Chapter Five
OSI Model

Data Communication and Computer Networks

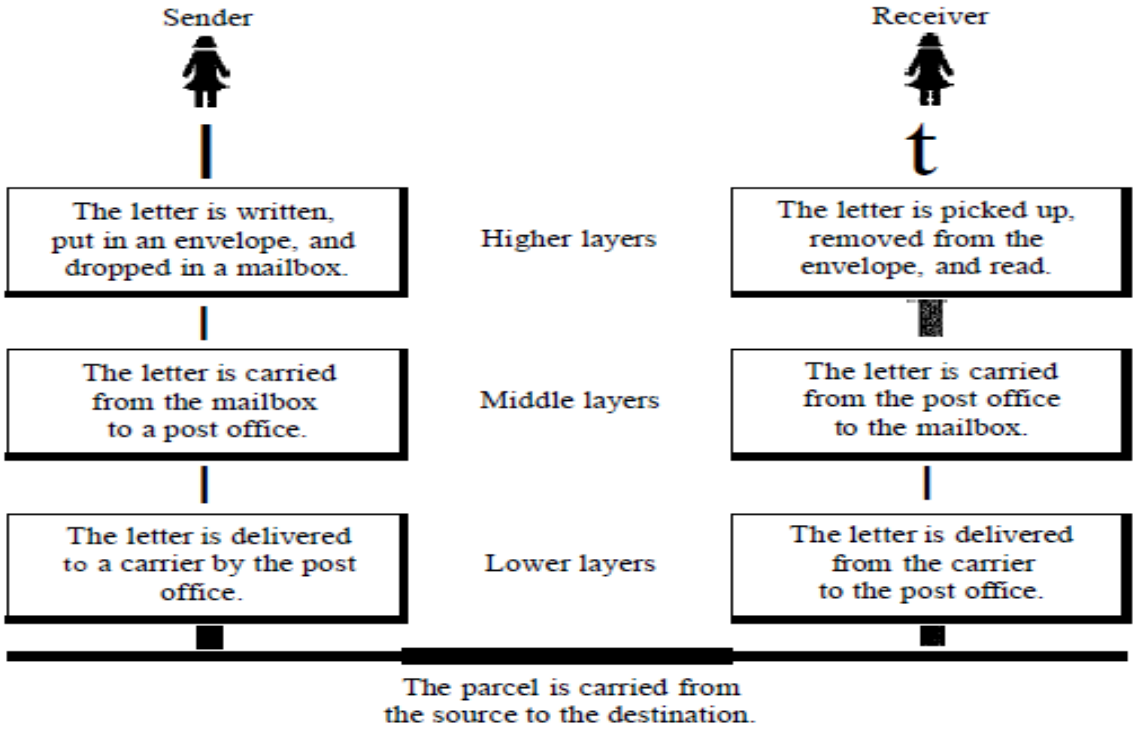
haleluyaluya@yahoo.com

Communication and Layer Architecture

- A network is a combination of hardware and software that sends data from one location to another.
- The hardware consists of the physical equipment that carries signals from one point of the network to another.
- The software consists of instruction sets that make possible the services that we expect from a network
- For example, the task of sending an e-mail from one point in the world to another can be broken into several tasks, each performed by a separate software package.
- Each software package uses the services of another software package.
- At the lowest layer, a signal, or a set of signals, is sent from the source computer to the destination computer.

Layered Tasks

- We use the concept of layers in our daily life.
  - Eg. let us consider two friends who communicate through postal mail.
- The process of sending a letter to a friend would be complex if there were no services available from the post office.



Contd.

- A communication architecture is a strategy for connecting host computers and other communicating equipment.
- It defines necessary elements for data communication between devices.
- A communication architecture, therefore, defines a standard for the communicating hosts.
- A programmer formats data in a manner defined by the communication architecture and passes it on to the communication software.
- Separating communication functions adds flexibility, for example, we do not need to modify the entire host software to include more communication devices.

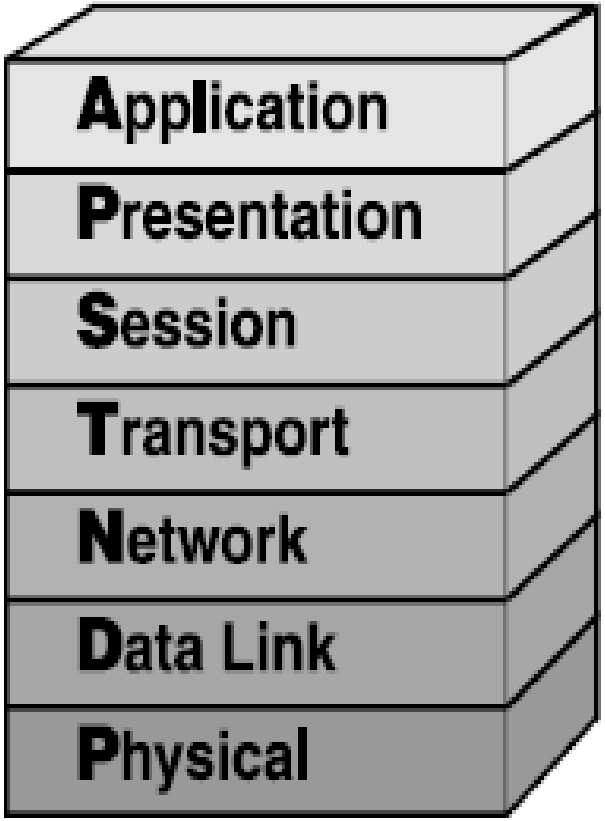
Contd.

- Layer architecture simplifies the network design.
- It is easy to debug network applications in a layered architecture network.
- The network management is easier due to the layered architecture.
- Network layers follow a set of rules, called protocol.
- The protocol defines the format of the data being exchanged, and the control and timing for the handshake between layers.

Open Systems Interconnection (OSI)

- 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.

The Seven Layers



All
People
Seem
To
Need
Data
Processing

Please
Do
Not
Throw
Susage
Pizza
Away

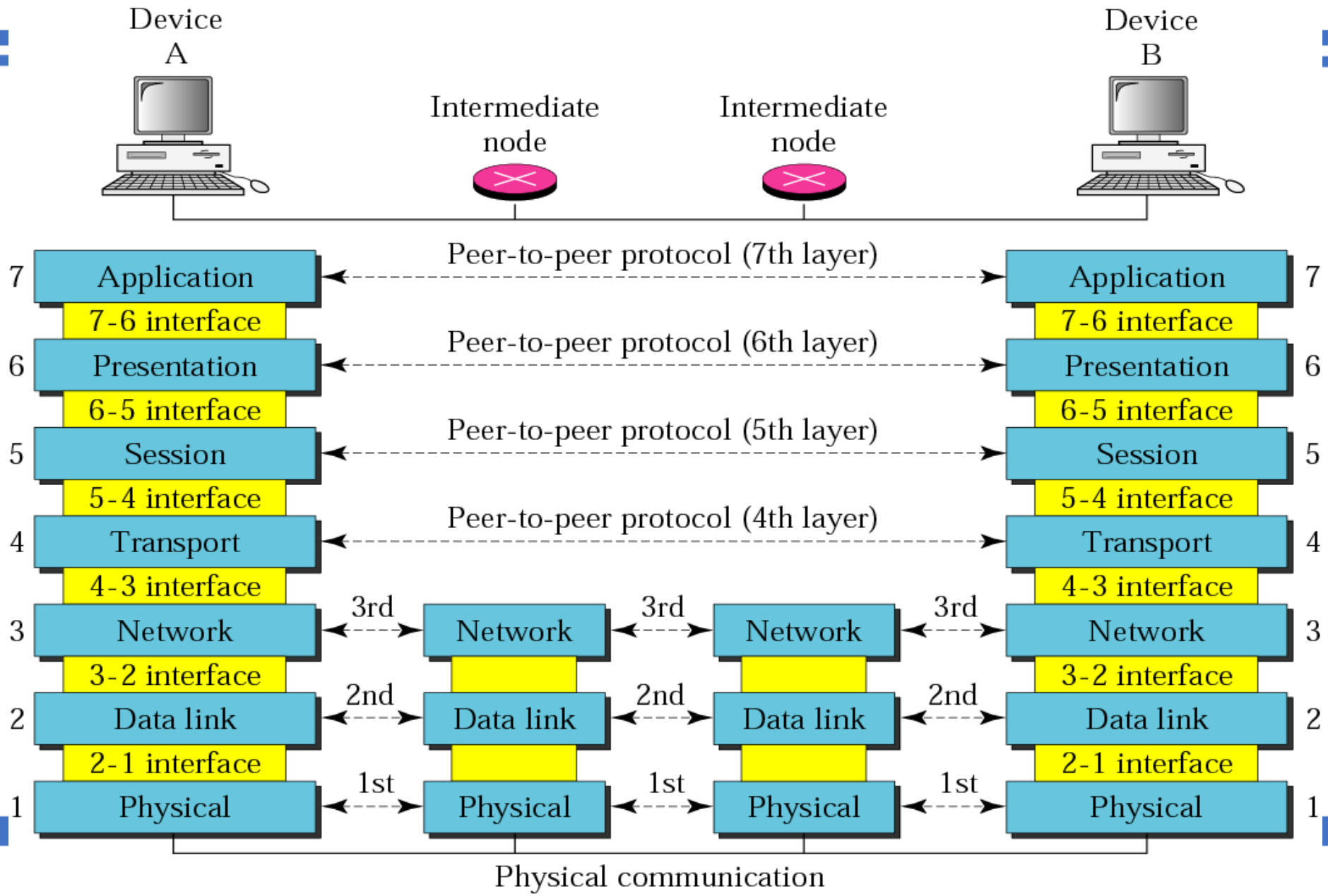
Contd.

Application	• File, print, message, database, and application services
Presentation	• Data encryption, compression, and translation services
Session	• Dialog control
Transport	• End-to-end connection
Network	• Routing
Data Link	• Framing
Physical	• Physical topology

Contd.

- The OSI model is composed of seven ordered layers:
  - Physical (layer 1),
  - Data link (layer 2),
  - Network (layer 3),
  - Transport (layer 4),
  - Session (layer 5),
  - Presentation (layer 6), and
  - Application (layer 7).
- The figure in the next slide shows the layers involved when a message is sent from device A to device B. As the message travels from A to B, it may pass through many intermediate nodes.
- These intermediate nodes usually involve only the first three bottom layers of the OSI model.

Contd.


Device A
Intermediate node
Intermediate node
Device B
Peer-to-peer protocol (7th layer)
Peer-to-peer protocol (6th layer)
Peer-to-peer protocol (5th layer)
Peer-to-peer protocol (4th layer)
7 Application
7-6 interface
6 Presentation
6-5 interface
5 Session
5-4 interface
4 Transport
4-3 interface
3 Network
3-2 interface
2 Data link
2-1 interface
1 Physical
3rd
2nd
1st
Physical communication

Contd.

- In *developing the model, the designers distilled the process of transmitting data to* its most fundamental elements.
- They identified which networking functions had related uses and collected those functions into discrete groups that became the layers.
- Each layer defines a family of functions distinct from those of the other layers.
- By defining and localizing functionality in this fashion, the designers created an architecture that is both comprehensive and flexible.
- Most importantly, the OSI model allows complete interoperability between otherwise incompatible systems.
- Within a single machine, each layer calls upon the services of the layer just below it.

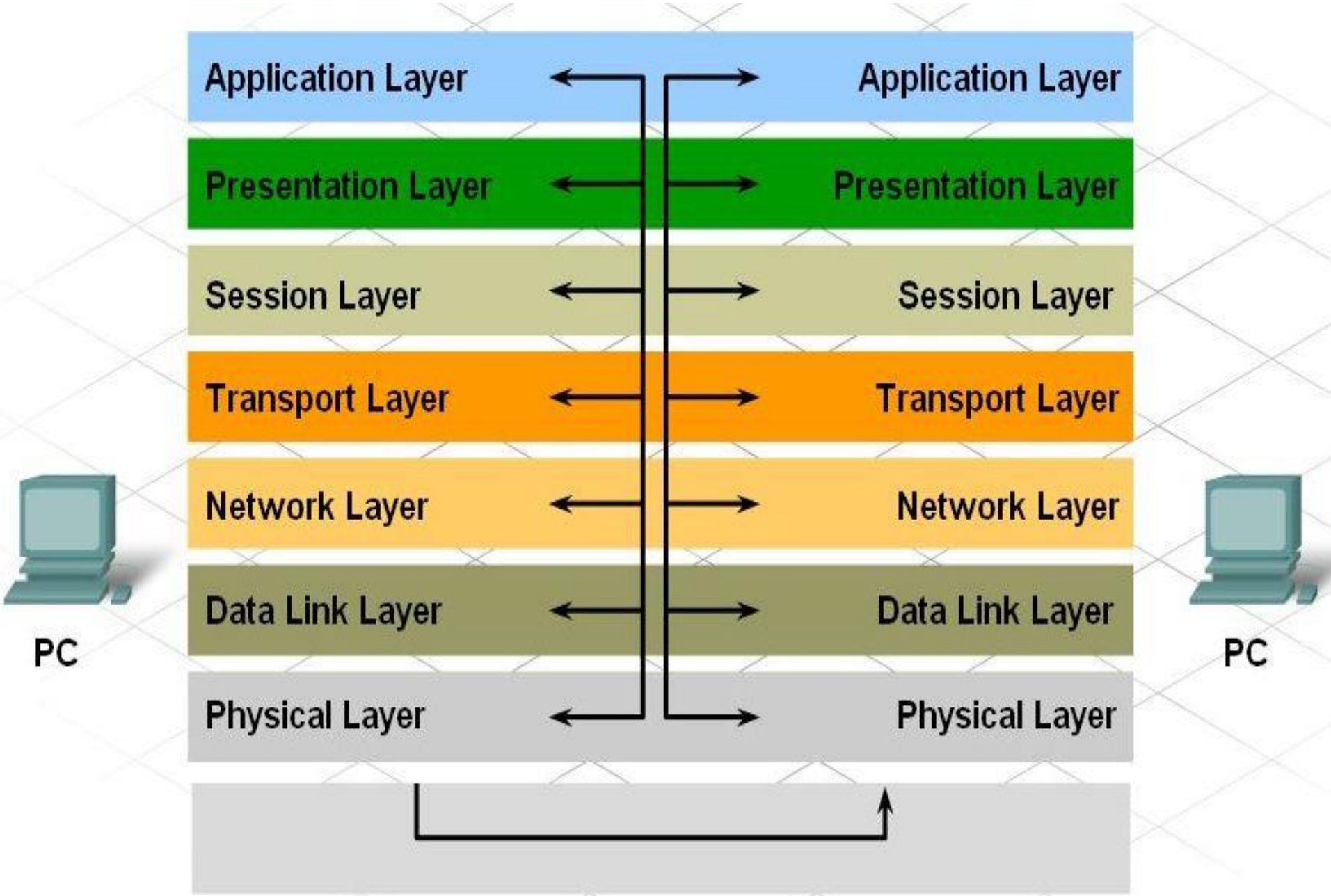
Contd.

- Layer 3, for example, uses the services provided by layer 2 and provides services for layer 4. Between machines, layer *x on one machine communicates with layer x on* another machine.
- This communication is governed by an agreed-upon series of rules and conventions called protocols.
- The processes on each machine that communicate at a given layer are called peer-to-peer processes.
- Communication between machines is therefore a peer-to-peer process using the protocols appropriate to a given layer.

Peer-to-Peer Processes

- At the physical layer, communication is direct: At the higher layers, however, communication must move down through the layers on device A, over to device B, and then back up through the layers.
- Each layer in the sending device adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it.
- At layer 1 the entire package is converted to a form that can be transmitted to the receiving device.
- At the receiving machine, the message is unwrapped layer by layer, with each process receiving and removing the data meant for it.
- For example, layer 2 removes the data meant for it, then passes the rest to layer 3. Layer 3 then removes the data meant for it and passes the rest to layer 4, and so on.

Contd.


Application Layer
Application Layer
Presentation Layer
Presentation Layer
Session Layer
Session Layer
Transport Layer
Transport Layer
Network Layer
Network Layer
Data Link Layer
Data Link Layer
Physical Layer
Physical Layer
PC
PC

Interfaces Between Layers

- The passing of the data and network information down through the layers of the sending device and back up through the layers of the receiving device is made possible by an interface between each pair of adjacent layers.
- Each interface defines the information and services a layer must provide for the layer above it.
- Well-defined interfaces and layer functions provide modularity to a network.
- As long as a layer provides the expected services to the layer above it, the specific implementation of its functions can be modified or replaced without requiring changes to the surrounding layers.

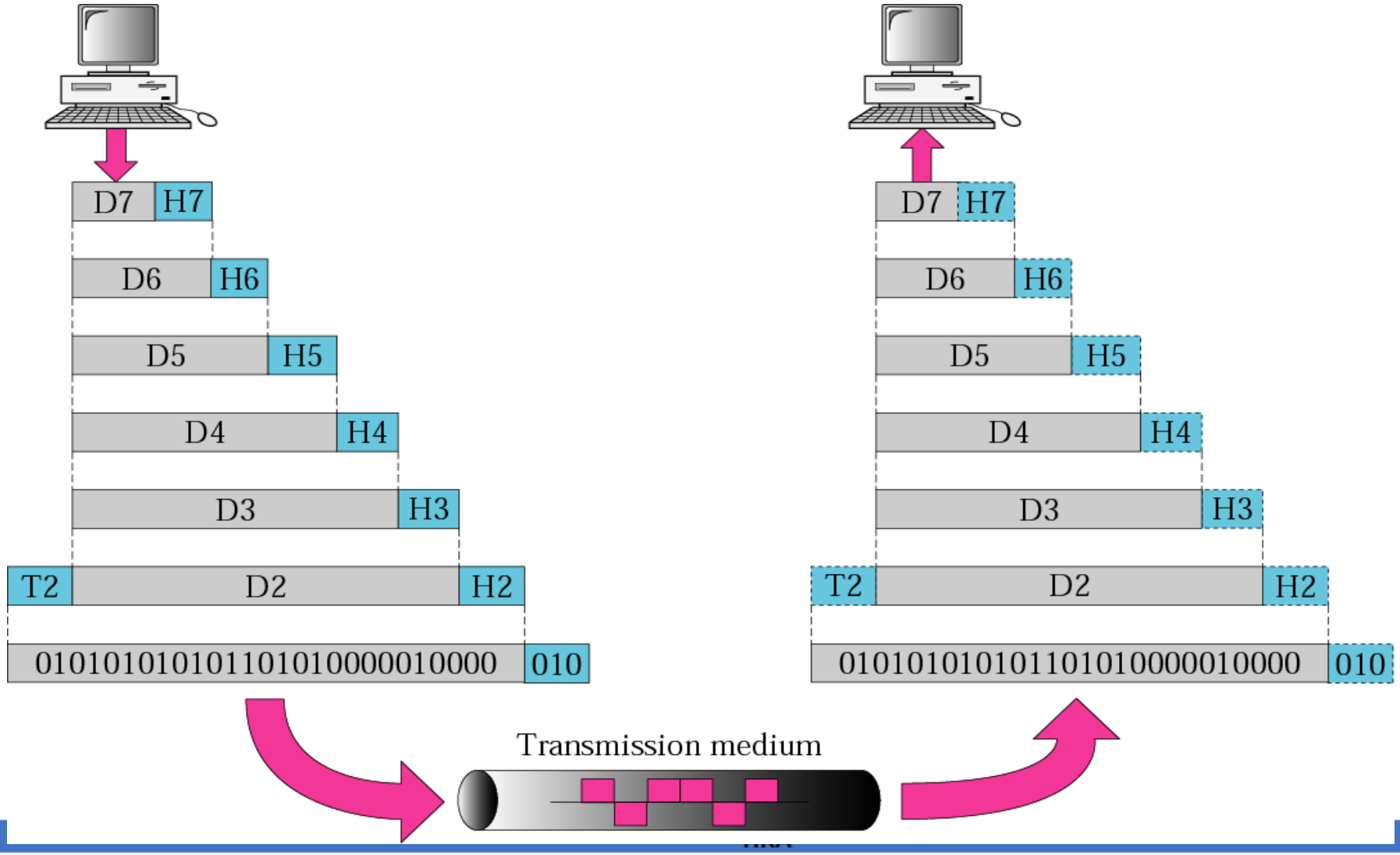
Organization of the Layers

- The seven layers can be thought of as belonging **to three subgroups**.
- Layers 1, 2, and 3 - physical, data link, and network - are the network support layers; they deal with the physical aspects of moving data from one device to another (such as electrical specifications, physical connections, physical addressing, and transport timing and reliability).
- Layers 5, 6, and 7- session, presentation, and application - can be thought of as the user support layers; they allow interoperability among unrelated software systems.
- Layer 4, the transport layer, links the two subgroups and ensures that what the lower layers have transmitted is in a form that the upper layers can use.
- The upper OSI layers are almost always implemented in software; lower layers are a combination of hardware and software, except for the physical layer, which is mostly hardware.

Contd.

- The figure shown in the next slide, gives an overall view of the OSI layers, D7 means the data unit at layer 7, D6 means the data unit at layer 6, and so on. The process starts at layer 7 (the application layer), then moves from layer to layer in descending, sequential order.
- At each layer, a header, or possibly a trailer, can be added to the data unit.
- Commonly, the trailer is added only at layer 2.
- When the formatted data unit passes through the physical layer (layer 1), it is changed into an electromagnetic signal and transported along a physical link.

An exchange using the OSI model



Contd.

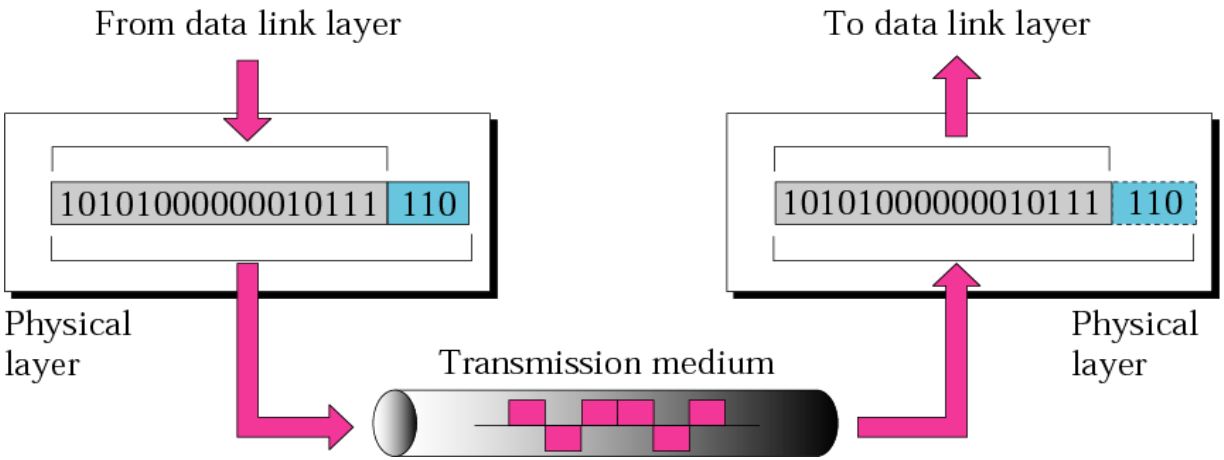
- Upon reaching its destination, the signal passes into layer 1 and is transformed back into digital form. The data units then move back up through the OSI layers.
- As each block of data reaches the next higher layer, the headers and trailers attached to it at the corresponding sending layer are removed, and actions appropriate to that layer are taken.
- By the time it reaches layer 7, the message is again in a form appropriate to the application and is made available to the recipient.

Encapsulation

- A packet (header and data) at level 7 is encapsulated in a packet at level 6. The whole packet at level 6 is encapsulated in a packet at level 5, and so on.
- In other words, the data portion of a packet at level *N - 1 carries the* whole packet (data and header and may be trailer) from level *N. The concept is called encapsulation; level N - 1 is not aware of which part of the encapsulated packet is data and which part* is the header or trailer.
- For level *N - 1, the whole packet coming from level N is treated* as one integral unit.

Physical Layer

- The physical layer coordinates the functions required to carry a bit stream over a physical medium.
- It deals with the mechanical and electrical specifications of the interface and transmission medium.
- It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur.



The physical layer is responsible for movements of individual bits from one hop (node) to the next.

The physical layer is also concerned with the following:

1. Physical characteristics of interfaces and medium. The physical layer defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.
2. Representation of bits. The physical layer data consists of a stream of bits (sequence of 0s or 1s) with no interpretation. To be transmitted, bits must be encoded into signals - electrical or optical. The physical layer defines the type of encoding (how 0s and 1s are changed to signals) (Refer chapter one).
3. Data rate. The transmission rate - the number of bits sent each second - is also defined by the physical layer. In other words, the physical layer defines the duration of a bit, which is how long it lasts.
4. Synchronization of bits. The sender and receiver not only must use the same bit rate but also must be synchronized at the bit level. In other words, the sender and the receiver clocks must be synchronized.

Contd.

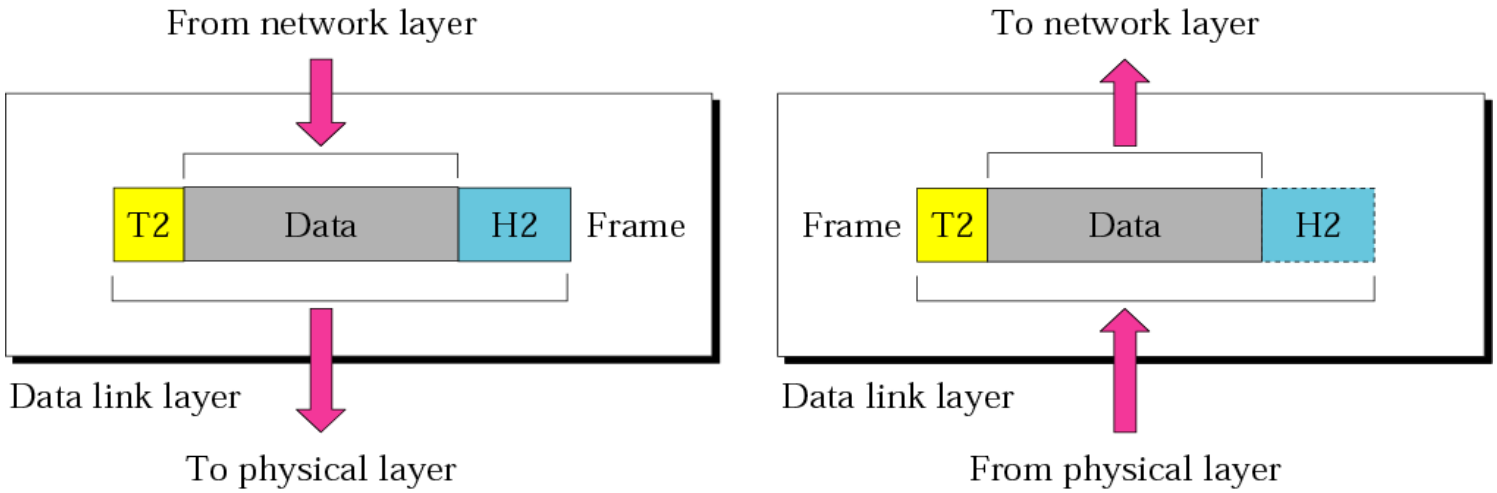
5. **Line configuration**. The physical layer is concerned with the connection of devices to the media (point – to – point or multipoint).

6. **Physical topology**. The physical topology defines how devices are connected to make a network.

6. **Transmission mode**. The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex.

Data Link Layer

- The data link layer transforms the physical layer, a raw transmission facility, to a reliable link.
- It makes the physical layer appear error-free to the upper layer (network layer). The following figure shows the relationship of the data link layer to the network and physical layers.



The data link layer is responsible for moving frames from one hop (node) to the next.

