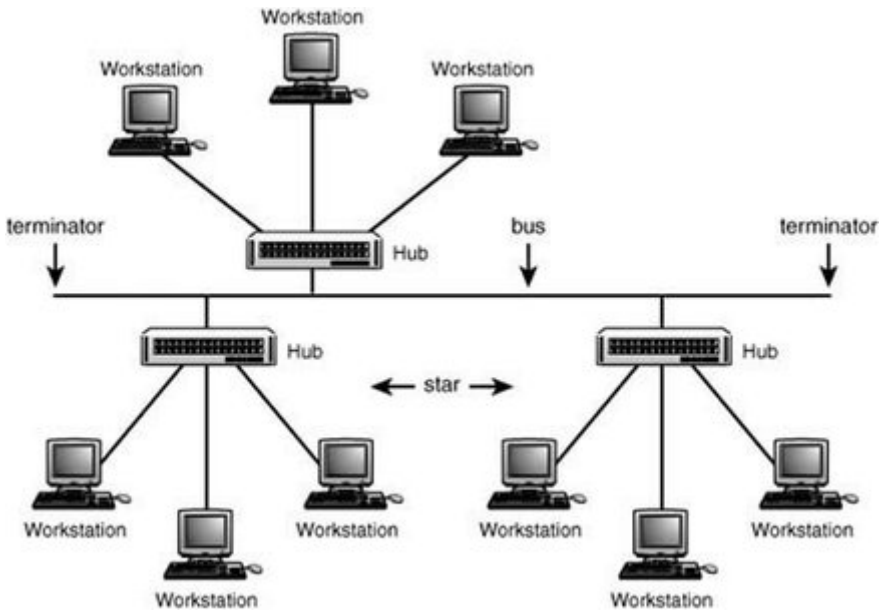

Figure 1.11: Mesh topology.

1.8.0.6 Hybrid Topology

- It two or more topologies are combined together, then it is called hybrid topology.
- Hybrid topology inherits merits and demerits of all the incorporating topologies.
- Most WANs are connected by means of hybrid topology.
- Internet is the best example of the largest hybrid topology.

1.9 Networking Architecture

On the basis of transmission technology or service provided by nodes, there are three types of networking architecture, *client/server network, peer-to-peer network, and active network.*

1.9.1 Client/Server

- The client server model is widely used network model.
- Here, the client refers to the computer or terminal that access the shared resource by another computer (i.e. server) remotely.

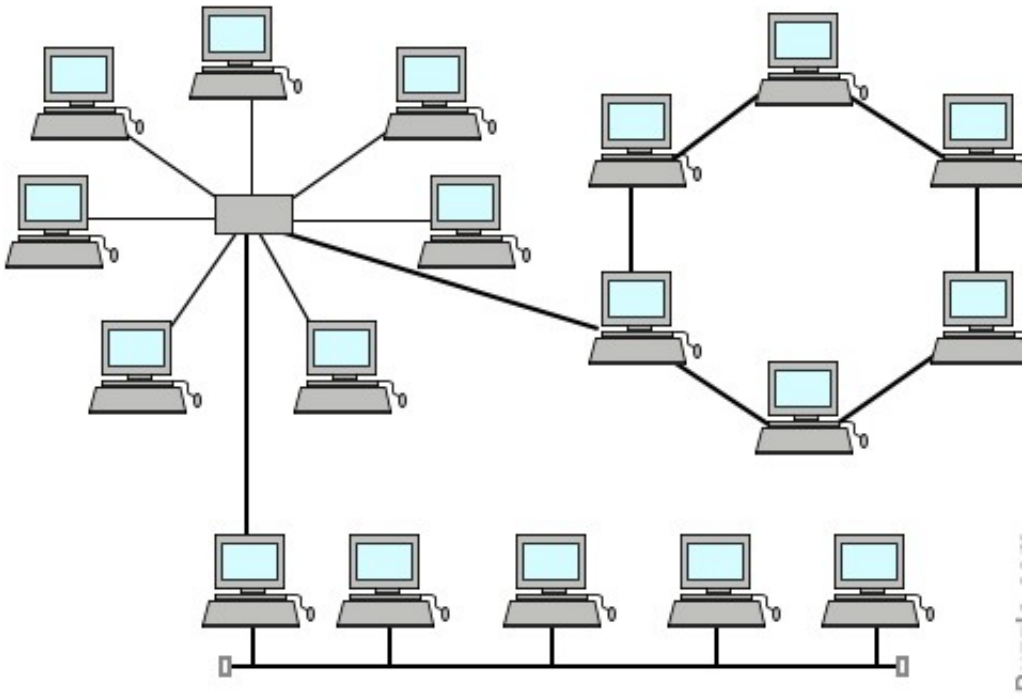

Figure 1.12: Hybrid topology.

- The server is a powerful computer that stores data and information, runs administrative software that controls the access to the network and its resources, and provides the function to the computer working as workstations in the network.

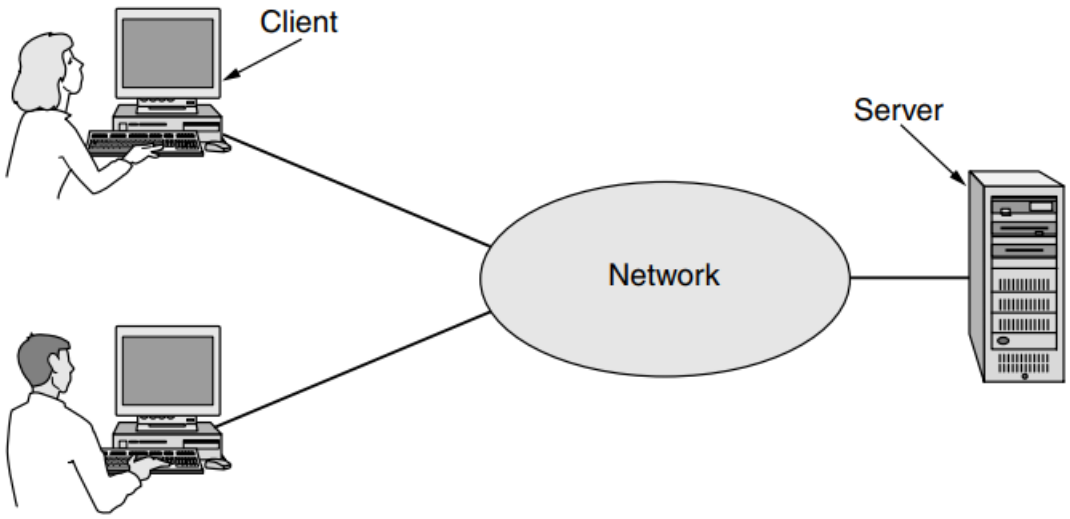

Figure 1.13: A network with two clients and one server

- The system administrator manages the data on the server. The client machine and the

server are connected through a network. It allows the clients to access data even if the client machine and server are far apart from each other.

- For communication in client-server model to take place, the client process on the client machine sends the requests to the server process on the server machine. When the server receives the client request, it lookouts for the requested data and send it back with the reply.

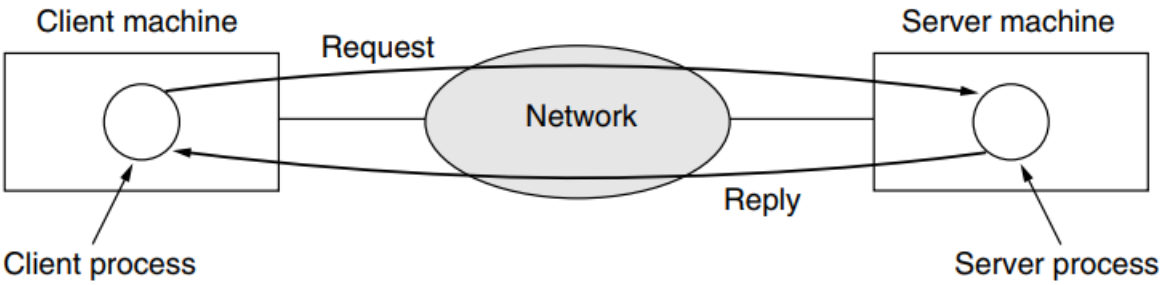

Figure 1.14: The client-server model involves request and replies

1.9.1.1 Features of client-server model

- Dedicated server running NOS software
- Centralized administration
- Backups made easy
- Security
  - Permission - access rights to network resources
    - Authentication: User ID, Password
- Privileges - actions a user can perform on a network
- User accounts with rights to change the system

1.9.1.2 Advantages of Client-server Network

1. A Client/Server network contains the centralized system. Therefore we can back up the data easily.
2. A Client/Server network has a dedicated server that improves the overall performance of the whole system.
3. Security is better in Client/Server network as a single server administers the shared resources.
4. It also increases the speed of the sharing resources.

1.9.1.3 Disadvantages of client-server networks

1. Resources are centralized to the server, so if any problem occurs in the server, the entire network will down.
2. There may be maximum data traffic at server so there may be chances of data collision.
3. It is more expensive due to dedicated requirement of memory and secondary storage and additional network utilized and NOS such as MS Window Server, UNI or Linux etc.
4. It requires dedicated network administrator.

1.9.2 Peer-to-Peer Model

- In peer-to-peer model,network computers are not distinguish as client or server instead each computer can be either client or server depending on whether the computer is providing service requesting service. Each computer acts like a peer with equal privileges and responsibilities for processing the data.
- Many peer-to-peer system, such BitTorrent, do not have any central database of content. Instead, each user maintain his own database locally and provides a list of other nearby people who are members of the system. A new user can then go to any existing member to see what he has and get the names of other members to inspect for more content and more names. This lookup process can be repeated indefinitely to build up a large local database of what is our there.
- Peer-to-peer communication is often used to share music and video. E.g. Napster (1999-2000), an online music file sharing service created by Shawn Fanning.
- One of the most popular internet applications of all, email, is inherently peer-to-peer.

