Unit 1: Introduction to Data Communications
LH-3

Contents

- Introduction; Data Communications Networks (Components of a Network, Types of Networks); Network Models (Open Systems Interconnection Reference Model, Internet Model, Message Transmission Using Layers); Network Standards (The Importance of Standards, The Standards-Making Process, Common Standards); Future Trends (Wireless LAN and BYOD, The Internet of Things, Massively Online).

Introduction

- **Data Communication:**

Communication is defined as transfer of information such as messaged between two entities. Data communication concerns itself with the transmission of information between two locations by means of electrical signals.

Data communications is the name given to the communication where exchange of information takes place in the form of 0s and 1s over some kind of media such as wired or wireless.

Data:

It is the raw facts or entities that convey some meaning when these data are processed, they are usually converted into binary number i.e 0s and 1s.

- **Effectiveness of Data communication/Features:**

To send the data from source to destination following characteristics should be incorporated:

1. **Accuracy:**

For the effectiveness of the data communication the data must be accurately transmitted to the receiver that there should not be any interference.

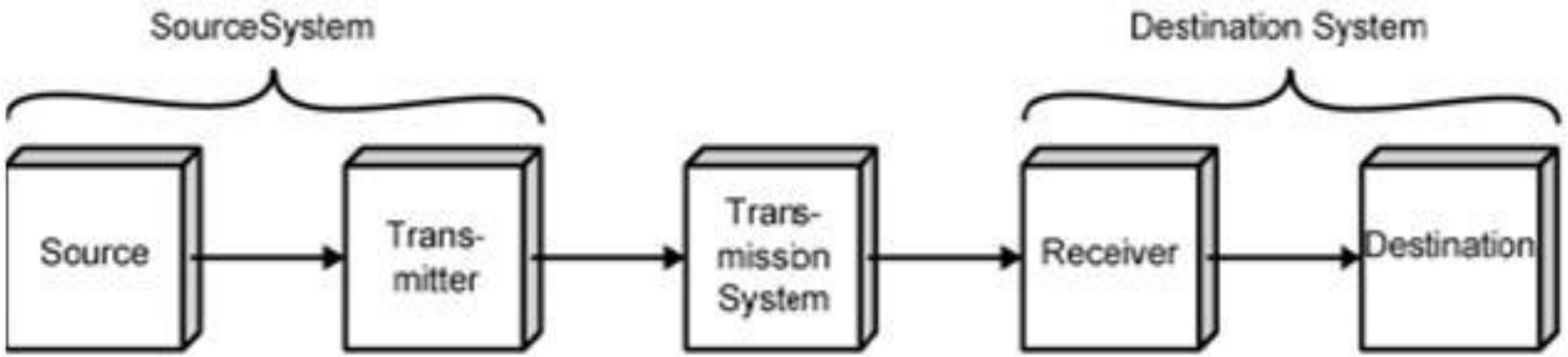
2. **Delivery**:

If and only if the data are transmitted accurately to the right or accurate destination then only data communication is effective.

3. **Timeliness:**

Certain time is allocated for communication and within that allocated time frame data must be transmitted. If not the acknowledgement is send to the sender and once again it has to be send.

Basic Communication Model/ Data Communication Model:



(a) General block diagram

- The main aim of the communication model is to transmit information from one point to another point. The main component of communication system are: source, transmitter, transmission medium, receiver and destination.

1. Source/ Sender:

- Generates data to be transmitted (voice, data, video).
- Out put of the source are either continuous time signals or sequence of symbols.
- Devices that are used to generate the data for transmission are computers, phone, etc.

2. **Transmitter:**

- Converts data into transmittable signals.
- Usually, data generated by the source is not transmitted directly.
- Transmitter encodes the information (assign different sequence of symbol format to common format, adds redundant bits to message bit stream) [For Digital Communication]
- Converts into electrical form or electromagnetic signals and make it appropriate for transmission through transmission system.

3. **Transmission Medium:**

- Carries data from source to destination.
- Could be transmission line or Complex network.
- Connects source and destination.
- May be guided or unguided media.

4. Receiver:

- Converts received signal into data.
- Decodes and convert the received signal from transmission system into form suitable for destination device to handle.

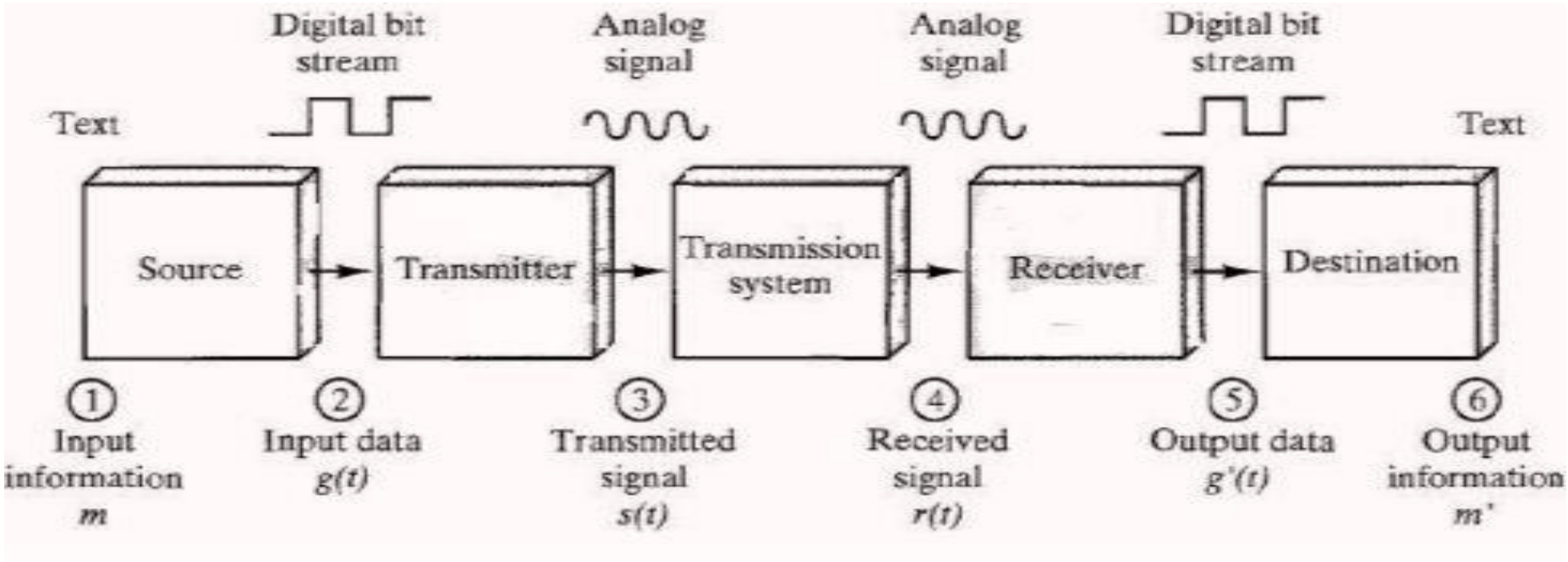
5**. Destination:**

- Takes incoming data from receiver.
- Example: Terminal, Computer, People, etc.

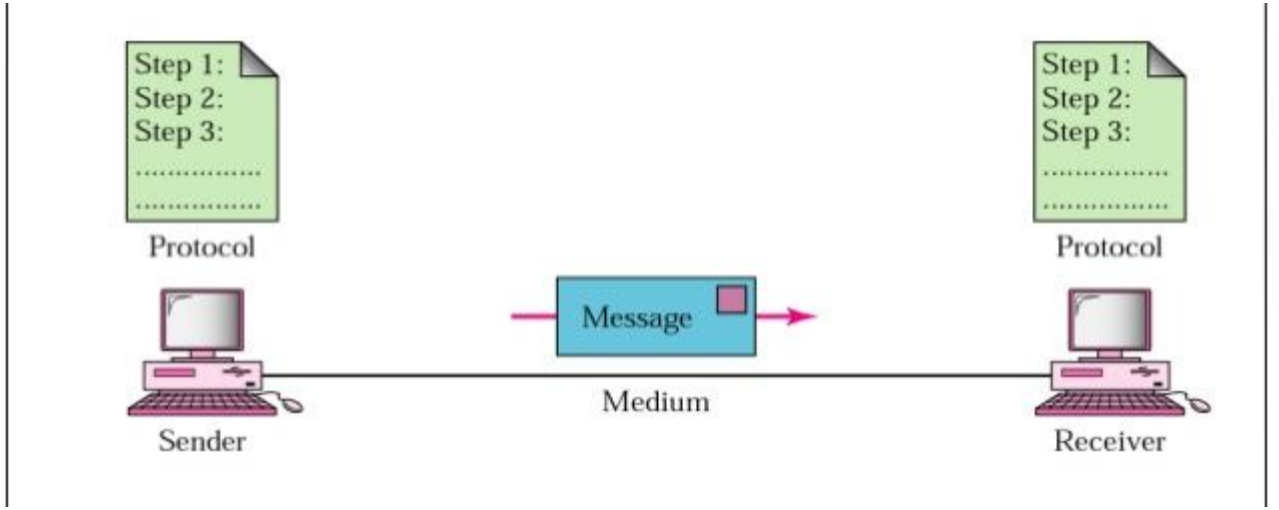
Typical Dial Up Network:

- On the basis of communication model figure above shows one particular example which establishes a link between a workstation and a server over a public telephone network.
- One more example can be the exchange of voice signals between two telephone over the same network.

Data Communication Model Example:



- **Components of Data Communication System:**



The five components are :

1. **Message** - It is the information to be communicated. Popular forms of information include text, pictures, audio, video etc.

2. Sender - It is the device which sends the data messages. It can be a computer, workstation, telephone handset etc.

3. Receiver - It is the device which receives the data messages. It can be a computer, workstation, telephone handset etc.

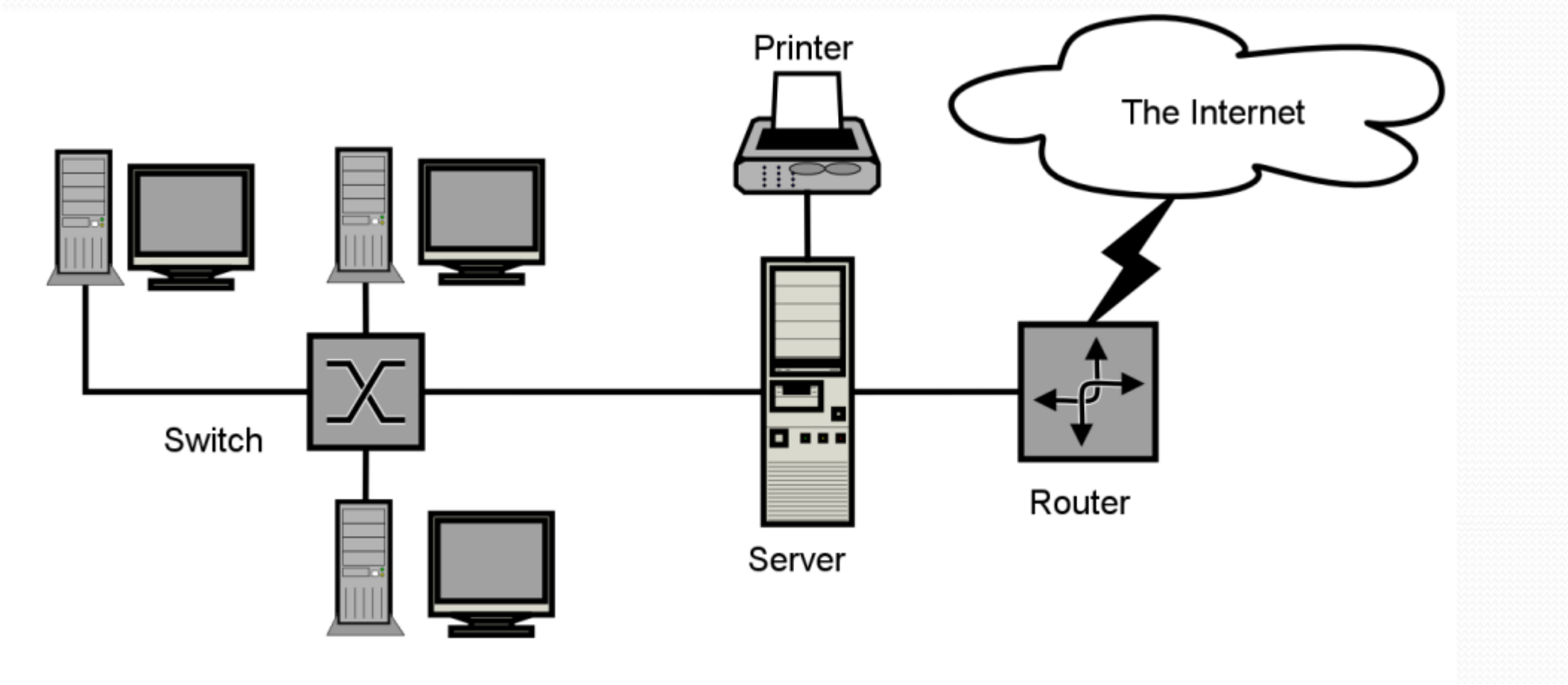
4. Transmission Medium - It is the physical path by which a message travels from sender to receiver. Some examples include twisted-pair wire, coaxial cable, radio waves etc.