Layer 2 frame structure

<table>
<tr><td rowspan="2">Start Frame (Flag)</td><td colspan="2">Header</td><td rowspan="2">Data</td><td>Trailer</td><td rowspan="2">Stop Frame (Flag)</td></tr>
<tr><td>Address</td><td>Type/Length</td><td>FCS</td></tr>
</table>

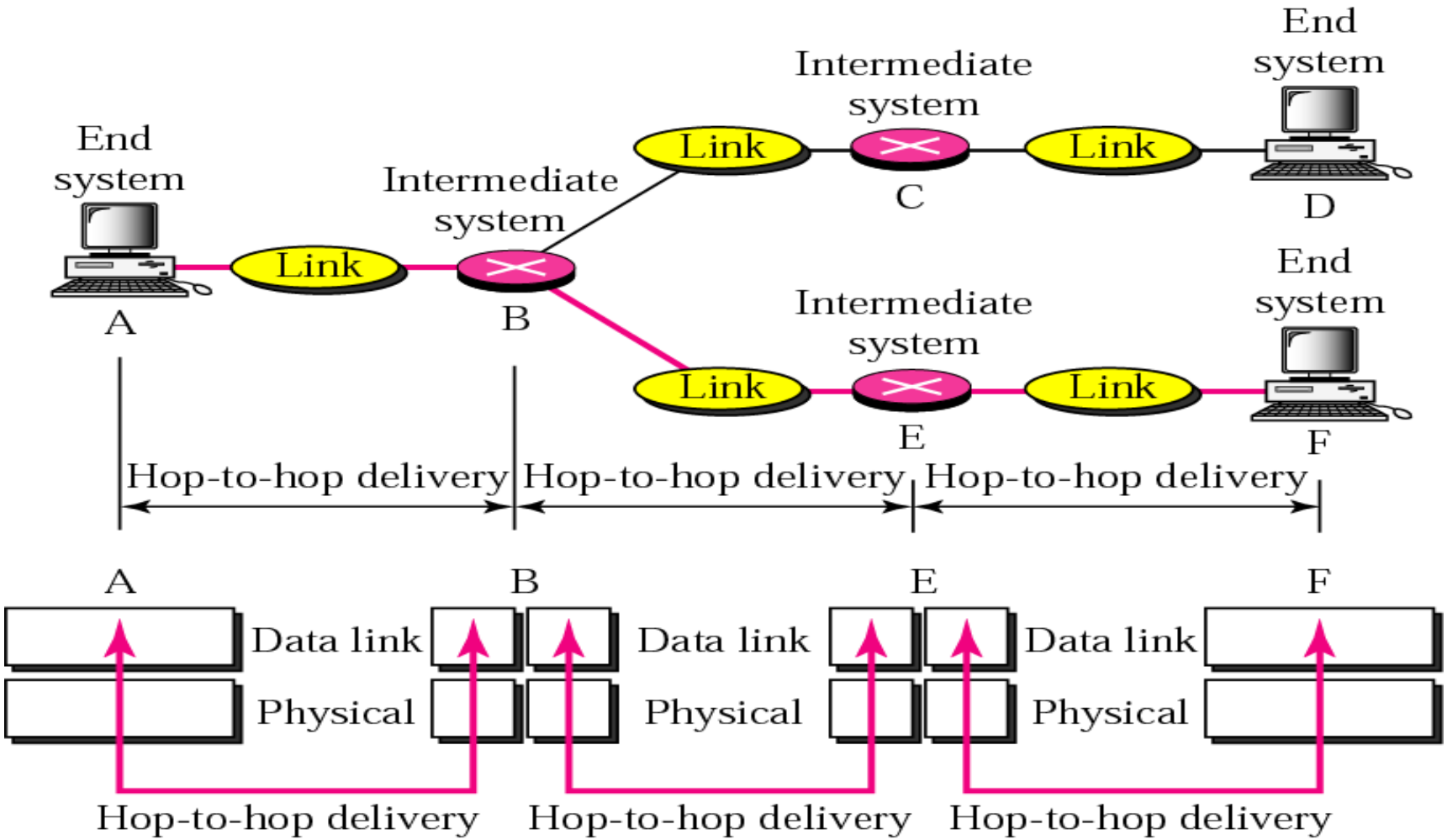
Data Link Layer Responsibilities

1. Framing. The data link layer divides the stream of bits received from the network layer into manageable data units called frames.
2. 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.
   - If the frame is intended for a system outside the sender‘s network, the receiver address is the address of the device that connects the network to the next one.

Contd.

3. 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.
4. 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.
5. 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.

Hop-to-hop (node-to-node) delivery by data link layer



Contd.

- As the figure above shows, communication at the data link layer occurs between two adjacent nodes.
  - To send data from A to F, three partial deliveries are made.
  - First, the data link layer at A sends a frame to the data link layer at B (a router).
  - Second, the data link layer at B sends a new frame to the data link layer at E.
  - Finally, the data link layer at E sends a new frame to the data link layer at F.
- Note that the frames that are exchanged between the three nodes have different values in the headers. The frame from A to B has B as the destination address and A as the source address. The frame from B to E has E as the destination address and B as the source address. The frame from E to F has F as the destination address and E as the source address. The values of the trailers can also be different if error checking includes the header of the frame.

Framing

- The data link layer, needs to pack bits into frames, so that each frame is distinguishable from another. Our postal system practices a type of framing.
- The simple act of inserting a letter into an envelope separates one piece of information from another; the envelope serves as the delimiter.
- In addition, each envelope defines the sender and receiver addresses since the postal system is a many-to-many carrier facility.
- Framing in the data link layer separates a **message** from one source to a destination, or from other messages to other destinations, by adding a sender address and a destination address.
- The destination address defines where the packet is to go; the sender address helps the recipient acknowledge the receipt.

Contd.

- NB: Addressing here is about the next node in the LAN
- Although the whole message could be packed in one frame, that is not normally done.
- One reason is that a frame can be very large, making flow and error control very inefficient.
- When a message is carried in one very large frame, even a single-bit error would require the retransmission of the whole message.
- When a message is divided into smaller frames, a single-bit error affects only that small frame.

Frames can be of fixed or variable size

1. **Fixed-Size Framing:-** In fixed-size framing, there is no need for defining the boundaries of the frames; the size itself can be used as a delimiter. An example of this type of framing is the ATM wide-area network, which uses frames of fixed size called cells.

2. **Variable-Size Framing:-** variable-size framing is prevalent in local area networks. In variable-size framing, we need a way to define the end of the frame and the beginning of the next. Historically, two approaches were used for this purpose: a character-oriented approach and a bit-oriented approach.

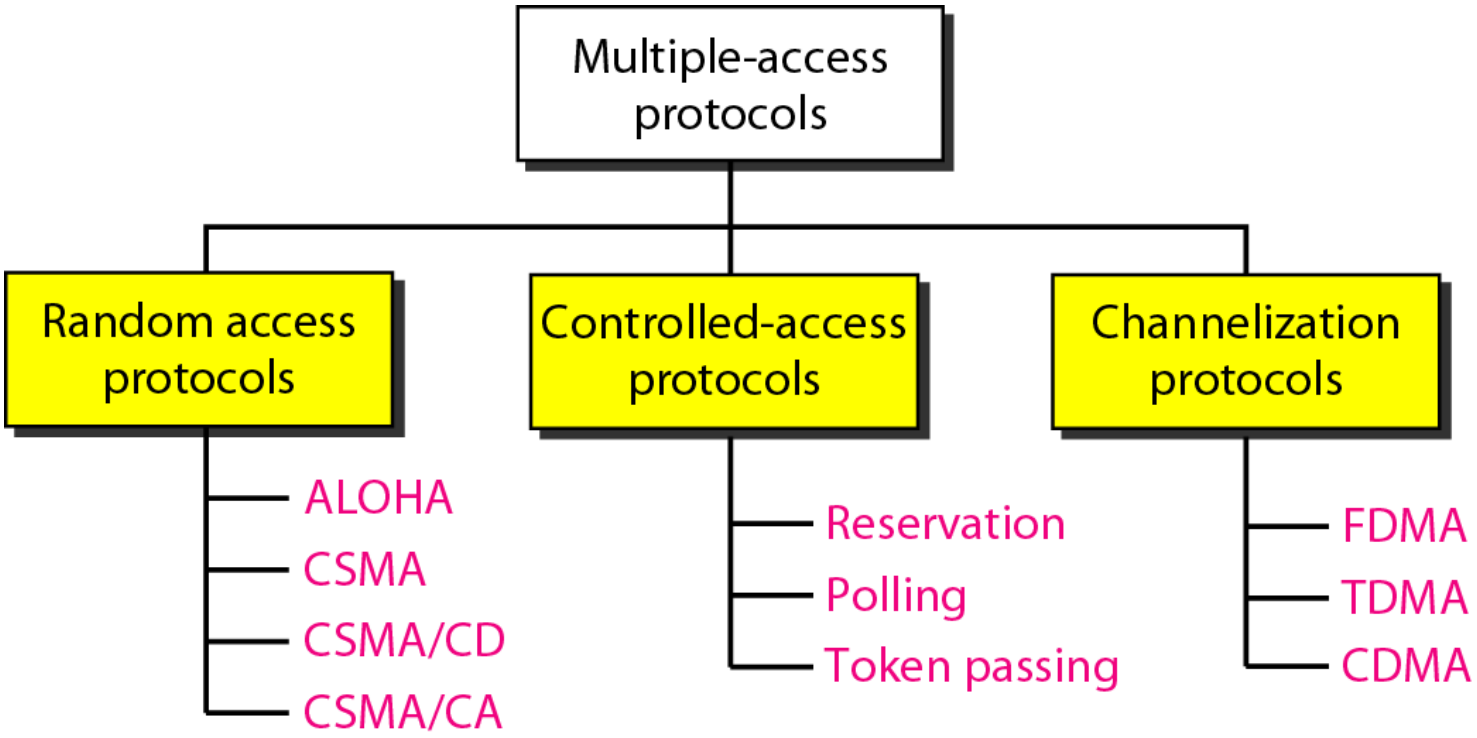
Structure of the Ethernet Frame

Preamble	SFD	Destination MAC Address	Source MAC Address	Length / Type	Encapsulated Data	FCS
7	1	6	6	2	46 to 1500	4

Media Access control

- The data link layer can further be divided in to two layers: the upper sub-layer that is responsible for flow and error control is called the logical link control (LLC) layer; the lower sub-layer that is mostly responsible for multiple access resolution is called the media access control (MAC) layer
- When nodes or stations are connected and use a common link, called a multipoint or broadcast link, we need a multiple-access protocol to coordinate access to the link. The problem of controlling the access to the medium is similar to the rules of speaking in an assembly. The procedures guarantee that the right to speak is upheld and ensure that two people do not speak at the same time, do not interrupt each other, do not monopolize the discussion, and so on.

Contd.



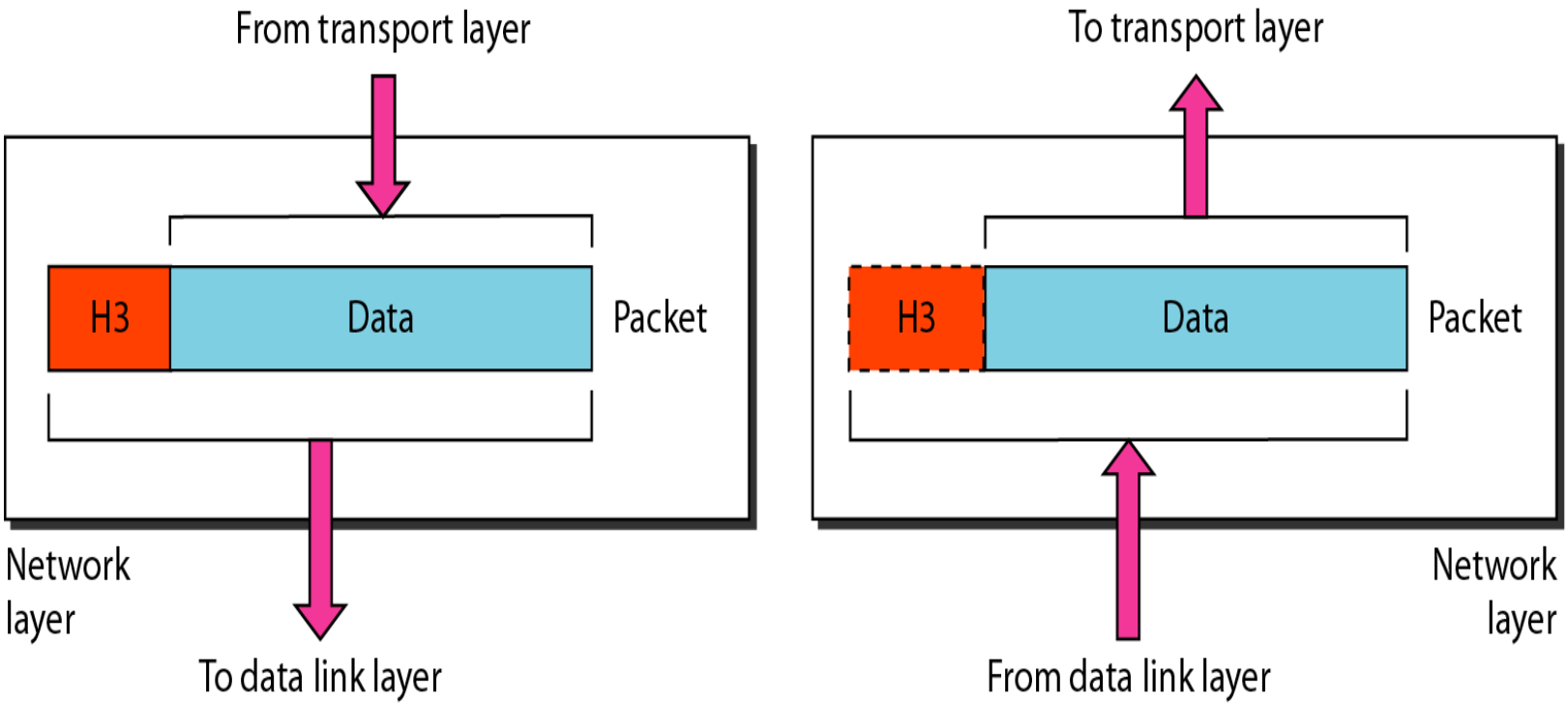
- Read about these?

Network Layer (3rd OSI Layer)

- Concerned with getting packets from source to destination.
- The network layer must know the topology of the subnet and choose appropriate paths through it.
- When source and destination are in *different networks*, the network layer must deal with these differences.
- The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks.
- Whereas the data link layer oversees the delivery of the packet between two systems on the same network, the network layer ensures that each packet gets from its point of origin to its final destination.
- If two systems are connected to the same local network, there is usually no need for a network layer. However, if the two systems are attached to different networks with connecting devices between the networks, there is often a need for the network layer to accomplish source-to-destination delivery.

Contd.

- The network layer is responsible for the delivery of individual packets from the source host to the destination host.

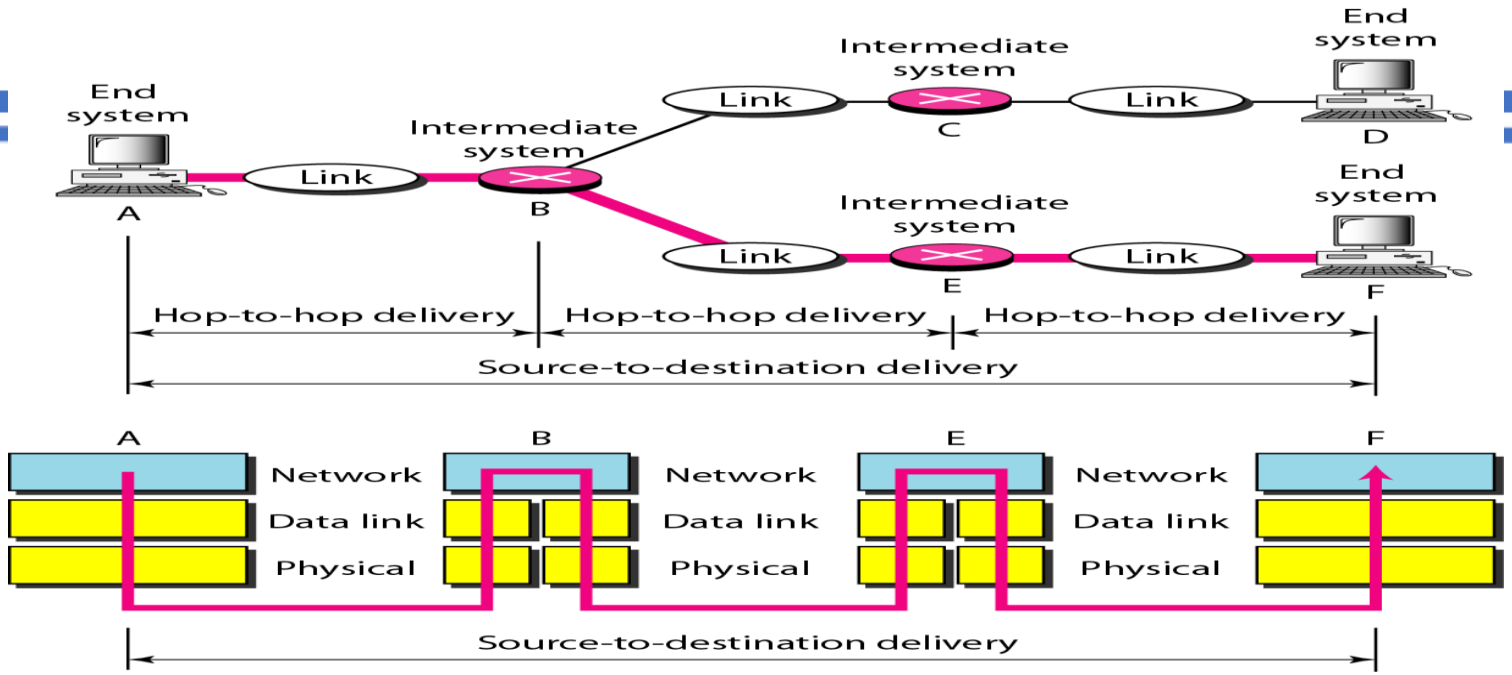


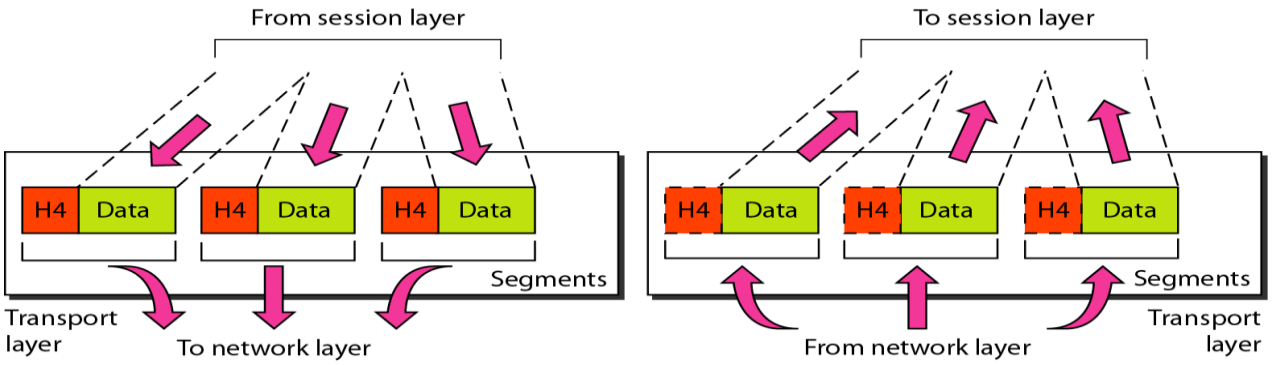
Contd.

Other responsibilities of the network layer include the following:

1. **Logical addressing:-** The physical addressing implemented by the data link layer handles the addressing problem locally.
   - If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems.
   - The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver. We discuss logical addresses later in chapter Six.
2. **Routing:-** When independent networks or links are connected to create *internetworks* (network of networks) or a large network, the connecting devices (called *routers or switches) route or switch the packets to their final destination*.
   - One of the functions of the network layer is to provide this mechanism.

Contd.


End system
A
Link
Intermediate system
B
Link
Intermediate system
C
Link
End system
D
Link
Intermediate system
E
Link
End system
F
Hop-to-hop delivery
Hop-to-hop delivery
Hop-to-hop delivery
Source-to-destination delivery
A
B
E
F
Network
Data link
Physical
Network
Data link
Physical
Network
Data link
Physical
Source-to-destination delivery


From session layer
H4
Data
H4
Data
H4
Data
Segments
Transport layer
To network layer
To session layer
H4
Data
H4
Data
H4
Data
Segments
From network layer
Transport layer

Transport layer (4th OSI layer)

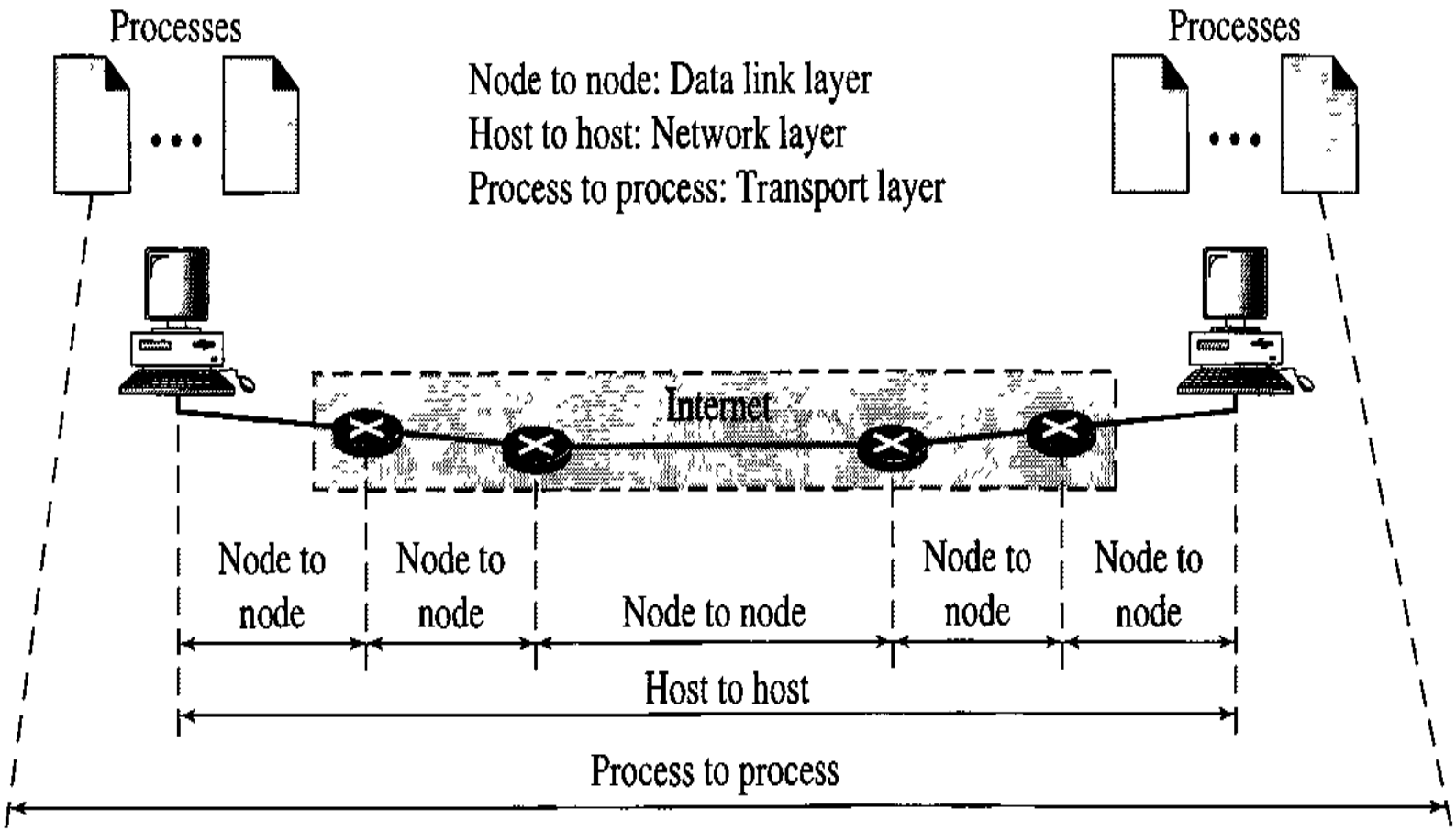
- The transport layer is responsible for process-to-process delivery of the entire message.
- A process is an application program running on a host.
- Whereas the network layer oversees source-to-destination delivery of individual packets, it does not recognize any relationship between those packets.
- The network layer treats each packet independently, as though each piece belonged to a separate message, whether or not it does.
- The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level.

Major functions of the transport layer

- The Transport layer encompasses these functions:

1. **Enables multiple applications to communicate over the network at the same time on a single device**
2. **Ensures that, if required, all the data is received reliably and in order by the correct application**
3. **Employs error handling mechanisms**

Contd.


Processes
Processes
Node to node: Data link layer
Host to host: Network layer
Process to process: Transport layer
Internet
Node to node
Node to node
Node to node
Node to node
Node to node
Host to host
Process to process

Responsibilities of the transport layer include the following:

1. **Service-point addressing:-** Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process on the other. The transport layer header must therefore include a type of address called a **service-point address** *(or* **port address***).*

   - *The network layer gets each packet to the correct computer*; the transport layer gets the entire message to the correct process on that computer.

2. **Segmentation and reassembly:-** A message is divided into transmittable segments, with each segment containing a sequence number.

   - These numbers enable the transport layer to **reassemble** the message correctly upon arriving at the destination and to identify and replace packets that were **lost** in transmission.

Contd.

3. Flow control:- Like the data link layer, the transport layer is responsible for flow control.
   - However, flow control at this layer is performed end to end rather than across a single link.
4. Error control:- Like the data link layer, the transport layer is responsible for error control.
   - However, error control at this layer is performed process-to-process rather than across a single link.
   - The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication).
   - Error correction is usually achieved through retransmission.

Contd.

5. Connection control:- The transport layer can be either connectionless or connection-oriented.

A. **Connectionless** transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine.

B. **Connection-oriented** transport layer makes a connection with the transport layer at the destination machine first before delivering the packets.

- After all the data are transferred, the connection is terminated.

Process-to-Process Delivery

- As a revision, the data link layer is responsible for delivery of frames between two neighboring nodes over a link. This is called *node-to-node delivery*.
- *The network layer is responsible for* delivery of datagrams between two hosts. This is called *host-to-host delivery*.
- *Communication* on the Internet is not defined as the exchange of data between two nodes or between two hosts. Real communication takes place between two processes (application programs). We need process-to-process delivery.
- However, at any moment, **several processes may be running on the source host and several on the destination host. To complete the delivery, we need a mechanism to deliver data from one of these processes running on the source host to the corresponding process running on the destination host**.
- The transport layer is responsible for *process-to-process* delivery-the delivery of a packet, part of a message, from one process to another.
  - Two processes communicate in a client/server relationship.

Transport layer addressing

- Whenever we need to deliver something to one specific destination among many, we need an address.
- At the data link layer, we need a MAC address to choose one node among several nodes if the connection is not point-to-point.
  - A frame in the data link layer needs a destination MAC address for delivery and a source address for the next node's reply.
- At the network layer, we need an IP address to choose one host among millions.
  - A datagram in the network layer needs a destination IP address for delivery and a source IP address for the destination's reply.

Contd.

- At the transport layer, we need a transport layer address, called a port number, to choose among multiple processes running on the destination host.
  - The destination port number is needed for delivery; the source port number is needed for the reply.
  - In the Internet model, the port numbers are 16-bit integers between 0 and 65,535.
  - The client program defines itself with a port number, chosen randomly by the transport layer software running on the client host. This is the ephemeral (temporal) port number. (next slide, more on port number)

Connectionless Versus Connection-Oriented Service

- A transport layer protocol can either be connectionless or connection-oriented.

1. *Connectionless Service*
   - In a connectionless service, the packets are sent from one party to another with no need for connection establishment or connection release.
   - The packets are not numbered; they may be delayed or lost or may arrive out of sequence. There is no acknowledgment either.
   - UDP is connectionless.
2. Connection-Oriented *Service*

   a. In a connection-oriented service, a connection is first established between the sender and the receiver.

   b. Data are transferred. At the end, the connection is released.

   c. TCP and SCTP are connection-oriented protocols.

Reliable Versus Unreliable

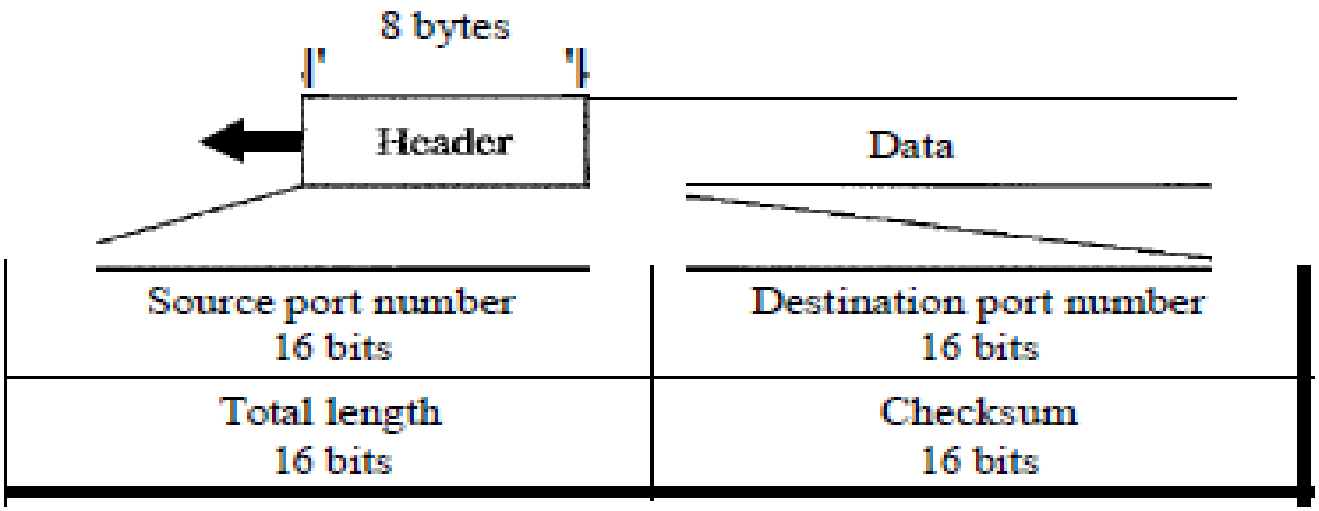
- The transport layer service can be reliable or unreliable.
- If the application layer program needs **reliability**, we use a reliable transport layer protocol by implementing flow and error control at the transport layer.
  - This means a slower and more complex service.
- On the other hand, if the application program does not need **reliability** because it uses its own flow and error control mechanism or it needs fast service or the nature of the service does not demand flow and error control (real-time applications), then an unreliable protocol can be used.
- In the Internet, there are two common different transport layer protocols, as we have already mentioned. UDP is connectionless and unreliable; TCP and SCTP are connection-oriented and reliable protocols. These three can respond to the demands of the application layer programs.

USER DATAGRAM PROTOCOL (UDP)

- The User Datagram Protocol (UDP) is called a **connectionless**, unreliable transport protocol.
  - It does not add anything to the services of IP except to provide process-to-process communication.
- Also, it performs very limited error checking. If UDP is so powerless, why would a process want to use it?
- With the disadvantages come some advantages. UDP is a very simple protocol using a minimum of overhead.
  - If a process wants to send a small message and does not care much about reliability, it can use UDP.
  - Sending a small message by using UDP takes much less interaction between the sender and receiver than using TCP or SCTP.

Contd.

- UDP packets, called user datagrams, have a fixed-size header of 8 bytes
- Source port number. This is the port number used by the process running on the source host.
- Destination port number. This is the port number used by the process running on the destination host.
- Length. This is a 16-bit field that defines the total length of the user datagram, header plus data.