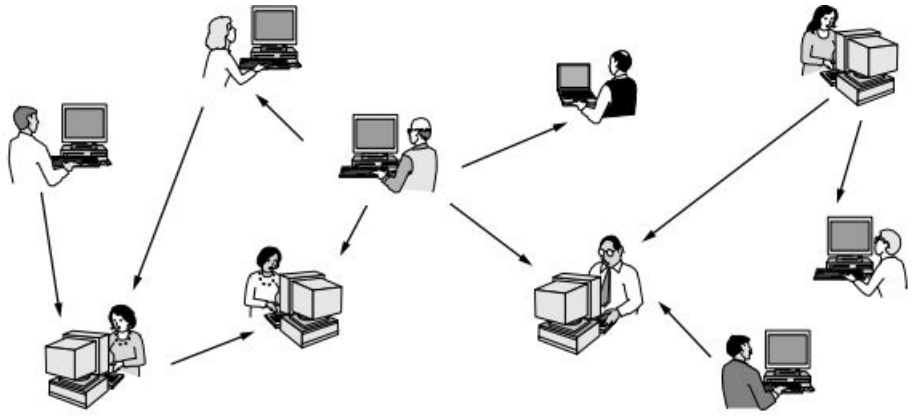

Figure 1.15: A peer-to-peer network

1.9.2.1 Feature of P2P

- Peer-To-Peer network is useful for small environments, usually up to 10 computers.
- Peer-To-Peer network has no dedicated server.
- Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.

1.9.2.2 Advantages of P2P

- As a peer joins the network, it adds resources to the existing network, adding more members to the system,increase the capacity or resources of the system itself. The throughput of the network increases. Such networks also scale better, an increase in members increases efficiency.
- Very robust as there is no single point of failure. If one fails, just that connection is lost, the network will go on functioning.
- Since the machine are independent of each other, operation and set up is easier and cheaper than client server model.
- Tt is less costly as it does not contain any dedicated server.

1.9.2.3 Disadvantages of P2P

- P2P networks have high bandwidth consumption rates, due to multiple request and responses taking place at the same time from different peers.
- Lack of security, no checking of authentication takes place. So anyone can send and receive data from anybody.

1.9.3 Active Network

- Active network model is a communication model in which packets flowing through a network can - dynamically change or modify the operation of the network. [1]
- The packets used are known as active packets.
- Active networking places computation within packets travelling through the network.
- It allows sending code along with packets of information allowing the data to change its form (code) to match the channel characteristics.
- One of the challenges of active networking has been the inability of information theory to mathematically model the active network paradigm and enable active network engineering.

[1] `https:link.springer.com/chapter/10.1007/3-540-47734-9_60`

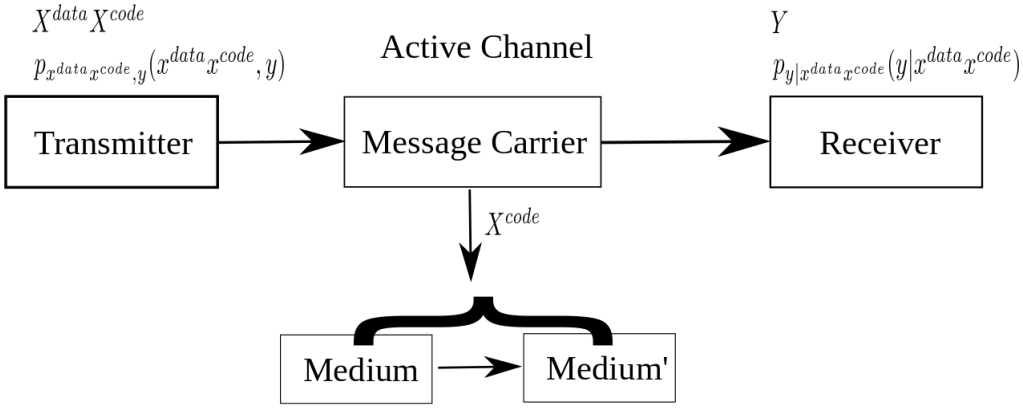

Figure 1.16: An active network channel uses executable code in the packet to impact the channel controlling the relationship between the transmitted sequence $\boldsymbol{X}$ and the received sequence $\boldsymbol{Y}.\boldsymbol{X}$ is composed of a data portion X^{data} and a code portion X^{code}. Upon incorporation of X^{code} , the channel medium may change its operational state and capabilities.

1.10 Network Software

Network software is a set of primitives that define the protocol between two machines. The network software resolves an ambiguity among different types of network making it possible for all the machines in the network connect and communicate with one another and share information.

Network software is the information, data or programming used to make it possible for computer to communicate or connect to one another.

Network software is used to efficently share information among computers. It encloses the information to be sent in a "package" that contains a "header" and a "trailer". The header and trailer contain information for the receiving computer, such as the address of that computer and how the information package is coded. Information is transferred between computers as either electrical signals in electric wires, as lights in fiber-optic cables, or as electromagnetic waves through space.

1.10.1 Protocol Hierarchies

- To reduce the design complexity, most networks are organized as a stack of layers or levels, each one built upon one below it.
- The number of layers, the name of each layers, the contents of each layers, the function of each layer differ from network to network.
- Each layer offer certain service to the higher layer but do no show the actual implementation of those services. In a sense, each layer is a kind of virtual machine offering certain services to the layer above it.
- When layer n of one computer communicates with layer n of another computer within a network, the set of rules specified for this communication is known as layer *n protocol*.
- Basically, a **protocol** is a special set of rules ,agreed between communicating parties, that should be followed to communicate within a network.
- Each layer passes data and information to the layer below it until it reaches lowest layer (physical layer). The actual communication occurs in physical layer via a physically connected mediums.
- Between each pair of adjacent layers, there is an ***interface*** that defines the set of *services* offered by the lower layer to the upper layer.

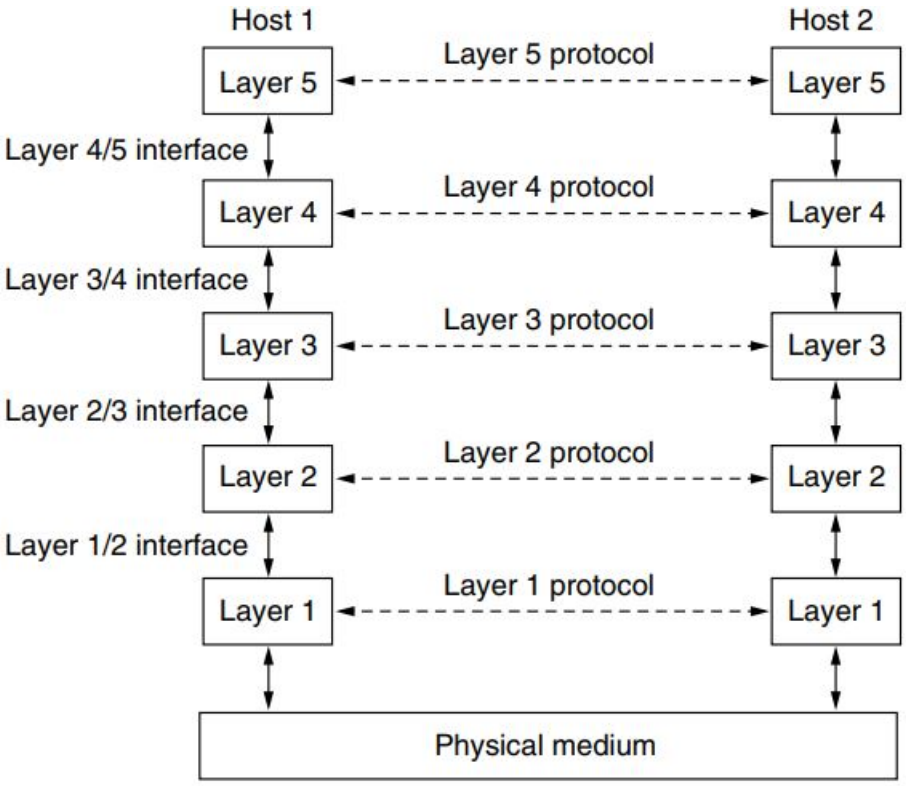

Figure 1.17: Layers protocols and interfaces.

Figure 1.17 illustrates the five-layer network. The entities comprising the corresponding layers on different machines are called ***peers***. The peers may be software process, hardware devices, or even human beings. It is the peer that communicate by using the protocol to talk to each other.

Network protocols have three basic components: syntax, semantics and timing.

Syntax defines the structure or format of the data i.e. it defines the order in which pieces of information will be packaged by the sender and received by the receiver. For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of bits to be the message.

Semantics means how the individual pieces of information within a network protocol is interpreted. It helps the network know which fields define what action within the send or receive stream of bytes.

Timing defines what data should be sent/receive and when to sent/receive it. To effectively communicate, a protocol needs to ensure the speed at which the data should be send, and the speed at which it is being received i.e speed should not be too high or low for other. For example, if a sender is sending data 100 Mbps, but the receiver can process data at 10 Mbps, then the receiver buffer may be overfull soon and data may be lost during transmission.

Standards

- A formalized regulations that must be followed.
- Are guidelines that explain to all IT stakeholders-from device manufacture to software programmers and network administrators-how a particular protocol should operate.
- Defines interoperability between different devices or systems of different vendors.
- Data communications standards fall under two categories: De facto (meaning "by fact" or "by convention") and De jure (meaning "by law" or "by regulation").

Network Architecture

- A set of layers and protocols is called *network architecture*.
- The specification of an architecture must contain enough information to allow an implementer to write the program or build hardware for each layer so that it will correctly obey the appropriate protocol.
- The details of the implementation and the specification of the interfaces are not part of the architecture because these are hidden away inside the machines and not visible form the outside.
- A list of the protocols used by a certain system, one protocol per layer, is called **protocol stack**.