5. Protocol - It is a set of rules that governs the data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating.

Network

- A network is a group of computers and other devices, such as printers and modems, connected to each other. This enables the computers to effectively share data and resources.
- A computer network, often simply referred to as a network, is a collection of hardware components and computers interconnected by communication channels that allow sharing of resources and information.
- A collection of computing devices connected in order to communicate and share resources.
- Connections between computing devices can be physical using wires or cables or wireless using radio waves or infrared signals.
- By definition, a computer network is a group of computers that are linked together through a communication channel.

Basic Structure of Network



Description of Network Structure

- All the computer devices are called hosts or end systems. Hosts sending requests are called clients while hosts receiving requests are called servers.
- End systems are connected together by a network of communication links and packet switches.
- Communication links are made up of different types of physical media, including coaxial cable, copper wide, optical fiber, and radio spectrum.
- Different links can transmit data at different rates, with the transmission rate of a link measured in bits/second.
- When one end system has data to send to another end system, the sending end system segments the data and adds header bytes to each segment.
- The resulting packages of information, known as packets, are then sent through the network to the destination end system, where they are reassembled into the original data.
- A packet switch takes a packet arriving on one of its incoming communication links and forwards that packet on one of its outgoing communication links. Common packet switches are routers and link-layer switches.

Network Components

- **Servers:** Servers are high-configuration computers that manage the resources of the network. The network operating system is typically installed in the server and so they give user accesses to the network resources. Servers can be of various kinds: file servers, database servers, print servers etc.
- **Clients:** Clients are computers that request and receive service from the servers to access and use the network resources.
- **Peers:** Peers are computers that provide as well as receive services from other peers in a workgroup network.
- **Transmission Media:** Transmission media are the channels through which data is transferred from one device to another in a network. Transmission media may be guided media like coaxial cable, fibre optic cables etc; or maybe unguided media like microwaves, infra-red waves etc.
- Connecting Devices: Connecting devices act as middleware between networks or computers, by binding the network media together. Some of the common connecting devices are:

a. Routers b. Bridges

c. Hubs d. Repeaters

e. Gateways f. Switches

Types of Network

- There are several different types of computer networks.
- Computer networks can be characterized by their size as well as their purpose.
- The size of a network can be expressed by the geographic area they occupy and the number of computers that are part of the network. Networks can cover anything from a handful of devices within a single room to millions of devices spread across the entire globe.
- Some of or some the different networks based on size are:
- Personal Area Network (PAN)
- Local Area Network (LAN)
- Campus Area Network (CAN)
- Metropolitan Area Network (MAN)
- Wide Area Network (WAN)
- In terms of purpose, many networks can be considered general purpose, which means they are used for delivery, everything from sending files to a printer to accessing the Internet.
- Some types of networks, however, serve a very particular purpose. Some of the different networks based on their main purpose are:
- Storage Area Network (SAN)
- Enterprise Private Network (EPN)
- Virtual Private Network (VPN)

Personal Area Network (PAN):

- The smallest and most basic type of network, a Personal Area Network or PAN is made up of a wireless modem, a computer or two, phones, printers, tablets, etc., and revolves around one person in one building. These types of networks are typically found in small offices or residences, and are managed by one person or organization from a single device.
- If multiple individuals use the same network within a residence, the network is sometimes referred to as a home area network, or HAN.
- In a very typical setup, a residence will have a single wired Internet connection connected to a modem.
- This modem then provides both wired and wireless connections for multiple devices.
- The network is typically managed from a single computer but can be accessed from any device.

Advantages of PAN:

No wires are required. The connecting devices in a PAN only require Bluetooth to be enabled, which eliminates the need for extra wires. This also eradicates the need for cable management and wasted floor space, making it a highly cost-effective network.

Reliable and secure. A PAN network ensures a reliable and stable connection if it's established within the 10-meter range.

Easy data synchronization. A PAN provides easy data synchronization between different devices. As an example, all devices connected within a PAN can be used to exchange, download and upload data with each other.

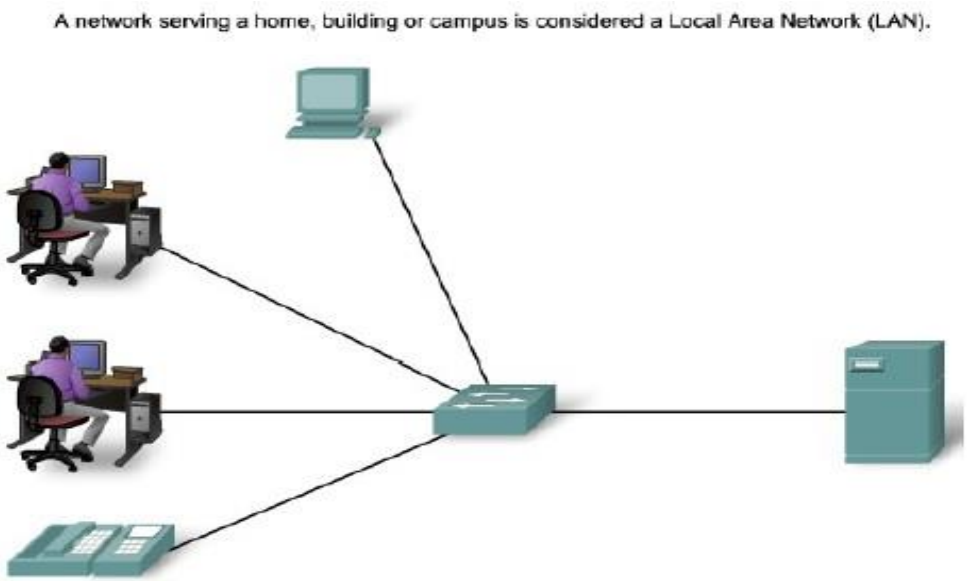
Portability. A PAN provides extreme portability, as it's wireless, and users can transport devices and exchange data wherever they want.

Disadvantages of Personal Area Network

- **Less distance range:** Signal range is maximum 10 meters which makes limitation for long distance sharing.
- **Interfere with radio signals:** As personal area network also use infrared so it can interfere with radio signals and data can be dropped.
- **Slow data transfer:** Bluetooth and infrared have a slow data transfer rate as compared to another type of networks like LAN (local area network).
- **Health problem:** In some cases, PAN uses microwave signals in some digital devices which have a bad effect on the human body like brain and heart problems may occur.
- **Costly in terms of communication devices**: Personal area network is used in digital devices which are costly so it is another disadvantage of PAN. Examples are smart phones, PDA, laptops, and digital cameras.
- **Infrared signals travel in a straight line:** TV remote use infrared signals which have a problem that they travel in straight line. So, this counts another disadvantage of PAN.

- **Local Area Network (LAN):**
- A LAN is a network that is used for communicating among computer devices, usually within an office building or home.
- LAN’s enable the sharing of resources such as files or hardware devices that may be needed by multiple users
- Is limited in size, typically spanning a few hundred meters, and no more
- than a mile
- Is fast, with speeds from 10 Mbps to 10 Gbps
- Requires little wiring, typically a single cable connecting to each device
- Has lower cost compared to MAN’s or WAN’s.
- A Local Area Network (LAN) is a computer network covering a small geographic area, like a home, office, or group of buildings

- LAN’s can be either wired or wireless. Twisted pair, coax or fiber optic cable can be used in wired LAN’s.
- Every LAN uses a protocol – a set of rules that governs how packets are configured and transmitted.
- LANs are capable of very high transmission rates (100s Mb/s to G b/s)



Advantages of LAN

- The basic LAN implementation does not cost too much.
- It is easy to control and manage the entire LAN as it is available in one small region.
- The LAN configuration is very easy due to availability of required protocols in the Operating System (OS) itself.
- The systems or devices connected on LAN communicates at very high speed depending upon LAN type and ethernet cables supported. The common speeds supported are 10 Mbps, 100 Mbps and 1000 Mbps. Gigabit ethernet versions are evolving very fast. Cheaper versions will be available once the technology matures and mass production has been carried out.
- With the help of file servers connected on the LAN, sharing of files and folders among peers will become very easy and efficient.
- It is easy to setup security protocols to protect the LAN users from intruders or hackers.
- It is easy to share common resources such as printers and internet line among multiple LAN users.
- LAN users do not require their own harddisk and CD-ROM drives. They can save their work centrally on network file server.
- Application softwares such as MS Office, Anti-Virus, Adobe reader are stored at one system and are shared for all the LAN users.

Disadvantages of LAN:

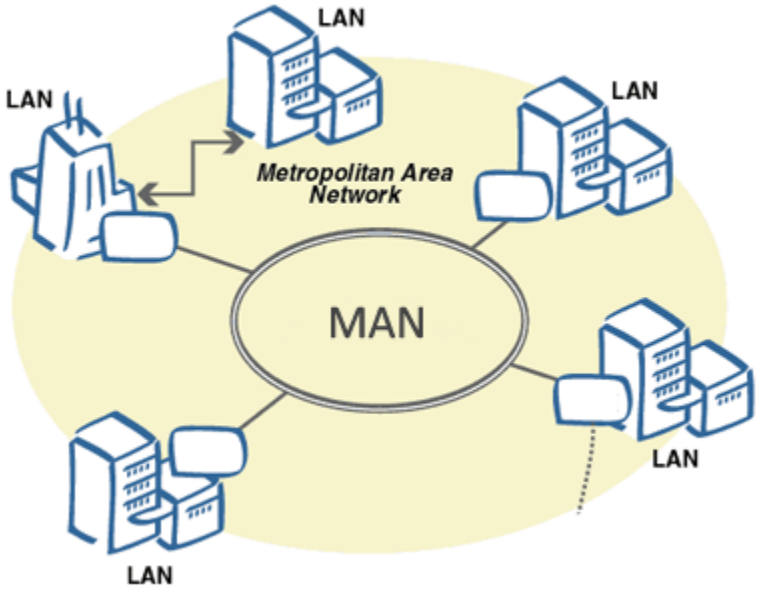
- LAN covers small geographical area.
- Security issues are big concern as it is easy to have access to programs and data of peers. Special security measures are needed to stop unauthorized access.
- It is difficult to setup and maintain LAN and requires skilled technicians and network administrators.
- In the server based LAN architecture, if server develops some fault, all the users are affected.
- Appearance of virus in one system can spread very fast to all the LAN users very easily.