Contd.

- UDP does not perform:
  - Flow control
  - Error control
  - Connection control
    - All these functions are done by the processes (application layer programs) using UDP
  - UDP is **not capable of segmenting and reassembling frames** and **does not implement sequence numbers**
- But UDP, like TCP, performs:
  - Service point addressing
- UDP can transmit only **small portions of data** at a time because it is not capable of segmenting and reassembling frames and does not implement sequence numbers

Use of UDP

1. UDP is suitable for a process that requires simple request-response communication with little concern for flow and error control. It is not usually used for a process such as FTP that needs to send bulk data
2. UDP is suitable for a process with internal flow and error control mechanisms. For example, the Trivial File Transfer Protocol (TFTP) process includes flow and error control. It can easily use UDP.
3. UDP is a suitable transport protocol for multicasting. Multicasting capability is embedded in the UDP software but not in the TCP software.
4. UDP is used for management processes such as SNMP.
5. UDP is used for some route updating protocols such as Routing Information Protocol (RIP).

Transmission Control Protocol (TCP)

- TCP, like UDP, is a process-to-process (program-to-program) protocol.
- TCP, therefore, like UDP, uses port numbers. Unlike UDP, TCP is a connection-oriented protocol; it creates a virtual connection between two TCPs to send data.
- In addition, TCP uses flow and error control mechanisms at the transport level.
- In brief, TCP is called a *connection-oriented, reliable transport protocol. It adds* connection-oriented and reliability features to the services of IP.

TCP Services

1. ***Process-to-Process Communication:-*** Like UDP, TCP provides process-to-process communication using port numbers.
2. ***Stream Delivery Service***
3. ***Full-Duplex Communication***
4. ***Connection-Oriented Service***
5. ***Reliable Service***

Stream Delivery Service

- TCP, unlike UDP, is a stream-oriented protocol.
- In UDP, a process (an application program) sends messages, with predefined boundaries, to UDP for delivery.
- UDP adds its own header to each of these messages and delivers them to IP for transmission.
- Each message from the process is called a user datagram and becomes, eventually, one IP datagram.
- Neither IP nor UDP recognizes any relationship between the datagrams.
- Each application using UDP must send small data to fit into one user datagram as it is. (UDP does not segment/reassemble)

Contd.

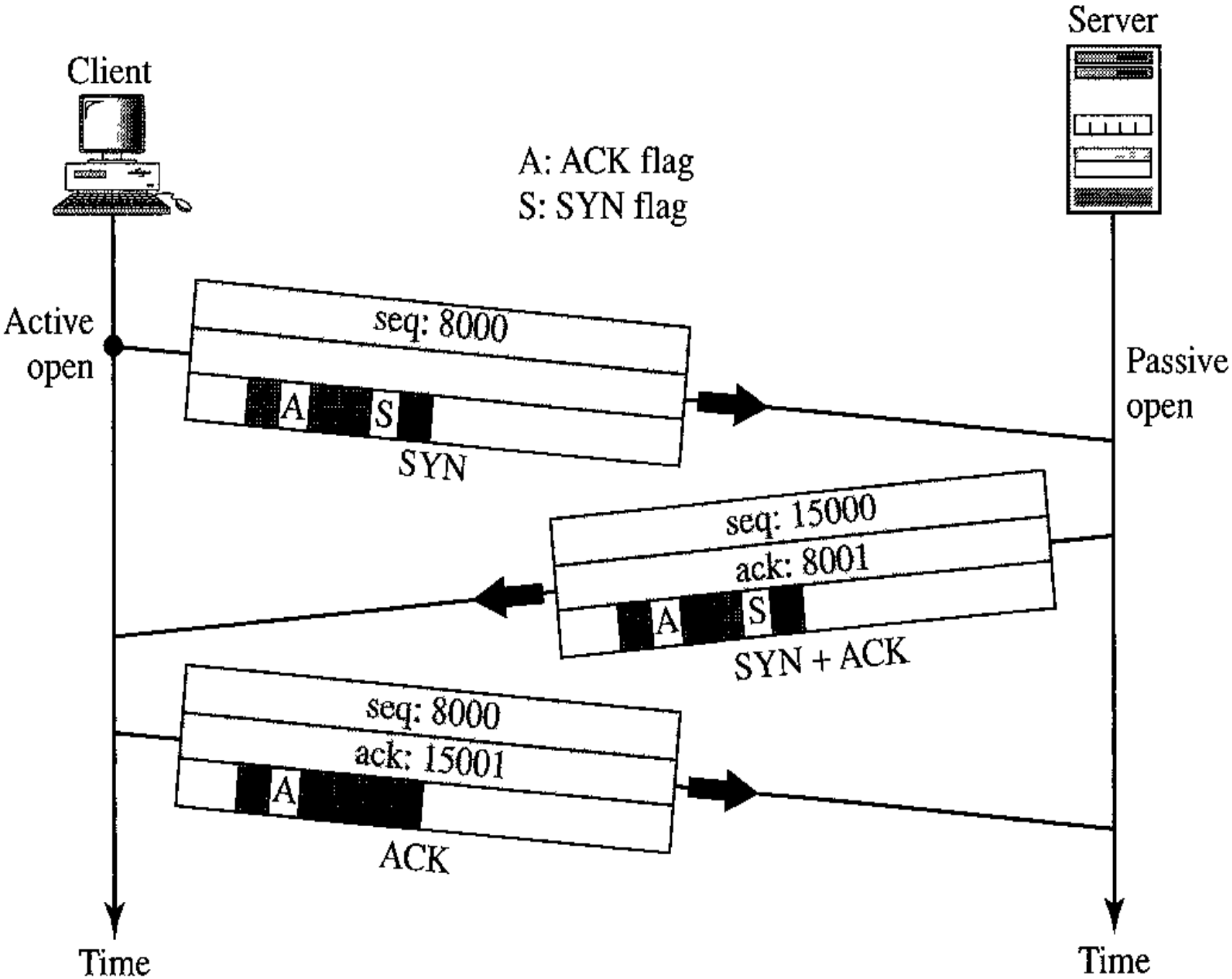
- TCP, on the other hand, allows the sending process to deliver data as a stream of bytes and allows the receiving process to obtain data as a stream of bytes.
- TCP creates an environment in which the two processes seem to be connected by an imaginary "tube" that carries their data across the Internet.
- The sending process produces (writes to) the stream of bytes, and the receiving process consumes (reads from) them (Fig. next slide)

Connection-Oriented Service

- TCP, unlike UDP, is a connection-oriented protocol.
- When a process at site A wants to send and receive data from another process at site B, the following occurs:

  1. **The two TCPs establish a connection between them.**
  2. **Data are exchanged in both directions.**
  3. **The connection is terminated.**

- Note that this is a virtual connection, not a physical connection. The TCP segment is encapsulated in an IP datagram and can be sent out of order, or lost, or corrupted, and then resent.
- Each may use a different path to reach the destination. There is no physical connection.
- TCP creates a stream-oriented environment in which it accepts the responsibility of delivering the bytes in order to the other site.


Client
Server
A: ACK flag
S: SYN flag
Active open
Passive open
seq: 8000
A
S
SYN
seq: 15000
ack: 8001
A
S
SYN + ACK
seq: 8000
ack: 15001
A
ACK
Time
Time

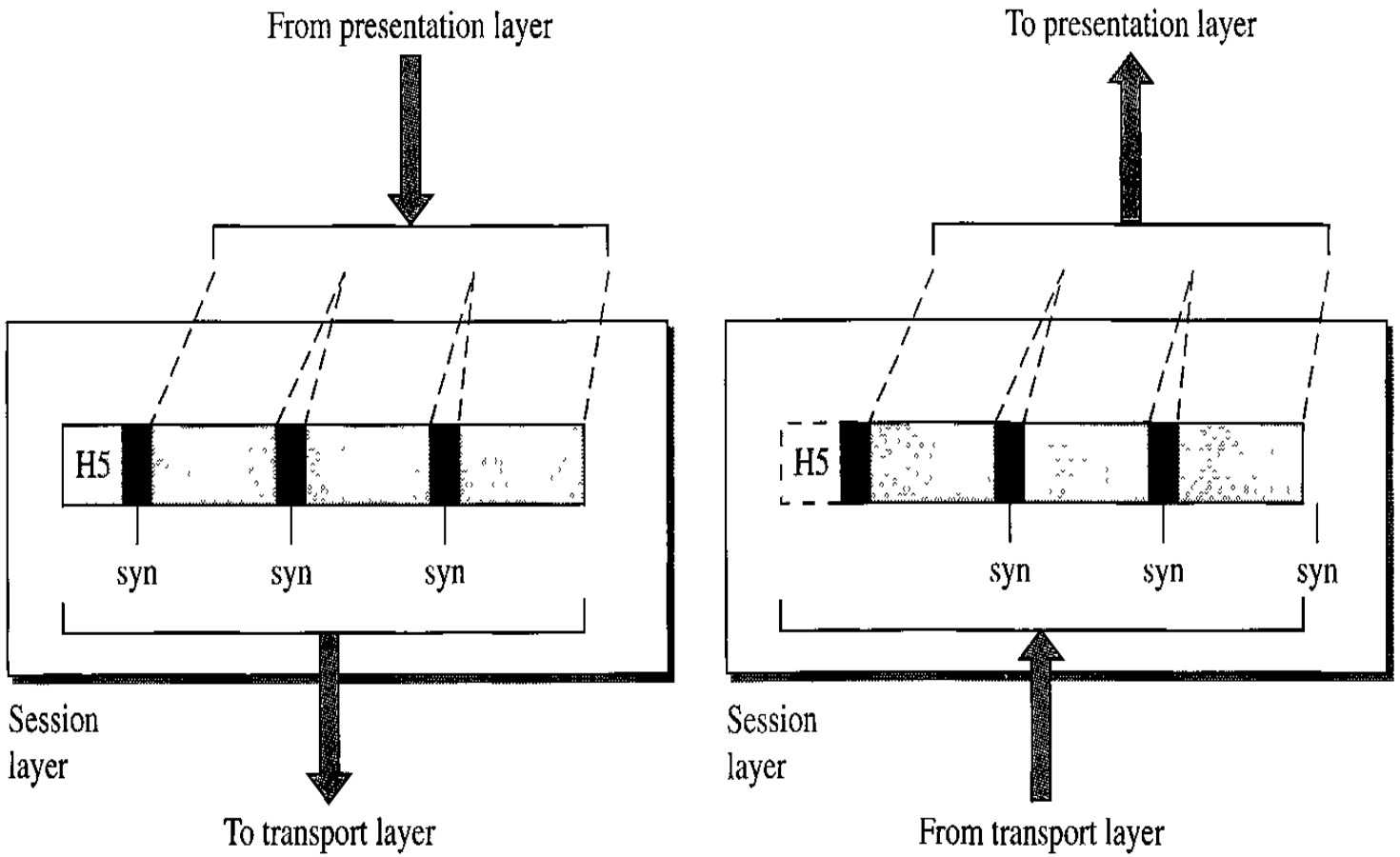
Session Layer

- The lowest four layers of the OSI model (Physical, Data link, Network, and Transport) provide the means for the reliable exchange of data and provide a fast data service.
- For example, a remote terminal access application might require a half-duplex dialogue.
- A transaction-processing application might require checkpoints in the data-transfer stream to permit backup and recovery.
- A message processing application might require the ability to interrupt a dialogue in order to prepare a new portion of a message and later to resume the dialogue where it was left off.

Contd.

- All these capabilities could be embedded in specific applications at layer 7.
- However, because these types of dialogue-structuring tools have widespread applicability, it makes sense to organize them into a separate layer: the session layer.
- The session layer provides the mechanism for controlling the dialogue between applications in end systems.
- In many cases, there will be little or no need for session-layer services, but for some applications, such services are used.

Contd.


From presentation layer
H5
syn
syn
syn
Session
layer
To transport layer
To presentation layer
H5
syn
syn
syn
Session
layer
From transport layer

The key services provided by the session layer include

- The primary job of session layer protocols is to provide the means necessary to **set up, manage, and end sessions**

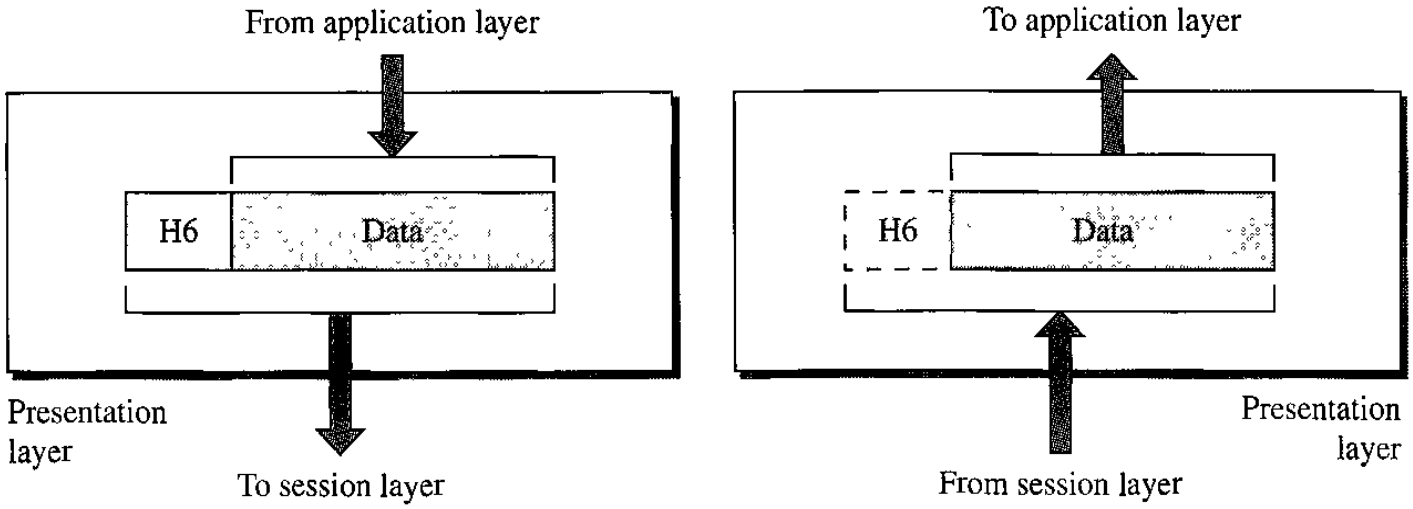
1. **Dialogue discipline.** This can be two-way simultaneous (full duplex) or two way alternate (half duplex) communication between processes.
2. **Grouping.** The flow of data can be marked to define groups of data.
   - For example, if a retail store is transmitting sales data to a regional office, the data can be marked to indicate the end of the sales data for each department; this would signal the host computer to finalize running totals for that department and start new running counts for the next department.

Contd.

3. **Recovery.** The session layer can provide a check pointing mechanism, so that if a failure of some sort occurs between checkpoints, the session entity can retransmit all data since the last checkpoint, as in the example shown below:
   - 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.

Presentation Layer

- The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.



Specific responsibilities of the presentation layer :

1. 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.
   - The presentation layer at the sender changes the information from its **sender-dependent format into a common format**.
   - The presentation layer at the receiving machine changes the common format into its receiver-dependent format.

Contd.

2. 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.
3. 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.

Application Layer

- The application layer enables the user, whether human or software, to access the network.
- It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.
- Application layer is where users actually communicate to the computer.
  - Take the case of Internet Explorer (IE).
- It is also responsible for identifying and establishing the availability of the intended communication partner

Contd.

- Typical application layer protocols
  - Domain Name System (DNS)
  - Hyper Text Transfer Protocol (HTTP)
  - File Transfer Protocol (FTP)
  - E-mail (SMTP,POP,IMAP)

1. Domain Name System (DNS)

- Thousands of servers, installed in many different locations, provide the services we use over the Internet.
- Each of these servers is assigned a unique IP address
- It would be impossible to remember all of the IP addresses

Contd.

- DNS provides a way for hosts to use this name to request the IP address of a specific server.
- DNS names are registered and organized on the Internet within specific high level groups, or domains.
  - Some of the most common high level domains on the Internet are .com, .edu, and .net
- A DNS server contains a table that associates hostnames in a domain with corresponding IP addresses

2. Web client and web server

- A web client first receives the IP address of a web server from DNS server
- Then the client browser uses that IP address and port 80 to request web services
- This request is sent to the server using the Hypertext Transfer Protocol (HTTP)
- The information content of a web page is encoded using specialized 'mark-up' languages.
  - E.g. HTML (Hypertext Mark-up Language)
- Many different web servers and web clients from many different manufactures work together seamlessly because of HTTP and HTML

3. File Transfer Protocol (FTP)

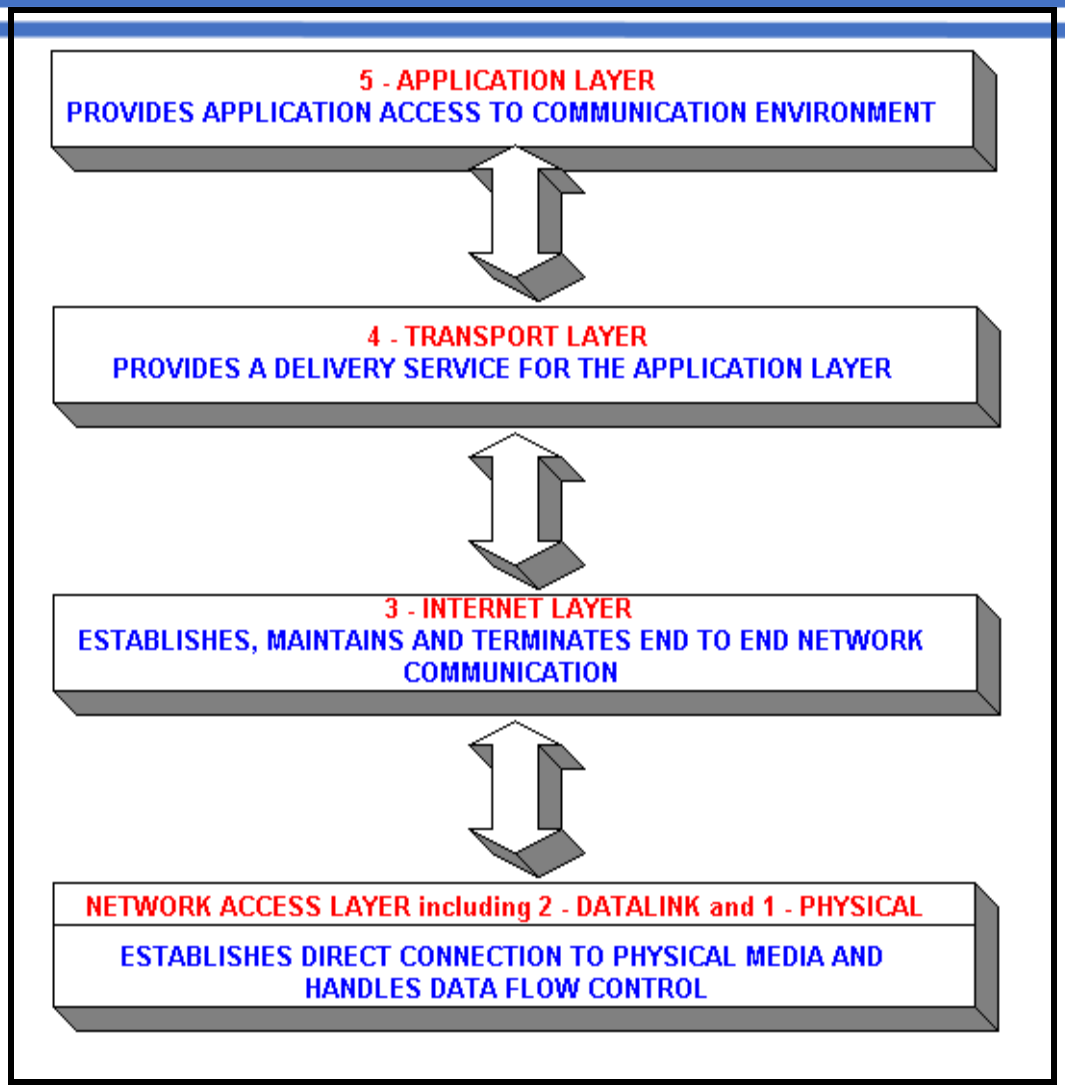
- FTP is another common service used across the Internet that allows users to transfer files
- A host running FTP client software can access an FTP server to perform various file management functions including file uploads and downloads
- FTP service uses two different ports to communicate between client and server
  - Requests to begin an FTP session are sent to the server using destination port 21.
  - Once the session is opened, the server will change to port 20 to transfer the data files
- FTP client software is built into computer operating systems and into most web browsers

4. Email Servers (SMTP, POP3 and IMAP4)

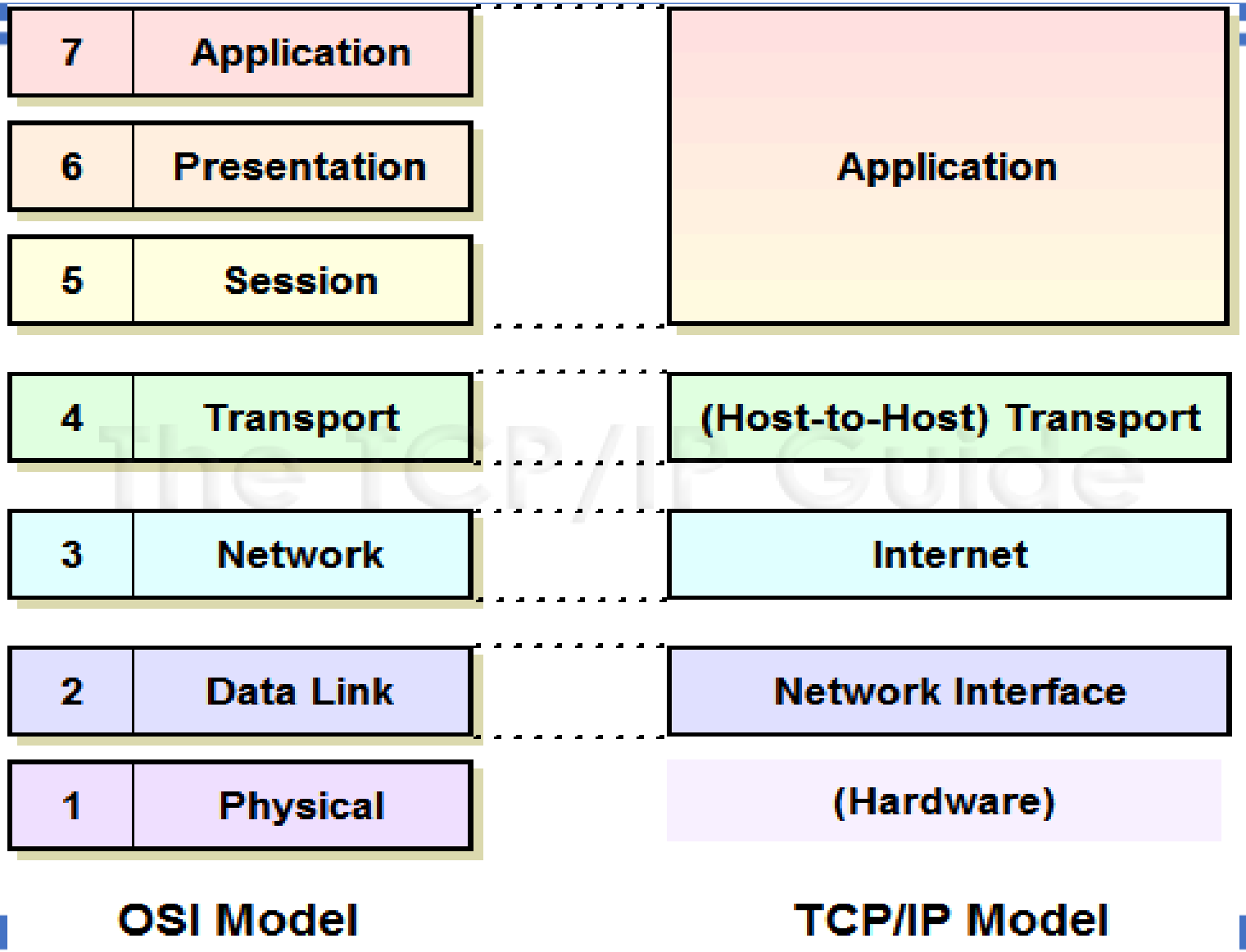
- Each mail server receives and stores mail for users who have mailboxes configured on the mail server
- Each user with a mailbox must then use an email client to access the mail server and read these messages
  - Mailboxes are identified by the format: **user@company.domain**
- Three application protocols used in processing email include
  1. **Simple Mail Transfer Protocol (SMTP):-** to send mail from client to server or server to server
  2. **Post Office Protocol (POP3):-** to download email from server to client, and the server deletes the mail
  3. **Internet Message Access Protocol (IMAP4):-** to download email from server to client, and the server does not delete (keeps) the mail

TCP/IP Network Model Layers

- As with the OSI model, the TCP/IP suite uses a layered model.
- TCP/IP model has four or five - depending on who you talk to and which books you read!
- Some people call it a four layer suite - **Application**, **Transport**, **Internet** and **Network Access**, others split the **Network Access** layer into its **Physical** and **Datalink** components.

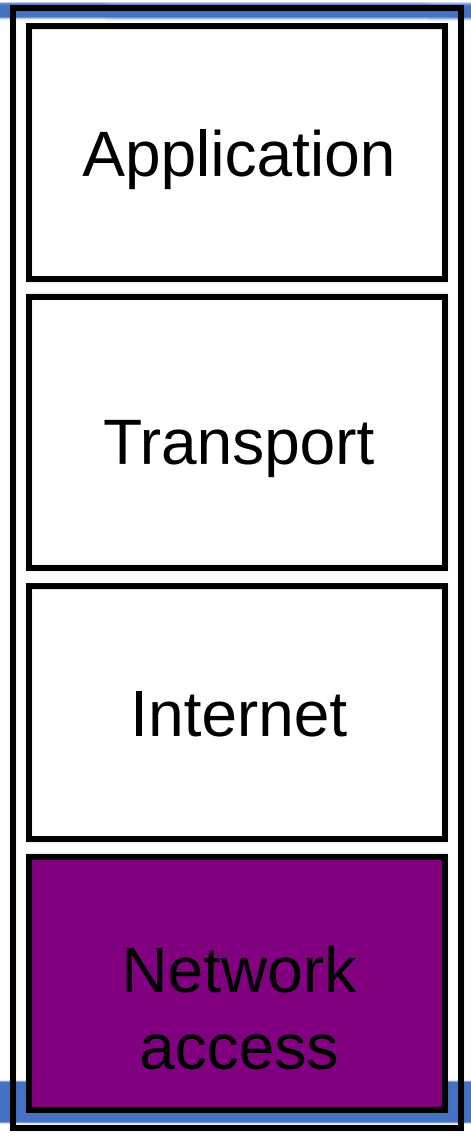


OSI Model Vs. TCP/IP Model Layers



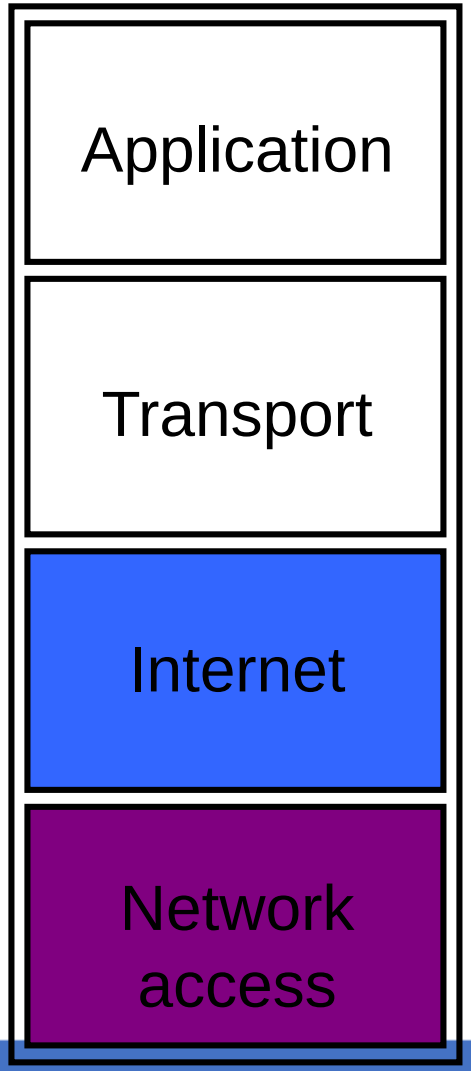
The TCP/IP Guide

TCP/IP Layers- What does each layer do?



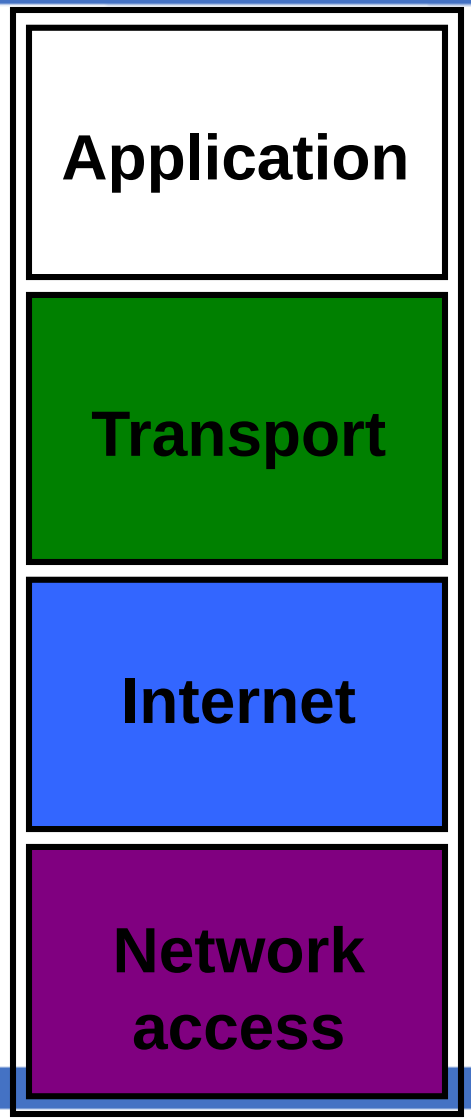
- Network access layer is the combination of data link and physical layers and it deals with pure hardware issues (wires, satellite links, network interface cards, etc.)
- Access methods such as **CSMA/CD** (carrier sensed multiple access with collision detection)
- Ethernet exists at the network access layer - its hardware operates at the physical layer and its medium access control method (CSMA/CD) operates at the data link layer.