The important thing to understand about figure 1.18 is the relation between the virtual

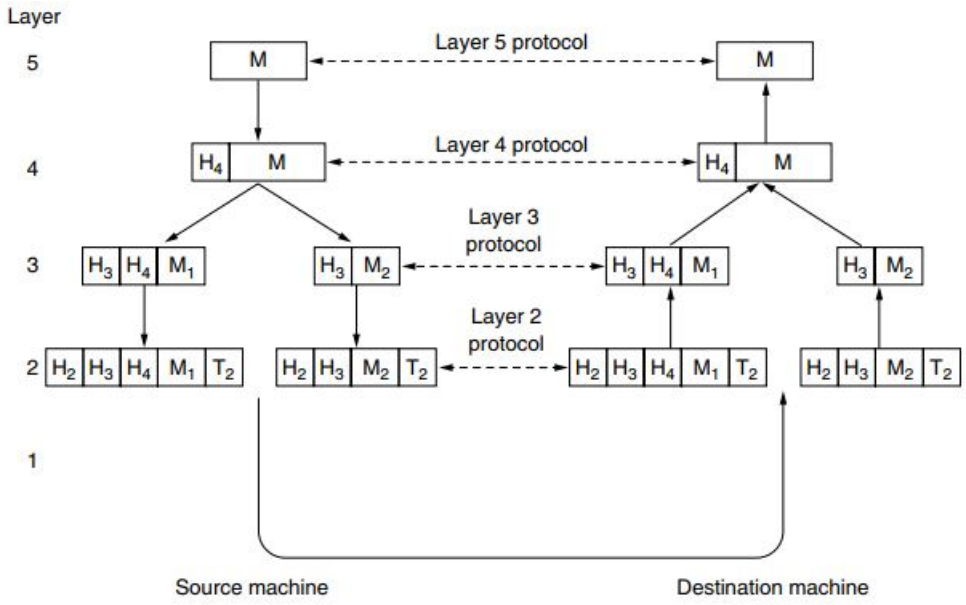

Figure 1.18: Example information flow supporting virtual communication in layer 5.

and actual communication and the difference between protocols and interfaces. The peer processes in layer 4, for example, conceptually think of their communication as begin "horizontal" using the layer 4 protocol. Each one is likely to have procedures called something like *SendToOtherSide* and *GetFromOtheSide*, even though these procedures actually communicate with lower layers across the 3/4 interface, and not with other side.

The peer process abstraction is crucial to all network design. Using it, the unmanageable task of designing the complete network can be broken into several smaller, manageable design problems, namely, the design of the individual layers.

1.10.2 Design Issues of the Layers

1.10.2.1 Reliability

- Reliability is the design issue of making a network that operates correctly even though it is made up of a collection of components that are themselves unreliable. Packets travelling through network may get corrupted, lost or duplicated due to fluke electrical noise, random wireless signals, hardware flaws, software bugs and so on.

- The possible errors can be detected using **error detection** code in sending information. Information that is incorrectly received can then be retransmitted until it is received correctly. Moreover, **error correction** code can be implemented to recover correct message from possible incorrect bits that were originally received.

- Another reliability issue is finding a suitable path through a network to route the in-

formation from source to destination as there exist multiple paths to destination, and possibly some paths, or links may be broken. For this **routing** is to be taken automatically.

1.10.2.2 Evolution of Network

- A second design issue is concerned with evolution of network as over time, network can grow large and new designs emerges that need to be connected to existing system. The change in network is supported by **protocol layering**.
- Design that continue to work well when the network get large are said to be **scalable**.
- In addition, proper **addressing** or **naming** mechanism is to be considered to identify proper sender and receiver that involve in particular message on each layer.

1.10.2.3 Resource Allocation

- A third design issue is resource allocation. Networks provide a service to hosts from their underlying resources, such as the capacity of transmission lines i.e bandwidth. Different **multiplexing** techniques are used to share bandwidth among the hosts.
- Also, **flow control** mechanism is employed between sender and receiver to synchronize the sending and receiving data. In addition, **congestion control** method is deployed to overcome the overloading of the network.
- **Quality of Service** is to be maintained for providing high throughput and less delay for real-time delivery of packets for such as live video.

1.10.2.4 Security

- The last major design is to secure the networks by defending it against different kinds of threats.
- The threats can be eavesdropping on communication.
- To prevent threat, **confidentiality, authentication and integrity** are used.
- Confidentiality maintains the data to be secure through encryption, authentication prevents intruder from impersonating, while integrity prevents surreptitious changes to messages, such as altering "debit my account Rs.1000" to "debit my account Rs.100000".
- All these issues are based on cryptography.

1.10.3 Connection-Oriented Verus Connectionless Service

- Layers can offer two different types of service to the layers above them: *connection-oriented* and *connectionless*.

- Connection-oriented service is modeled after the telephone system.
- In a connection-oriented network service, the service user first establishes a connection, uses the connection, and then releases the connection.
- In some case when a connection is established, the sender, receiver, and subnet conduct a negotiation about the parameters to be used,such as maximum message size, quality of service required, and other issues.
- Each kind of service can further be characterized by its reliability. Some services are reliable in the sense that they never lost data. Usually, a reliable service is implemented by having the receiver acknowledge the receipt of each message so that the sender is sure that it arrived.
- Reliable connection-service has two minor variations: message sequences and byte streams. In the former variant, the message boundaries are preserved. When two 1024-bye messages are sent, they arrive as two distinct 1024 byte messages, never as one 2048-byte message. In the latter, the connection is simply a stream of bytes, with no message boundaries. When 2048 bytes arrive at receiver, there is no way to tell if they were sent as one 2048 byte message, two 1024 byte message, or 2048 1-byte message.
- Data in connection-oriented network is generally called **packet**.

- Unlike connection-oriented service, connectionless service does not require connection establishment between two parties; the sender simply send the data and it travels through the network unreliably to the destination. For example: spammers sending electronics junk-mail to many recipients.
- Unreliable (meaning not acknowledged) connectionless service is often called **datagram** service.
- In some application, acknowledged datagram service is used in which initial connection establishment is not prior important, but reliability is essential. E.g. text messaging in mobile phone.
- Still another service is r**equest-reply service**.

1.10.4 Service Primitives

- A service is formally specified by a set of primitives (operations) available to user processes to access the service.
- These primitives tell the service to perform some action or report an action taken by a peer entity.
- If the protocol stack is located in the operating system, as it often is, the primitives are normally system calls. These call cause a trap to kernel mode, which then turns control

	Service	Example
Connection-oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Movie download
	Unreliable connection	Voice over IP
Connection-less	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Text messaging
	Request-reply	Database query

Figure 1.19: Six different types of services.

of the machine over to the operating system to send the necessary packets.
- The set of primitives for connection-oriented service are different from those of connectionless service.

Table 1.1: Six services primitives that provide a simple connection-oriented service.

Primitives	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection with a waiting peer
ACCEPT	Accept an incoming connection from a peer
RECEIVE	Block waiting fro an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection

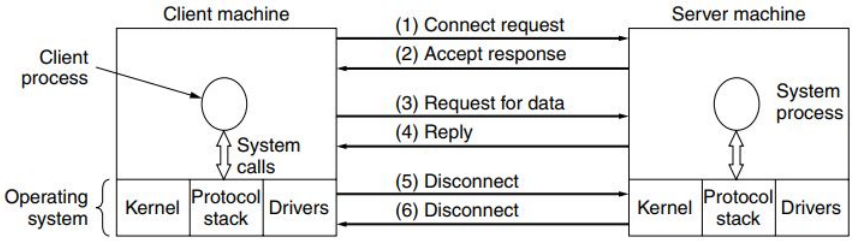

Figure 1.20: A simple client-server interaction using acknowledge datagrams.

1.10.5 The Relationship of Services to Protocols

Service and protocols are different. A ***service*** is a set of primitives (operations) that a layer provides to the layer above it. The service defines what operations the layer is

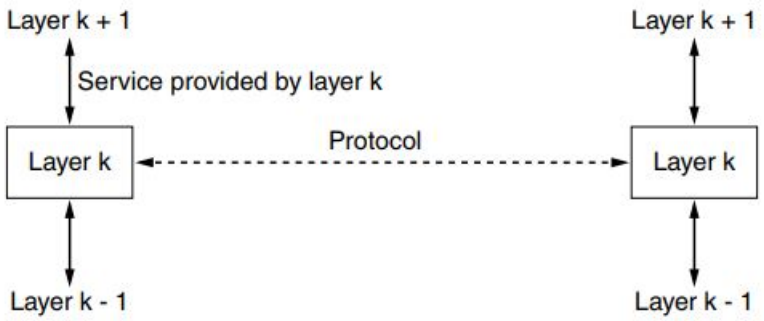

Figure 1.21: The relationship between a service and protocol.

prepared to perform on behalf of its users, but it says nothing at all about how these operations are implemented. A servive relates to an interface between two layers, with the lower layer being the service provider and the upper layer being the service user.

A layer's interface tells the processes above it how to access it. It specifies what the parameters are and what results to expect. It, too, say nothing about how the layers work inside.

A ***protocol***, in contrast, is a set of rules governing the format and meaning of the packets, or messages that are exchanged by the peer entities within a layer. Entities use protocols to implement their service definitions. They are free to change protocols at will, provided they do not change the service visible to their users.

Service relates to the interfaces between layers. In contrast, protocols relate to the packets sent between peer entities on different machines.

1.11 Reference Models

- A *reference model* is a conceptual blueprint of how communication should take place.
- It addresses all the processes required for effective communication and divides them into logical groupings called layers.
- When a communication system is designed in this manner, it's known as a hierarchical or ***layered architecture***.

1.11.1 Advantages of Reference Model

1. It divides the network communication process into smaller and simpler components, facilitating component development, design, and troubleshooting.
2. It allows multiple-vendor development through the standardization of network components.

3. It encourages industry standardization by clearly defining what function occur at each layer of the model.
4. It allows various types of network hardware and software to communicate.
5. It prevents changes in one layer from affecting other layers to expedite development.

1.11.2 Internetworking Model

History: When networks first came into being, computers could typically communicate only with computer from the same manufacture. For example, companies ran either a compete DECnet solution or an IBM solution, never both together. In the late 1970s, the *Open System Interconnection (ISO) reference model* was created by the International Organization for Standardization (ISO) to break through this barrier.
The OSI model was meant to help vendors create interporable network devices and software in the form of protocols so that different vendor networks could work in peaceable accord with each other.
The OSI model is the primary architectural model for networks. It describes how data and network information are communicated from an application on one computer through the network media to an application on another computer. The OSI reference model breaks this approach into layers.

1.11.3 The OSI Reference Model

- The Open System Interconnection reference model (OSI-RM) is the primary architectural network. It describes how data and network information are communicated from an application on one computer through the network media to an application on another computer.
- The Open Systems Interconnection (OSI) Model was developed by International Organization for standardization (ISO) in 1978 and revised in 1984.
- It is developed to allow systems with different platforms to communicate with each other. Platform could mean hardware, software or operating system.
- Although, the OSI model incorporates protocols, that can be used to implement a network stack, these protocols are not quite used due to the popularity of the TCP/IP protocol suite.
- The OSI has seven layers, divided into two groups. The top three layers define how the applications within the end stations will communicate with each other as well as with users. The bottom four layers define how data is transmitted end-to-end.

The OSI Reference model has following seven layers:

- Application layer (layer 7)
- Presentation layer (layer 6)
- Session layer (layer 5)
- Transport layer (layer 4)
- Network layer (layer 3)
- Data layer (layer 2)
- Physical layer (layer 1)

Mnemonic to remember the seven layers: **A**ll **P**eople **S**eem **T**o **N**eed **D**ata **P**rocessing.