Campus Area Network

- A campus area network (CAN) is a network of multiple interconnected local area networks (LAN) in a limited geographical area.
- The networking equipments (switches, routers) and transmission media (optical fiber, Twisted pair cabling etc.) are almost entirely owned by the campus , an enterprise, university, government etc.
- A campus area network is larger than a local area network but smaller than a metropolitan area network (MAN) or wide area network (WAN).
- In most cases, CANs own shared network devices and data exchange media.
- CAN benefits are as follows:
- Cost-effective
- Wireless, versus cable
- Multi departmental network access
- Single shared data transfer rate (DTR)

- **Metropolitan Area Network**
- A metropolitan area network (MAN) is a large computer network that usually spans a city or a large campus.
- A MAN is optimized for a larger geographical area than a LAN, ranging from several blocks of buildings to entire cities.
- A MAN might be owned and operated by a single organization, but it usually will be used by many individuals and organizations.
- A MAN often acts as a high speed network to allow sharing of regional resources.
- A MAN typically covers an area of between 5 and 50 km diameter.
- Examples of MAN: Telephone company network that provides ahigh speed DSL to customers and cable TV network.
- A metropolitan area network (MAN) is a network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large local area network (LAN) but smaller than the area covered by a wide area network (WAN).

- **Advantages of MAN:**
- It utilizes drawbacks of both LAN and WAN to provide larger and controllable computer network.
- MAN requires fewer resources compare to WAN. This saves the implementation cost.
- It helps people interface fast LANs together. This is due to easy implementation of links
- It provides higher security compare to WAN.
- It helps in cost effective sharing of common resources such as printers etc.
- Like LAN and WAN, it also offers centralized management of data and files



- **Disadvantages of MAN:**
- It is difficult to manage the network once it becomes large.
- It is difficult to make the system secure from hackers and industrial surveillance.
- Network installation requires skilled technicians and network administrators. This increases overall installation and management costs.
- It requires more cables for connection from one place to the other compare to LAN

- **Wide Area Network**
- WAN covers a large geographic area such as country, continent or even whole of the world.
- A WAN is two or more LANs connected together. The LANs can be many miles apart.
- To cover great distances, WANs may transmit data over leased high-speed phone lines or wireless links such as satellites.
- Multiple LANs can be connected together using devices such as bridges, routers, or gateways, which enable them to share data.
- The world's most popular WAN is the Internet.
- Wide Area Network (WAN) is a computer network that covers a broad area (i.e., any network whose communications links cross metropolitan, regional, or national boundaries).
- WANs are used to connect LANs and other types of networks together, so that users and computers in one location can communicate with users and computers in other locations

- **Advantages of WAN:**
- WAN covers larger geographical area. Hence business offices situated at longer distances can easily communicate.
- Like LAN, it allows sharing of resources and application softwares among distributed workstations or users.
- The software files are shared among all the users. Hence all will have access to latest files. This avoids use of previous versions by them.
- Organizations can form their global integrated network through WAN. Moreover it supports global markets and global businesses.
- The emergence of IoT (Internet of Things) and advanced wireless technologies such as LAN or LAN-Advanced have made it easy for the growth of WAN based devices.

- **Disadvantages of WAN:**
- Initial investment costs are higher.
- It is difficult to maintain the network. It requires skilled technicians and network administrators.
- There are more errors and issues due to wide coverage and use of different technologies. Often it requires more time to resolve issues due to involvement of multiple wired and wireless technologies.
- It has lower security compare to LAN and MAN due to wider coverage and use of more technologies.
- Security is big concern and requires use of firewall and security softwares/protocols at multiple points across the entire system. This will avoid chances of hacking by intruders

- **Storage Area Network (SAN):**
- As a dedicated high-speed network that connects shared pools of storage devices to several servers, these types of networks don't rely on a LAN or WAN. Instead, they move storage resources away from the network and place them into their own high-performance network.
- SANs can be accessed in the same fashion as a drive attached to a server: Types of storage area networks include converged, virtual and unified SANs.
- **Enterprise Private Network (EPN):**
- These types of networks are built and owned by businesses that want to securely connect its various locations to share computer resources.

- **Virtual Private Network (VPN):**
- A virtual private network extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across the VPN may therefore benefit from the functionality, security, and management of the private network.

Network Models

- A network model reflects a design or architecture to accomplish communication between different systems.
- Network models are also referred to as network stacks or protocol suites.
- Examples of network models includes TCP/IP, Sequenced Packet Exchange/Internet Packet Exchange (SPX/IPE) used by Novelle Netware, the Network Basic Input Output System (Net-BIOS), which comprises the building blocks for most Microsoft networking and network applications; and AppleTalk, the network model for Apple Macintosh computers.
- A network model usually consists of layers. When a communication system is designed in this manner, it's known as a hierarchical or layered architecture. Each layer of a model represents specific functionality. Within the layers of a model, there are usually protocols specified to implement specific tasks. Protocol is a set of rules or a language. Thus, a layer is normally a collection of protocols.

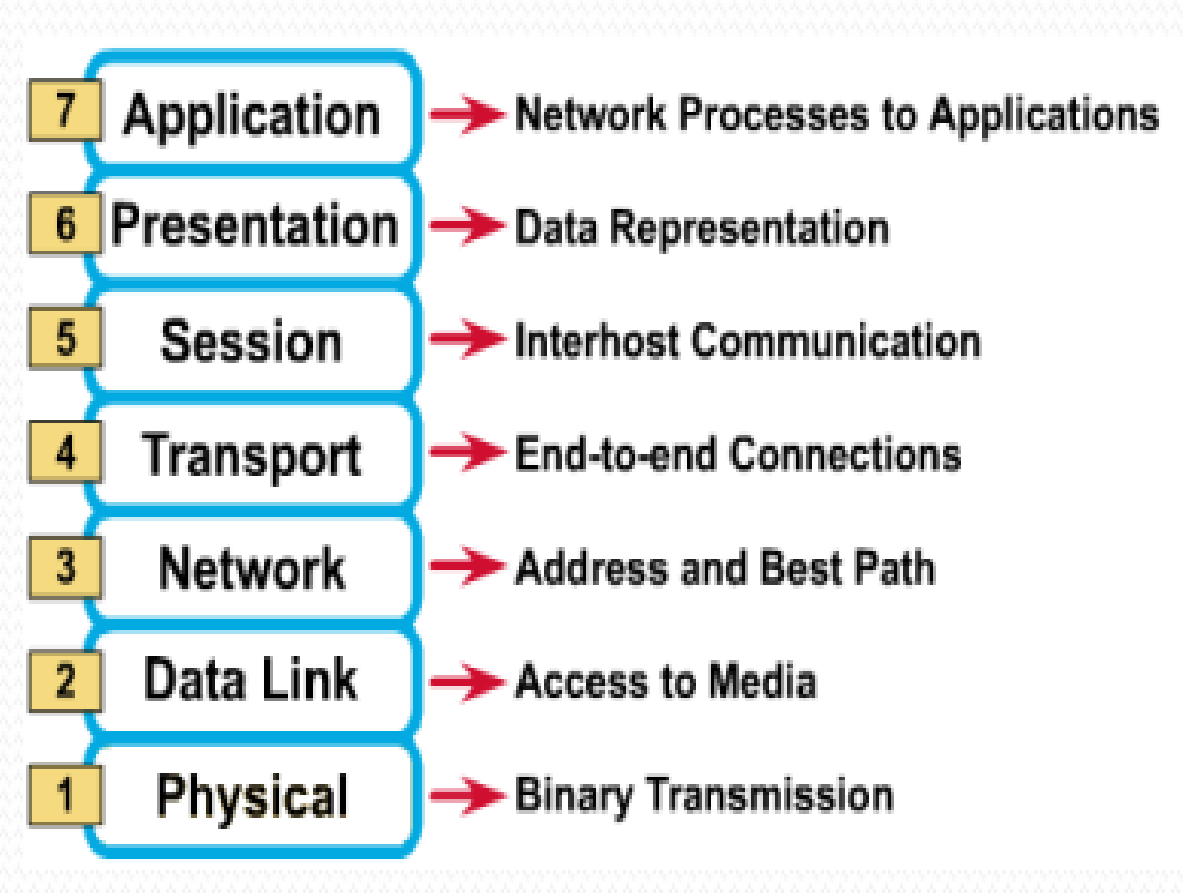
- There are a number of different network models. Some of these models relate to a specific implementation, such as the TCP/IP network model. Others simply describe the process of networking, such as the International Organization for Standardization/Open System Interconnection Reference Model (ISO/OSI-RM).
- **A reference model** is a non-implementation specific foundation that provides a clear understanding of the functions and processes necessary for consistent nonproprietary protocol development. The OSI reference model satisfies this definition since it provides a set of standards to ensure networking compatibility and interoperability and serves as a guideline for protocol design and instruction. The OSI reference model generically describes the communications process and therefore does not regulate it as manufacturers may create products that combine functions of one or more layers.
-

- In contrast, a protocol model closely matches the structure of a protocol suite and may in fact be defined by the protocol suite's implementation. As an example, the TCP/IP protocol model describes the communication process and functions at each layer of the Internet standard TCP/IP protocol suite.
- A layered architecture facilitates development in complex environments by grouping specific related functions into separate well-defined layers with clear interfaces. This methodology reduces complexity by breaking the problem space into smaller and simpler components and standardizes interfaces facilitating multi-vendor development and modular component-based engineering.
- Layered architectures in conjunction with open standards define a common vocabulary necessary for understanding and cooperation in multi-vendor environments and positively results in increased competition and innovation. The architecture's layers may also be called the architecture's stack and these two terms will be used interchangeably.