TCP/IP Layers- What does each layer do?



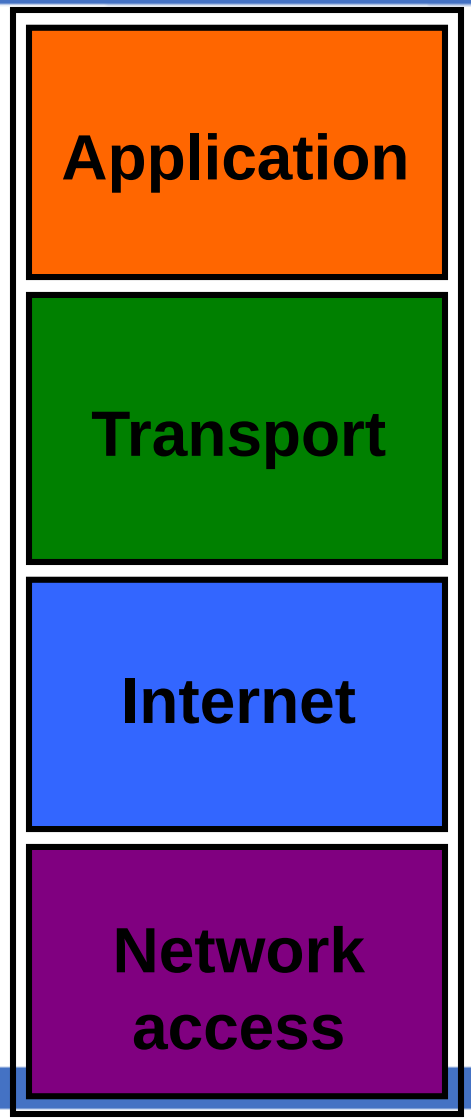
- The Internet layer is responsible for the routing and delivery of data across networks.
- It allows communication across networks of the same and different types and carries out translations to deal with dissimilar data addressing schemes.
- IP (Internet Protocol) and ARP (Address Resolution Protocol) are both to be found at the Internet layer.

TCP/IP Layers- What does each layer do?



- The Transport layer is similar to the OSI transport model, but with elements of the OSI session layer functionality.
- The two protocols found at the transport layer are:
  A. TCP (Transmission Control Protocol): reliable, connection-oriented protocol that provides error checking and flow control through a virtual link that it establishes and finally terminates. Examples include FTP and Email
  B. UDP (User Datagram Protocol): unreliable, connectionless protocol that not error check or offer any flow control. Examples include SNMP

TCP/IP Layers- What does each layer do?



- The Application layer is broadly equivalent to the application, presentation and session layers of the OSI model.
- It gives an application access to the communication environment.
- Some examples: FTP, HTTP, SMTP

?

Debre Markos University
Institute of Technology
Information Technology Academy Program

Course Title: Data Communication and Computer Networks

Chapter one

Introduction to Data Communication and Computer Networks

Haleluya Kiflu (Ass. Prof.)

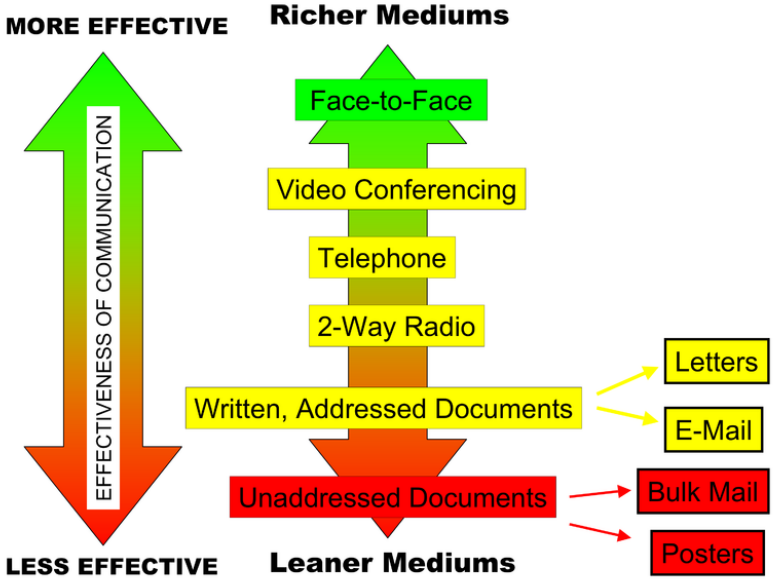
Presentation outline

- Introduction to Data Communication
- Data Communication Component
- Modes Of Data Transmission
- Signal Encoding techniques
- Error Detection and Correction

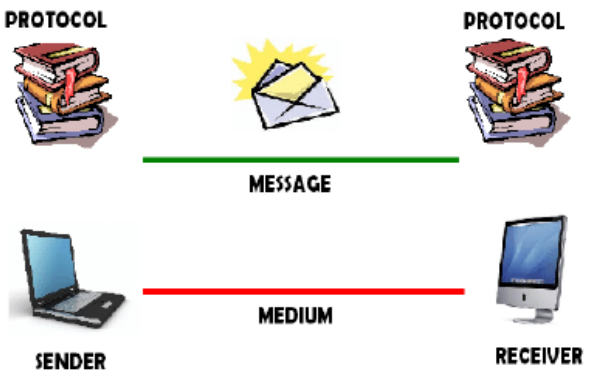
Introduction to Data Communication and Computer Networks …

- The word ***data*** refers to information presented in whatever form is agreed upon by the parties creating and using the data.
- ***Data communications (Transmission)*** are the **exchange of data** between two or more devices **via some form of transmission medium** such as a wire cable or wireless media using appropriate signal.
- **Computer data communications:** Is the movement of computer information from one point to another by means of electrical or optical transmission systems (called networks).

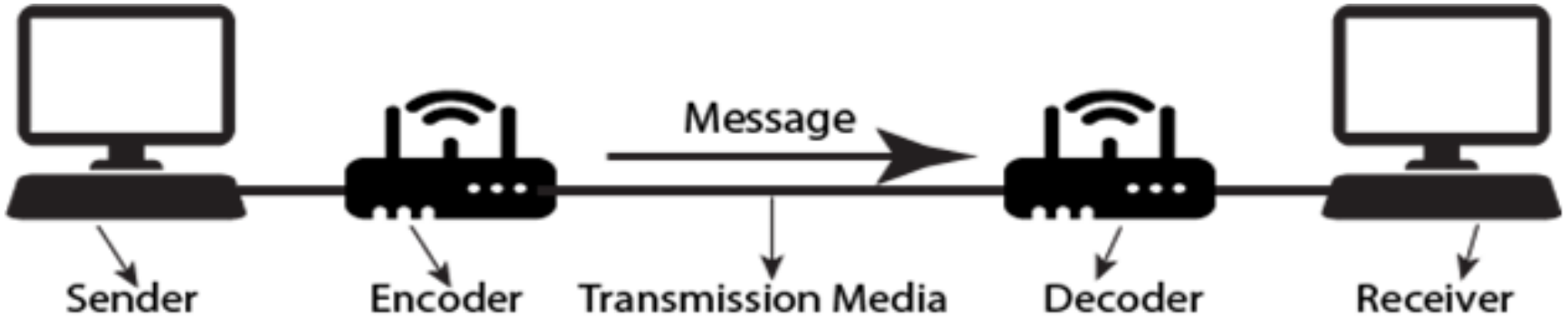
- Data communication system effectiveness depends:
  - Delivery
  - Accuracy
  - Timeliness
  - Jitter



Components of Data Communication



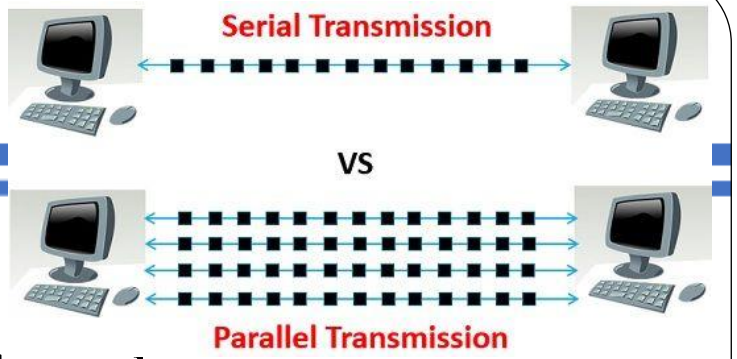
- Communication involves many devices that enable the communication (data transmission)
- A meaningful computer communication must have fulfil the following five components:
  - Message
  - Sender
  - Transmission medium
  - Receiver
  - protocol



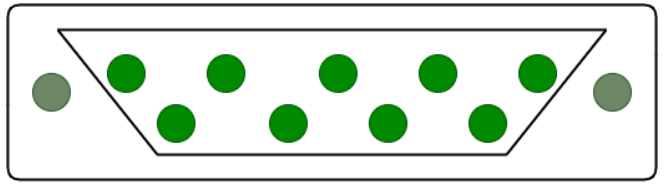
Components of Data Communication…

1. **Message:** the information (data) to be communicated such as: **text, numbers, pictures, audio, and video**.
2. **Transmitter/ source / Sender:** is the device that sends / encodes the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
3. **Receiver / Destination :** is the device that receives / decodes the message. It can be a computer, workstation, telephone handset, television, and so on.
4. **Transmission medium:** is the physical path by which a message travels from sender to receiver. Some examples of transmission media include cables and radio waves.
5. **Protocol:** is a set of rules that govern data communications. It represents an agreement between two devices. French cannot be understood by Japanese.

Serial vs. parallel communications

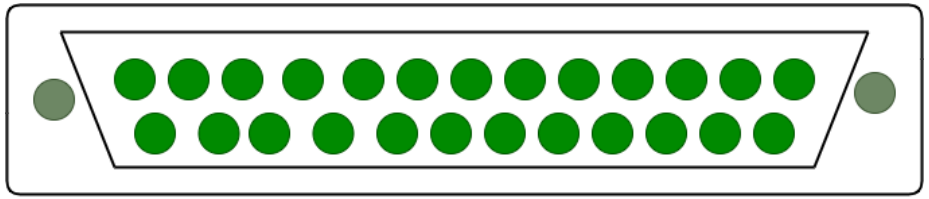


- In serial communications
  - A single bit will be transferred at a time using the communication channel
  - Bits will be reassembled at the destination
  - Mostly used by computer peripherals like **mouse & Modems**



DB-9

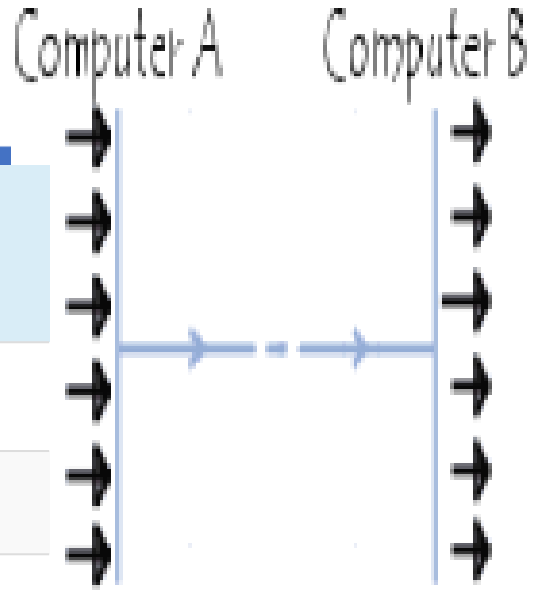
- In parallel communications
  - Multiple bits (eg. Eight bits) will be transferred at a time
  - Needs multiple (parallel) communication channels
  - Like **printers & Hard drives**



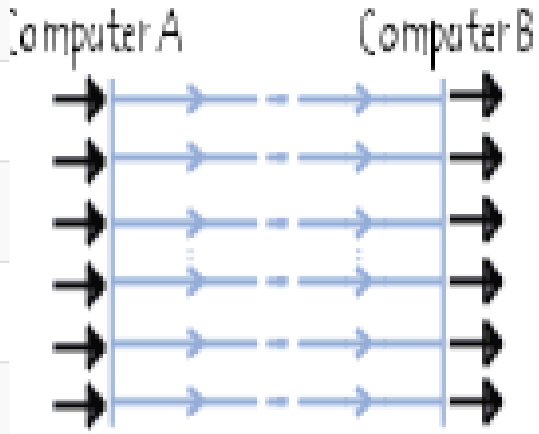
DB-25

Contd.

Basis for Comparison	Serial Communication	Parallel Communication
Data transmission speed	Slow	Comparatively fast
Number of communication link used	Single	Multiple
Number of transmitted bit/clock cycle	only one bit.	n number of link will carry n bits.
Cost	Low	High
Crosstalk	Not present	Present
System Up-gradation	Easy	Quite difficult
Mode of transmission	Full duplex	Half duplex
Suitable for	Long distance	Short distance
High frequency operation	More efficient	Less efficient



Serial connection



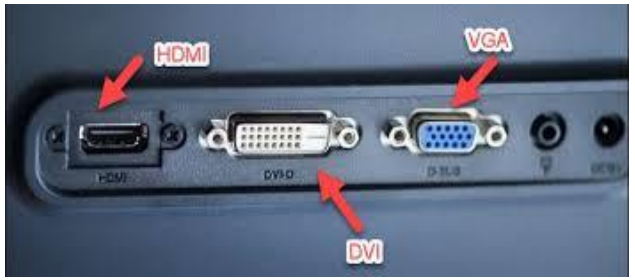
Parallel connection

Modes of data transmission

- Three different transmission modes characterized according to the direction:

1. **A simplex connection** is a connection in which the data flows in only **one direction**, from the transmitter to the receiver.

   - This type of connection is useful if the data do not need to flow in both directions (for example, TV, Radio, from your computer to the printer or from the mouse to your computer…).



Contd.

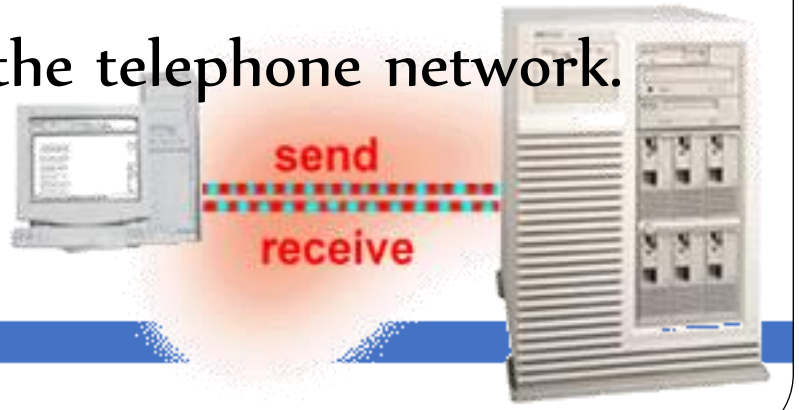
2. **A half-duplex connection** (sometimes called an *alternating connection or semi-duplex) the* data flows in one direction or the other alternatively (not same time)

- Each end of the connection transmits in turn.
- It possible to have bidirectional communications using the full capacity of the line.
- The entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time.
- Walkie-talkies and CB (citizens band) radios are both half-duplex systems.

Contd.

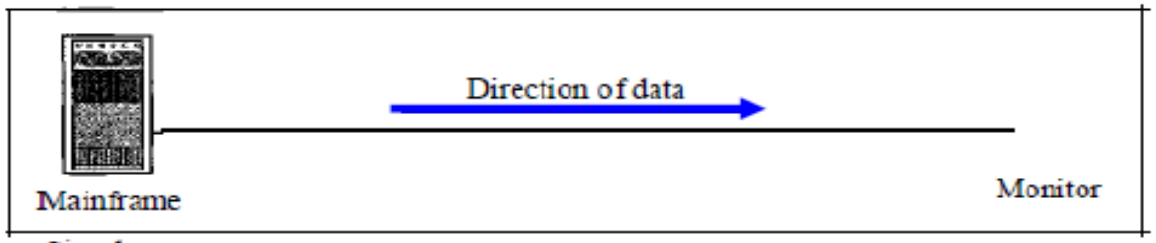
3. ***Full-Duplex:*** also called duplex, both stations can transmit and receive simultaneously

- It is like a two-way street with traffic flowing in both directions at the same time.
- Signals going in one direction share the capacity of the link: with signals going in the other direction.
- This sharing can occur in two ways: Either the link must contain two physically separate transmission paths; or the capacity of the channel is divided between signals travelling in both directions.
- One common example of full-duplex communication is the telephone network.

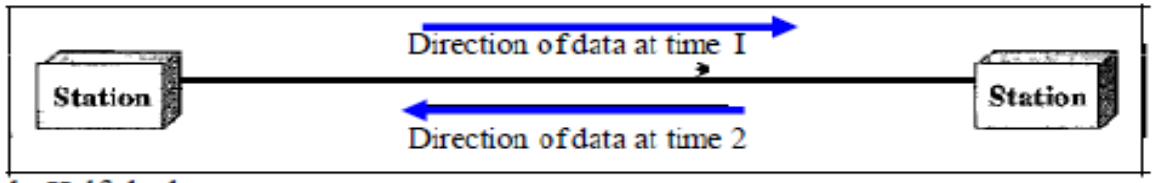


Contd.

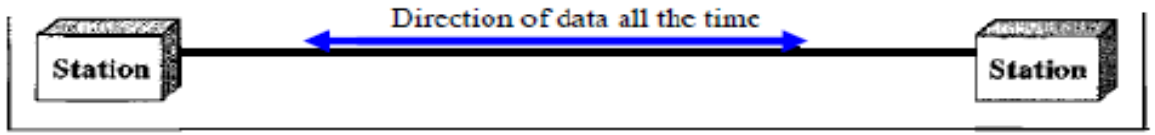
- **Simplex** –
  - data flows in only **one direction**
- **Half-duplex** –
  - data flows both direction, but d/t time
- **Full-duplex** –
  - both stations can transmit and receive simultaneously
- **Echo-plex** –
  - retransmitted to the sender for error-checking purposes.



a. Simplex



b. Half-duplex



c. Full-duplex

Signalling Encoding

- Data is transmitted in the form of signal over communication channel whether wired or wireless.
- Signal is detectable transmitted energy that carries information.
- Two types of data:
  - **Digital data:-** information that has discrete states – counts
  - **Analog Data:-** information that is continuous – measures
- Two types of signals:
  - Digital signal
  - Analog signal

Signal Encoding techniques

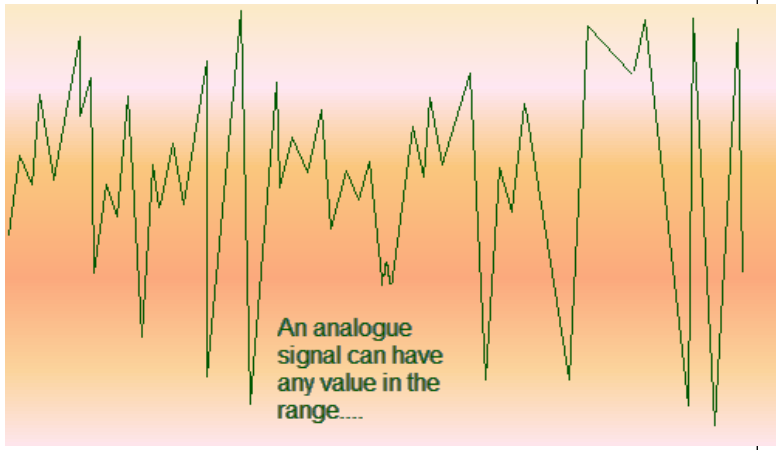
- **Digital Signal:-** can have only a limited number of defined values.
  - Although each value can be as 1 and 0.
- **Analog signal**:- has infinitely many levels of intensity over a period of time.
  - As the wave moves from value A to value B, it passes through and includes an infinite number of values along its path.

Analog Signals

- Are Continuous wave that carries information by altering the characteristics of waves.
- Analogue means that the original information is retransmitted to the receiver/listener **without any manipulation**.
- Here the signal can take on **any value** (within the limits set by the recording equipment and the transmitter).
- It measures rather than counts
  - For instance, Voice & all sounds are analog, traveling to human ears in the forms of waves.

Contd.

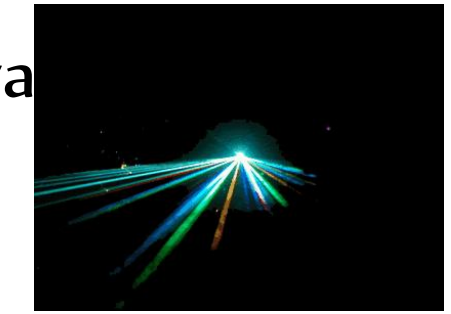
- Radio, telephone and recording equipment historically have been analog, but they are beginning to change – due to large to computers to the other types of signals- digitals
- **The disadvantage of analogue signals** is that any **'noise'**, interference, added to the signal at any point cannot be removed from the audio signal and this degrades the audio quality of the signal.



Digital Signals

- Are a discrete series of pulses - either **high or low - on or off** - sometimes expressed as binary code 1s and 0s.

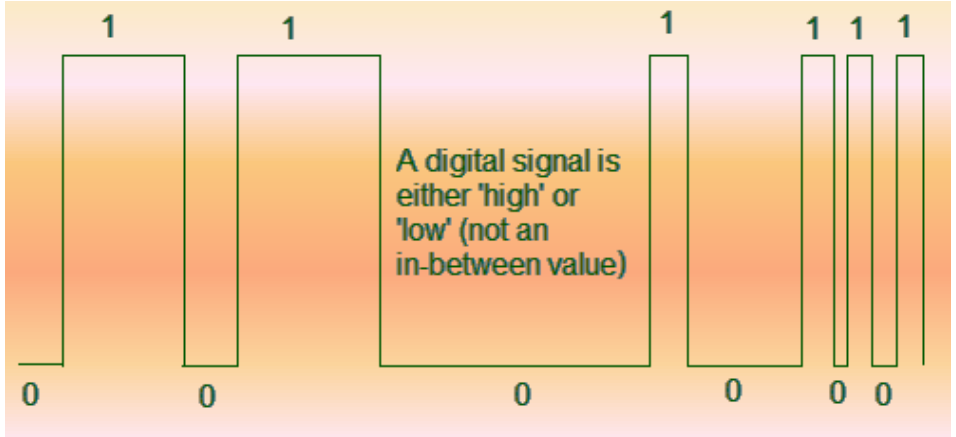
- It counts but not measures
- Discrete pluses of data transmission rather than continues wa

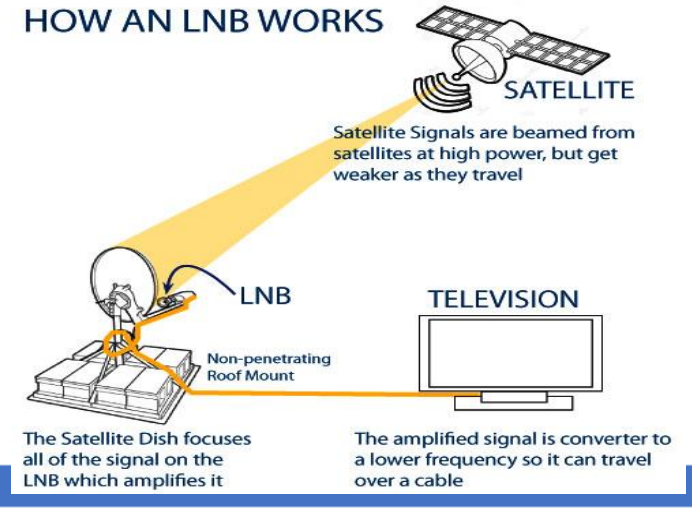


- More prevalent in computer based devices
- **Flashing light and telegraph message** are traditional examples of on-off pluses.

Contd.

- The signals from a satellite are digital.
- They use a system called 'packet switching' which is the same as used in computer networks and for the internet.
- This system is particularly effective for dealing with noise elimination.





Contd.

The advantage of digital signals is that

1. Digital is more **robust** than analog to noise and interference
2. Digital is more viable to using regenerative **repeaters**
3. Digital signals are easily **encrypted** for security purposes
4. Also it is possible to **send a lot more** information digitally
5. They can be **transmitted effectively along fiber optic** cables.
6. Can be coded to yield extremely **low error rates** with error correction.
7. **Cost** is coming down in digital systems faster than in analog systems

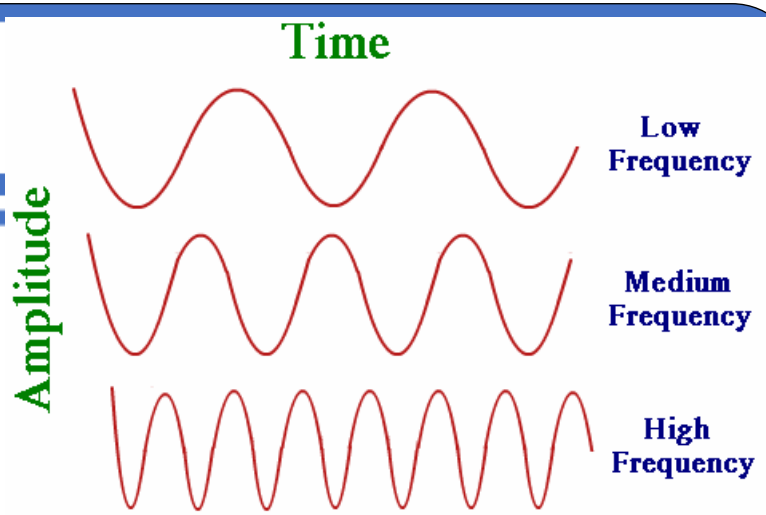
	Analog	Digital
Signal	is a continuous signal which represents physical measurements.	are discrete time signals generated by digital modulation.
Waves	Denoted by sine waves	Denoted by square waves
Representation	Uses continuous range of values to represent information	Uses discrete or discontinuous values to represent information
Example	Human voice in air, analog electronic devices.	Computers, CDs, DVDs, and other digital electronic devices.
Technology	Analog technology records waveforms as they are.	Samples analog waveforms into a limited set of numbers and records them.
Data transmissions	Subjected to deterioration by noise during transmission and write/read cycle.	Can be noise-immune without deterioration during transmission and write/read cycle.
Response to Noise	More likely to get affected reducing accuracy	Less affected since noise response are analog in nature
Flexibility	Analog hardware is not flexible.	Digital hardware is flexible in implementation.
Uses	Can be used in analog devices only. Best suited for audio and video transmission.	Best suited for Computing and digital electronics.
Applications	Thermometer	PCs, PDAs
Bandwidth	Analog signal processing can be done in real time and consumes less bandwidth.	There is no guarantee that digital signal processing can be done in real time and consumes more bandwidth to carry out the same information.
Memory	Stored in the form of wave signal	Stored in the form of binary bit
Power	Analog instrument draws large power	Digital instrument draws only negligible power
Cost	Low cost and portable	Cost is high and not easily portable
Errors	Analog instruments usually have a scale which is cramped at lower end and give considerable observational errors.	Digital instruments are free from observational errors like parallax and approximation errors.

Data communication Contd.

Which of the following signals are Analog and which are Digital?

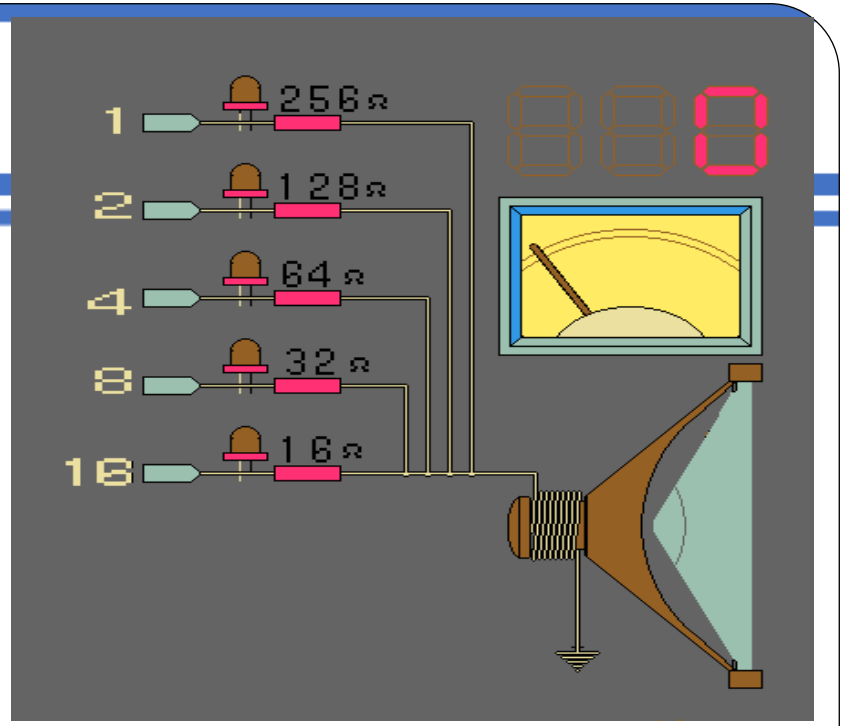
- Volume control on a radio
- Traffic lights
- Motor bike throttle
- Water tap
- Dimmer switch
- Light switch
- In Music on a CD
- Music on a tape

Data communication Contd.