Application	• Provides a user interface
Presentation	• Presents data • Handles processing such as encryption
Session	• Keeps different applications' data separate

Figure 1.22: The three upper layers of OSI and their function

Transport	• Provides reliable or unreliable delivery • Performs error correction before retransmit
Network	• Provides logical addressing, which routers use for path determination
Data Link	• Combines packets into bytes and bytes into frames • Provides access to media using MAC address • Performs error detection not correction
Physical	• Moves bits between devices • Specifies voltage, wire speed, and pinout of cables

Figure 1.23: The four bottom layers of OSI and their functions.

Data Encapsulation:

All network on a network originates at a source, and are sent to a destination. The information sent on a network is referred to as data or data packets. If one computer (Host A) wants to send data to another computer (Host B), the data must first be packaged through a process called encapsulation.

Encapsulation wraps data with the necessary protocol information before network transit. Therefore, as the data packet moves down through the layers of the OSI model, it receives header, trailers, and other information.

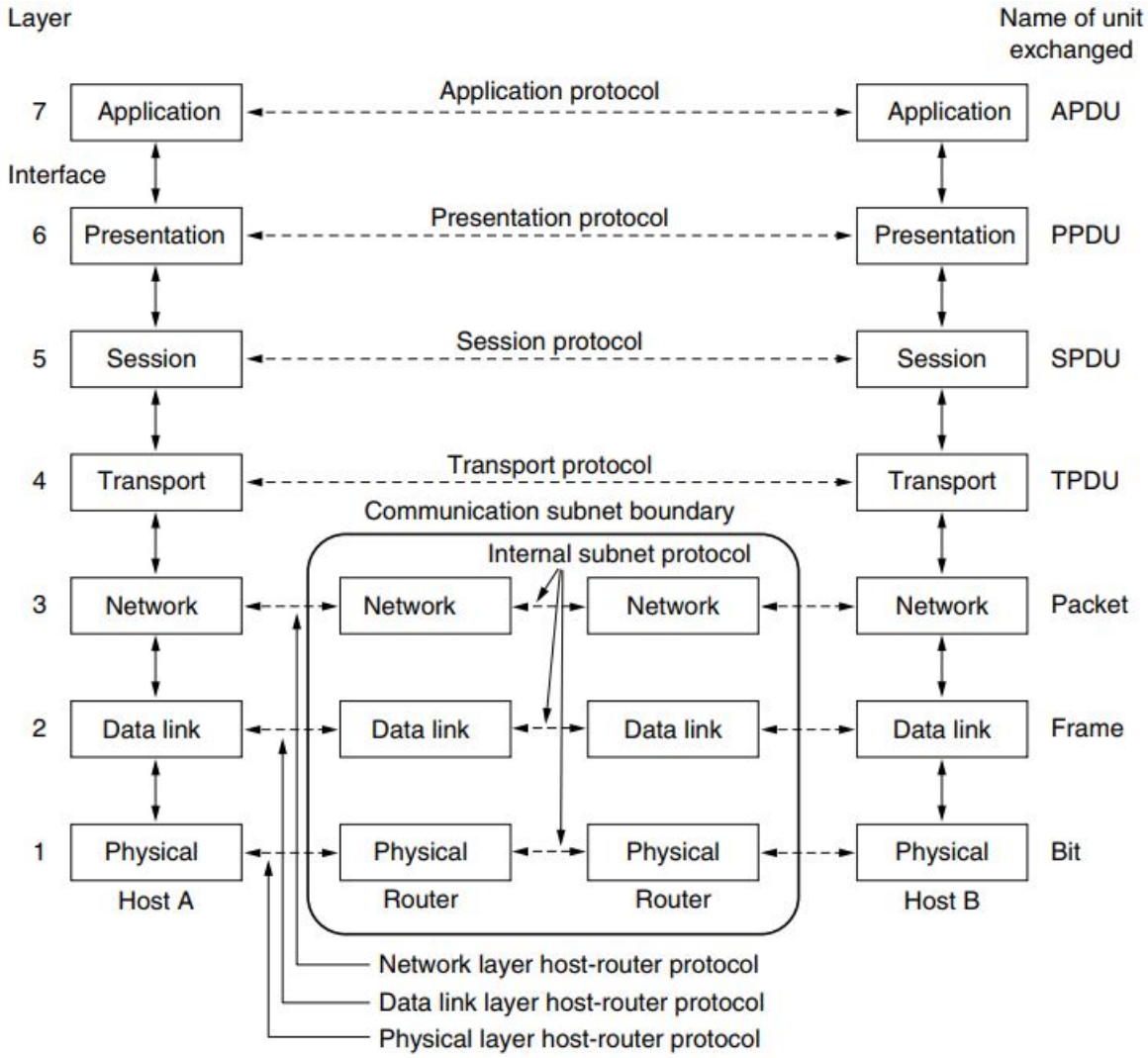

Figure 1.24: The OSI reference model.

Encapsulation:
Data-> Segment -> Packet -> Frame -> Bits

How data is referred in OSI?

1.11.4 Seven Layers of OSI Reference Model

Layer 1: Physical Layer

- The physical layer is concerned with transmitting raw bits over a communication channel.
- The physical layer deals with the physical characteristics of the transmission medium.
- It defines the electrical, mechanical, procedural, and functional specifications for activating, maintaining, and deactivating the physical link between end systems.

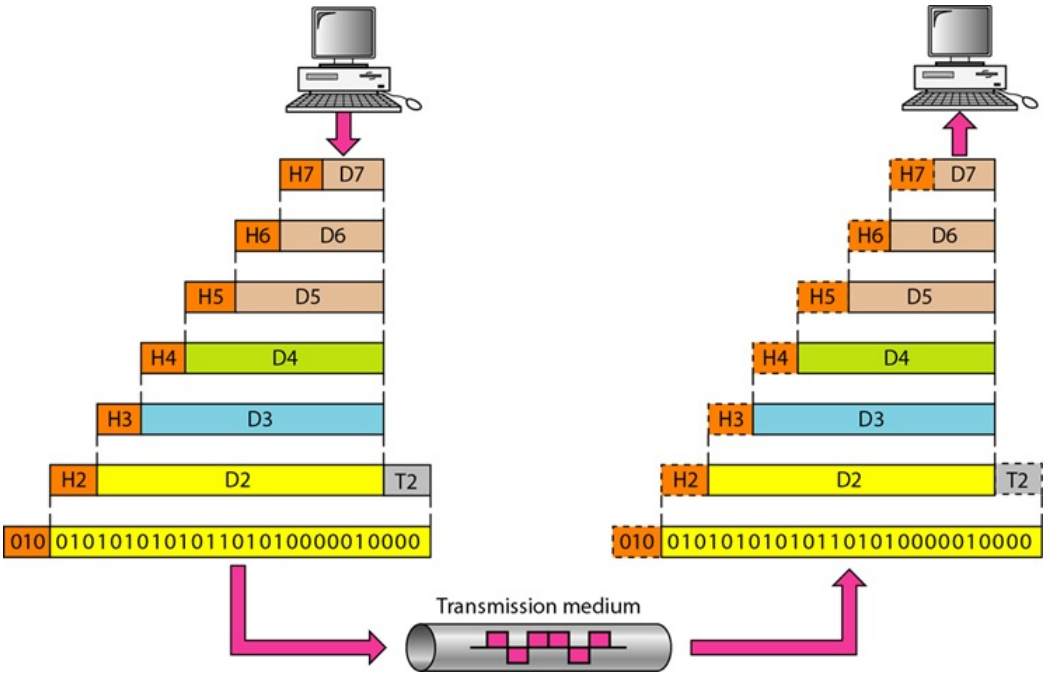

Figure 1.25: Data Exchange using OSI-Reference Model.

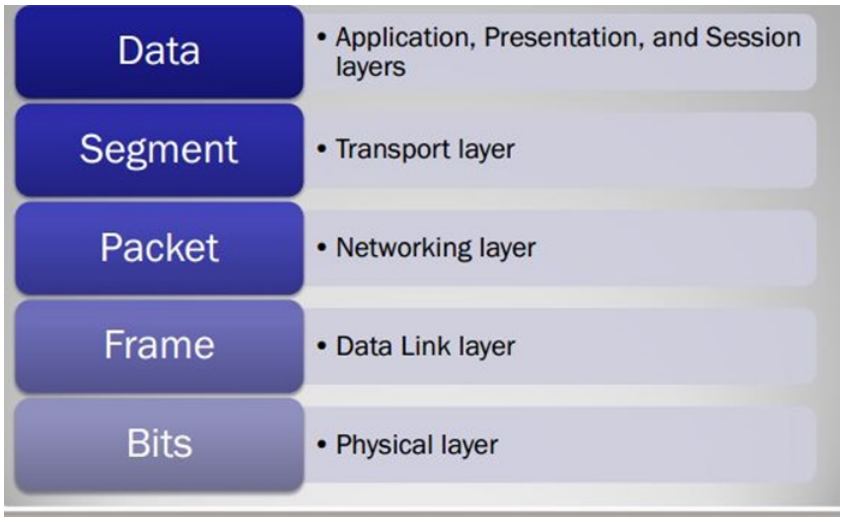

Figure 1.26: Data Encapsulation .

- Such characteristics as voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, physical connectors, and other similar attributes are defined by physical layer specifications.

Layer 2: Data Layer

- The Data Link layer provides the physical transmission of data to the device on LAN using physical addressing and handles error notification, network topology, access control, and flow control.