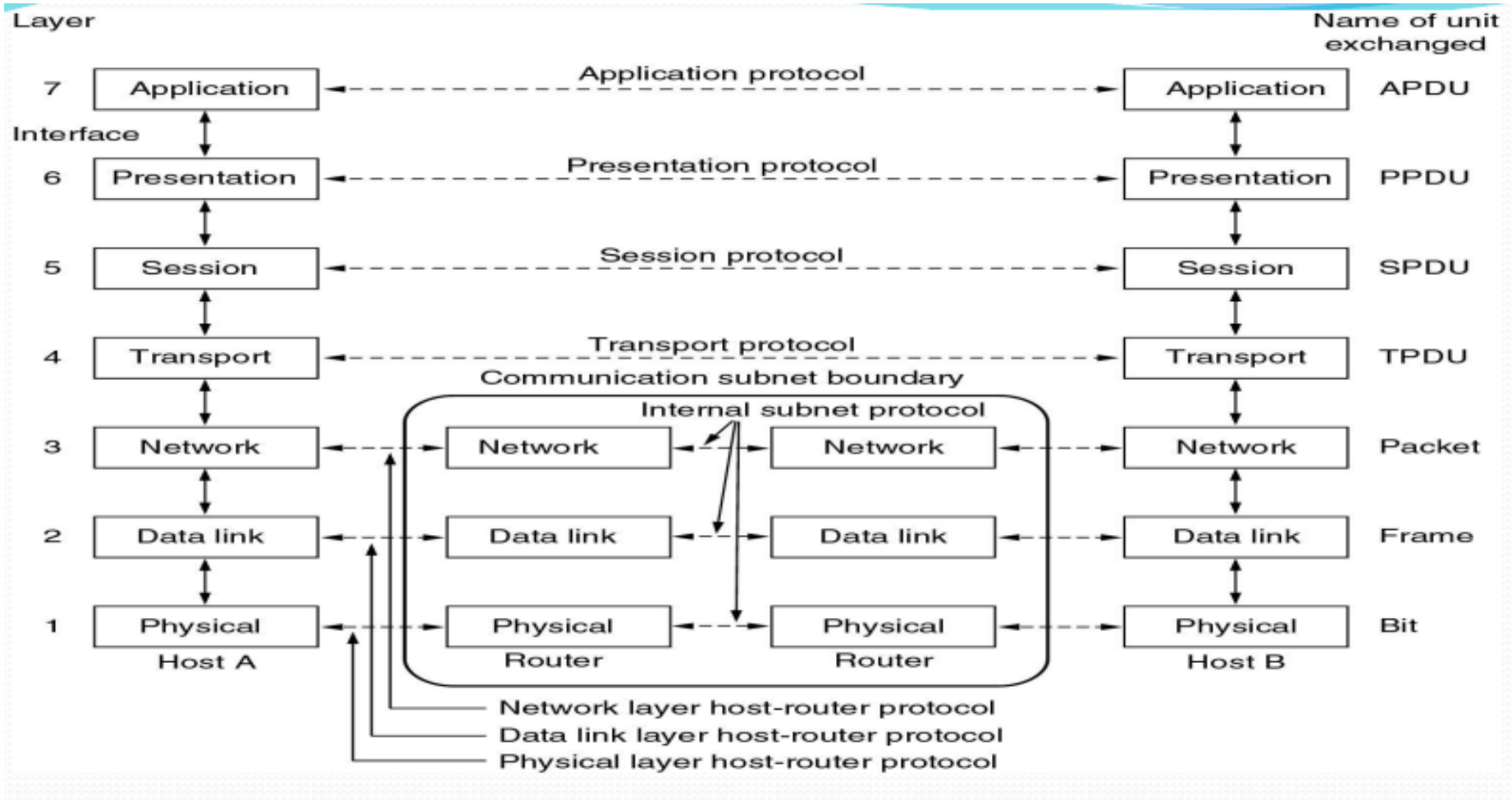
OSI Reference Model

- International standard organization (ISO) established a committee in 1977 to develop an architecture for computer communication.
- Open Systems Interconnection (OSI) reference model is the result of this effort.
- In 1984, the Open Systems Interconnection (OSI) reference model was approved as an international standard for communications architecture.
- Term “open” denotes the ability to connect any two systems which conform to the reference model and associated standards.
- The OSI model is now considered the primary Architectural model for inter-computer communications.
- The OSI model describes how information or data makes its way from application programmes (such as spreadsheets) through a network medium (such as wire) to another application programme located on another network.
- The OSI reference model divides the problem of moving information between computers over a network medium into SEVEN smaller and more manageable problems .
- This separation into smaller more manageable functions is known as layering.

OSI Reference Model: 7 Layers



How to remember
“All people seem to need data processing.
All = Application Layer.
People= Presentation Layer.
Seem = Session Layer.
To = Transport Layer.
Need = Network Layer.
Data = Data Link Layer.
Processing = Physical Layer

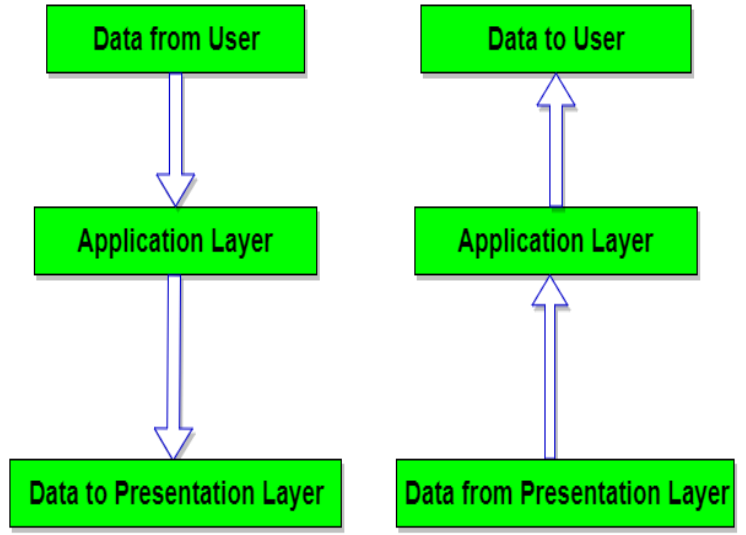

Layer
Name of unit exchanged
7
Application
Application protocol
Application
APDU
Interface
6
Presentation
Presentation protocol
Presentation
PPDU
5
Session
Session protocol
Session
SPDU
4
Transport
Transport protocol
Transport
TPDU
Communication subnet boundary
Internal subnet protocol
3
Network
Network
Network
Network
Packet
2
Data link
Data link
Data link
Data link
Frame
1
Physical
Physical
Physical
Physical
Bit
Host A
Router
Router
Host B
Network layer host-router protocol
Data link layer host-router protocol
Physical layer host-router protocol

OSI: A Layered Network Model

- The process of breaking up the functions or tasks of networking into layers reduces complexity.
- Each layer provides a service to the layer above it in the protocol specification.
- Each layer communicates with the same layer's software or hardware on other computers.
- The lower 4 layers (transport, network, data link and physical —Layers 4, 3, 2, and 1) are concerned with the flow of data from end to end through the network.
- The upper three layers of the OSI model (application, presentation and session—Layers 7, 6 and 5) are orientated more toward services to the applications.
- Data is Encapsulated with the necessary protocol information as it moves down the layers before network transit.

Application Layer (Layer 7)

- It provides a set of interfaces for sending and receiving application to gain access to and use network services like message handling, database query processing, file access and data transfer.
- It determines the identity and availability of communication patterns and determine if sufficient resources are available to start the program.
- It represents the window between the user and the network.
- The protocols that run at the application layer includes FTP, HTTP, etc.



Major Responsibilities of Application Layer

- **Mail services:**

  This application provides the basis of email forwarding and storing.

- **Directory Services:**

  This application provides distributed database sources and access for global information about various objects and services.

- **File Transfer/ Access and Management:**

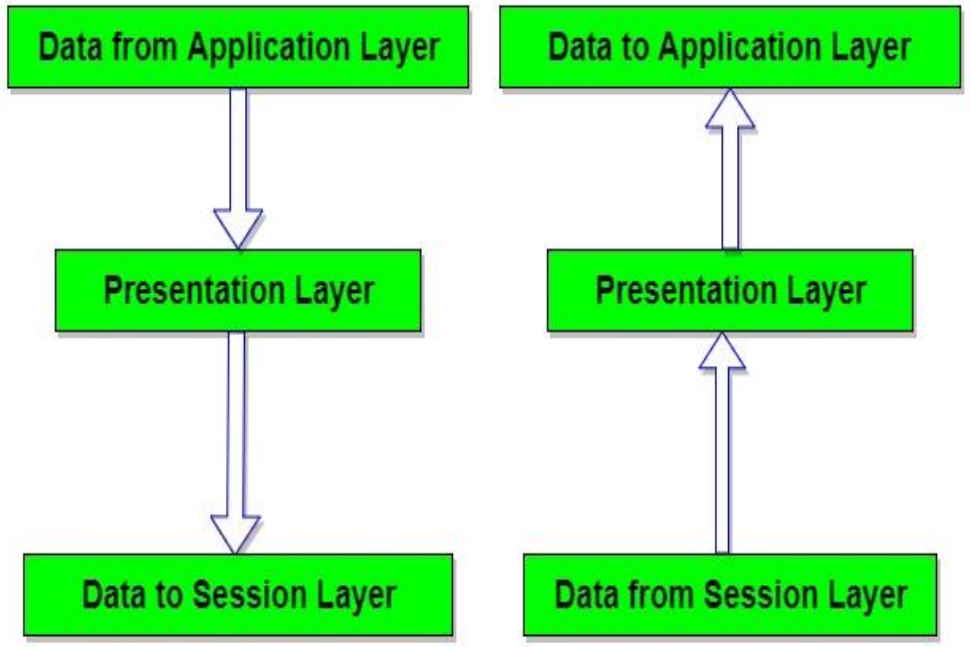
  This application allows a user to access files in a remote hosts, to retrieve files from remote computer for use in the local computer and to manage or control files in remote computer locally.

- **Network Virtual Terminal:**

  It is a software version of physical terminal and allows a user to log on to a remote host.

Presentation Layer (Layer 6)

- The presentation layer is concerned with the syntax and semantics of the information transmitted.
- The presentation layer is also concerned with other aspects of information representation such as data compression which can be used to reduce the size of information that has to be transmitted and cryptography which is frequently used for privacy and authentication. Example: JPEG



Major Responsibilities of Presentation Layer

- **Translation:**

The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The information must be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods.

- **Encryption:**

To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.

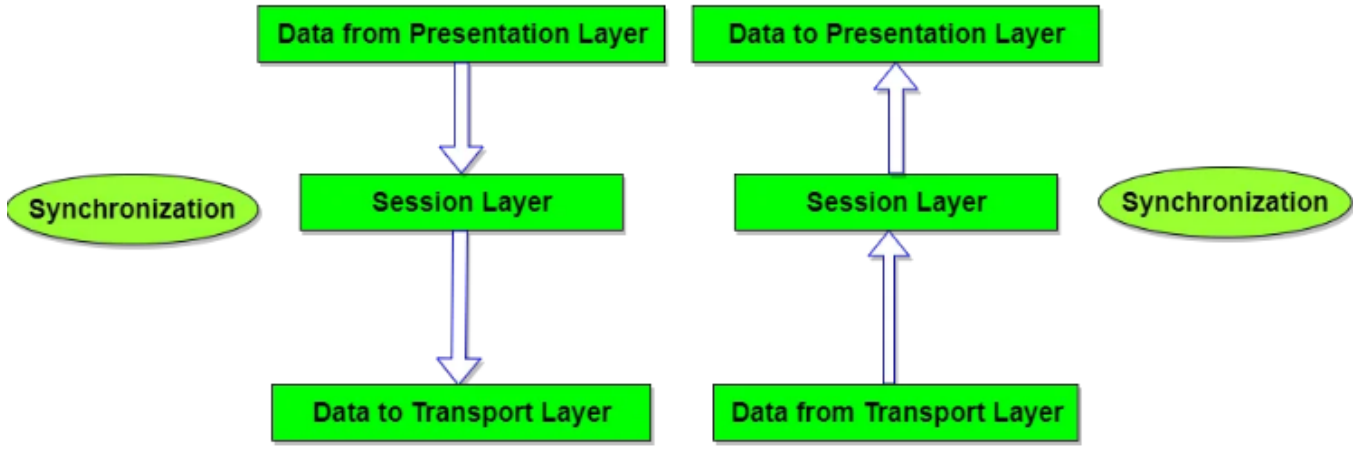
- **Compression:**

Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

Example of protocol that run at the presentation layer include SSL (Secure Sockets Layer). The Secure Socket Layer is a protocol that provides security to confidential data following the encryption process over the internet.

Session Layer (Layer 5)

- It enables two network resources to hold on going communication or session across a network as it is responsible for initiating, maintaining and terminating sessions.
- It is also responsible for security and access control to session. A session allows a ordinary data transfer but it also provides enhanced services useful in some applications.
- Examples of protocols that run at the session layer include Password Authentication Protocol(PAP).