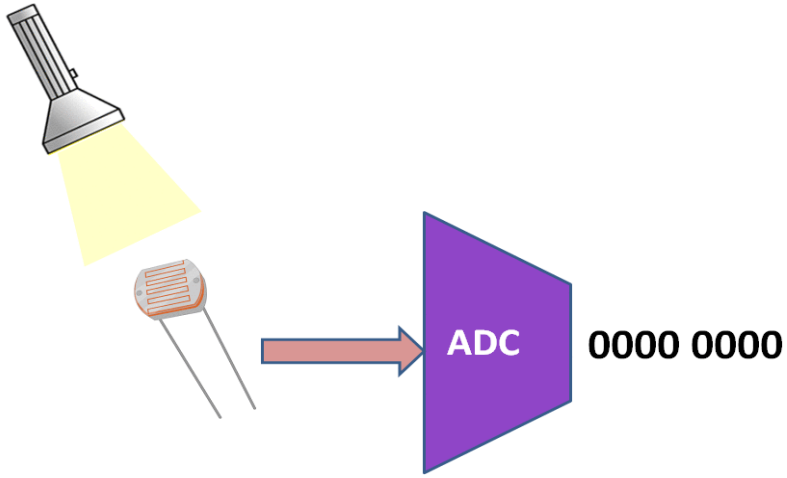
- ***Signal Encoding Techniques***
  - ***Basic Terminologies***
    - ***Data rate/bit rate*** - bits sent in one second.
      - bit interval (instead of period) and bit rate (instead of frequency)
    - ***Signal*** - is electrical, electronic data, sent over a communication medium
    - ***Signal rate*** - number of signal elements sent in 1s. The unit is the baud. Also called **pulse rate,** the **modulation rate,** or the **baud rate**
    - ***Amplitude*** - the strength of a signal, usually measured in volts
    - ***Period*** - amount of time, in seconds, a signal needs to complete 1 cycle
    - ***Frequency*** - number of periods in 1 s
    - ***Phase/phase shift*** - describes the position of the signal relative to time 0

DIGITAL DATA, ANALOG SIGNALS



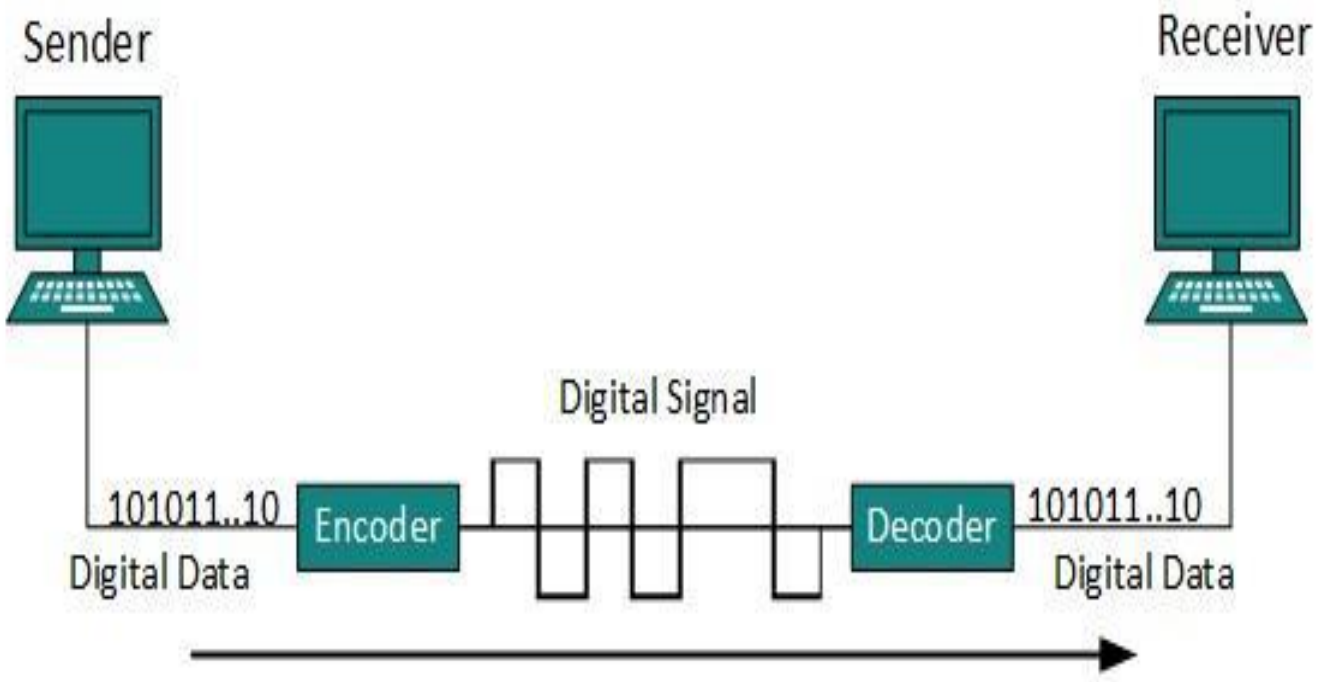
- Digital data:-
  - Digital Signal:-
  - Analog signal

- Analog Data:-
  - Digital Signal:-
  - Analog signal



Data communication Contd.

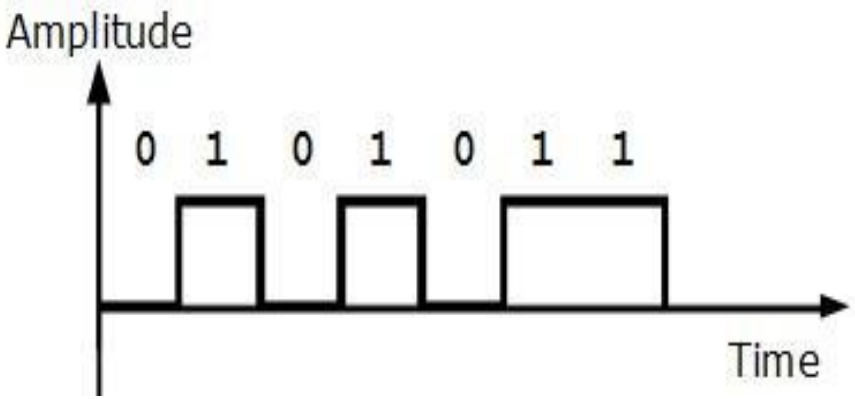
- ***Digital data to digital signal conversion***
  - Line coding
  - Block coding
  - Scrambling
- **Line Coding**
  - Unipolar -
  - polar -
  - bi-polar -



Data communication Contd.

- **Unipolar NRZ-**
  - Uses single voltage level to represent data
  - Signal levels are on one side of the time axis - either above or below
  - A High in data is represented by a positive pulse called as **Mark**
  - A Low in data input has no pulse.

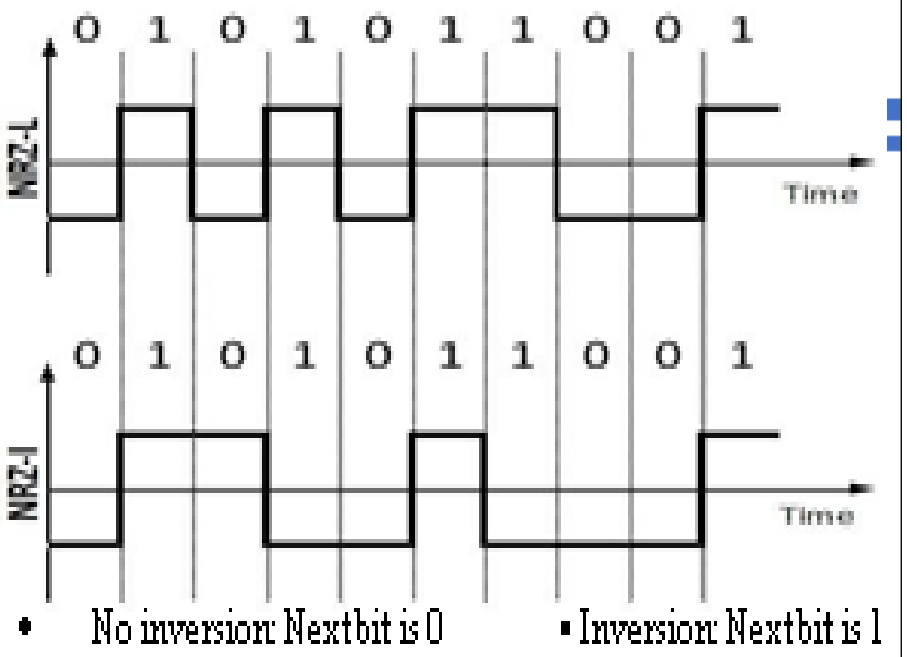
Ex. 0101011

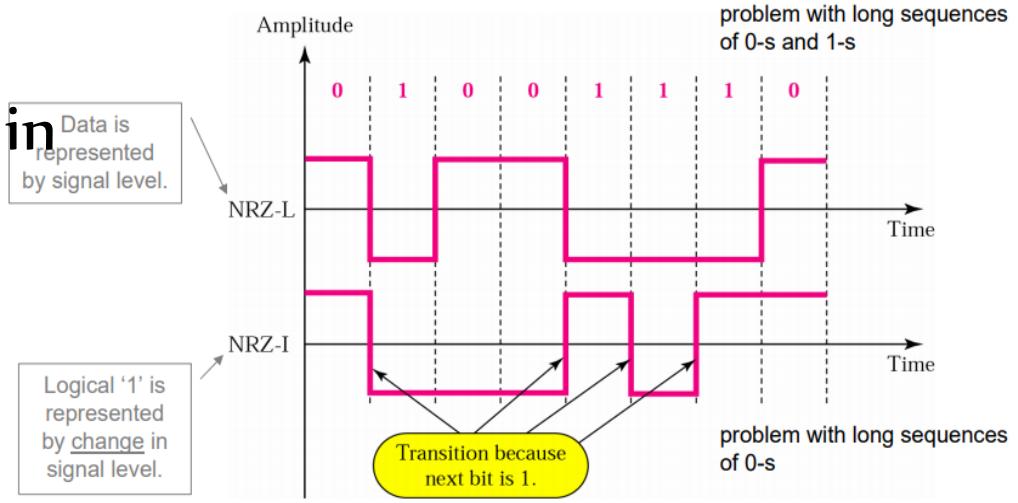


- What is Unipolar Return to Zero?

Data communication Contd.

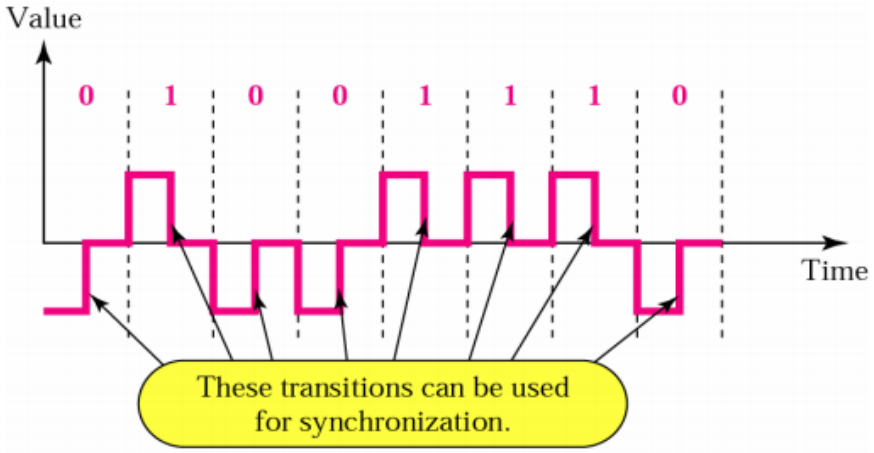
- **polar**
  - The voltages are on both sides of the time axis
  - Multiple voltage levels are used represent binary values
  - A High in data is represented by a positive pulse
  - A Low in data is represented by a negative pulse.
  - **N*RZ* (Non-Return to Zero)**
    - **NRZ-L (NRZ-Level)** - positive voltage for one symbol and negative for the other
    - **NRZ-I (NRZ-Invert)** - the change or lack of change in polarity determines the value of a symbol.
      - "1" inverts the polarity a "0" does not

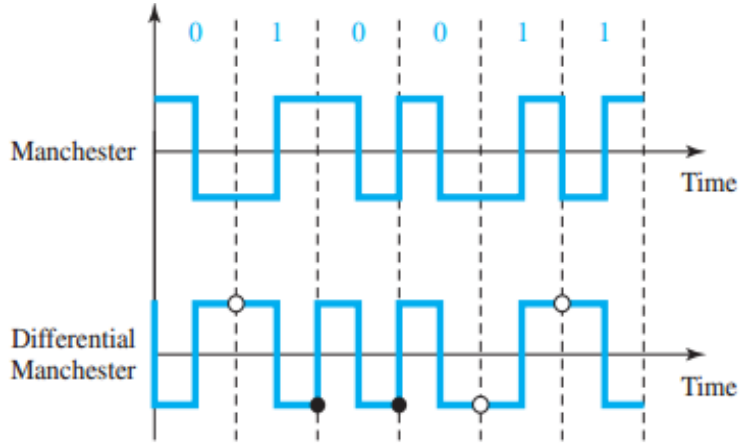


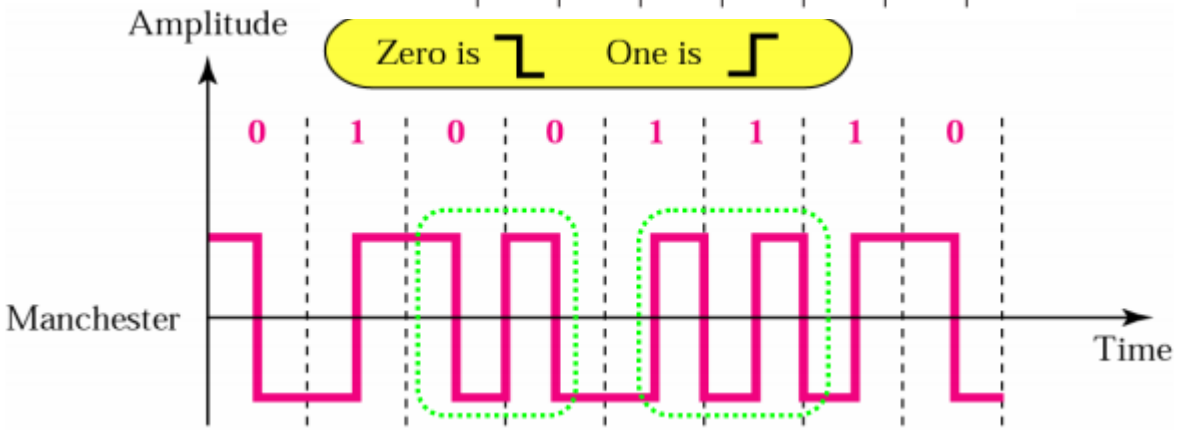


Data communication Contd.

- **Polar**
  - **RZ (Return to Zero)**
    - uses three voltage values. +, 0, -.
    - Each symbol has a transition in the middle. Either from high to zero or from low to zero.
- **Manchester**
  - we can use voltage *transitions*, instead of voltage *levels*. to represent ones and zeros
  - 0 = pos-to-neg transition, 1 = neg-to-pos transition

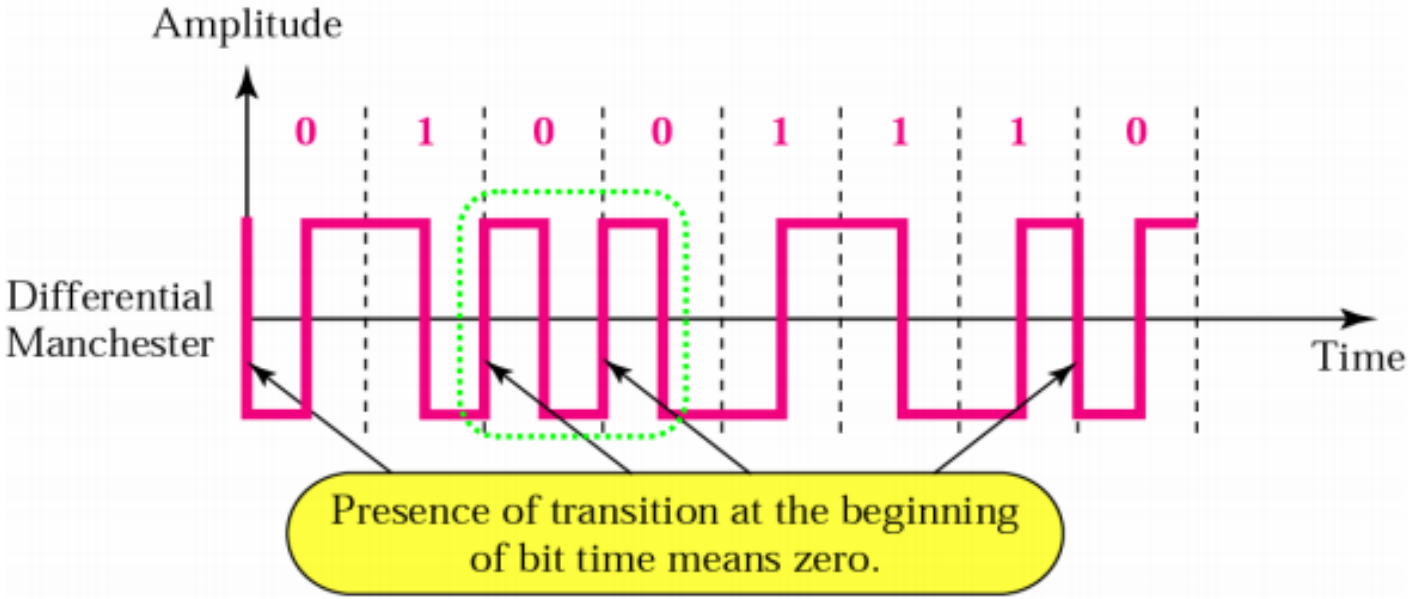


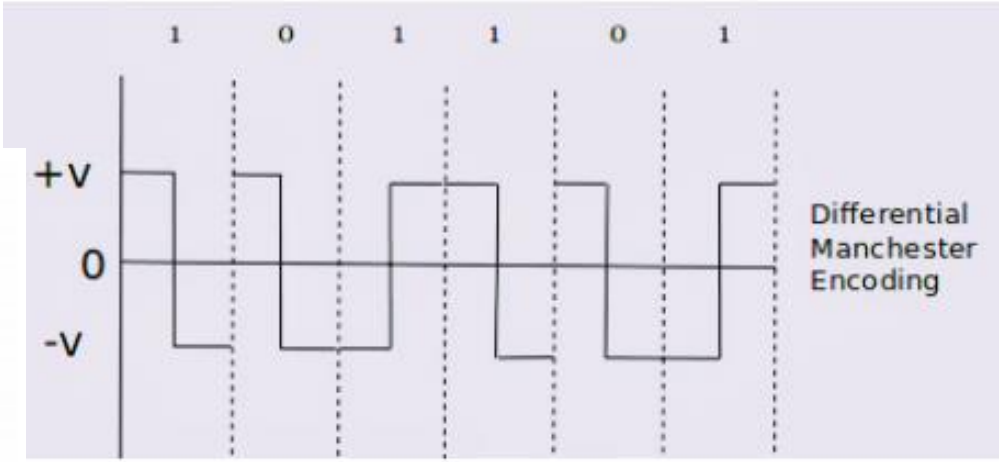




Data communication Contd.

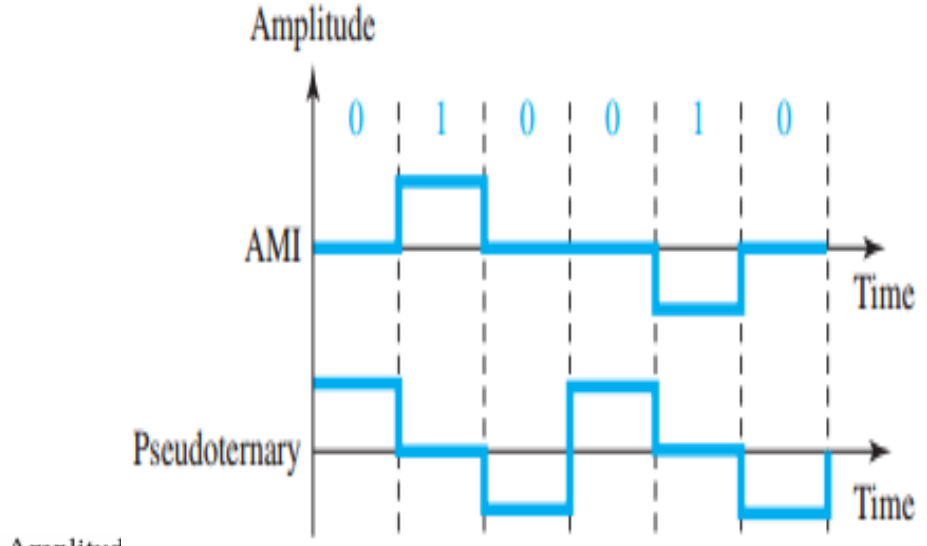
- **Differential Manchester**
  - The Bit 0 represent Inversion whereas 1 represents no inversion.
  - ❖ 0 = transition, 1 = no transition

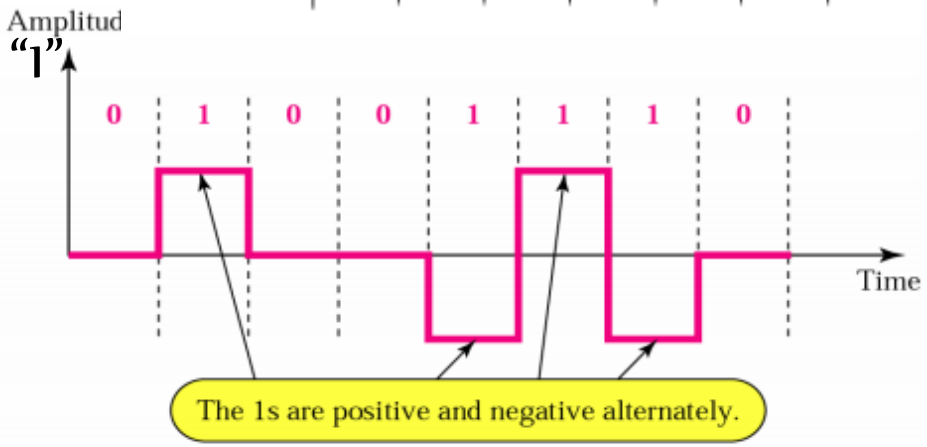




Data communication Contd.

- **bi-polar** - three voltage levels: positive, negative, and zero
  - Such a signal is called as **duo-binary signal**.
  - Uses two non-zero and zero voltage level for representation of two data levels
  - 0 = zero level; 1 = alternating pos and neg level
    - **AMI** (Alternate Mark Inversion)
      - The '0' symbol is represented by zero voltage and the "1" symbol alternates between +V and -V.
    - **Pseudoternary**
      - is the reverse of AMI

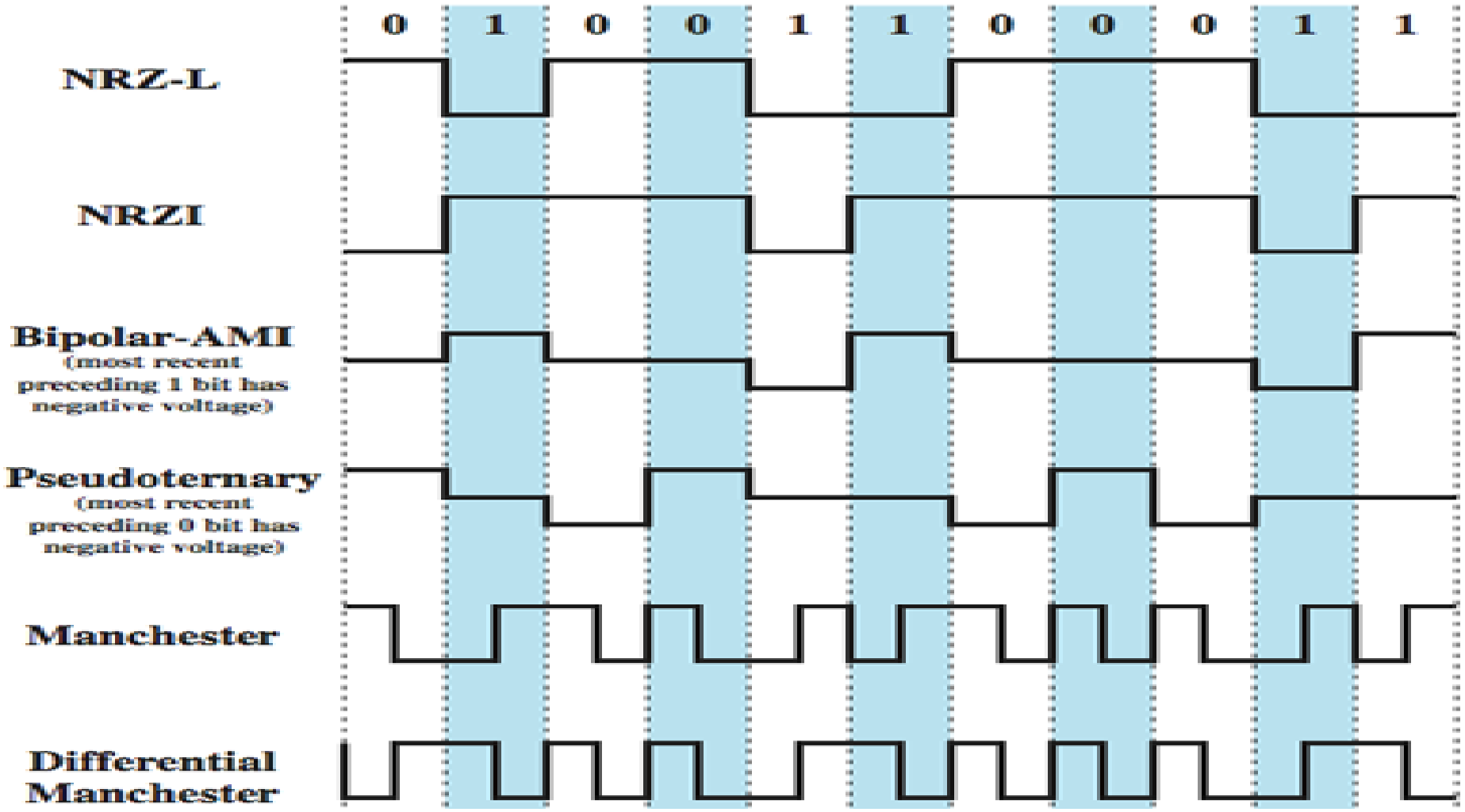




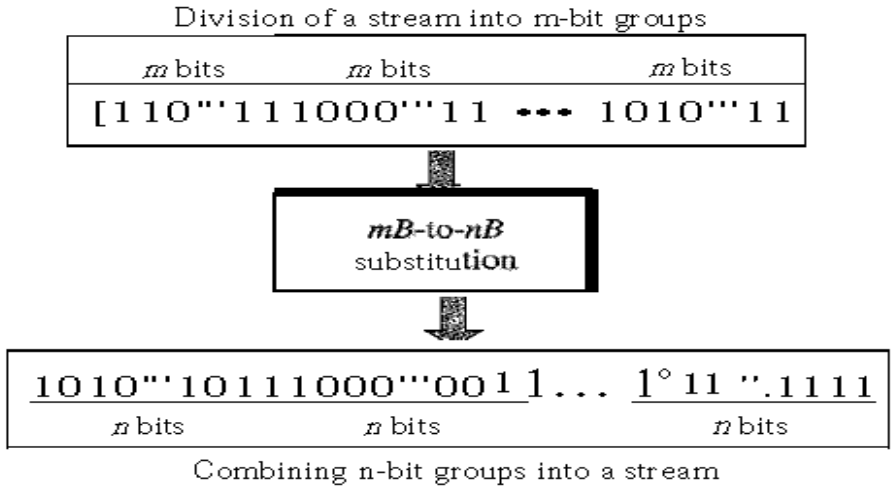
Data communication Contd.

- **What is bipolar return to zero?**

- **Exercise**: Given 01001100011 represent this data to:
  - Unipolar
  - NRZ-L,
  - NRZ-Invert,
  - RZ,
  - Non Differential -Manchester,
  - Differential Manchester
  - AMI,
  - Pseudoternary


0 1 0 0 1 1 0 0 0 1 1
NRZ-L
NRZI
Bipolar-AMI
(most recent preceding 1 bit has negative voltage)
Pseudoternary
(most recent preceding 0 bit has negative voltage)
Manchester
Differential Manchester

Data communication Contd.