- On the sender side, the Data Link layer receives the data from Network Layer and divides the stream of bits into fixed size manageable units called as Frames and sends it

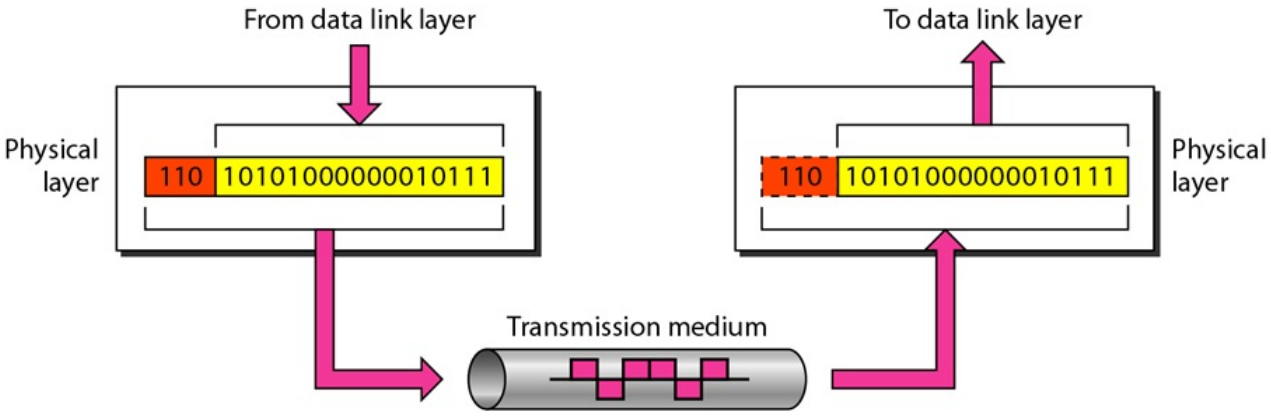

Figure 1.27: Physical Layer .

to the physical layer. This process is called Framing. On the receiver side, the data link layer receives the stream of bits from the physical layer and regroups them into frames and sends them to the Network layer.
- The IEEE Ethernet Data Link Layer has two sublayers: Media Access Cotrol (MAC) layer and Logical Link Control (LLC) layer.

- Functions of data link layer are:

- **Framing** - Divides the stream of bits into data unit called frames.
- **Physical Addressing** - If frames are to be distributed to different system on the network, data link layer adds a header to the frame to define the sender and receiver.
- **Flow Control** - If the rate at which the data are received by the receiver is less than the rate at which data are sent by sender, the data link layer imposed a flow control mechanism to avoid overwhelming of the receiver.
- **Error Control** - Used for detecting and retransmitting damaged or lost frames and prevent duplication of frames. This is achieved through a trailer added to the end of the frame.
- **Access Control** - When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

Layer 3: Network Layer
- The network layer routes the packets from source to destination host. Hence it may have to route the data through multiple networks via multiple intermediate devices. In order to achieve this the network layer relies on two things, logical addressing and routing.
- The network layer at the sending side accepts data from the transport layer, divides

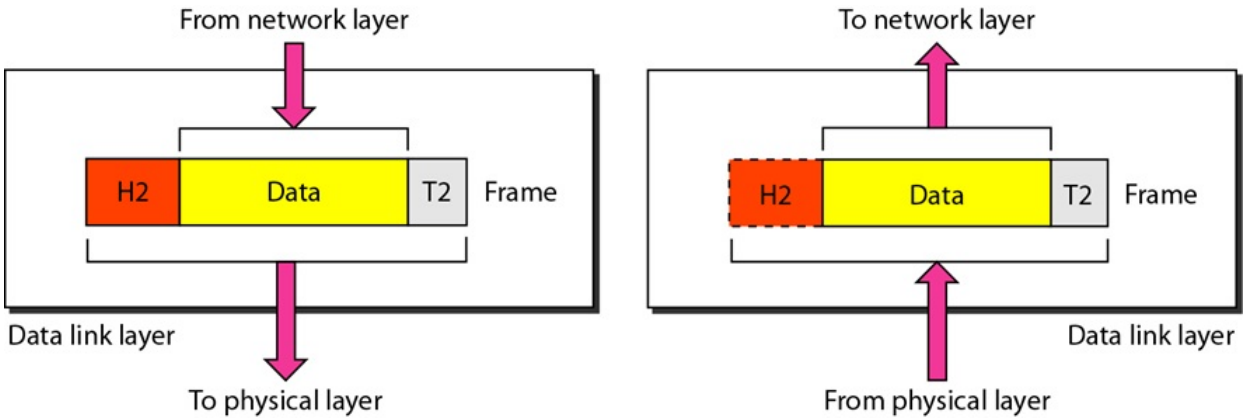

Figure 1.28: Data Layer .

it into packets, adds addressing information in the header and passes it to the data link layer. At the receiving end the network layer receives the frames sent by data link layer, converts them back into packets, verifies the physical address (verifies if the receiver address matches with its own address) and the send the packets to the transport layer.
- The network layer handles the congestion in subnet as well as quality of service (delay, transit time, jitter etc,) of the network.
- The router works on this layer. - If two systems are connected to the same link, there is usually no need for network layer. However, if the two systems are attached to different networks (links) with connecting devices between networks, there is often a need for the network layer to accomplish source-to-destination delivery (i.e host-to-host delivery).

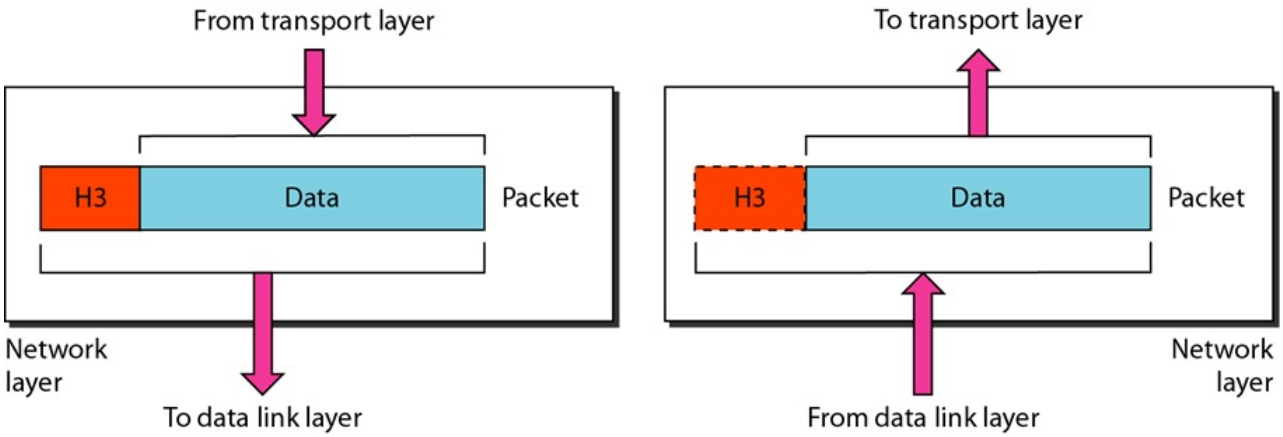

Figure 1.29: Network Layer.

Layer 4: Transport Layer

- The transport layer accepts a message from the (session) layer above it, splits the message into smaller unit (segments) and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.

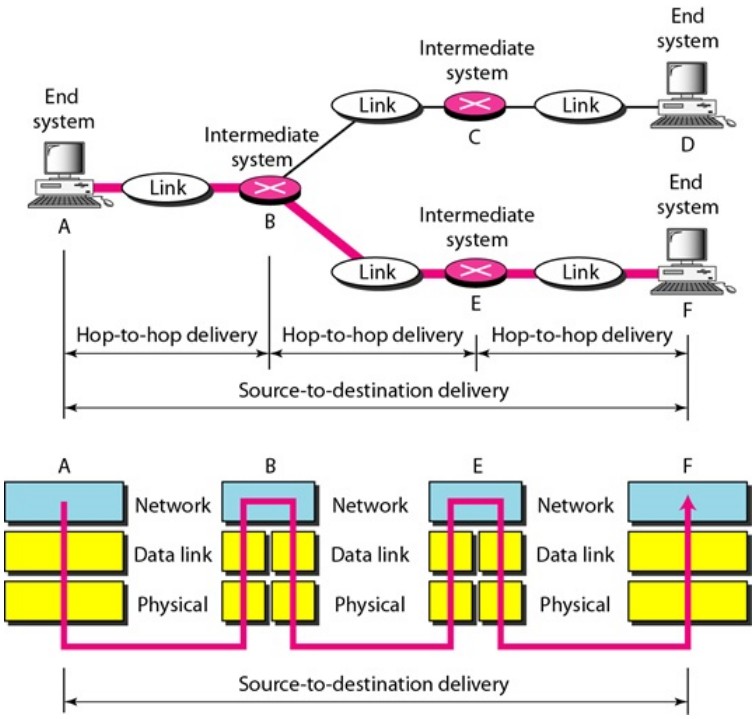

Figure 1.30: End-to-End Delivery.

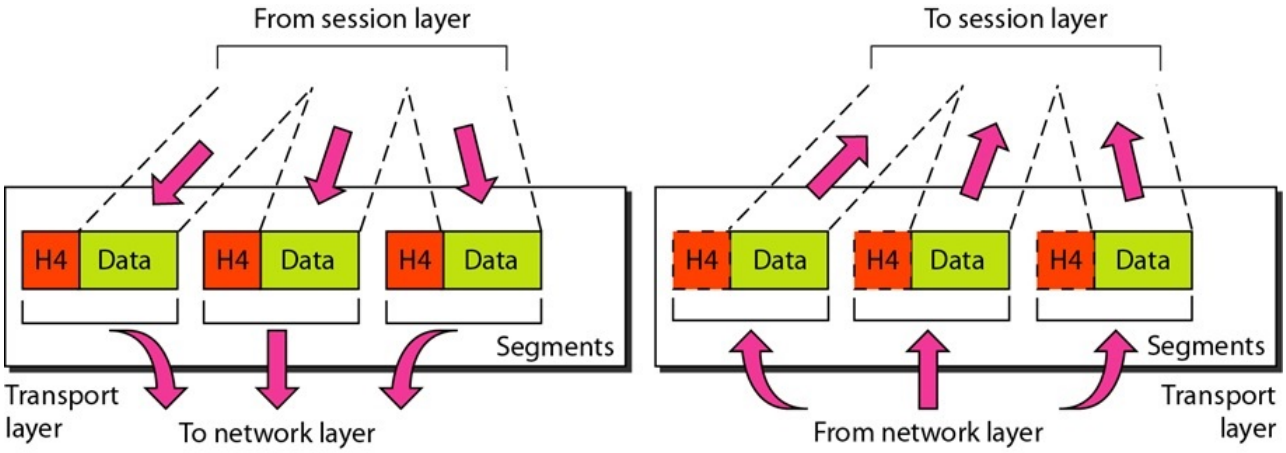

Figure 1.31: Transport Layer.

- The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. using flow control.
- To ensure process to process delivery the transport layer makes use of port address to identify the data from the sending and receiving process (port addressing).
- The data can be transported in a connection oriented or connectionless manner. (i.e TCP and UDP protocol resides in it)
- Also, transport layer multiplexs data from several sources for transmission over one data path.