Major Responsibilities of Session Layer

- **Dialog control:**

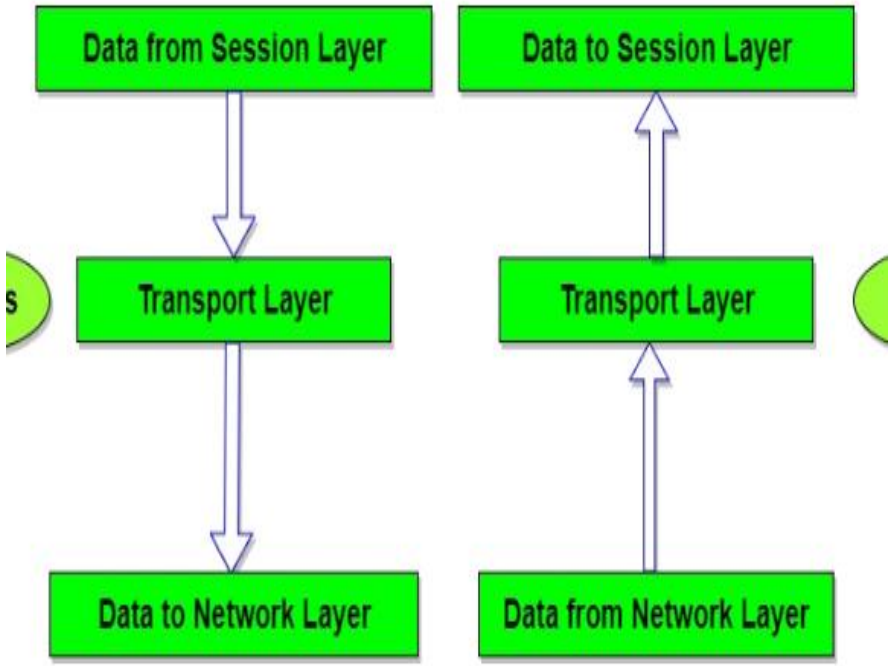
The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half- duplex (one way at a time) or full-duplex (two ways at a time) mode.

- **Synchronization:**

The session layer allows a process to add checkpoints, or synchronization points, to a stream of data. For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. In this case, if a crash happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent.

Transport Layer (Layer 4):

- The main purpose of this layer is making sure that data is delivered error free and in the correct sequence.
- It provides end to end network connection. It is also responsible for reassembling of the packets that may have been broken up to travel across certain media.
- It is concerned with reliable and unreliable transport. When using a connection oriented reliable transport protocol such TCP, acknowledgement are sent back to the sender to confirm that the data transmitted is received.
- The basic function of the transport layer is to accept data from the session layer, split it up to the smaller units if the need arises, pass the pieces to the network layer to ensure that all pieces arrive end to end. Eg: TCP (Transmission Control Protocol), UDP (User Datagram Protocol)



Major Responsibilities of Transport Layer

- **Segmentation and Reassembling:**

A message is divided into segment and each segment contains a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination. The packets lost in the transmission is identified and resent.

- **Service Point (Port Addressing):**

Computers run several programs at the same time. Source and destination delivery means delivery from a specific process on one computer to a specific process on the other. The transport layer header includes the type of address called a service point address.

- **Connection Control:**

The transport layer can be either connection oriented or connectionless. A connectionless transport layer treats segments as an independent packet and delivered it to the transport layer. A connection oriented transport layer makes the connection with the transport layer at the destination and delivers the packets. After all the data are transmitted the connection is terminated. TCP is connection oriented and UDP is connection less.

- **Flow Control:**

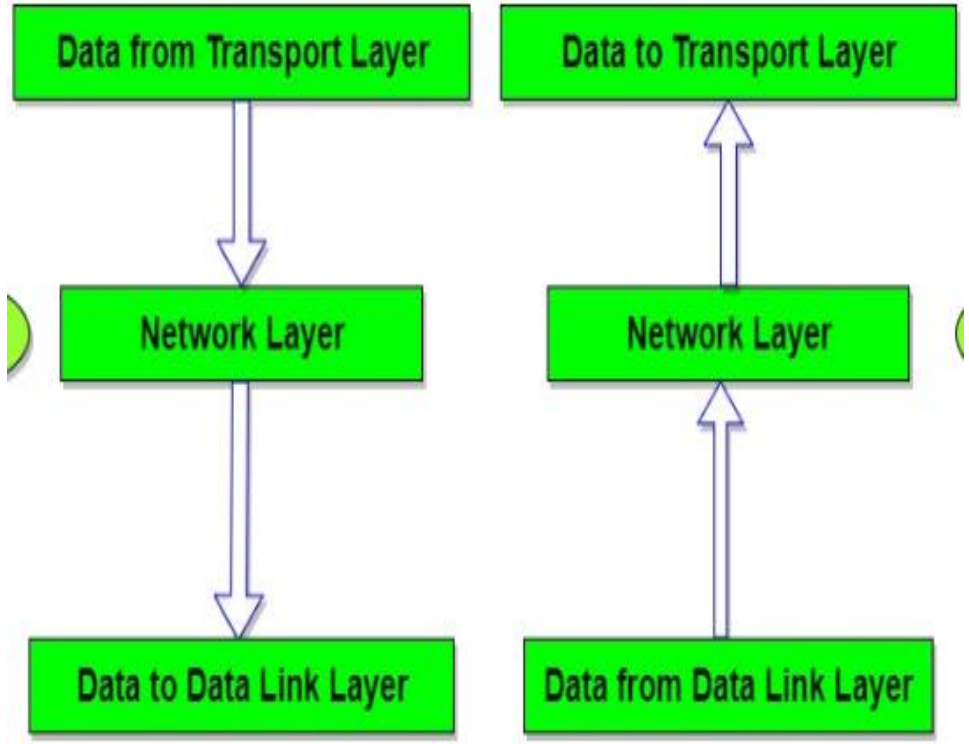
End to end flow control is performed.

- **Error Correction:**

At the sending side the transport layer makes sure that the entire message arrives at the receiving transport layer without error. Error correction is achieved through retransmission and performed end to end.

Network Layer (Layer 3)

- It is responsible for source to destination delivery of a packet across multiple network.
- It ensures that each packet gets from its point of origin to its final destination. It treats each packet independent as though each belong to separate message.
- It defines logical network layout so router can determine how to forward packets through an entire network.
- Routing occurs at this layer and hence routed protocols recites in this layer.
- Examples of protocols that run at the network layer include IPv4, Open Shortest Path First etc.



Major Responsibilities of Network Layer

- **Internetworking:**

  The main duty of the network layer is providing internet working of similar physical network together to look like a single network to the upper transport and application layer.

- **Logical Addressing (IP Addressing):**

  At the network layer we need to uniquely identify each device on the internet to allow global communication between all devices.

- **Routing:**

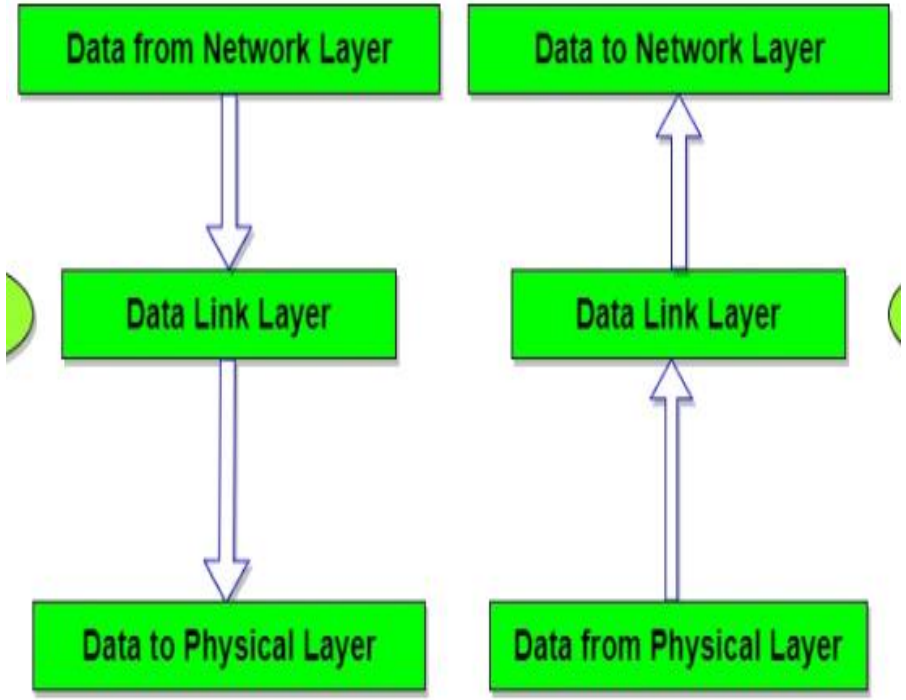
  Choosing the best path from the multiple using different techniques. Routing can be static or dynamics.

- **Congestion Control:**

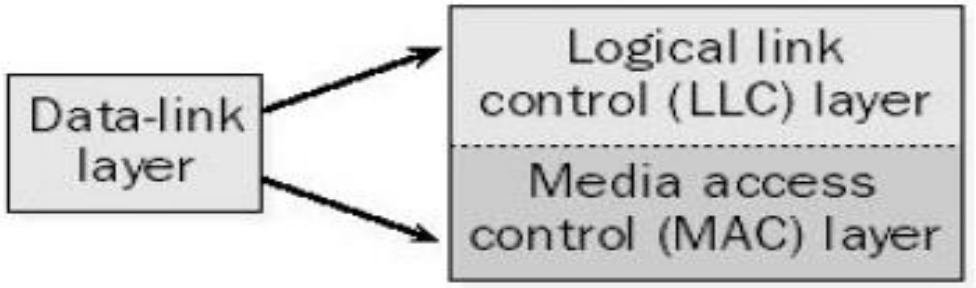
  If too many packets temporarily available in the subnet, it can also be regarded as bottleneck problem which is served by the netwrok layer.

Data Link Layer (Layer 2)

- Provides access to the networking media and physical transmission across the media
- Provides well-defined service interface to the network layers
- Uses MAC (medium access control) address to define hardware in order to control access to media by multiple stations
- The sender breaks the input data into frames, transmits the frames sequentially and process the acknowledge frames sent back by the receiver.



- The data-link layer is separated into two sub layers:
- The logical link control (LLC) layer, the upper of the two layers, which is responsible for flow control, error correction, and resequencing functions for connection-oriented communication, but which also supports connectionless communication.
- •The media access control (MAC) layer, the lower of the two layers, which is responsible for providing a method for stations to gain access to the medium. It determines hardware address.
- Examples of protocols that run at the data link layer include Point-to-Point Protocol (PPP), High-Level Data Link Control(HDLC).



Major Responsibilities of Data Link Layer

- **Framing:**

  The data link layer divides the stream of bits received from the network layer into manageable data units called frames.

- **Physical addressing:**

  If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame.

- **Flow control:**

  If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.

- **Error control:**

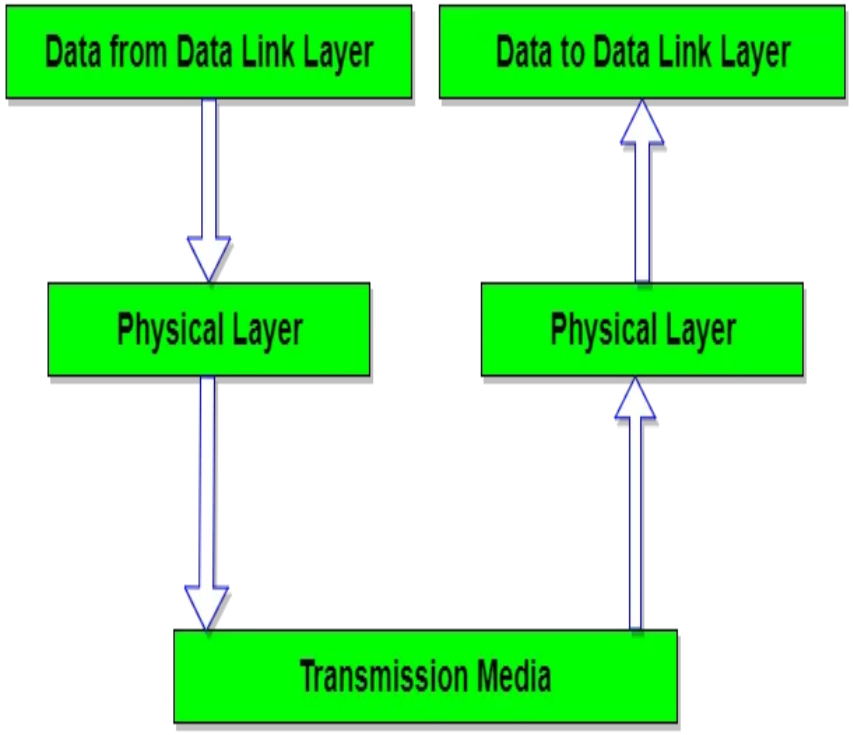
  The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.