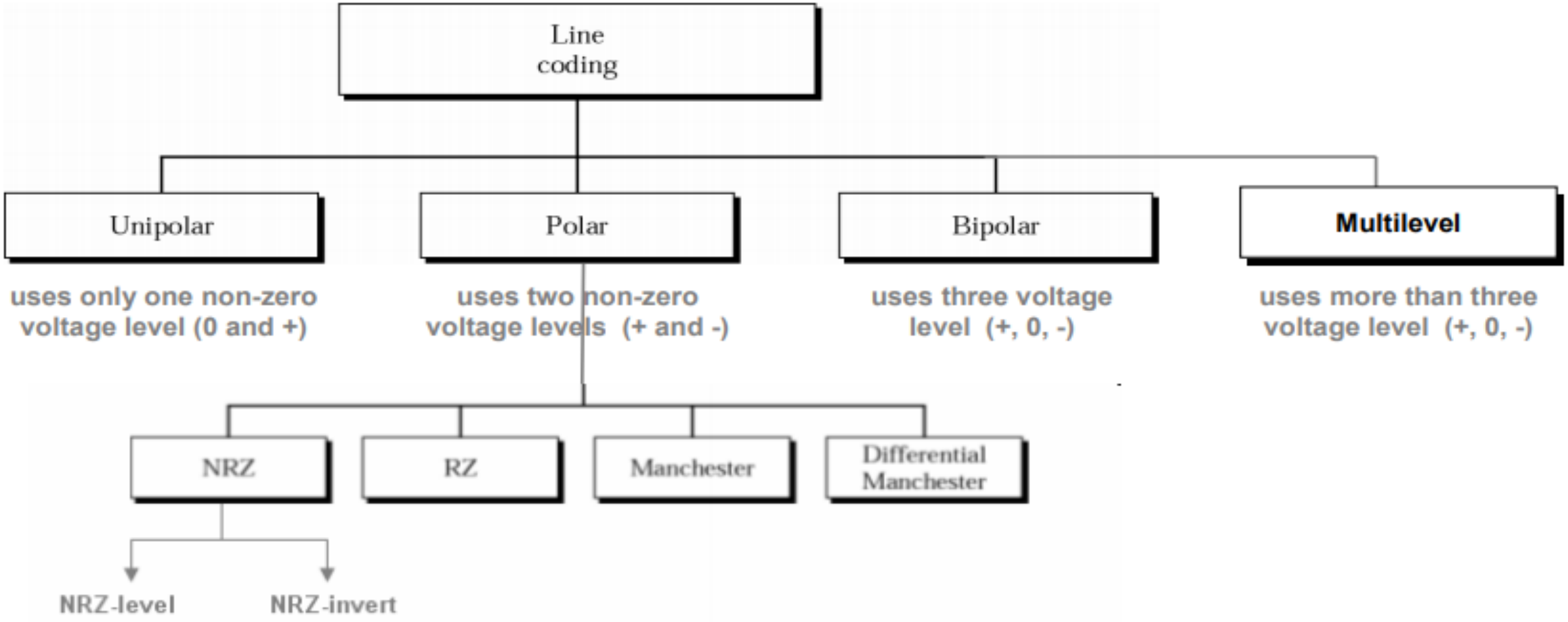


- **Block Coding**
  - To ensure accuracy of data frame received, redundant bits are used - improve the reliability of transmission
  - Block coding is represented by **slash notation**, mB/nB, that is m-bit block is substituted with n-bit block where n > m (4b/5b).
  - Block coding involves three steps:
    - **Division** - bits is divided into groups of *m* bits
    - **Substitution** - substitute an m-bit group for an n-bit group
    - **Combination** - n-bit groups are combined together to form a stream

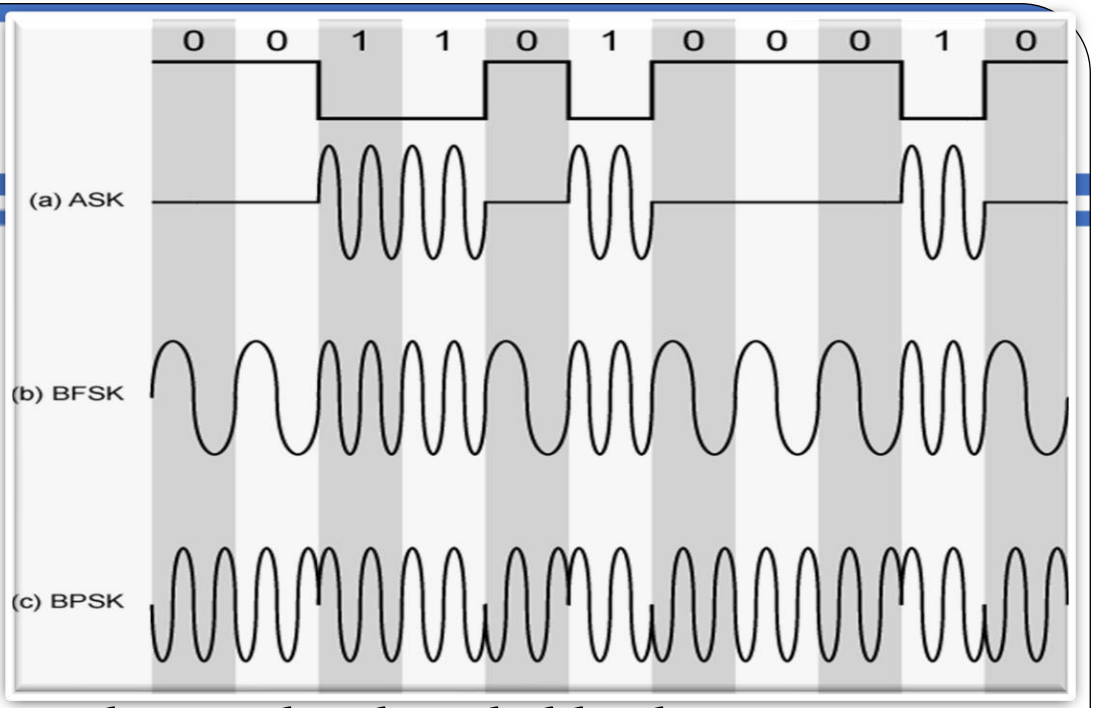
Data communication Contd.

- Scrambling (reading?)
- **Scrambling** is a technique that does not increase the number of bits and does provide synchronization.
- Problem with technique like Bipolar AMI(Alternate Mark Inversion) is that continuous sequence of zero's create synchronization problems one solution to this is Scrambling.
- There are two common scrambling techniques:
  - B8ZS(Bipolar with 8-zero substitution)
  - HDB3(High-density bipolar3-zero)

Data communication Contd.

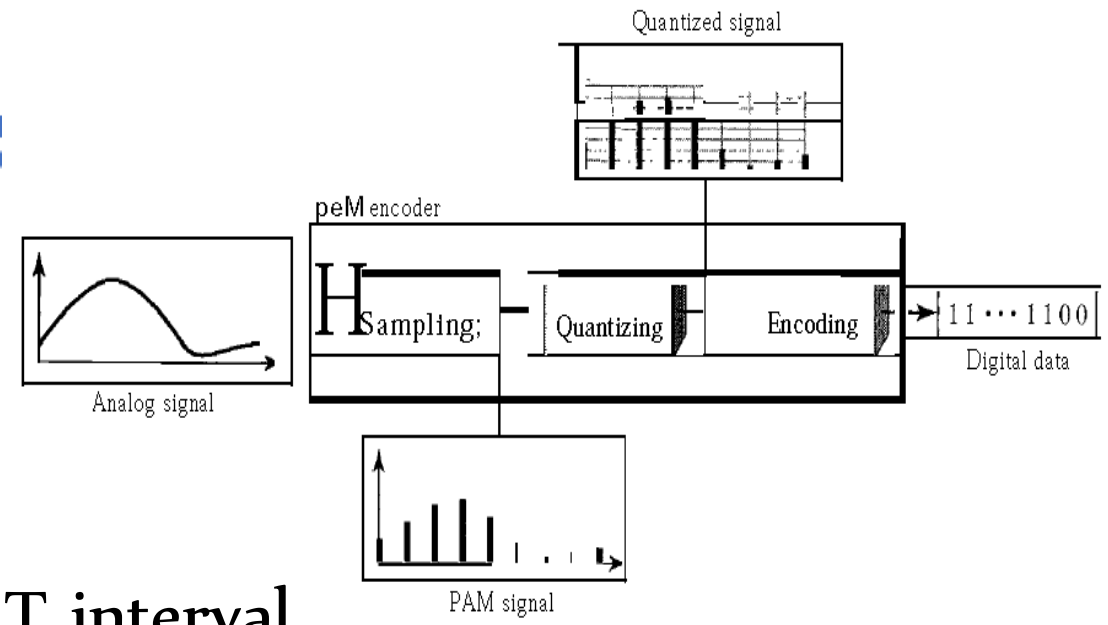


Data communication Contd.



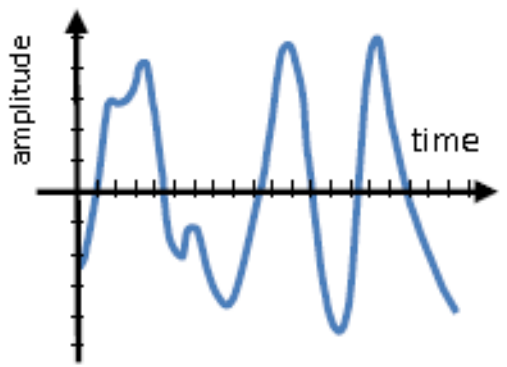
- **Digital-to-Analog Conversion –**
  - Used for transmitting digital data through the public telephone network
- Use a modem (modulator-demodulator), which converts digital data to analog signals, and vice versa
  - **Amplitude shift keying-** binary data represents digit 1, the amplitude is held otherwise it is set to 0
  - **Frequency shift keying** - chosen one to represent binary digit 1 and the other one is used to represent binary digit 0.
  - **Phase shift keying** - When a new binary symbol is encountered, the phase of the signal is altered
  - **Quadrature phase shift keying** - combination of ASK and PSK.

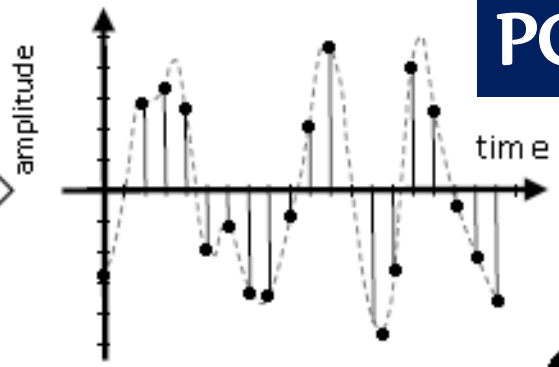
Data communication Contd.

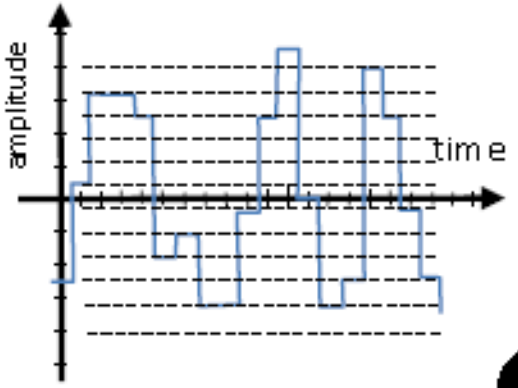


- ***Analog Signal to digital data conversion***
  - Pulse Code Modulation
  - Delta Modulation
- **Pulse Code Modulation**
  - **Sampling** - analog signal is sampled every T interval
  - **Quantization** - a method of assigning integral values in a specific range to sampled instances
  - **Encoding** - each approximated value is then converted into binary format
- **Delta Modulation**
  - PCM finds the value of the signal amplitude for each sample; DM finds the change from the previous sample

PCM







0100101101011001
1110101010101000
0100011000100011
0101001111010101
1110110111010001

❶ Sample → ❷ Quantize → ❸ Encode

Analog Signal → Sample → **Captured Sampled Data Values** → Quantize → **Quantized Sampled Data** → Encode → **Digital Signal**

Analog signal is continuous in time & amplitude

Sampling selects the data points we use to create the digital data

Discrete time values: few amplitudes from analog signal

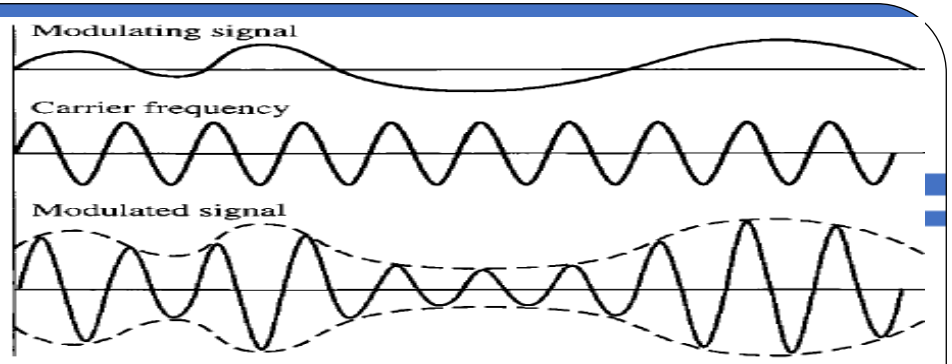
Quantizing chooses the amplitude values used to encode

Now have discrete Values in both time & amplitude

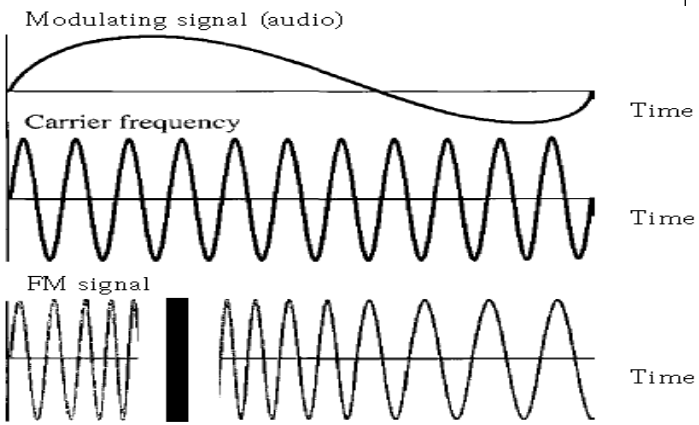
Encoding assigns binary numbers to those amplitude values

Now have the digital data which is the final result

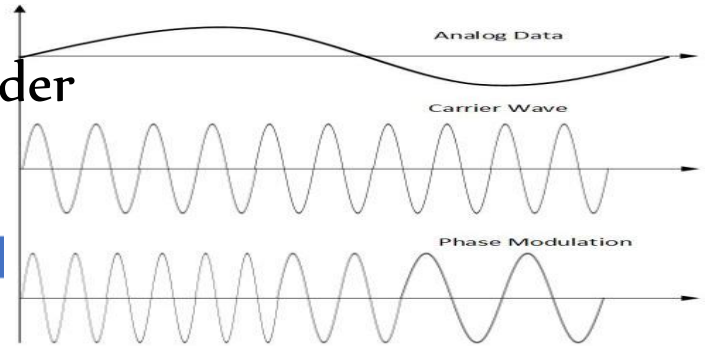
Data communication



- **Analog-to-analog conversion –**
- is the representation of analog information by an analog signal
  - **Amplitude modulation** - amplitude of modulating signal (analog data) is multiplied by the amplitude of carrier frequency



  - **Frequency modulation** - the frequency of the carrier signal is modified to reflect the change in the **voltage levels** of the modulating signal (analog data).
  - **Phase modulation** - the phase of carrier signal is modulated in order to reflect the change in voltage (amplitude) of analog data signal.

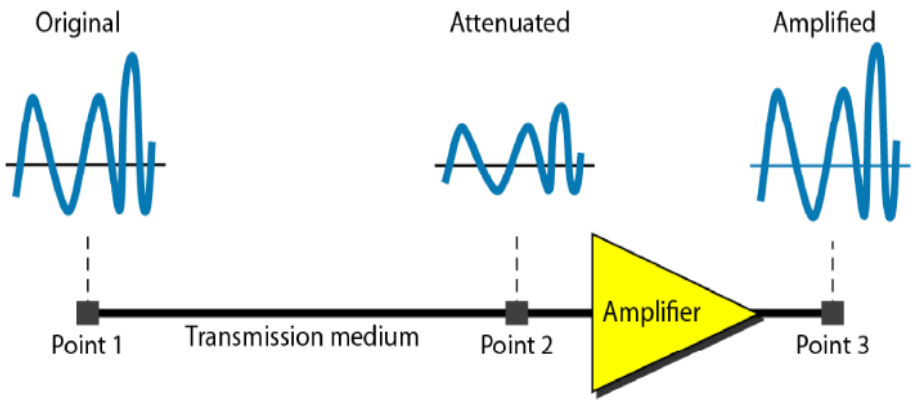


Data communication Contd.

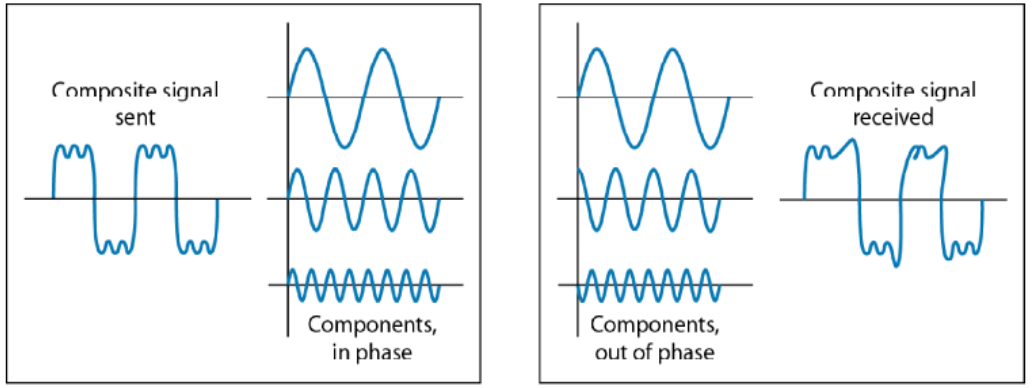
- **Error Detection and Correction**
  - A variety of reasons. Some errors are due to:
    - **Equipment failure.**
    - **Dispersion in optical fibers** (i.e. light pulses spread out).
    - **Attenuation** (loss of signal power over a line).
    - **Noise:**
      - **Thermal noise** - random motion of electrons
      - **Induced noise** - from sources such as motors and appliances
      - **Crosstalk** - effect of one wire on the other
      - **Impulse noise** - a spike that comes from power lines, lightning,

Data communication Contd.

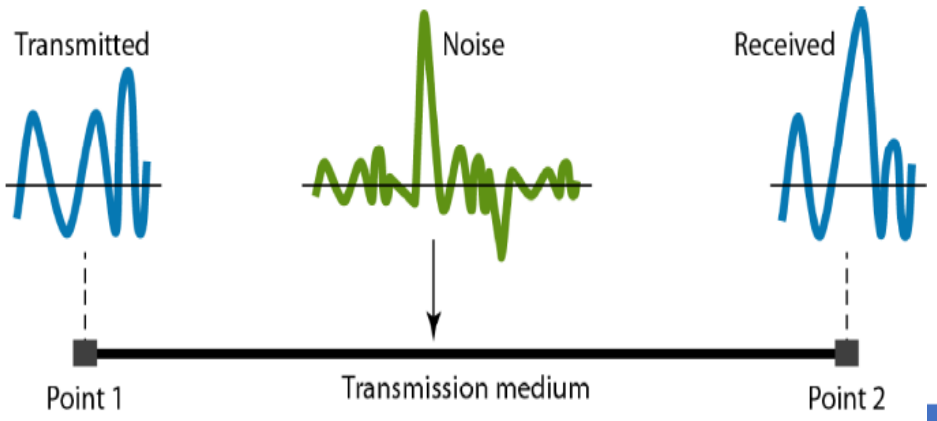
- Transmission impairments –
  - Data at beginning not the same as ending.
    - **Attenuation** – need amplifiers
    - **Distortion** – constant speed on medium quality
    - **Noise** – increase medium quality



Attenuation



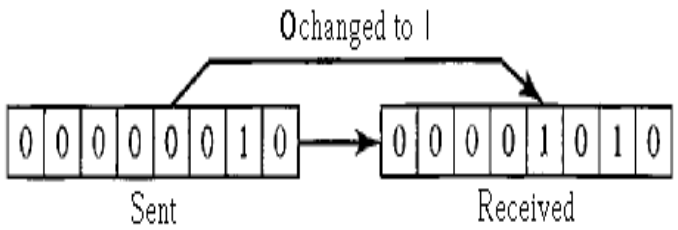
Distortion

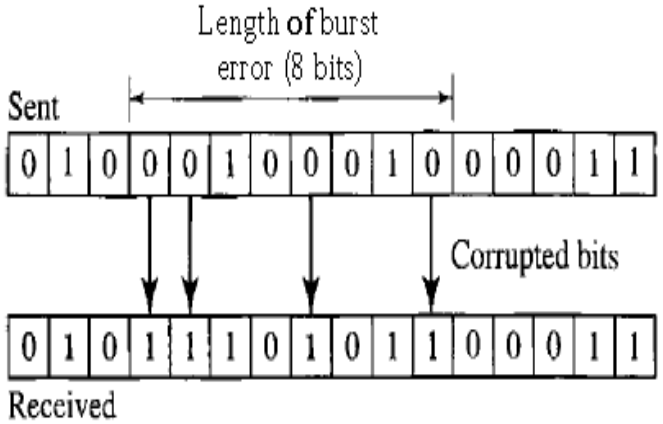


Noise

Data communication Contd.

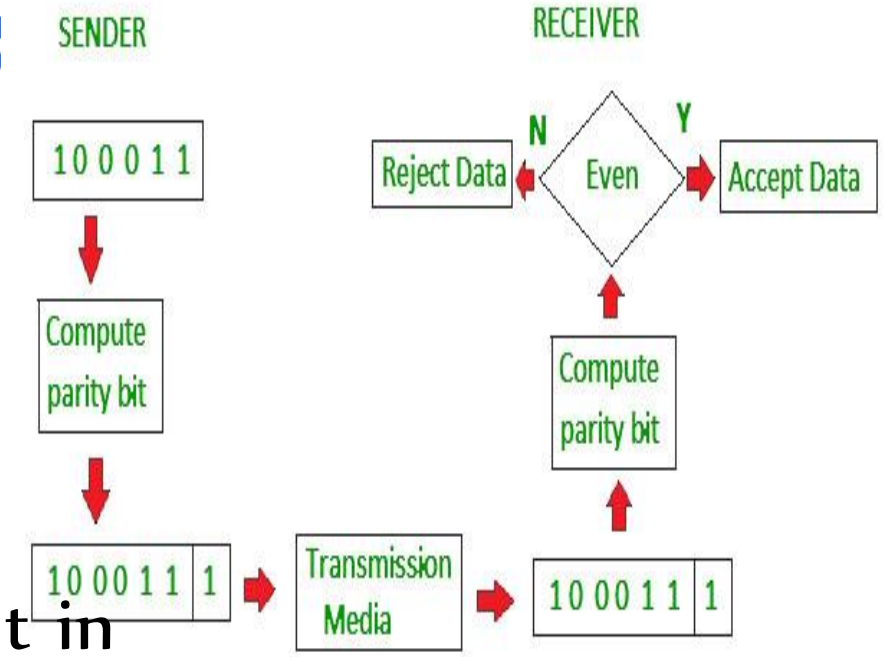
- **Type of errors**
  - **Content error** - missing bit/bits
    - **Single Bit error** - a 0 is changed to a 1 or a 1 to a 0.
    - **Burst Errors** - multiple bits are changed
  - **Flow integrity error** - missing frame/s
- **Error detection/Redundancy –**
- **Correction of errors is more difficult than the detection**
  1. Parity Checking (VRC)
  2. Cyclic Redundancy Check (CRC)
  3. Longitudinal Redundancy Check (LRC)
  4. Check Sum





Data communication

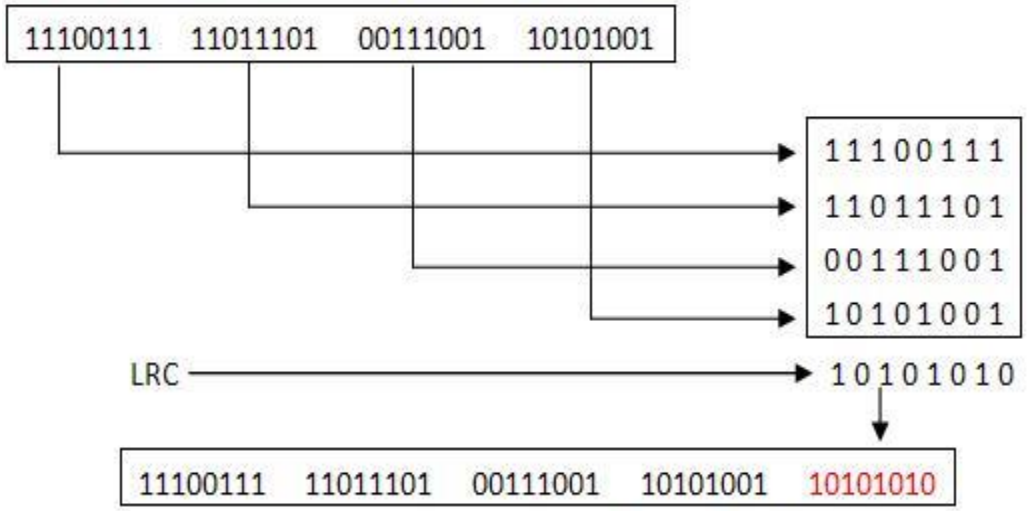
- **Vertical Redundancy Check** (VRC)
  - An additional **bit added** to the data at the transmitter before transmitting the data
  - Parity bit (a 0 or 1) is appended to make total number of 1's in the **unit even**
  - The addition of parity bit to the data will result in the **change of data string size**.
- Types of parity bits in error detection
  - Even parity
  - Odd parity



VRC problem:
If value of two bits changed?

Data communication

- **Longitudinal Redundancy Check** (LRC)
  - A block of bits is organized in a table (rows and columns), calculate the Parity bit for each column and create a new row



Original data message including LRC

Original Data

10011001	11100010	00100100	10000100

Row parities

10011001	0
11100010	0
00100100	0
10000100	0
11011011	0

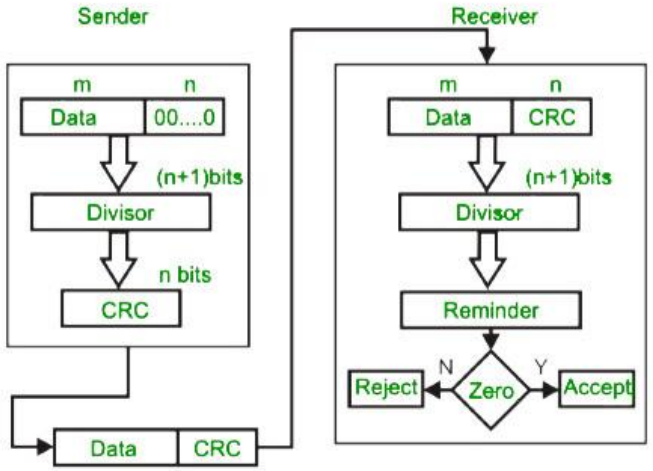
Column parities

100110010	111000100	001001000	100001000	110110110

Data to be sent

Data communication

- **Cyclic Redundancy Check** (CRC) – CRC is based on Binary Division
  1. Compare the data with the agreed divisor
  2. Take the **equal zeros** with the number of **difference in bits** and
  3. Append those bits on the original data. Data **1010110** divisor **1011** number of bits to be added **000** zeros on data before division
  4. Divide the number till the end
  5. Attach the last remainder number of bits with the data (should only be the size of bits on number three above, eg, after division if remainder is four bits take only three from the right)
  6. The receiver do the same division until the end
- If the last remainder is 0 the data is accepted



original message
1010000

@ means X-OR

Generator polynomial
x^3+1
$1.x^3+0.x^2+0.x^1+1.x^0$
CRC generator
1001 4-bit

If CRC generator is of n bit then append (n-1) zeros in the end of original message

Sender

```
1001 | 1010000000
     @1001
       0011000000
       @1001
         01010000
         @1001
           0011000
           @1001
             01010
             @1001
               0011
```

Message to be transmitted

```
1010000000
      +011
1010000011
```

```
1001 | 1010000011
     @1001
       0011000011
       @1001
         01010011
         @1001
           0011011
           @1001
             01001
             @1001
               0000
```

Receiver

Zero means data is accepted

Data communication

- **Checksum** – Finding one's complement
  1. Add the original data including the carry over each time
  2. Take the one's complement of the last summation as checksum
  3. Forward the checksum with the data
  4. Add the numbers on receiver and finally add the checksum
  5. Complement the last summation
- If all 0 accept the data

Original Data

10011001	11100010	00100100	10000100
1	2	3	4

k=4, m=8

Sender

```
1   10011001
2   11100010
   (1)01111011
            1
    01111100
3   00100100
    10100000
4   10000100
   (1)00100100
            1
Sum: 00100101
CheckSum: 11011010
```

Reciever

```
1   10011001
2   11100010
   (1)01111011
            1
    01111100
3   00100100
    10100000
4   10000100
   (1)00100100
            1
    00100101
    11011010
Sum: 11111111
Complement: 00000000
```

Conclusion: Accept Data

Example:

```
k=4,  m=8
10110011
10101011
01011110
       1
01011111
01011010
10111001
11010101
10001110
       1
Sum :  10001111
Checksum 01110000
```

(a)

Example: Received data

```
10110011
10101011
01011110
       1
01011111
01011010
10111001
11010101
10001110
       1
10001111
01110000
Sum: 11111111
Complement = 00000000
Conclusion = Accept data
```

(b)

Data communication

- **Error correction**
  - Receiver can ask sender for retransmission.
  - Receiver can use an error-detecting code, which automatically correct certain errors
    - *Redundancy bit (r)*
    - Hamming Code

Hamming Code

- Hamming code is a set of error-correction codes that can be used to **detect and correct the errors** that can occur when the data is moved or stored from the sender to the receiver
  - $2^r \geq m + r + 1$
  - where, r = redundant bit, m = data bit
- **Parity bits –**
  A parity bit is a bit appended to a data of binary bits to ensure that the total number of 1's in the data is even or odd. Parity bits are used for error detection. There are two types of parity bits:
  - **Even parity bit:**
    If the number of 1's counted is odd, the parity bit value is set to 1, making the total count of occurrences of 1's an even number. else the parity bit's value is 0.
  - **Odd Parity bit –**
    If the number of 1's counted is even, the parity bit value is set to 1, making the total count of occurrences of 1's an odd number. Else the parity bit's value is 0

Hamming code

D12	D11	D10	D9	P8	D7	D6	D5	P4	D3	P2	P1
1	1	0	1		1	0	1		1		

- Assume you have data **11011011**
- **All bits with power of two are parity bits** 2^0, 2^1, 2^2, 2^3, 2^4,…
- How many places we need? Formula of Hamming= **2^r>=m+r+1**
  - M is size data = 8 so 8+1=9+r
    - If r is 3 → 2^3>=9+3 (false →), 2^4>=9+4 (true)
  - r is no of parity = 4 bits to accommodate data size 2^4=16
    - So we need P_1, P_2, P_3, P_4
    - P1= d3+d5+d7+d9+d11 →1+1+1+1+1= it is odd, add 1
    - P2= d3+d6+d7+d10+d11 → 1+0+1+0+1 = it is odd, add 1
    - P4= d5+d6+d7+d12 → 1+0+1+1 = it is odd, add 1
    - P8= d9+d10+d11+d12 → 1+0+1+1 = it is odd, add 1
- **Data to e transmitted is 110101010111**