Layer 5: Session Layer

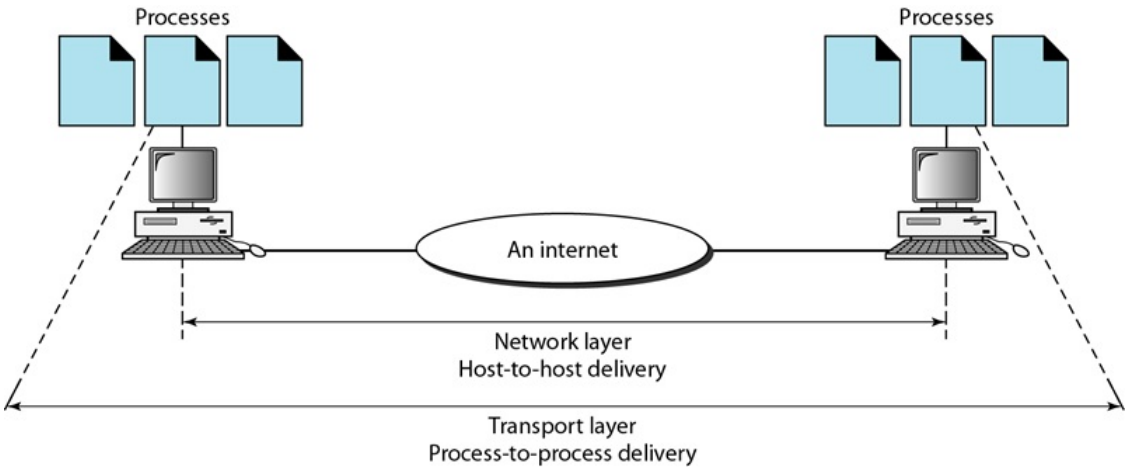

Figure 1.32: Process-to-process delivery.

- The session allows users on different machines to establish *sessions* (set up, manage and terminate) between them.
- Session offers various services such as:

  - dialog control (keeping track of whose turn it is to transmit, defines communication mode i.e. simple, half duplex and full duplex),
  - token management (preventing two parties from attempting the same critical operation simultaneously), and
  - synchronization (checkpointing long transmission to allow them to pick up from where they left off in the event of a crash and subsequent recovery.

- Also, session layer keeps different application data separate from other application data.

Layer 6: Presentation Layer

- The presentation layer is concerned with the syntax and semantics of information of transmitted.
- In order to make it possible for computers with different internal data representation to communicate, presentation layer defines the format in which the data is to be exchanged between the two communicating entities before transmission.
- The presentation layer at sending side receives the data from the application layer adds header which contains information related to encryption and compression and sends it to the session layer.
- At the receiving side, the presentation layer receives data from the session layer decompresses and decrypts the data as required and translates it back as per the encoding scheme used at the receiver.
- Major Functions: data translation and code formatting, data compression, decompression, encryption and decryption

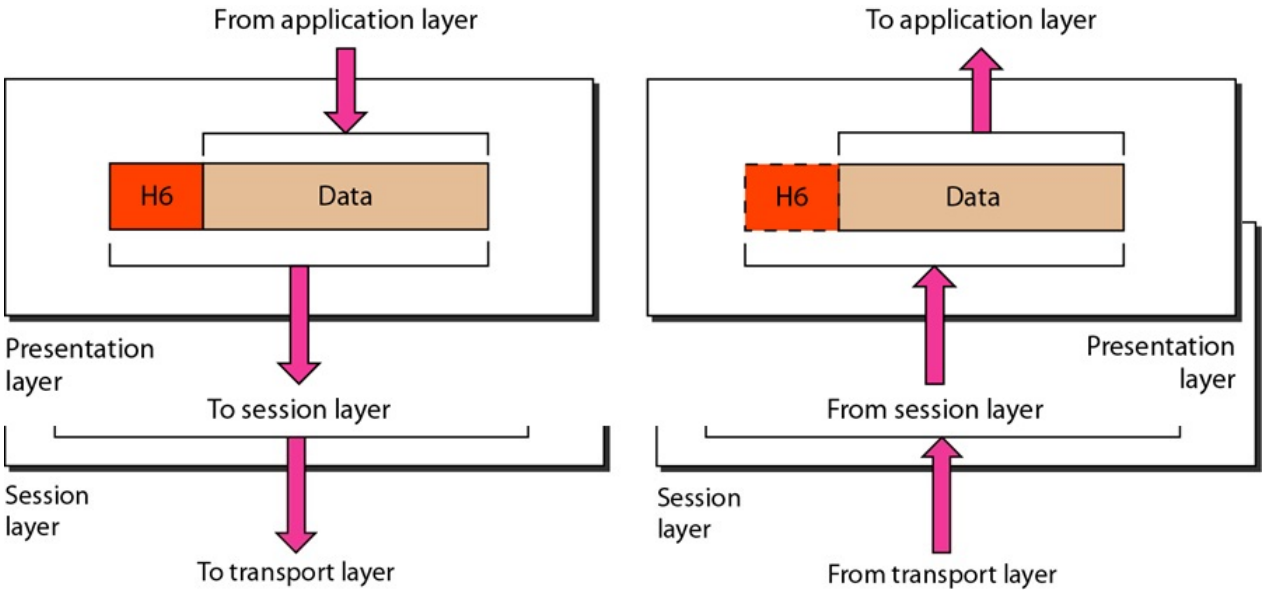

Figure 1.33: Session layer.

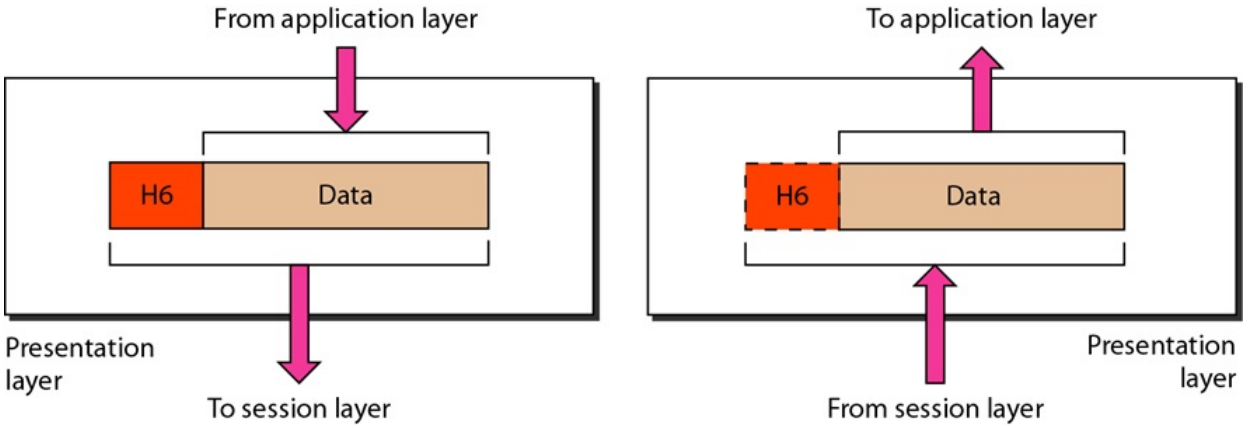

Figure 1.34: Presentation layer.

Layer 7: Application Data

- The application layer acts as user interface between application program and the network.

- Various protocols needed by user are implemented in application layer such as HPPT, FTP, Telnet etc., and similar protocols that can be implemented as utilites the user can interface with.

- Network Virtual Terminal- A network virtual terminal is a software version of a physical terminal and allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal, which, in turn, talks to the host,and vice-versa. The remote host believes it is communicating with one of its own terminals and allows you to log on.

- File transfer, access and management (FTAM)- This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
- Mail services - This application provides the basis for e-mail forwarding and storage.
- Directory services - This application provides distributed database sources and access for global information about various objects and services.

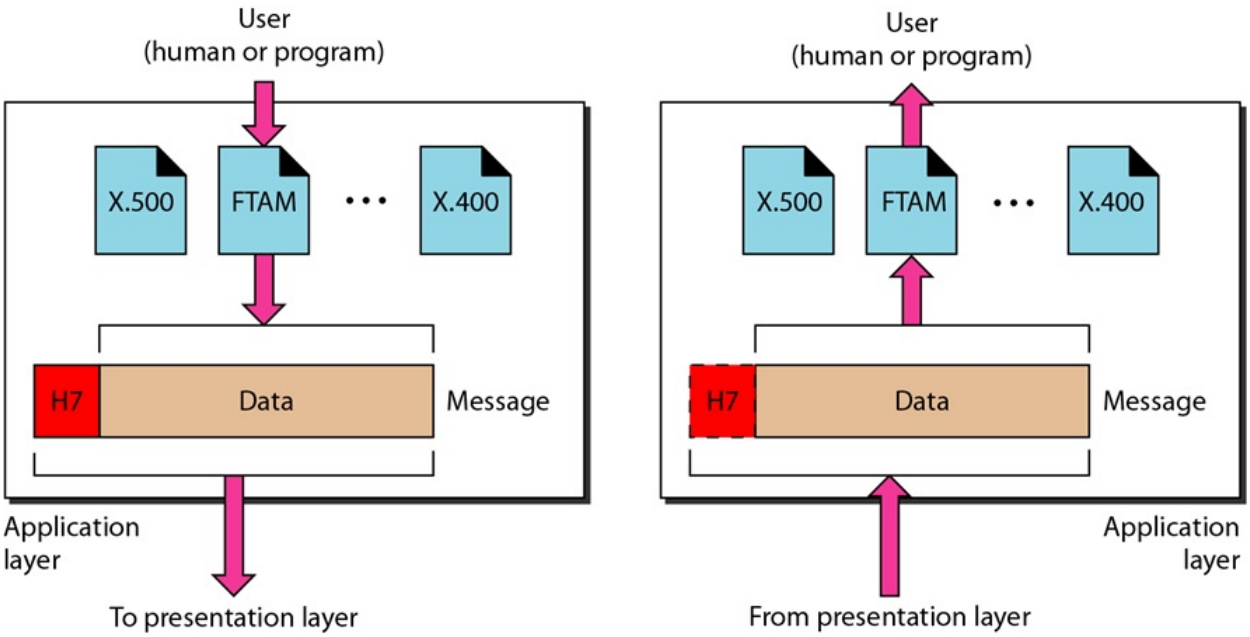

Figure 1.35: Application layer.