- **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

Physical Layer (Layer 1)

- The physical layer is concerned with transmitting raw bits over a communication channel and other physical aspects of the media being used to transmit the data.
- These characteristics include modulation and encoding of data bits on carrier signal and ensure bit synchronization.
- The major task of physical layer is to provide services to the data link layer. It deals with the mechanical and electrical specification of the interface of the transmission media.
- Mechanical includes cables, pins, etc. Electrical or optical includes modulation, voltage level, signal strength.



Major Responsibilities of Physical Layer

- **Representation of Bits(Encoding):** Data in this layer consists of stream of bits. The bits must be encoded into signals for transmission. It defines the type of encoding i.e. how 0's and 1's are changed to signal.
- **Data Rate:** This layer defines the rate of transmission which is the number of bits per second.
- **Synchronization:** It deals with the synchronization of the transmitter and receiver. The sender and receiver are synchronized at bit level.
- **Line Configuration**: This layer connects devices with the medium: Point to Point configuration and Multipoint configuration.
- **Physical Topology**: The physical topology determines how devices are connected to create a network. Devices can be using a mesh topology, a star topology, a ring topology or a bus topology..
- **Transmission Modes:** Physical Layer defines the direction of transmission between two devices: Simplex, Half Duplex, Full Duplex.
- Example of protocol that run at the physical layer include token ring.

Detail Encapsulation Process:

- All communications on a network originate 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 headers, trailers, and other information.
- Once the data is sent from the source, it travels through the application layer down through the other layers.
- The packaging and flow of the data that is exchanged goes through changes as the layers perform their services for end users. Networks must perform the following five conversion steps in order to encapsulate data:

1. Build the data:

As a user sends an e-mail message, its alphanumeric characters are converted to data that can travel across the internetwork.

2. **Package the data for end-to-end transport:**

The data is packaged for internetwork transport. By using segments, the transport function ensures that the message hosts at both ends of the e-mail system can reliably communicate.

3. Add the network IP address to the header:

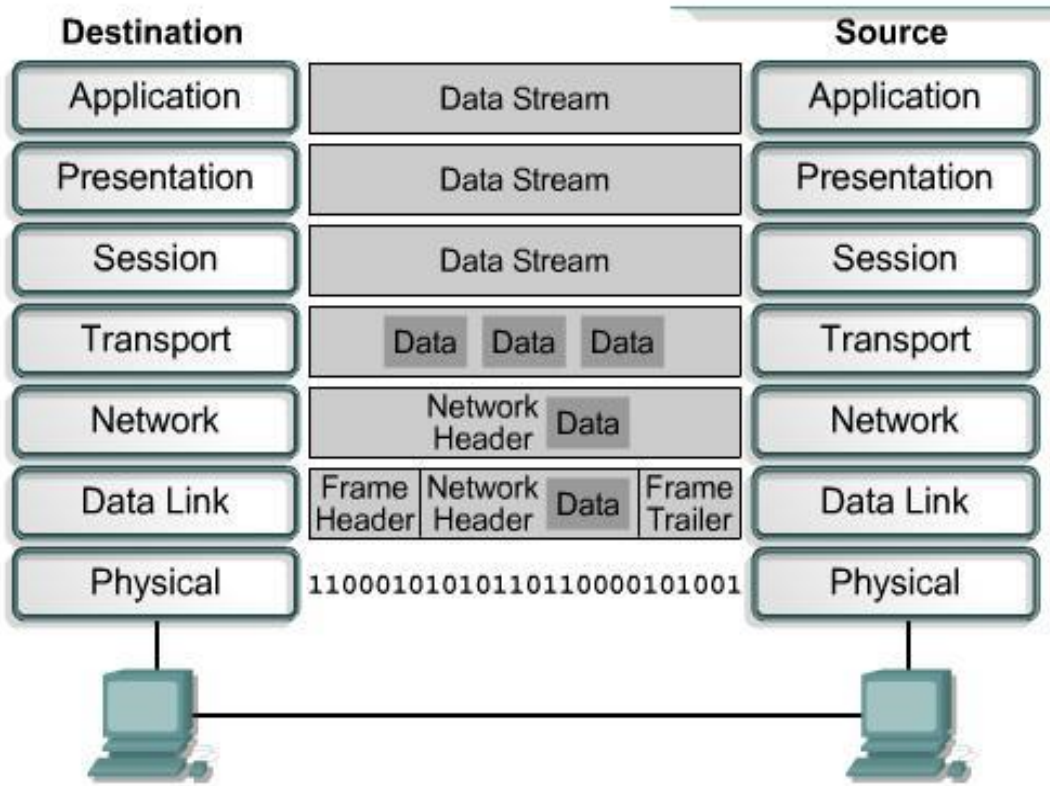
The data is put into a packet or datagram that contains a packet header with source and destination logical addresses. These addresses help network devices send the packets across the network along a chosen path.

4. Add the data link layer header and trailer:

Each network device must put the packet into a frame. The frame allows connection to the next directly-connected network device on the link. Each device in the chosen network path requires framing in order for it to connect to the next device.

5.Convert to bits for transmission:

The frame must be converted into a pattern of 1s and 0s (bits) for transmission on the medium. A clocking function enables the devices to distinguish these bits as they travel across the medium. The medium on the physical internetwork can vary along the path used. For example, the e-mail message can originate on a LAN, cross a campus backbone, and go out a WAN link until it reaches its destination on another remote LAN.

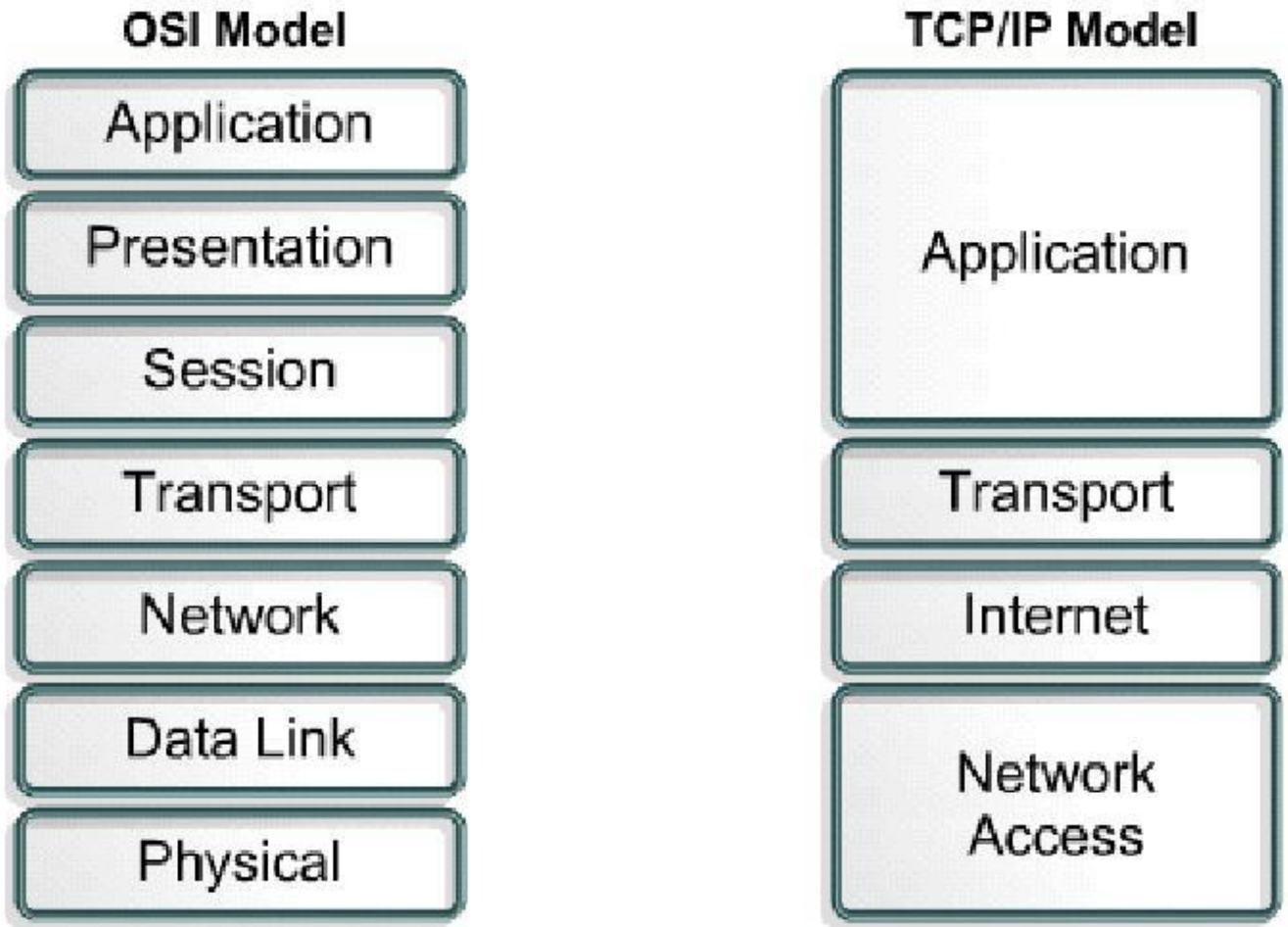

Destination
Source
Application
Presentation
Session
Transport
Network
Data Link
Physical
Data Stream
Data Stream
Data Stream
Data
Data
Data
Network Header
Data
Frame Header
Network Header
Data
Frame Trailer
1100010101011011000010100 1

TCP/IP

- **Transmission Control Protocol / Internet Protocol) Model:** The Internet uses a system of telecommunications protocols that has become so widely used that it is now accepted as a network architecture.
- The Internet's Protocol suite is called Transmission Control Protocol/ Internet Protocol and is known as TCP/IP. TCP/IP is used by the internet and by all intranets and extranets.
- The term TCP/IP refers to a set of protocols, or a protocol suite, that defines the rules governing how messages are exchanged in a computer network.
- The TCP/IP protocol suite grew out of a research project that began in 1969 and was funded by U.S. Department of Defense. It is result of protocol research and development conducted on the experimental packet-switched network, ARPANET (Advanced Research Projects Agency)

- The main purpose of the TCP/IP protocol suite is to allow diverse types of physical networks to be tied together so that any networked computer can talk to any other computer.
- The TCP/IP protocols allow the interconnected individual networks to give the appearance of a single, unified network called the Internet.
- In this all computers can freely exchange data as if they were all directly connected. The TCP/IP protocols make it appear to a system that there is a simple point to point connection to any other system in the Internet, even though data might have to follow a quite complex path in travelling from one system to another. The TCP/IP has become the de facto method we use for data communications on the Internet.