12	11	10	9	8	7	6	5	4	3	2	1
1	1	0	1	1	1	0	1	1	1	1	1

Hamming code

D12	D11	D10	D9	P8	D7	D6	D5	P4	D3	P2	P1
1	1	0	1		1	0	1		1		

- Assume the receiver received the following data
- Original Data **110111011111**
- Received Data **100111011111**

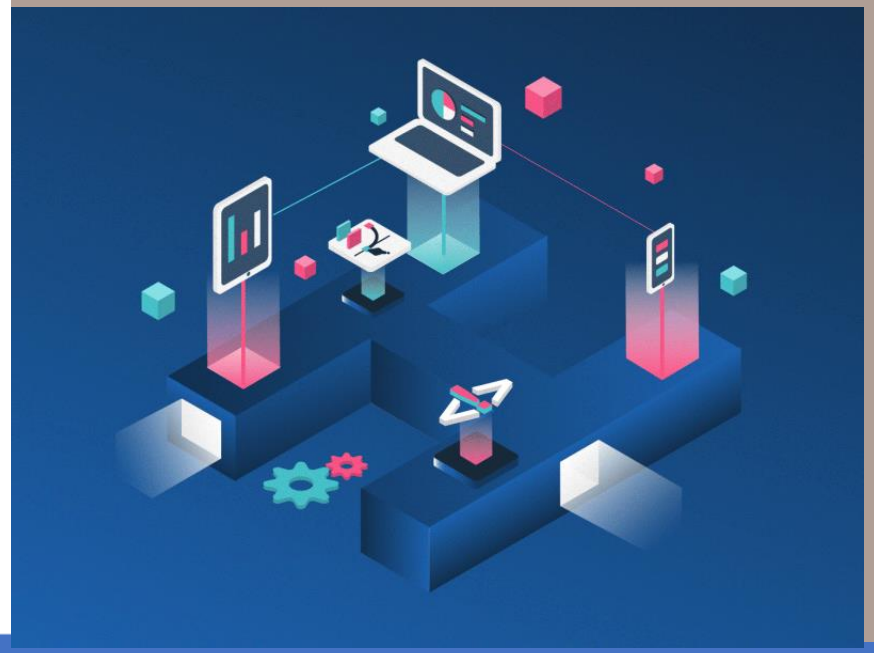
12	11	10	9	8	7	6	5	4	3	2	1
1	0	0	1	1	1	0	1	1	1	1	1

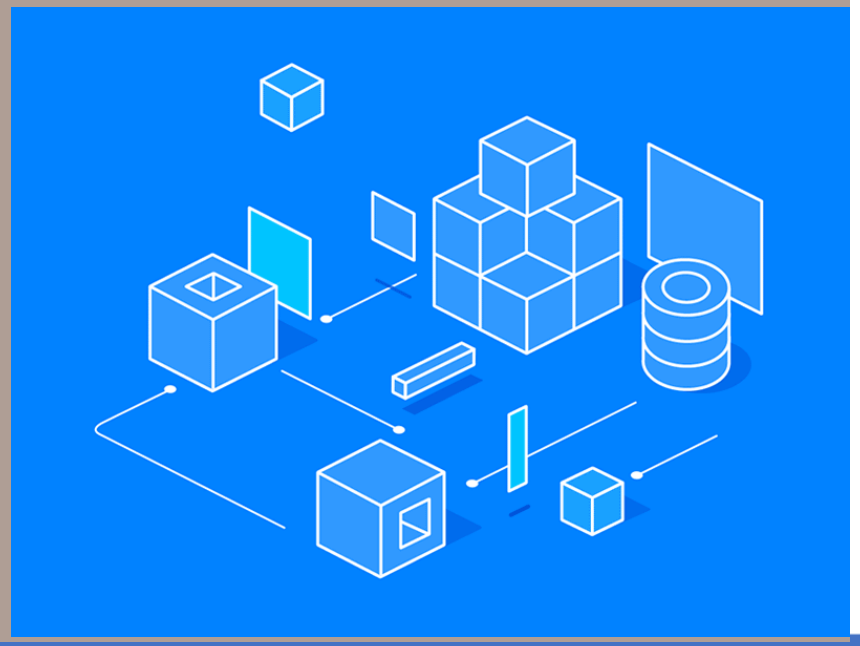
- **Question**: Correct the error using hamming code?
- Calculate and check the value of each parity
  - P1= d3+d5+d7+d9+d11 → 1+1+1+1+0= it is even, but above it is 1, so Flag 1
  - P2= d3+d6+d7+d10+d11 → 1+0+1+0+0 = it is even, but above it is 1, so Flag 1
  - P4= d5+d6+d7+d12 → 1+0+1+1 = it is odd, it is 1 above perfect Flag 0
  - P8= d9+d10+d11+d12 → 1+0+0+1 = it is even, but above it is 1, so Flag 1
- **So the error bit is summation of bits with 1= 8+0+2+1 =11**
- **The error bit is the 11th bit change that bit to 1**

P8	P4	P2	P1
1	0	1	1

Thanks

???





Debre Markos University
Institute of Technology
Information Technology Academy Program

Course Title: Data Communication and Computer Networks ()

Chapter: Two

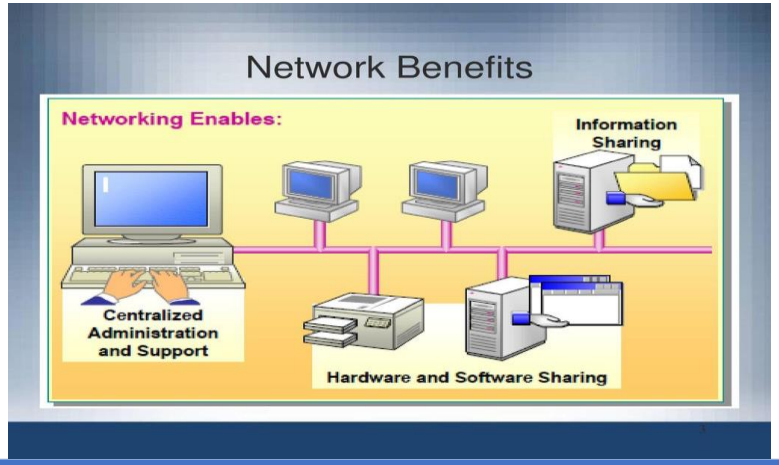
Introduction Computer Network

Data communication

1. What is a computer network?
2. Applications & Uses of Networks
3. Networking Impacts In Our Daily Lives
4. Evolution of Network
5. Types of networks
6. Computer network components
7. Computer network design and management

1. What is a computer network?

- A computer network is a system in which a number of independent computers are linked together (wired, wireless) to:
  - Sharing Information and Resources (HW, SW), services
    - File, folder, printer, disk drive, internet
  - Client-server Configurations
    - Administration, sharing
  - E-commerce
    - Buying and selling
  - Communication
    - VOIP, Chatting, email



2. Applications & Uses of Networks

- Marketing and sales
- Financial services
- Manufacturing
- Electronic messaging
- Directory services
- Information services
- Electronic data interchange (EDI)
- Teleconferencing
- Cellular telephone
- Cable television

2. Applications & Uses of Networks

- **Disadvantages of computer network**
  - **Data security** is therefore an important concern in a networked environment.
  - The danger of **computer viruses** entering the network is greatly increased.
  - **Equipment malfunctions**
    - System failures, media failure, server failure
  - **Cost** –
    - Hardware, software, setup
    - Management and administration

Networking Impacts In Our Daily Lives

- Efficient and easy communication
- Easy access to education
- Connectivity

3. Types of networks

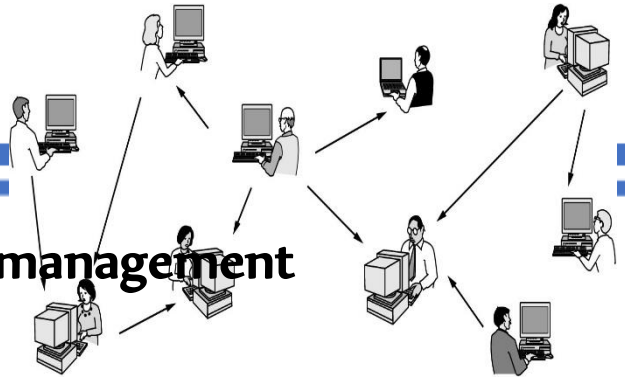
- Depending on one's perspective, we can classify networks in different ways.
  - Based on transmission **media**: Wired (TP, coaxial cables, fiber-optic cables) and Wireless
  - Based on network **size**: LAN, WAN, and MAN
  - Based on **management** method: Peer-to-peer and Client/Server
  - Based on **topology** (connectivity): Logical (Ethernet, token pass), physical (Bus, Star, Ring …)

3. Types of networks

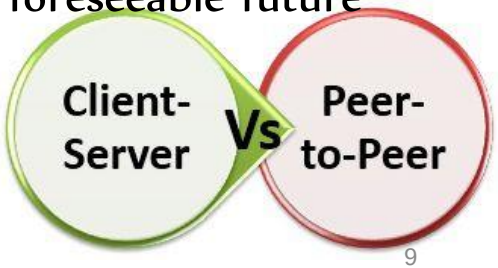
- **What are**
  - Wireless Local Area Network (WLAN)
  - Campus Area Network (CAN)
  - Storage-Area Network (SAN)
  - System-Area Network (also known as SAN)
  - Personal Area Network (PAN)
  - Virtual Private Network (VPN)

- **Types of NW based on network size (coverage)**
  - **Local Area Networks (LANs)**
    - Relatively **small** geographical area such as a home, an office, or a campus.
    - Owned, controlled, and managed by a **single** person or organization
    - Use certain **connectivity** technologies, primarily Ethernet and Token Ring.
  - **Metropolitan Area Network (MAN)**
    - It is a network that transmits data and information over **city** wide distance.
    - A network that is utilized across multiple buildings.
    - Is larger than a LAN, but smaller than a WAN. interconnection of several LANs
  - **Wide area network (WAN)**
    - has **no** geographical **limit**,
    - Ultimate WAN is the Internet
    - slower and less reliable than a LAN
    - Mostly **owned** by the public

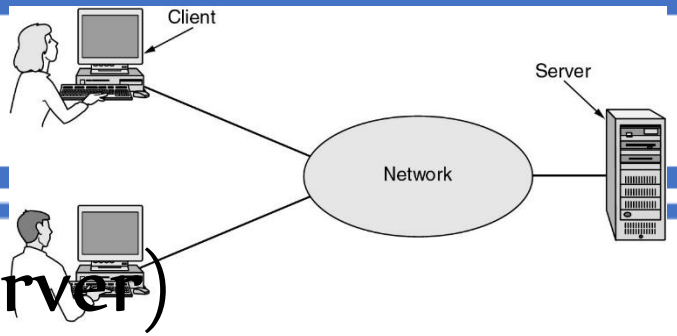
3. Types of networks



- **Types of networks based on node relationship / management**
  - Peer-to-peer networks
  - Server-based networks
- **Peer-to-peer networks**
  - No **dedicated servers**, and there is **no hierarchy** among the computers
  - All the computers are equal, Each computer functions as **both a client and a server**
  - Sometimes called **workgroups**.
  - Are relatively **simple**, **less expensive** than server-based networks
  - Users act as their **own administrators** and plan their own **security**
  - Peer-to-peer networks are good choices for environments where:
    - Less users (10 users or fewer), Users share resources, such as printers, but no specialized servers exist
    - **Security** is **not an issue**, only limited growth within the foreseeable future

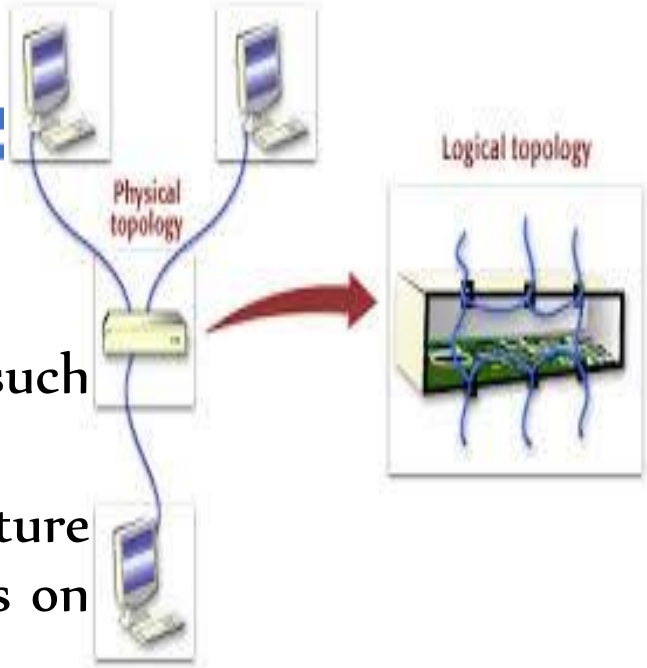


3. Types of networks



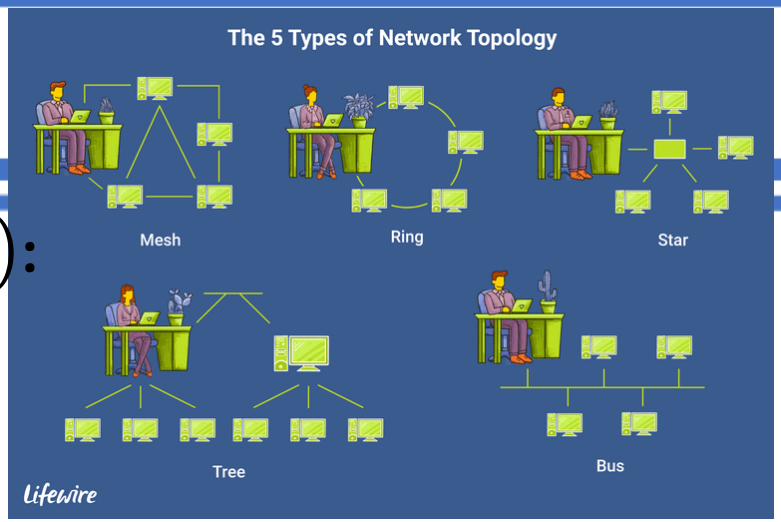
- Server-based networks (client/server)
  - More computers (10 or more), have **dedicated servers**
  - May have **separate servers** for file storage, web, printing, email and for storing and running application software.
  - More **complex** to install, configure, and manage, a server-based network
  - Centrally **administered** and controlled
  - **Security** is often the primary reason for choosing, backups can be scheduled, support thousands of users

3. Types of networks



- **Network Topologies**
  - **physical topology** –
    - Actual layout of the physical components such as computer, media etc.
    - The arrangement or physical layout / structure of computers, cables, and other components on the network,
      - Also called Physical layout, Design, Diagram or Map.
  - **logical topology** –
    - How the media is accessed by the hosts,
    - How data is transmitted between nodes or
    - How the network message is travel from one node to another

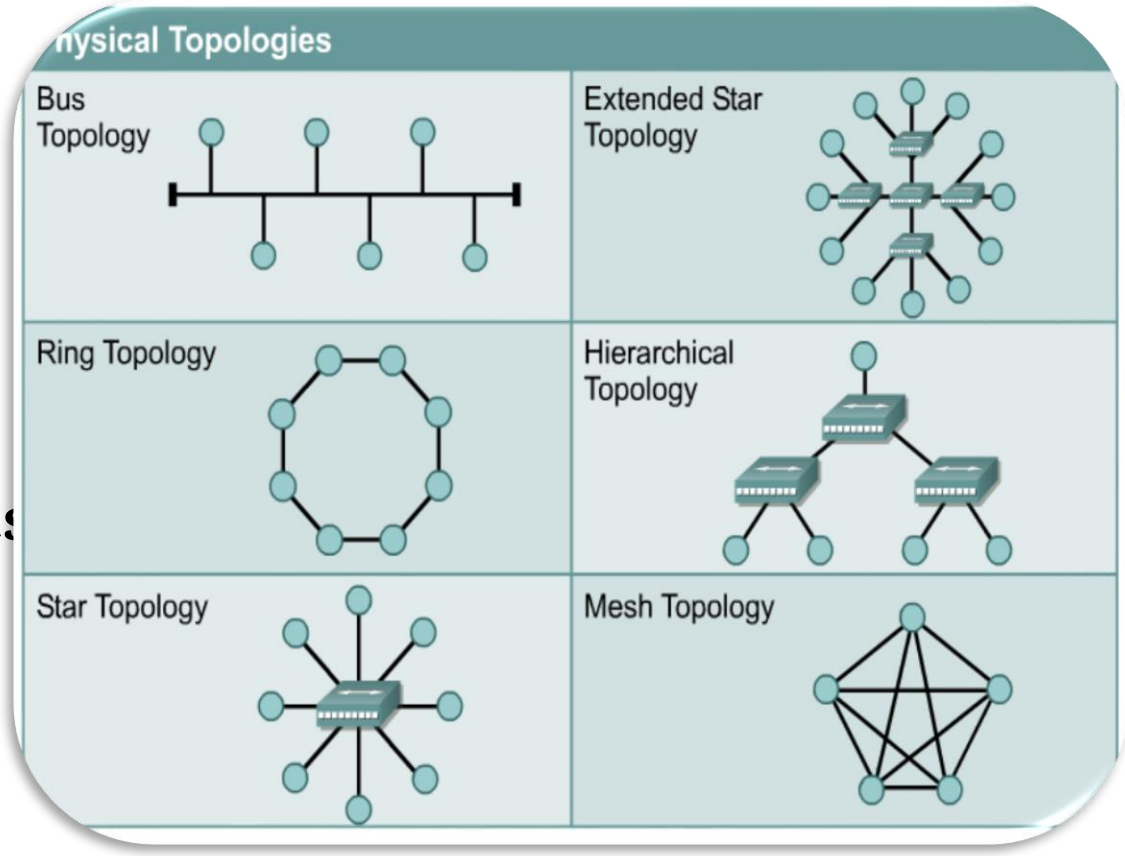
3. Types of networks



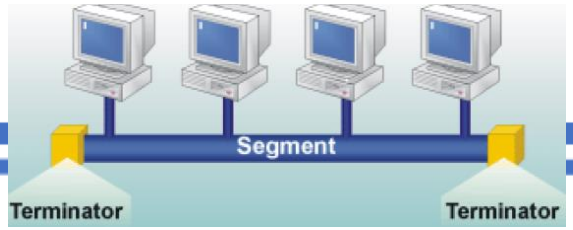
- The **choice** of topology (Physical):
  - Type of equipment that the network needs
  - Capabilities of the network
  - Growth of the network
  - Way the network is managed
  - Different types of cable, different network cards, network operating systems, how the cabling runs through floors, ceilings, and walls.
  - How computers communicate on the network.

3. Types of networks

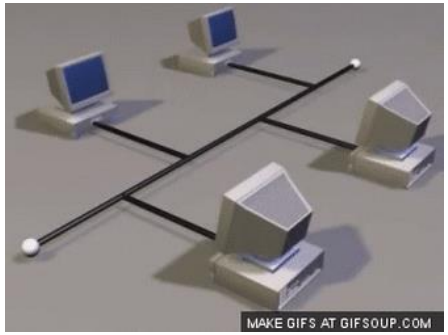
- **Physical Topology**
  1. Bus Topology
  2. Star topology
  3. Ring topology
  4. Mesh topology
  5. Hybrid topologies
     - Hierarchical
     - Extended star
     - Tree
     - . . . .



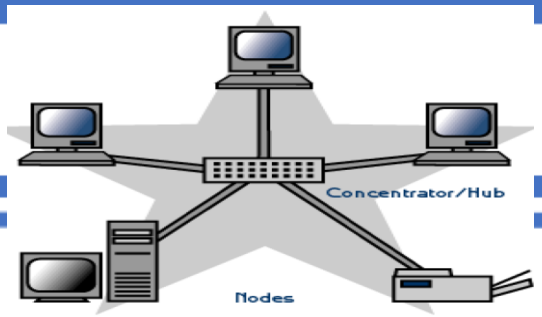
3. Types of networks



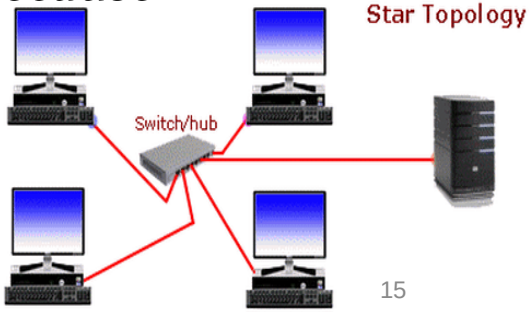
- **Bus Topology**
  - linear bus , connected in a **straight line**, **Inexpensive**, **simplest** and most common, single cable called a trunk, also called a backbone or segment, Easily extended
  - Three concepts:
    - **Sending the signal** - signals to all the computer. if more computers, others waiting – so slower network, if one computer fails, it does not affect the rest of the network
    - **Signal bounce** - bouncing back and forth along the cable and prevent other computers from sending signals - **collision or noise** - must be stopped
    - **Terminator** - placed at each end of the cable to absorb free signals / To stop bouncing. if a break in the cable occurs so the signal will bounce, and all network activity will stop
  - Bus topologies use **coaxial cable**. **T connectors** are often used to connect the computer to the trunk cable.



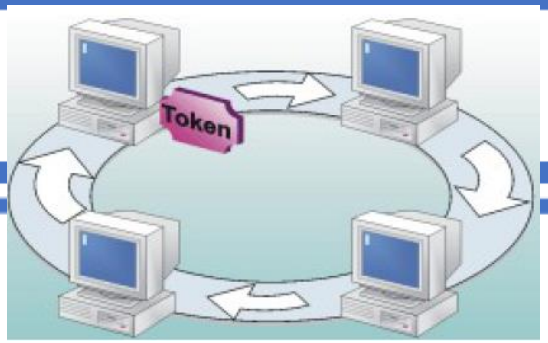
3. Types of networks



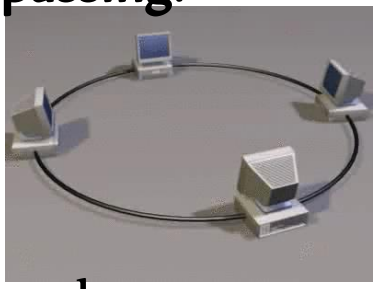
- **Star topology**
  - Each computer are connected to a **centralized component** called a concentrator, making it very easy to add a new workstation
  - Requires a great deal of **cable**
  - **Most common network configuration in use today**
  - If the **central point/device fails**, the entire network goes down
  - If **one** computer or the **cable fails**. The rest of the network continues to function normally.
  - Are more **expensive** to install than bus networks, because there are several more cables
  - Plus the **cost** of the **concentrator** / hubs



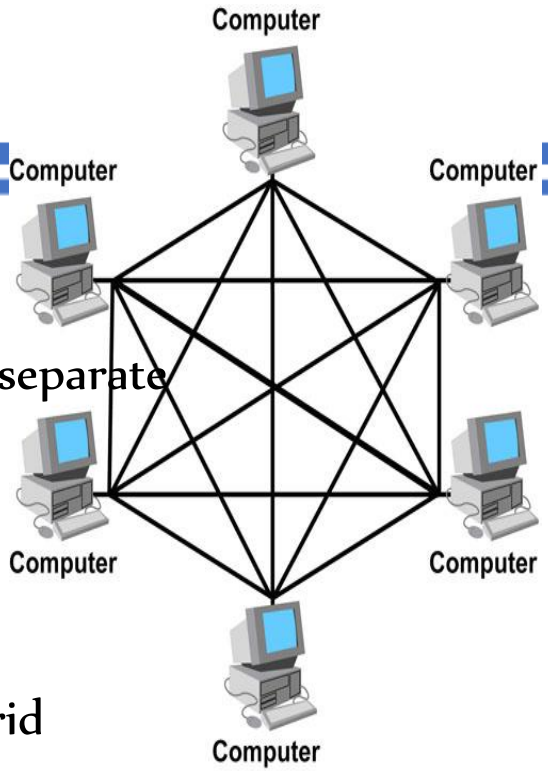
3. Types of networks



- **Ring topology**
  - Connects computers on a **single circle** of cable
  - Each node is connected to the two nearest nodes so the entire network forms a circle.
  - **Signals** travel around the **loop in one direction** and pass through each computer (act as a **repeater**).
  - failure of one computer can have an impact on the entire network
  - One method for passing data on ring networks is **token passing**.
  - **Easier to manage**
  - Easier to **locate a defective** node or cable problem
  - In short ring topology enables **reliable communication**
  - **Expensive**, requires more cable and network equipment at the start, not used as widely as bus topology
  - **only one computer** at a time **can send**

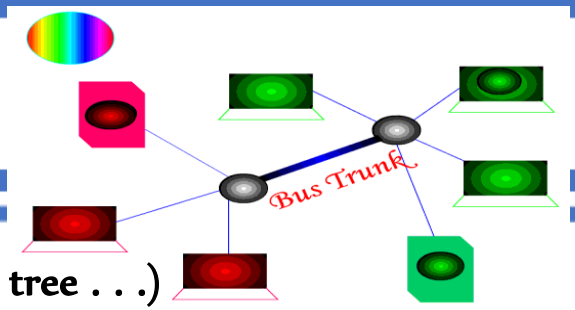


3. Types of networks



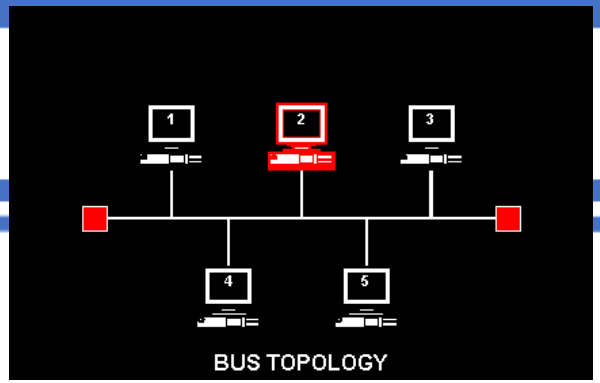
- **Mesh topology**
  - Offers superior **redundancy** and reliability
  - Each computer is connected to every other computer by separate cabling.
  - If **one cable fails**, another will take over the traffic
  - Ease of **troubleshooting** and increased **reliability**
  - Are **expensive** to install because they use a lot of cabling
  - Used in **conjunction** with other topologies to form a hybrid topology
  - The **simplest** logical topology in terms of data flow, but it is the most **complex** in terms of physical design
  - If there are x computers, there will be **(x × (x–1)) ÷ 2 cables**

3. Types of networks

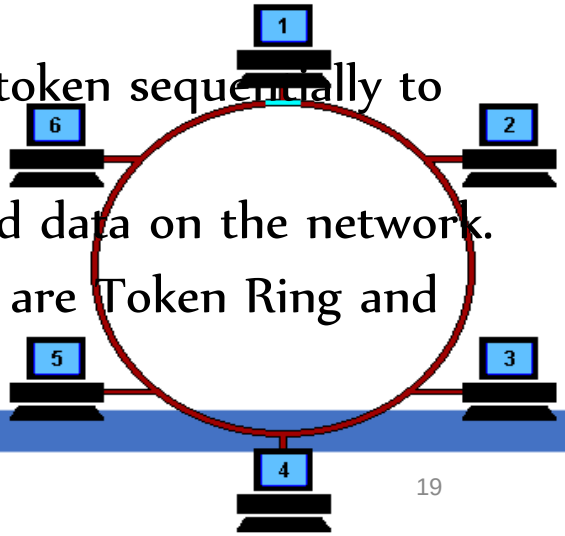


- **Hybrid topologies** (star-bus, star-ring, extended-star, tree . . .)
  - **Star bus topology**
    - If one computer goes down, it will not affect the rest of the network. The other computers can continue to communicate.
    - If a hub goes down, all computers on that hub are unable to communicate
  - **Star ring topology**
    - The star ring (sometimes called a star-wired ring) appears similar to the star bus.
    - Both the star ring and the star bus are centered in a hub that contains the actual ring or bus

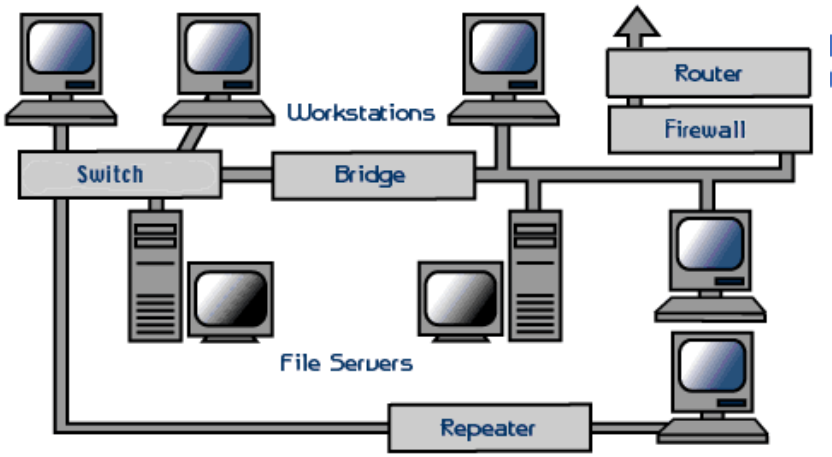
3. Types of networks



- Logical Topologies
  - Defines how the **hosts communicate** across the medium
- The two most common types of logical topologies are:
  - **Broadcast topology / Ethernet**
    - Each host sends its data to all other hosts on the network medium.
    - It is first come, first serve FIFO.
    - Commonly supported by networks that use a bus, a star, or a star-wired bus physical topology
  - **Token passing**
    - Controls network access by passing an electronic token sequentially to each host.
    - When a host receives the token, that host can send data on the network.
    - Two examples of networks that use token passing are Token Ring and Fiber Distributed Data Interface (FDDI).