Summary of Layers

1.11.5 TCP/IP Protocol Suite

- The TCP/IP protocol suite is the computer networking model and set of communications protocols used on the Internet today and similar computer networks.
- TCP/IP provides end-to-end connectivity specifying how data should be packetized, addressed, transmitted, routed and received at the destination.
- Often also called the *Internet model*, it was originally also known as the DoD model, because the development of the networking model was funded by DARPA, an agency of the United States Department of Defense.
- It is a hierarchical model, i.e. There are multiple layers and higher layer protocols are supported by lower layer protocols. - It existed even before the OSI model was developed.

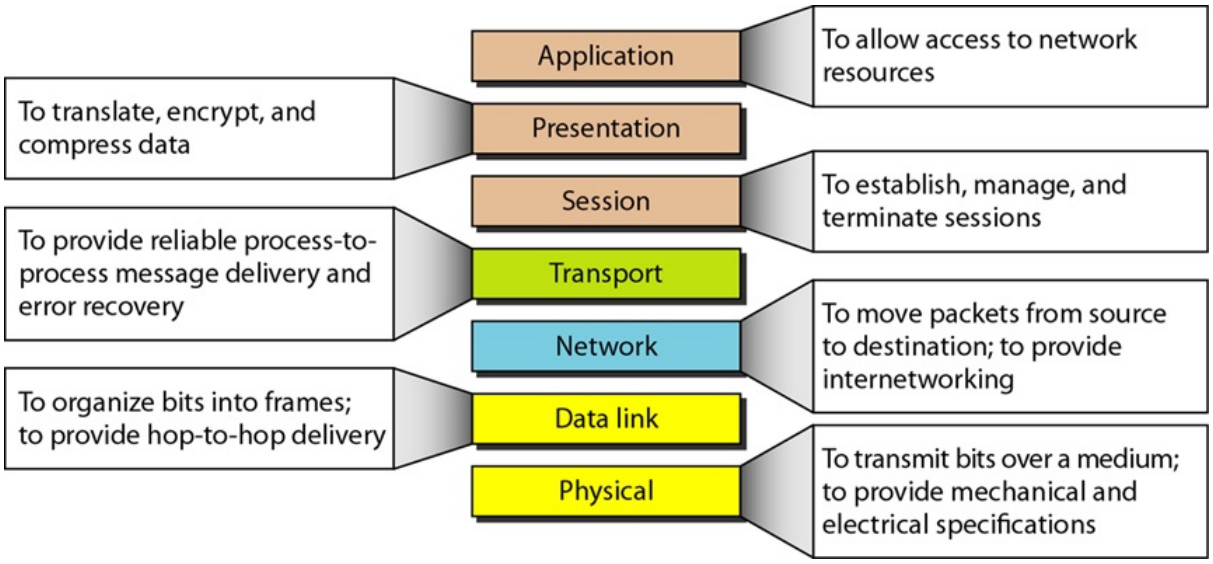

Figure 1.36: Summary of OSI Reference Layer.

- Originally had four layers (bottom to top):

1. Host to Network Layer/Network Access Layer/Network Interface Layer/Link Layer
2. Internet Layer
3. Transport Layer, or Host-to-Host Layer
4. Application Layer

- However, when TCP/IP is compared to OSI, we can say that the TCP/IP protocol suite is made of five layers: *physical, data link, network, transport, and application*.

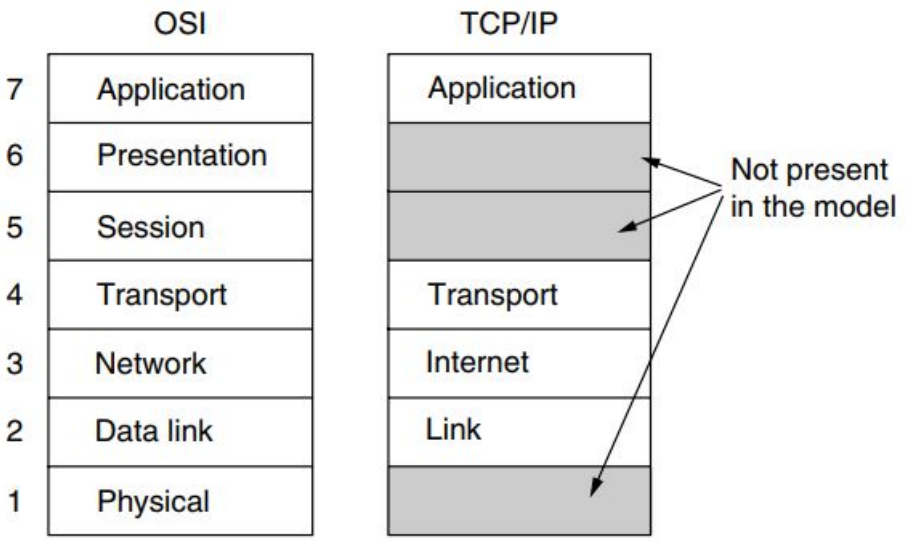

Figure 1.37: The TCP/IP Reference Model

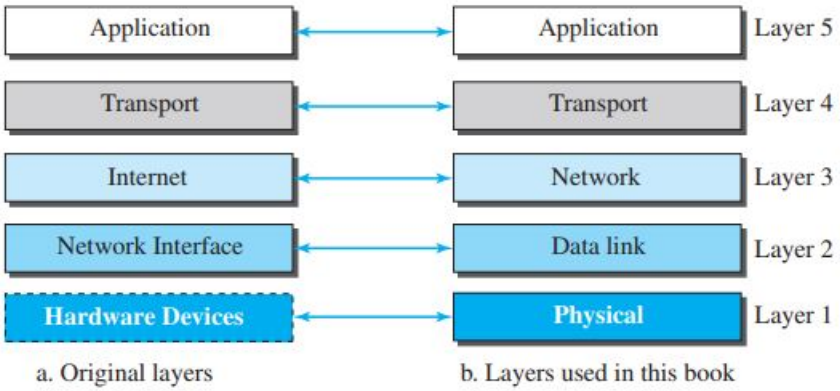

Figure 1.38: Layers in TCP/IP protocol suite

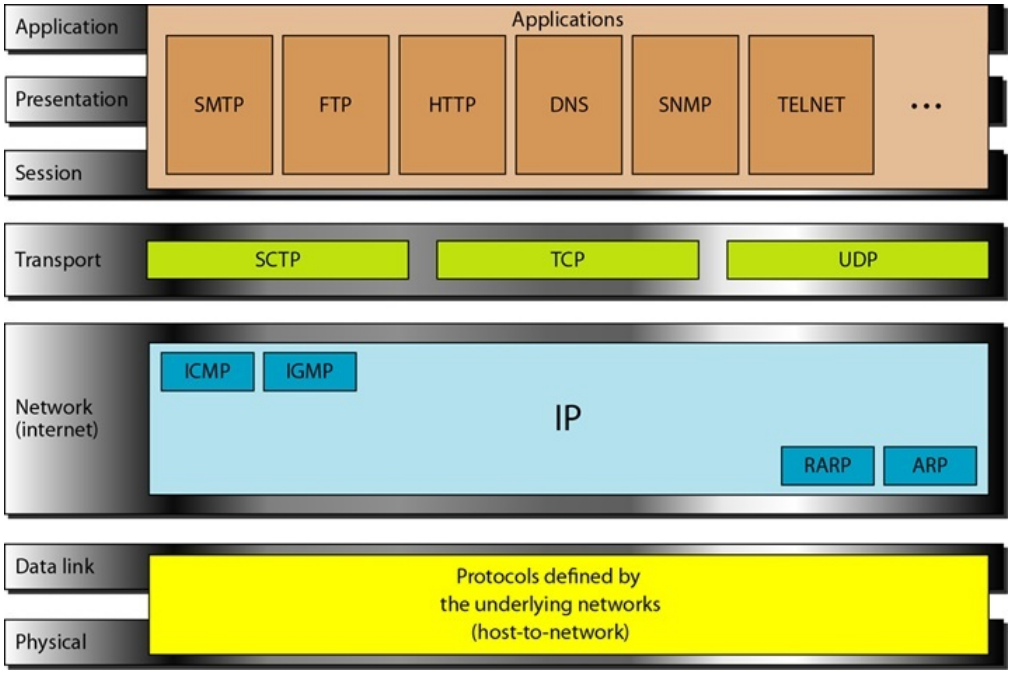

Figure 1.39: Protocols in TCP/IP protocol suite

The Physical Layer

- The Physical layer covers the physical interface between a data transmission devices (e.g., workstation, computer) and a transmission medium or network.
- It is responsible for carrying individual bits in a frame across the link.
- The layer is concerned with specifying the characteristics of the transmission medium, the nature of signals, the data rate, and related matters.

The Link Layer

- The link layer is concerned with taking datagram and moving it across the link. The link can be wired LAN with a link-layer switch, a wireless LAN, a wired WAN, or a wireless WAN.

- It encapsulates a datagram into frame.
- The link layer provides services such as error detection, error correction, or both.

The Internet Layer

- Also called as the Internetwork Layer (IP).
- It holds the IP protocol which is a network layer protocol and is responsible for source to destination transmission of data.
- The Internetworking Protocol (IP) is an connection-less and unreliable protocol.
- IP transports data by dividing it into packets called datagrams of same size. Each packet is independent of the other and can be transported across different routes and can arrive out of order at the receiver. It is the job of higher layers to rearrange them, if in-order delivery is desired.
- The network also include unicast and multicast routing protocols. A routing protocols does not take part in routing (it is responsibility of IP), but it creates forwarding tables for routers to help them in routing process.
- This layer has also addition auxiliary protocols that help in delivery and routing tasks, such as ICMP, IGMP, DHCP, ARP, RARP etc.

The Transport Layer

- The host-to-host layer, or transport layer may provide reliable end-to-end service, or merely an end-to-end delivery service without reliability.
- That is, it is responsible for giving services to the application layer: to get a message from application program running on the source host, and encapsulate into segment or user datagram in different protocols,and deliver it to the corresponding application program on the destination host.

The protocols used in transport layer are TCP, UDP and SCTP.

The Application Layer

- The TCP/IP protocol does not have session or presentation layer. Instead, applications simply include any session and presentation functions that they require.
- On the top of transport layer is the application layer.
- It contains all high level protocols such as File Transfer Protocol (FTP),Electronic Mail (SMTP), Virtual Terminal (TELNET), Domain Name Service (DNS), HTTP, etc.