The layers to TCP/IP layers are:



Layer 4: Application Layer:

- In TCP/IP, the Application layer also includes the OSI Presentation Layer and Session Layer.
- This layer deals with higher level protocols and provides user friendly environment to end user.
- The application determines the presentation of the data and controls the session. In TCP/IP the terms socket and port are used to describe the path over which the applications communicate.
- There are numerous application level protocols in TCP/IP including Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP) used for email, HTTP (Hyper Text Transfer Protocol) used for World Wide Web and FTP for file transfer. Most application level protocols are associated with one or more port number.

Layer 3: Transport Layer:

- The major function of transport layer is for end to end delivery of information from source to destination.
- Mainly two protocols are used for this purpose, the first protocol is **TCP (Transmission Control Protocol)**. It is connection oriented protocol; it means that before sending the data from source to destination, first it establishes the fixed path and transmits the data on that path for whole session. It has the acknowledgment facility, it means source is aware whether the packet reaches to the destination or not. If the packet does not reaches to the destination, then source retransmit it until it reaches to the destination.

- Second protocol is **UDP (User Datagram Protocol)**. It is connectionless protocol, it means source does not make the fixed path to send the data to the destination. Each and every packet follows the different route and finally reaches the destination. Packets may reach to the destination out of order, it is the responsibility of the receiver to make it in proper order. UDP is unacknowledged protocol, source is not aware whether the packet reaches to the destination or not.

Layer 2: Internet Layer:

- The IP is normally described as the TCP/IP network Layer. Because of the internetworking emphasis of TCP/IP, this is commonly referred as the Internet Layer. All upper and lower layer communication travel through IP as they are passed through TCP/IP protocol stack.
- It is concerned with access to and routing data across a network for two end systems attached to same network. It takes segment form the transport layer and forms packet, then it sends those packets to the network. The job of internet layer is to allow host to insert packets into any network and have them to deliver independently to the destination.

- The major protocol associated with this layer is IP. Other protocols are ICMP (Internet Control Message Protocol), IP, IGMP (Internet Group Management Protocol), RIP (Routing Information Protocol), OSPF (Open Shortest Path First), EGP (Exterior Gateway Protocol), BGP4 (Broader Gateway Protocol-4).
- ICMP is used for diagnostics and to report on problems with the IP layer and for obtaining information about IP parameters. IGMP is used for managing multicasting. RIP, OSPF, EGP and BGP4 are examples of routing protocols.

Layer 1: Network Access Layer (Host to Network Layer):

- In TCP/IP the data link layer and physical layer are normally grouped together. TCP/IP makes use of existing data link layer and physical layer standards rather than defining its own.
- Data link layer describes how IP utilizes existing data link protocol such as Ethernet, token ring, FDDI, ATM.
- The characteristic of the hardware that carries the common signal are typically defined by the physical layer. This describes attributes such as pin configuration, voltage levels, and cable requirements. Example of physical layer standards are RS232, IEEE 802.5.

Comparison of OSI and TCP/IP Models

- Both of them use a layered architecture to explain data communication process in computer networks.
- Each layer performs well-defined functions in both models.
- Similar types of protocols are used in both models.
- OSI and TCP/IP reference models are open in nature.
- Both models give a good explanation on how various types of network hardware and software interact during a data communication process.
- Data hiding principle is well maintained on each layer in the two models. The core level functional details of each layer are not revealed to other layers.
- Transport layer defines end-end data communication process and error-correction techniques in both the models.
- OSI and TCP/IP reference models process data in the form of packets to perform routing

Difference between OSI and TCP/IP

OSI MODEL	TCP/IP MODEL
. 7 layers present in the architecture.	Only 4 layers are present.
. Not practically implemented yet.	Practical Model.
. Layering aspects, functions of each layer and division of esponsibilities are specifically presented by this model.	Division of responsibilities on each layer is not so specific.
. The concept of services, interfaces and protocols are well explained.	No clear distinction between the three
. Model was devised first and protocols were latter fitted to ppropriate layers.	The protocols came first and model was just explanation of protocols based on 4 layers.
. Widely used as a standard reference model in the design f computer networks.	Not considered as a design standard due to the failure in distinguishing services, interfaces and protocols.
. Connectionless and connection oriented services are here in Network layer but only connection oriented ervices in Transport layer.	Connectionless and connection oriented services in transport layer but only connectionless service in Network layer.
. This is a protocol independent model.	This is a protocol specific model.

Message Transmission Using Layers

- Each computer in the network has software that operates at each of the layers and performs the functions required by those layers (the physical layer is hardware, not software).
- Each layer in the network uses a formal language, or protocol, that is simply a set of rules that define what the layer will do and that provides a clearly defined set of messages that software at the layer needs to understand. For example, the protocol used for Web applications is HTTP (Hypertext Transfer Protocol). In general, all messages sent in a network pass through all layers.
- All layers except the Physical layer add a Protocol Data Unit (PDU) to the message as it passes through them. The PDU contains information that is needed to transmit the message through the network.

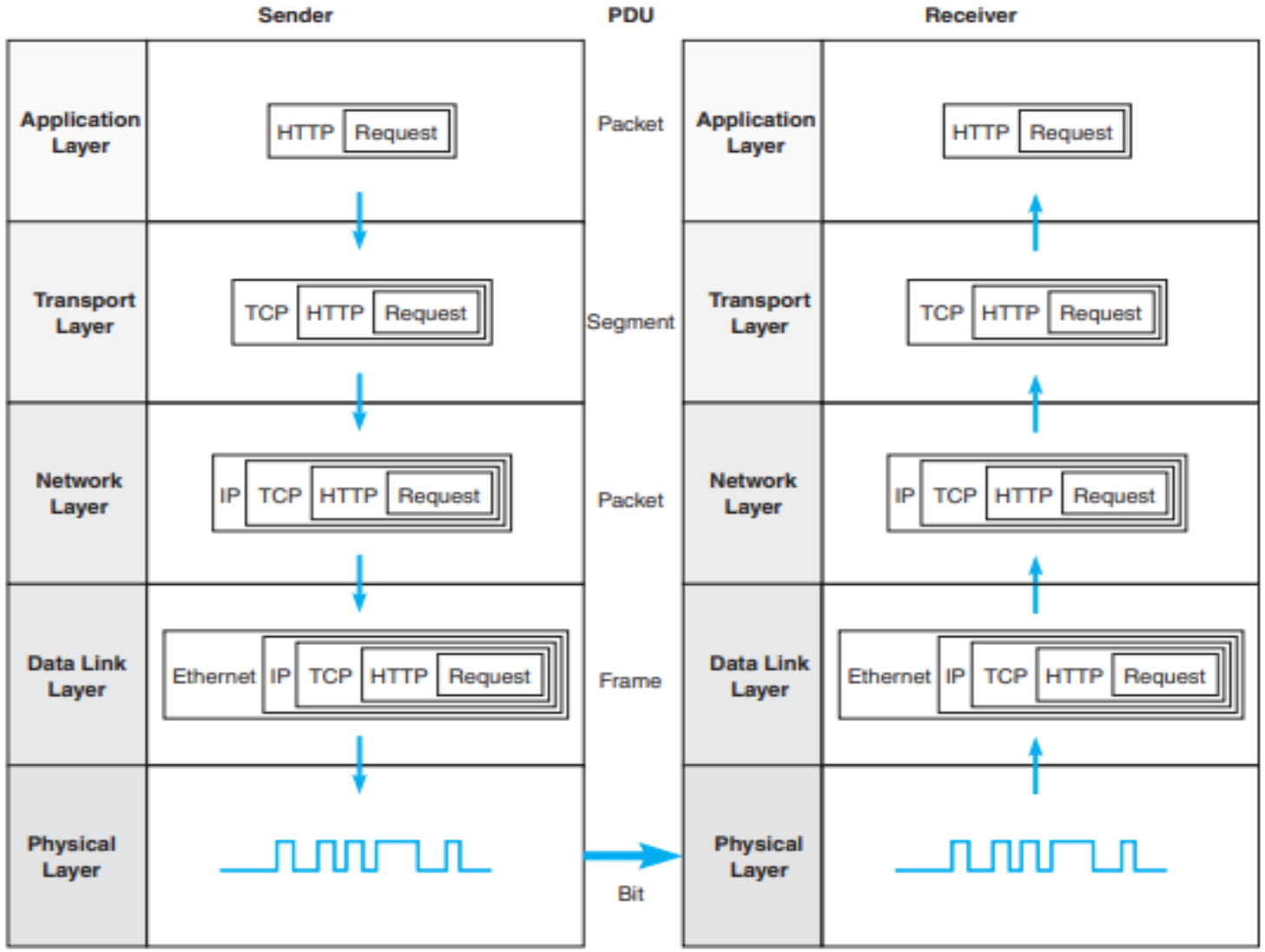


FIGURE 1.4 Message transmission using layers. IP = Internet Protocol; HTTP/Hypertext Transfer Protocol; TCP = Transmission Control Protocol

- **Application Layer:** First, the user creates a message at the application layer using a Web browser by clicking on a link (e.g., get the home page at www.somebody.com). The browser translates the user's message (the click on the Web link) into HTTP. The rules of HTTP define a specific PDU—called an HTTP packet—that all Web browsers must use when they request a Web page. For now, you can think of the HTTP packet as an envelope into which the user's message (get the Web page) is placed. In the same way that an envelope placed in the mail needs certain information written in certain places (e.g., return address, destination address), so too does the HTTP packet. The Web browser fills in the necessary information in the HTTP packet, drops the user's request inside the packet, then passes the HTTP packet (containing the Web page request) to the transport layer.
- **Transport Layer:** The transport layer on the Internet uses a protocol called TCP (Transmission Control Protocol), and it, too, has its own rules and its own PDUs. TCP is responsible for breaking large files into smaller packets and for opening a connection to the server for the transfer of a large set of packets. The transport layer places the HTTP packet inside a TCP PDU (which is called a TCP segment), fills in the information needed by the TCP segment, and passes the TCP segment (which contains the HTTP packet, which, in turn, contains the message) to the network layer.

- **Network Layer:** The network layer on the Internet uses a protocol called IP (Internet Protocol), which has its rules and PDUs. IP selects the next stop on the message's route through the network. It places the TCP segment inside an IP PDU, which is called an IP packet, and passes the IP packet, which contains the TCP segment, which, in turn, contains the HTTP packet, which, in turn, contains the message, to the data link layer.
- **Data Link Layer:** If you are connecting to the Internet using a LAN, your data link layer may use a protocol called Ethernet, which also has its own rules and PDUs. The data link layer formats the message with start and stop markers, adds error checking information, places the IP packet inside an Ethernet PDU, which is called an Ethernet frame, and instructs the physical hardware to transmit the Ethernet frame, which contains the IP packet, which contains the TCP segment, which contains the HTTP packet, which contains the message.
- **Physical Layer:** The physical layer in this case is network cable connecting your computer to the rest of the network. The computer will take the Ethernet frame (complete with the IP packet, the TCP segment, the HTTP packet, and the message) and send it as a series of electrical pulses through your cable to the server.

- When the server gets the message, this process is performed in reverse.
- The physical hardware translates the electrical pulses into computer data and passes the message to the data link layer.
- The data link layer uses the start and stop markers in the Ethernet frame to identify the message. The data link layer checks for errors and, if it discovers one, requests that the message be resent. If a message is received without error, the data link layer will strip off the Ethernet frame and pass the IP packet (which contains the TCP segment, the HTTP packet, and the message) to the network layer.
- The network layer checks the IP address and, if it is destined for this computer, strips off the IP packet and passes the TCP segment, which contains the HTTP packet and the message to the transport layer.
- The transport layer processes the message, strips off the TCP segment, and passes the HTTP packet to the application layer for processing.
- The application layer (i.e., the Web server) reads the HTTP packet and the message it contains (the request for the Web page) and processes it by generating an HTTP packet containing the Web page you requested. Then the process starts again as the page is sent back to you

Network Standards

The Importance of Standards

- Agreeing to common syntax, semantics, and timing definitions for a protocol is easy enough if you're dealing only with other computers in the same office or town, or if all parties are using the same hardware and software. But how do you ensure the whole world sticks to the same conventions within a protocol? That's where standards come in.
- Standards are guidelines that explain to all IT stakeholders from device manufacturers to software programmers and network administrators how a particular protocol should operate. As long as everyone adheres to a common standard and provided the definitions of that standard are open to the public, the protocol guarantees two devices can communicate, even if they were built by different companies or are running different operating systems.
- The use of standards makes it much easier to develop software and hardware that link different networks because software and hardware can be developed one layer at a time. The Standards-Making Process Data communication standards fall into two categories: de facto (meaning "by fact" or "by convention") and de jure (meaning "by law" or "by regulation").

- **The standards-Making Process**
- There are two types of standards: de jure and de facto.
- De facto (by fact or by convention): Standards that have not been approved by an organized body but have been adopted as standards through with approved by one facto standards. De facto standards are often established originally by manufacturers that seek to define the functionality of a new product or technology Examples of de facto standards are MS Office and various DVD standards.
- De jure (by law): De jure standards are those that have been legislated by an officially recognized body.

- # Standards Organizations:
- **International Organization for Standardization(ISO)**
- One of the most important standards-making bodies is the International Organization for Standardization (ISO), which makes technical recommendations about data communication interfaces (see www.iso.org). ISO is based in Geneva, Switzerland. The membership is composed of the national standards organizations of each ISO member country.
- **International Telecommunications Union-Telecommunications Group (ITU-T)**
- The International Telecommunications Union-Telecommunications Group (ITU-T) is the technical standards-setting organization of the United Nations International Telecommunications Union, which is also based in Geneva (see www.itu.int). ITU is composed of representatives from about 200 member countries. Membership was originally focused on just the public telephone companies in each country, but a major reorganization in 1993 changed this, and ITU now seeks members among public- and private-sector organizations who operate computer or communications networks (e.g., RBOCs) or build software and equipment for them (e.g., AT&T).

.

- **American National Standards Institute (ANSI)**
- The American National Standards Institute (ANSI) is the coordinating organization for the U.S. national system of standards for both technology and nontechnology (see www.ansi.org). ANSI has about 1,000 members from both public and private organizations in the United States. ANSI is a standardization organization, not a standards-making body, in that it accepts standards developed by other organizations and publishes them as American standards. Its role is to coordinate the development of voluntary national standards and to interact with the ISO to develop national standards that comply with the ISO's international recommendations. ANSI is a voting participant in the ISO.
- **Institute of Electrical and Electronics Engineers (IEEE)**
- The Institute of Electrical and Electronics Engineers (IEEE) is a professional society in the United States whose Standards Association (IEEE-SA) develops standards (see www.standards.ieee.org). The IEEE-SA is probably most known for its standards for LANs. Other countries have similar groups; for example, the British counterpart of IEEE is the Institution of Electrical Engineers (IEE).

- **Internet Engineering Task Force (IETF)**
- The Internet Engineering Task Force (IETF) sets the standards that govern how much of the Internet will operate (see www.ietf.org). The IETF is unique in that it doesn’t really have official memberships. Quite literally anyone is welcome to join its mailing lists, attend its meetings, and comment on developing standards.
- **Electronic Industries Association (EIA)**
- Aligned with ANSI, the Electronic Industries Association (EIA) is a nonprofit organization devoted to the promotion of electronics manufacturing concerns. Its activities include public awareness education and lobbying efforts in addition to standards development. In the field of information technology, the EIA has made significant contributions by defining physical connection interfaces and electronic signaling specifications for data communications.

- **World Wide Web Consortium (W3C)**
- The World Wide Web Consortium (W3C) is the main international standards organization World Wide Web (abbreviated WWW or W3). Tim Berners-Lee founded this consortium at Massachusetts Institute of Technology Laboratory for Computer Science. It was founded to provide computability in industry for new standards. W3C has created regional offices around the world.
- **Open Mobile Alliance (OMA)**
- The standards organization OMA was created to gather different forums in computer networking and wireless technology under the umbrella of one single authority. Its mission is to provide unified standards for application protocols.

- **Common Standards:**
- There are many different standards used in networking today. Each standard usually covers one layer in a network. Some of the most commonly used standards are shown in Figure

Layer	Common Standards
5. Application layer	HTTP, HTML (Web) MPEG, H.323 (audio/video) SMTP, IMAP, POP (email)
4. Transport layer	TCP (Internet and LANs)
3. Network layer	IP (Internet and LANs)
2. Data link layer	Ethernet (LAN) Frame relay (WAN) T1 (MAN and WAN)
1. Physical layer	RS-232C cable (LAN) Category 5 cable (LAN) V.92 (56 Kbps modem)

FIGURE 1–6 Some common data communications standards. HTML = Hypertext Markup Language; HTTP = Hypertext Transfer Protocol; IMAP = Internet Message Access Protocol; IP = Internet Protocol; LAN = Local Area Network; MPEG = Motion Picture Experts Group; POP = Post Office Protocol; TCP = Transmission Control Protocol

- For a network to operate, many different standards must be used simultaneously. The sender of a message must use one standard at the application layer, another one at the transport layer, another one at the network layer, another one at the data link layer, and another one at the physical layer.
- Each layer and each standard is different, but all must work together to send and receive messages.
- Either the sender and receiver of a message must use the same standards or, more likely, there are devices between the two that translate from one standard into another. Because different networks often use software and hardware designed for different standards, there is often a lot of translation between different standards.

Future Trends

- The field of data communications has grown faster and become more important than computer processing itself. Both go hand in hand, but we have moved from the computer era to the communication era. Three major trends are driving the future of communications and networking.

Wireless LAN and BYOD

- The rapid development of mobile devices, such as smartphones and tablets, has encouraged employers to allow their employees to bring these devices to work and use them to access data, such as their work email. This movement, called bring your own device, or Bring Your On Device (BYOD), is a great way to get work quickly, saves money, and makes employees happy. But BYOD also brings its own problems. Employers need to add or expand their Wireless Local Area Networks (WLANs) to support all these new devices.
- Another important problem is security. Employees bring these devices to work so that they can access not only their email but also other critical company assets, such as information about their clients, suppliers, or sales. Employers face myriad decisions about how to manage access to company applications for BYOD.

- Companies can adopt two main approaches: (1) native apps or (2) browser-based technologies.
- Native apps require an app to be developed for each application that an employee might be using for every potential device that the employee might use (e.g., iPhone, Android, Windows).
- The browser based approach (often referred to as responsive design using HTML5) doesn’t create an app but rather requires employees to access the application through a Web browser. Both these approaches have their pros and cons, and only the future will show which one is the winner.
- What if an employee loses his or her mobile phone or tablet so that the application that accesses critical company data now can be used by anybody who finds the device? Will the company’s data be compromised? Device and data loss practices now have to be added to the general security practices of the company. Employees need to have apps to allow their employer to wipe their phones clean in case of loss so that no company data are compromised (e.g., SOTI’s MobiControl). In some cases, companies require the employee to allow monitoring of the device at all times, to ensure that security risks are minimized. However, some argue that this is not a good practice because the device belongs to the employee, and monitoring it 24/7 invades the employee’s privacy.

The Internet of Things

- Telephones and computers used to be separate. Today voice and data have converged into unified communications, with phones plugged into computers or directly into the LAN using Voice over Internet Protocol (VoIP). Vonage and Skype have taken this one step further and offer telephone service over the Internet at dramatically lower prices than traditional separate landline phones, whether from traditional phones or via computer microphones and speakers.
- Computers and networks can also be built into everyday things, such as kitchen appliances, doors, and shoes. In the future, the Internet will move from being a Web of computers to also being an Internet of Things (IoT), as smart devices become common, that creates the Network of Things (NoT) where all this interaction between IoT devices will happen seamlessly, without human intervention. And you might already be asking Alexa or Siri for advice on where to eat, lock, and unlock your apartment, turn on/off your lights, or change the thermostat setting. For this to happen, Alexa/Siri must be able to communicate with your lock or thermostat without any intervention from you.
- Some examples of IoT systems in use today are:

- **Connected cars:** There are many ways vehicles, such as cars, can be connected to the internet. It can be through smart dashcams, infotainment systems, or even the vehicle's connected gateway. They collect data from the accelerator, brakes, speedometer, odometer, wheels, and fuel tanks to monitor both driver performance and vehicle health. Connected cars have a range of uses:
- Monitoring rental car fleets to increase fuel efficiency and reduce costs.
- Helping parents track the driving behavior of their children.
- Notifying friends and family automatically in case of a car crash.
- Predicting and preventing vehicle maintenance needs.

- **Connected homes:** Smart home devices are mainly focused on improving the efficiency and safety of the house, as well as improving home networking. Devices like smart outlets monitor electricity usage and smart thermostats provide better temperature control. Hydroponic systems can use IoT sensors to manage the garden while IoT smoke detectors can detect tobacco smoke. Home security systems like door locks, security cameras, and water leak detectors can detect and prevent threats, and send alerts to homeowners. Connected devices for the home can be used for.
- Automatically turning off devices not being used.
- Rental property management and maintenance.
- Finding misplaced items like keys or wallets.
- Automating daily tasks like vacuuming, making coffee, etc.

- **Smart cities:** IoT applications have made urban planning and infrastructure maintenance more efficient. Governments are using IoT applications to tackle problems in infrastructure, health, and the environment. IoT applications can be used for:
- Measuring air quality and radiation levels.
- Reducing energy bills with smart lighting systems.
- Detecting maintenance needs for critical infrastructures such as streets, bridges, and pipelines.
- Increasing profits through efficient parking management.

- **Smart buildings:** Buildings such as college campuses and commercial buildings use loT applications to drive greater operational efficiencies, IoT devices can be use in smart buildings for.
- Reducing energy consumption.
- Lowering maintenance costs.
- Utilizing work spaces more efficiently.

Massively Online

- You have probably heard of massively multiplayer online games, such as World of Warcraft, where you can play with thousands of players in real time. Well, today not only games are massively online. Education is massively online. Edx, Khan Academy, Lynda.com, or Code Academy have websites that offer thousands of education modules for children and adults in myriad fields to help them learn. Your class very likely also has an online component.
- You may even use this textbook online and decide whether your comments are for you only, for your instructor, or for the entire class to read. In addition, you may have heard about massive open online courses, or MOOC. MOOC enable students who otherwise wouldn’t have access to elite universities to get access to top knowledge without having to pay the tuition. These classes are offered by universities, such as Stanford, UC Berkeley, MIT, UCLA, Carnegie Mellon, and of course, Indiana University, free of charge and for no credit (although at some universities, you can pay and get credit toward your degree).

- Politics has also moved massively online. President Obama reached out to the crowds and ordinary voters not only through his Facebook page but also through Reddit and Google Hangouts. President Trump's use of Twitter is unprecedented. He can directly reach millions of followers—a strategy that paid off in the 2016 elections. Finally, massively online allows activists to reach masses of people in a very short period of time to initiate change. Examples of use of YouTube videos or Facebook for activism include the Arab Spring, Kony 2012, or the use of sarin gas in Syria.
- So what started as a game with thousands of people being online at the same time is being reinvented for good use in education, politics, and activism. Only the future will show what humanity can do with what massively online has to offer.
- What these three trends have in common is that there will be an increasing demand for professionals who understand development of data communications and networking infrastructure to support this growth. There will be more and more need to build faster and more secure networks that will allow individuals and organizations to connect to resources, probably stored on cloud infrastructure (either private or public). This need will call not only for engineers who deeply understand the technical aspects of networks but also for highly social individuals who embrace technology in creative ways to allow business to achieve a competitive edge through utilizing this technology.