1.11.5.1 Addressing

Physical Address

- Also known as hardware address or MAC address. - Physical Address is the lowest level of addressing, also known as link address.

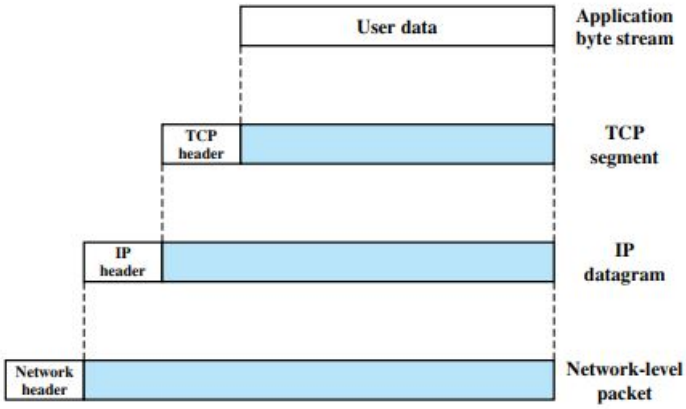

Figure 1.40: Protocol Data Units (PDUs) in TCP/IP Architecture

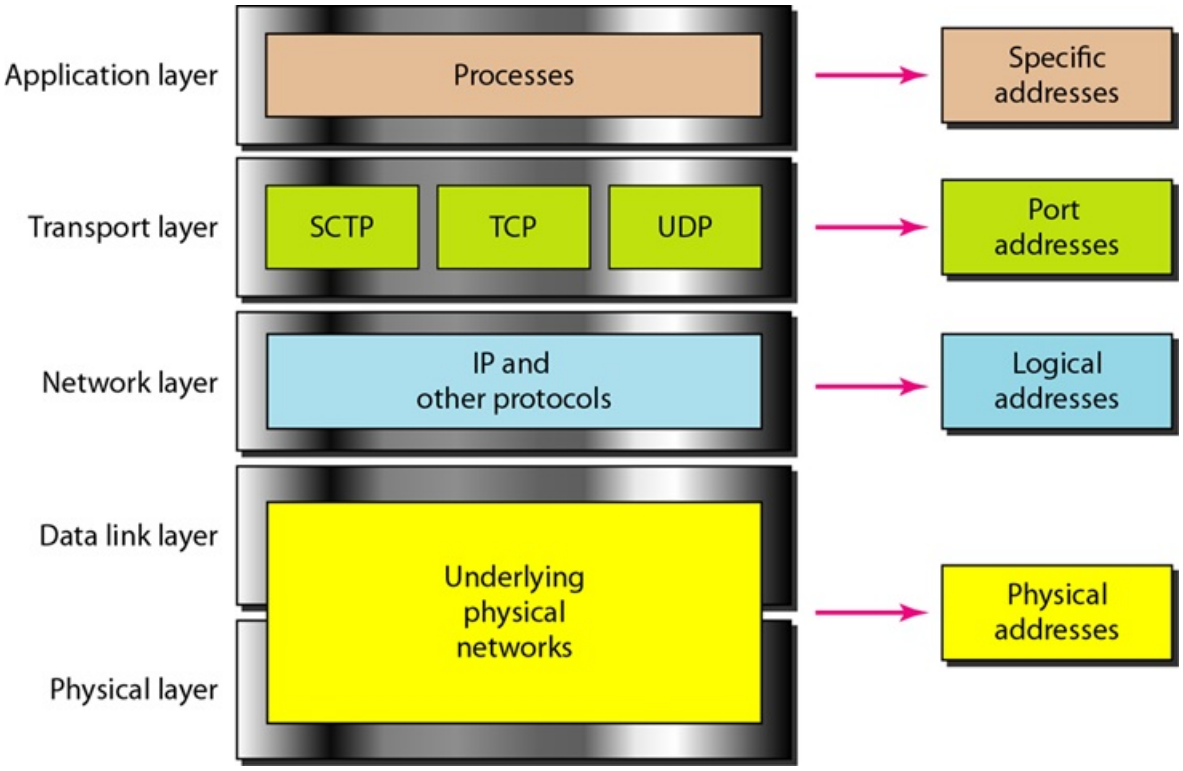

Figure 1.41: Addressing in TCP/IP protocol suite

- It is local to the network to which the device is connected and unique inside it.
- The physical address is usually included in the frame and is used at the data link layer.
- MAC is a type of physical address that is 6 byte (48 bit) in size and is imprinted on the Network Interface Card (NIC) of the device.
- The size of physical address may change depending on the type of network. Ex. An Ethernet network uses a 6 byte MAC address. Local Talk (Apple) use 1 byte dynamic address that changes each time the station comes up.

The Logical Address

- Logical Address is also called as IP Address (Internet Protocol address).
- At the network layer, device i.e. computers and routers are identified universally by their IP Address.
- IP addresses are universally unique.
- Currently there are two versions of IP addresses being used:
i. IPv4: 32 bit address, capable of supporting 2^{32} nodes.
ii. IPv6: 128 bit address, capable of supporting 2^{128} nodes.

Port Number/Port Address

- A Port Address is the name or label given to a process. It is a 16 bit address.
- Example. TELNET uses port address 23, HTTP uses port address 80.

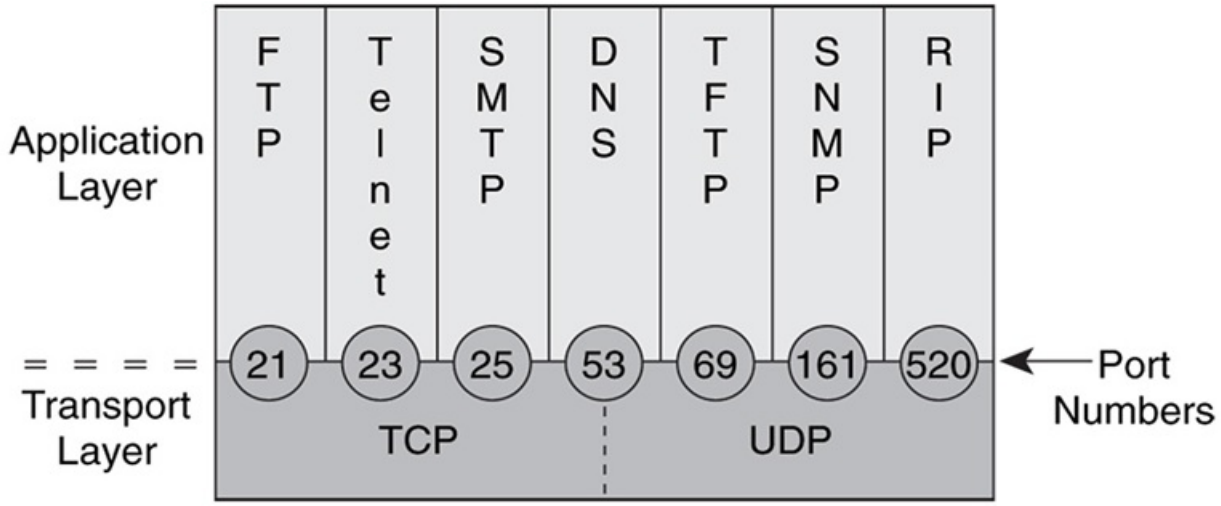

Figure 1.42: Some port numbers

Specific Address

- Some application have user friendly addresses and are called specific addresses.
- Examples: email address, URL (Universal Resource Locator).

1.11.6 A comparison of the OSI and TCP/IP Reference Models

Similarities:

- Both are based on stack of independent protocols i.e. based on layer's concept.
- Both have application layer, which is above the transport layer.
- Both use packet-switched instead of circuit-switched technology.

Dissimilarities:

1. Three concepts are central to OSI model: services, interfaces and protocols; while the TCP/IP does not clearly distinguish between these. As a result, protocols in the OSI model are better hidden than in the TCP/IP model and can be replaced relatively easily as the technology changes.
2. The OSI model was devised after the TCP/IP protocol suite. so, the model was not biased toward one particular set of protocols, a fact that made it quite general. While, in case of TCP/IP, protocols came first, and the model was really just a description of the exiting protocols. Protocols fit perfectly in model. The only problem was that the model did not fit any other protocols stack. Consequently, it was not especially useful for describing other, non-TCP/IP networks.
3. The OSI model has seven layers and the TCP/IP has four.
4. The OSI model supports both connectionless and connection-oriented communication in the network layer, but only connection-oriented communication in the transport layer. The TCP/IP model supports only one mode in the network layer (connectionless) but both in the transport layer, giving user a choice.

1.11.7 A Critique of the OSI Model and Protocols

Neither the OSI and its protocols nor the TCP/IP model and its protocols are perfect. Both have some flaws.
OSI model didn't get success. Following are some of the reasons:

1. Bad timing
2. Bad technology
3. Bad implementations
4. Bad politics

Bad Timing

The OSI model appeared after TCP/IP protocol suite. Most experts were at first excited and thought that the TCP/IP protocol would be fully replaced by the OSI model. This did not happended for several reaason. Frist, 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.

Bad Technology

- The second reason is that both the model and the protocols are flawed. The choice of seven layers was more political than technical,and the two of the layers (presentation and session) are nearly empty, whereas two other one (data link and network) are overfull.

- Ths OSI model, along with its associated service definitions and protocols, is extraordinarily complex. They are also difficult to implement an inefficient in operation.
- Some functions, such as addressing, flow control, and error control reappear again and again in each layer.

Bad Implementations

- The initial implementations were huge, unwieldy and slow while initial implementation of TCP/IP was quite good which grew later with improvements among larger community.

Bad Politics

- A bunch of government bureaucrats disregard and deride researchers and programmers; in effect, this mediocre attitude didn't aid OSI's development.

1.11.8 A Critique of the TCP/IP Reference Model

- The model does not clearly distinguish the concepts of services, interfaces and protocols, whose knowledge is must for software engineers for implementing design. Consequently, the TCP/IP model is not much of a guide for designing new networks using new technologies.
- Secondly, the TCP/IP does not incorporate any other protocols stack that itself. Consequently, if was not especially useful for describing other, non-TCP/IP network. For example, to describe Bluetooth using this model is completely impossible.
- Third, the link layer is not really a layer as described; it is an interface(between the network and physical layers).
- Fourth, the TCP/IP does not distinguish between the physical and data link layers. A proper model should include both as separate as their functionality are different.

1.12 Example of Networks

- The Internet
- X.25
- Frame Relay
- Ethernet
- VoIP
- NGN

- MPLS
- xDSL