4. Computer network components

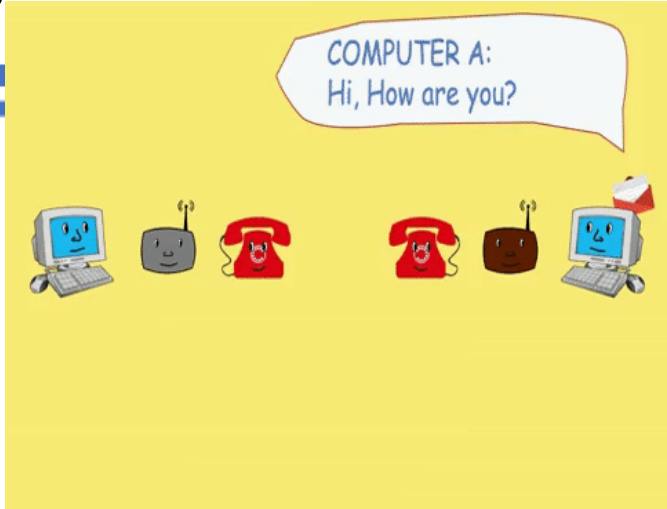


- Two basic components
  - Hardware
  - Software
- **Hardware** –
  - All physical parts that we can see and touch
    - Server
    - Workstation / Client / dump Terminals
    - Transmission media / Medium
    - Network Interface Cards (NIC) - transmitter" and "receiver" – transceiver. It use MAC address can be wired or wireless. **PCI slot** (desktop) and **ExpressCard slots** (laptop)
    - A concentrator / network connectivity devices / internetworking devices, or wiring center

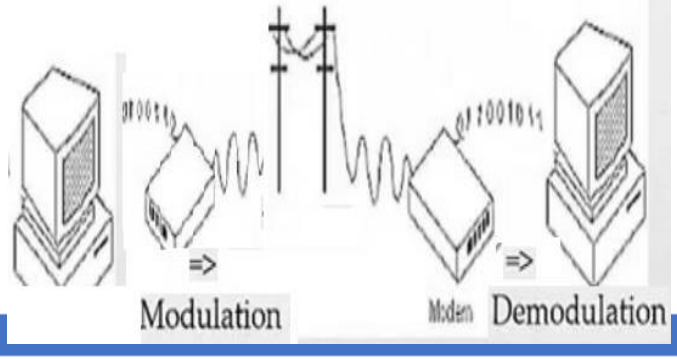
4. Computer network components

- A concentrator / network connectivity devices
  - **Hub** –
    - **Hubs can be:** A passive hub, An active hub, A switched hub
    - Currently Hubs are becoming obsolete and replaced by more advanced communication devices such as **Switches and Routers**
  - **Switch** –
    - amplify the signal as it moves from one device to another
    - Managed switch and unmanaged switch
  - **Repeaters** - amplifies the signal it receives and **rebroadcasts** it
  - **Bridges - segment** a large network into two smaller, more efficient networks
  - **Routers** - translates information from **one network to another**; it is similar to a super intelligent bridge
  - **Gateway** - A gateway is a translation tool. It is a server that acts as an **intermediary for some other server**.

4. Computer network components

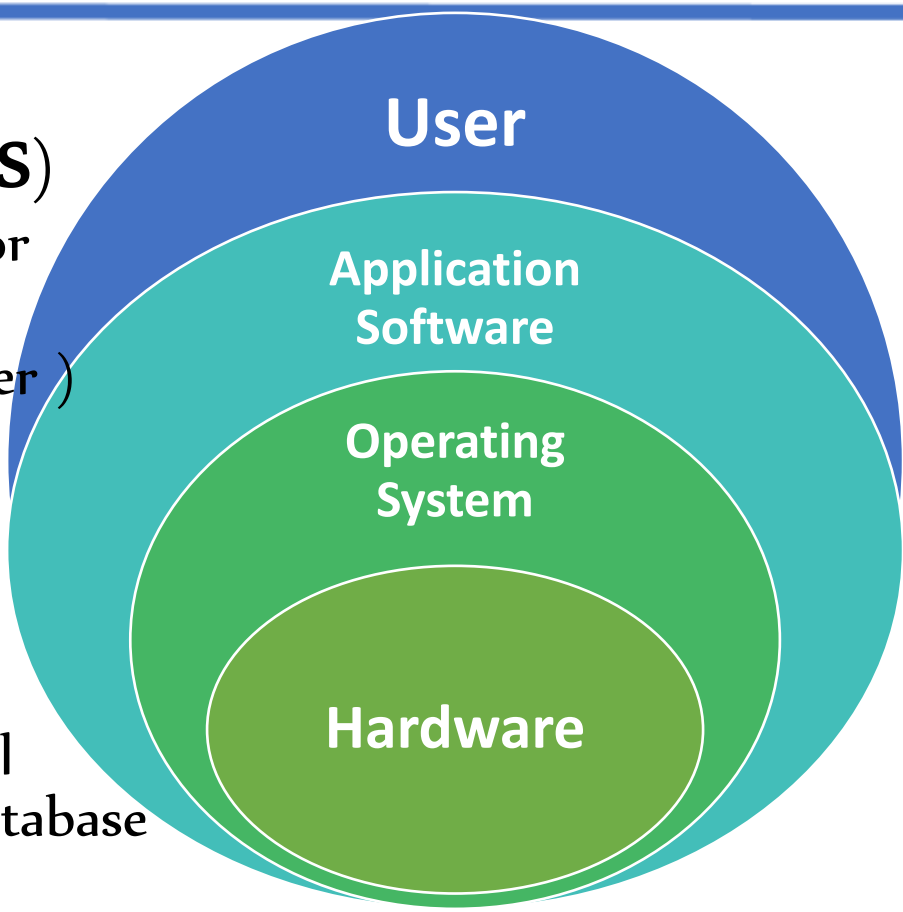


- **Modems** –
  - For internet connection over **the existing telephone line**.
  - Can be installed on the PCI slots found on motherboard.
  - It is not necessary for LAN, but required for internet connection such as dial-up and DSL.



4. Computer network components

- **Software**
  - Network operating system (**NOS**)
    - Peer-to-peer (such as Windows for Workgroup) and
    - client server (Windows 2012 Server)
  - The operating system of the workstation – (**WOS**) - such as windows 10
  - **Application Software**
    - **Server** software - web server, mail server, print server, file server, database server
    - **Client** software - web browsers, e-mail clients



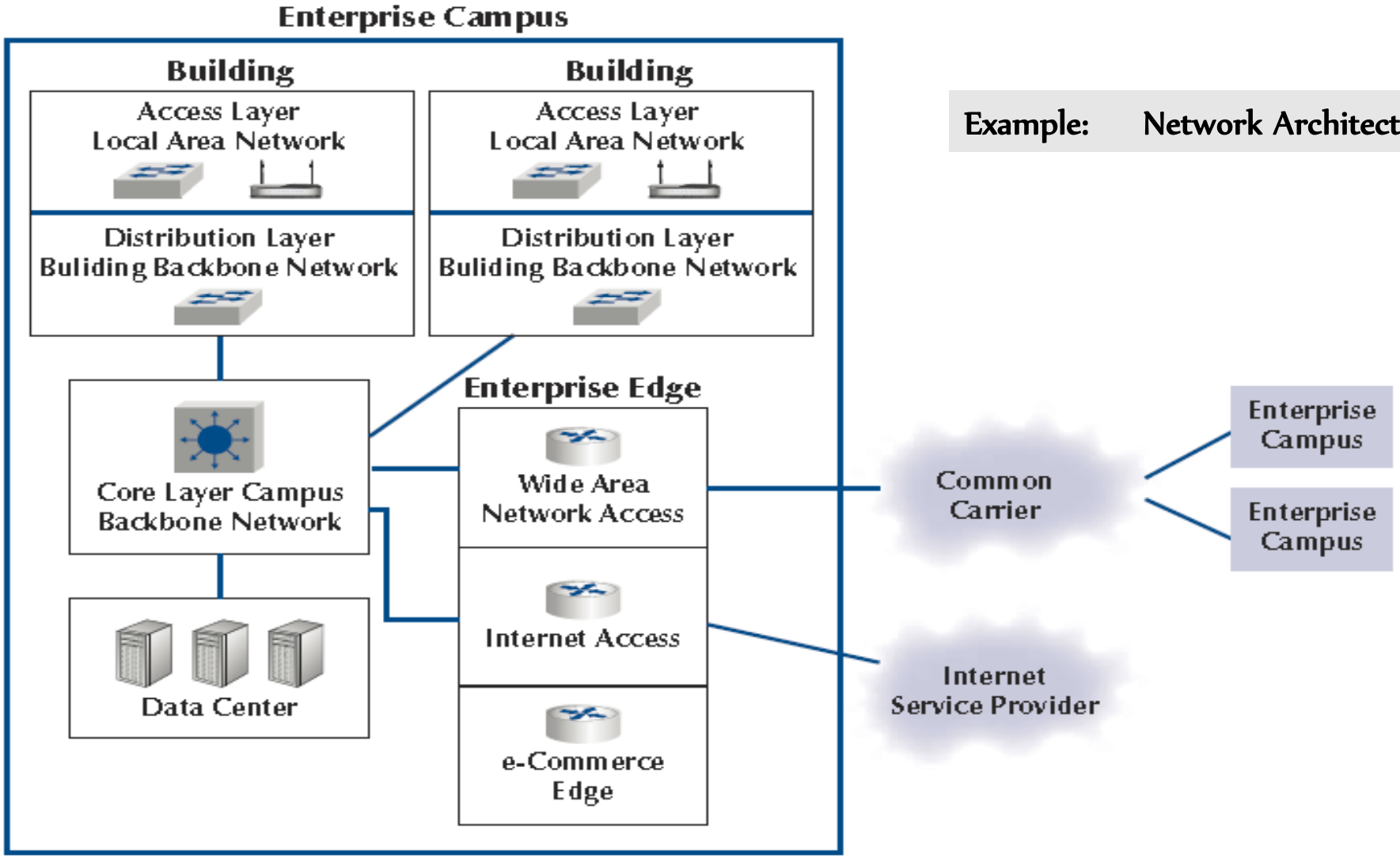
5. Computer network design and management

- **Network Design**
  - Identify the **organizational objective** and the **goal of the network** to be developed
- The most typical technical goals in an enterprise LAN/WAN design
  - **Scalability** – appropriate size or volume, minimal cost
  - **Availability** - 7 / 24 or according to need. Fast User Interface, Application availability
  - **Performance** / Reliability - capacity utilization, throughput, and delay
  - **Security** – policy, Roles and Privileges
  - **Flexibility** - Easy User Management, Handling Multiple Time-zones, Maintenance scheduling

5. Computer network design and management

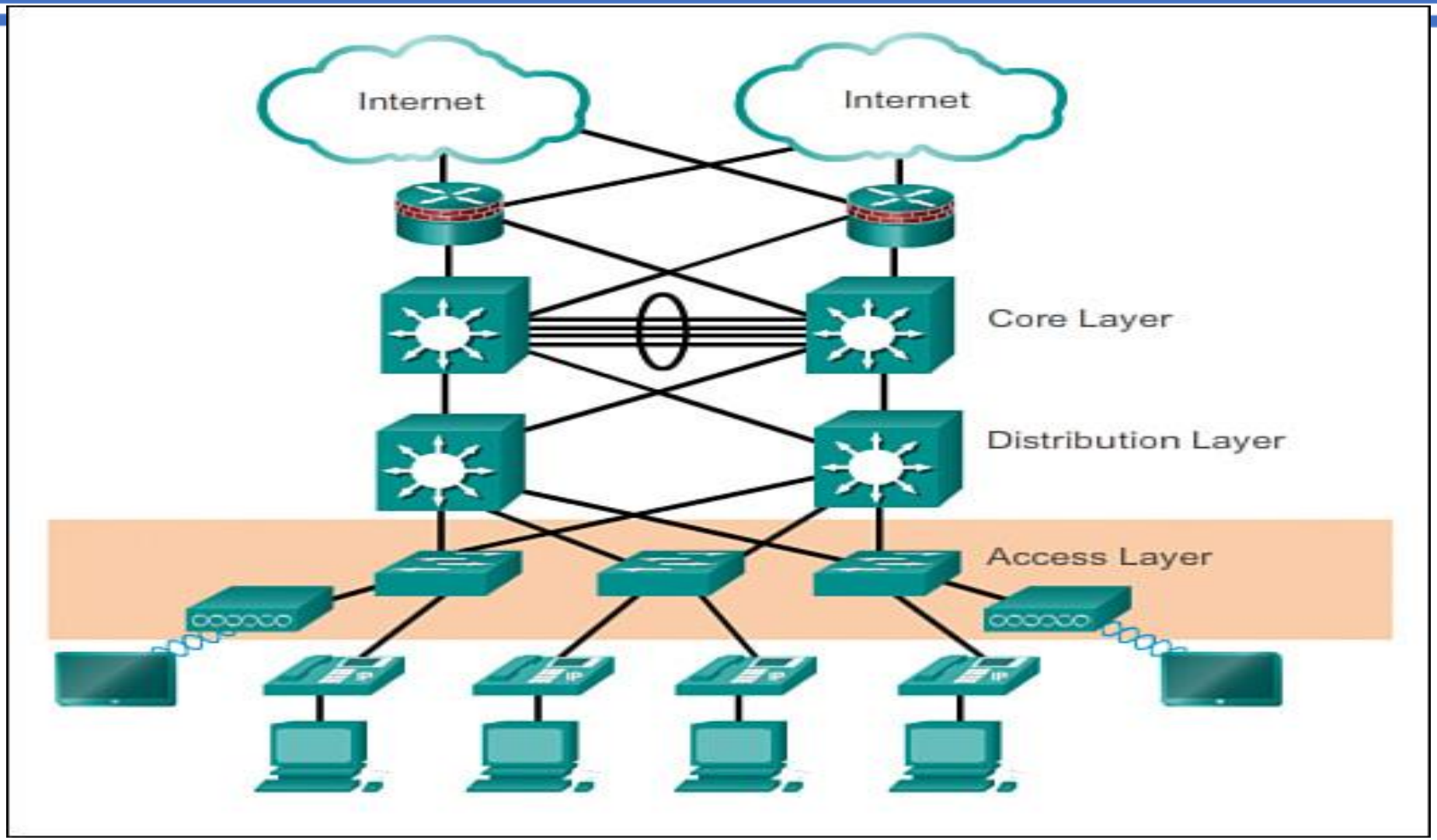
- First decide whether a peer-to-peer or a server-based network.
  - Factors:
    - Size of the network.
    - Level of security.
    - Type of business.
    - Level of administrative support available.
    - Amount of network traffic.
    - Needs of the network users.
    - Network budget.

5. Computer network design and management



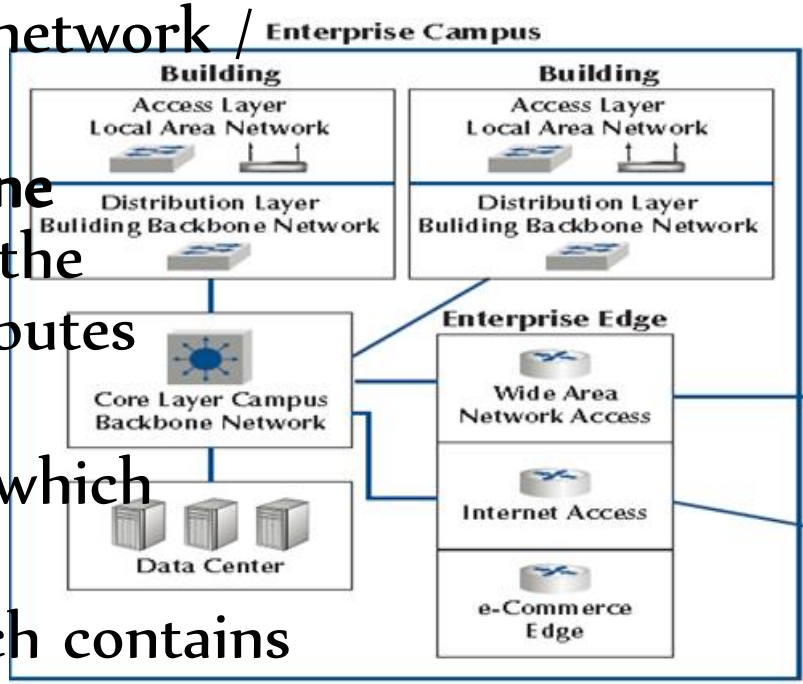
Example: Network Architecture

Layered Architecture



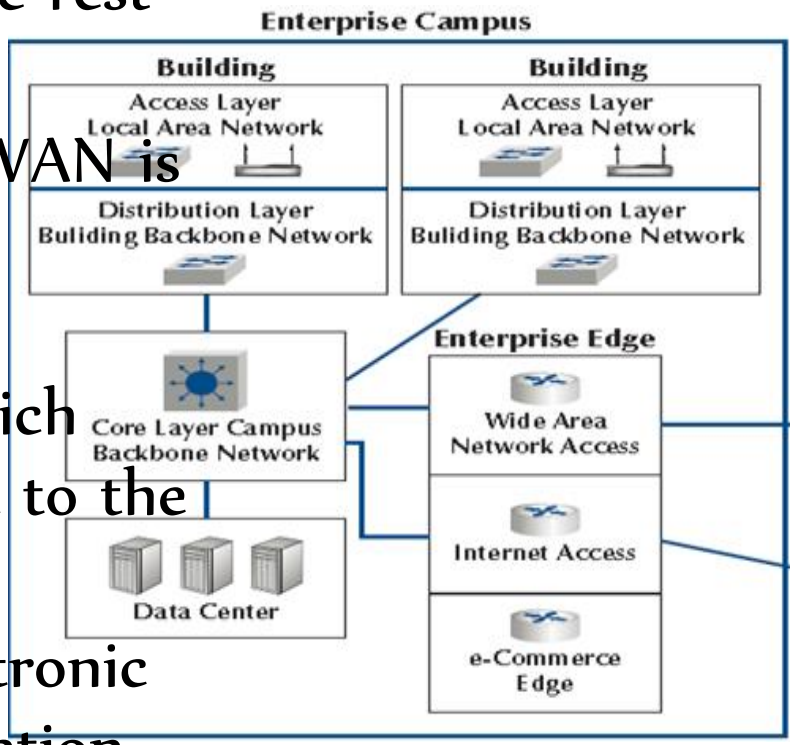
5. Computer network design and management

- **Components in the above Architecture**
  - **The first** is the **local area network (LAN)**, which enables users to access the network / **access layer**
  - **The second** is the **building backbone network**, which some vendors call the **distribution layer**, because it distributes
  - **The third** is the **campus backbone** (sometimes called the **core layer**), which connects all campus buildings.
  - **The fourth** is the **data center**, which contains the organization's servers (e.g., db. servers, email servers).



5. Computer network design and management

- **The last three** make up the **enterprise edge**, an enterprise campus connect with the rest of the world.
  - The **wide area network (WAN)**. A WAN is a private network that connects its different campus locations.
  - The **Internet access** component, which enables the organization to connect to the Internet.
  - The **e-commerce edge**. enables electronic data exchange between the organization and the external entities.

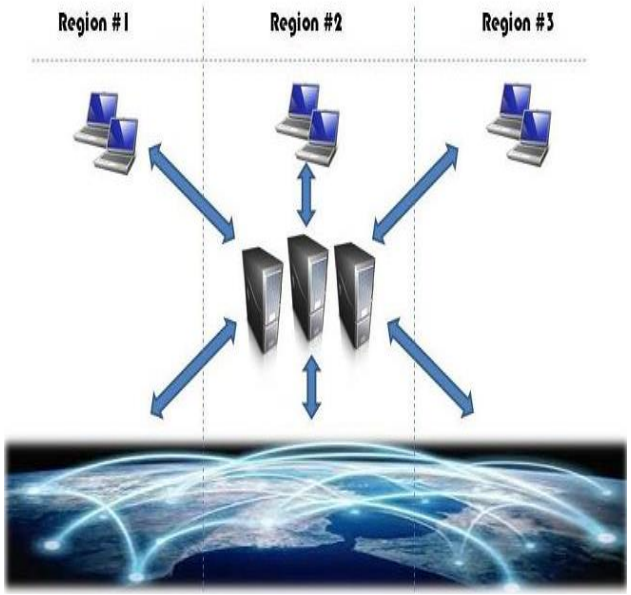


5. Computer network design and management

- **Network Management Architecture**
  - **Centralized**
  - **Distributed**
  - **Hierarchical**

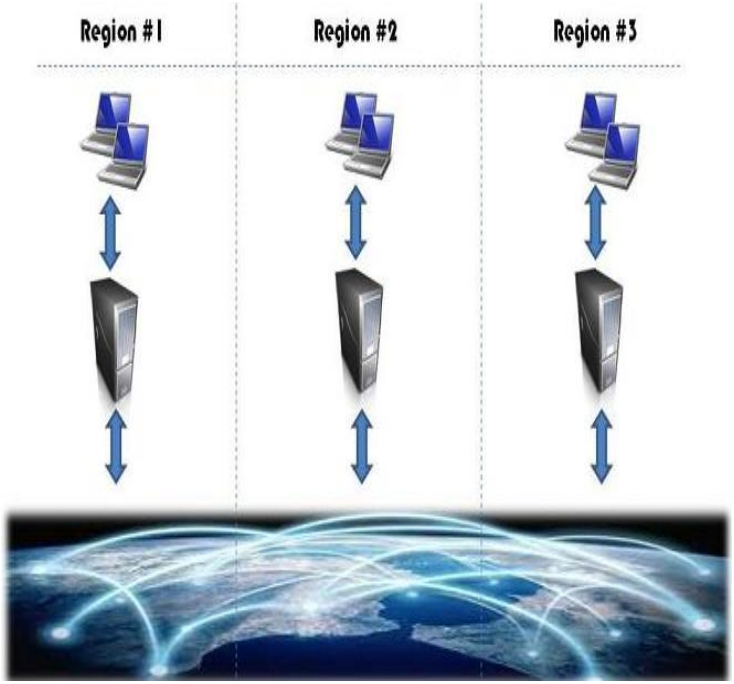
Network Architecture: The design of a network, including the hardware, software, access methods, and the protocols in use.

- **Centralized Network Management Architecture**
  - A **single management system installation** monitors the whole network.
  - This installation may consist of **one or more** servers due to hardware limitations.
  - If more than one server is used, it is considered as a centralized architecture when all servers are located at the same NOC.



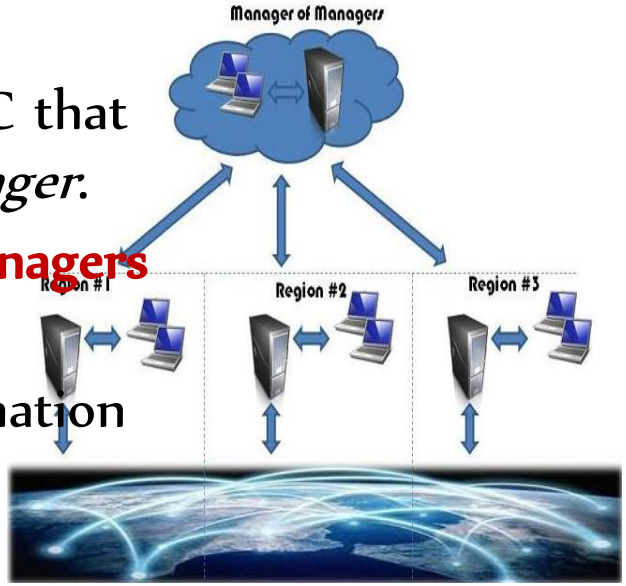
5. Computer network design and management

- **Distributed Network Management Architecture**
  - **Multiple installations of management systems** are used to monitor the whole network.
  - Each management system is installed at a NOC that is responsible to monitor a geographical or administration region / domain, i.e. it is a *Domain Manager*.



5. Computer network design and management

- **Hierarchical Network Management Architecture**
  - **Multiple installations of management systems** are used to monitor the whole network.
  - Each management system is installed at a NOC that is responsible to monitor, it is a *Domain Manager*.
  - It adds an additional layer, the **Manager of Managers (MoM)**.
  - MoM sits at a higher level and requests information from domain managers.
  - There is no communication between domain managers, information flow follows the hierarchy.
  - The hierarchy can be further expanded by adding **additional layers of MoMs** and therefore is quite scalable.



Criteria	Centralized	Distributed	Hierarchical
Reliability	Depends on Data Communications Network infrastructure (DCN), due to connectivity between regions.	Very Reliable, no single point of failure. Regions are independent.	Very Reliable and scalable. Regions are independent but also centrally monitored.
Scalability	Depends on DCN: as the network expands the DCN bandwidth between regions increases	Very Good, just add servers to increase the managed network size	Excellent, add servers to increase the managed network size and Manager of Managers for control
Flexibility	Limited, only one time-zone is possible per server, regions must follow the central region maintenance schedule	Very Flexible, can handle different time-zones; each region can schedule independent maintenance actions	Very Flexible, can handle different time-zones; each region can schedule independent maintenance actions
User Experience	Depends on DCN, as DCN performance affects client's remote access to servers	Very Good, local access to servers ensures UI speed and responsiveness	Excellent, local access to servers ensures User Interface speed and responsiveness. MoM gives end-to-end visibility
Overall	Good	Better	Best

5. Computer network design and management

- **Selecting a Logical Network Topology**
  - Identify the network segments and interconnection points between segments, size and scope of networks, and the types of required internetworking devices
  - **Preferable**: develop a layered and hierarchical design model
  - A typical hierarchical network topology includes the following three layers:
    - A **core layer** consisting of high-end routers and switches that are optimized for availability and performance
    - A **distribution layer** of routers and switches that implement network policies
    - **An access layer** that connects users via hubs, switches, and other interconnection devices

5. Computer network design and management

- **Requirements of the Network**
- Define requirements to the existing hardware, software, and telecommunications. At a minimum, you should consider the following:
  - The size of the facility (located on a single floor vs. multiple floors)
  - The number of users
  - Whether the LAN will be extended to several buildings
  - The environment (office, manufacturing, out-of-doors)
  - The current network media, if any
  - The technical competence of users
  - The amount of network traffic (initially, and anticipated for the future)
  - The level of security

5. Computer network design and management

- **Network Management**
  - **Network administrators** need tools to monitor the **functionality** of the network **devices**, the **connections** between them, and the **services** they provide. SNMP is de facto standard with RMON and BIM
- **Network Management Architecture**
  - **Network management system (NMS)**: A system that executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources that are required for network management.
  - **Network management protocol**: A protocol that facilitates the exchange of management information between the NMS and managed devices, including SNMP, MIB, and RMON.
  - **Managed devices**: A device (such as a router) managed by an NMS.
  - **Management agents**: Software, on managed devices, that collects and stores management information, including SNMP agents and RMON agents.
  - **Management information**: Data that is of interest to a device's management, usually stored in MIBs.

5. Computer network design and management

- ***Protocols and Standards***
  - **SNMP** - how management information is exchanged between network management applications and management agents
    - **Manager** – there is a trade-off between polling frequency and bandwidth usage
    - **Protocol** – SNMP is a protocol for message exchange, It uses the UDP
    - **Managed device** – A device (such as a router) managed by the manager.
    - **Management agents** – SNMP management agents reside on managed devices to collect and store a range of information about the device and its operation
    - **MIB** – a database of objects about the device. Is a collection of managed objects
    - **RMON** – allows packet and traffic patterns on LAN segments to be monitored
  - **NetFlow**
  - **CDP**
  - **Syslog**

5. Computer network design and management

- **Management Information Bases (MIB)**
  - A MIB is a collection of managed objects.
  - A MIB stores information, which is collected by the local management agent, on a managed device for later retrieval by a network management protocol.
  - Each object in a MIB has a unique identifier that network management applications use to identify and retrieve the value of the specific object.
  - The MIB has a tree-like structure in which similar objects are grouped under the same branch of the MIB tree.
  - For example, different interface counters are grouped under the MIB tree's interfaces branch.

5. Computer network design and management

- Remote Monitoring (RMON)
  - RMON is a MIB that provides support for proactive management of LAN traffic.
  - The RMON standard allows packet and traffic patterns on LAN segments to be monitored. RMON tracks the following items:
    - Number of packets
    - Packet sizes
    - Broadcasts
    - Network utilization
    - Errors and conditions, such as Ethernet collisions
    - Statistics for hosts, including errors generated by hosts, busiest hosts, and which hosts communicate with each other
  - Without RMON, a MIB could be used to check the device's network performance
  - RMON agents can reside in routers, switches, hubs, servers, hosts, or dedicated RMON probes

5. Computer network design and management

- **NetFlow**
  - Cisco NetFlow is a measurement technology that **measures flows** that pass through **Cisco** devices
  - Answers the questions of what, when, where, and how traffic is flowing in the network
  - NetFlow-collected data serves as the basis for a set of applications, including
    - Network traffic accounting
    - Usage-based network billing
    - Network planning
    - Network monitoring

5. Computer network design and management

- **Cisco Discovery Protocol** (CDP)
  - Is a Cisco-proprietary protocol that operates between Cisco devices at the data link layer.
  - CDP information is sent only between directly connected Cisco devices; a Cisco device never forwards a CDP frame.
  - CDP provides a summary of directly connected switches, routers, and other Cisco devices.

5. Computer network design and management

- **Syslog**
  - It alerts you when something goes wrong or down in your network.
  - Syslog is an excellent tool for system monitoring and is almost always included in your distribution

Level	Keyword	Description
0	emergencies	System is unusable
1	Alerts	Immediate action is needed
2	Critical	Critical conditions exist
3	Errors	Error conditions exist
4	Warnings	Warning conditions exist
5	Notification	Normal, but significant, conditions exist
6	Informational	Informational messages
7	Debugging	Debugging messages

Chapter Five
OSI Model

Data Communication and Computer Networks

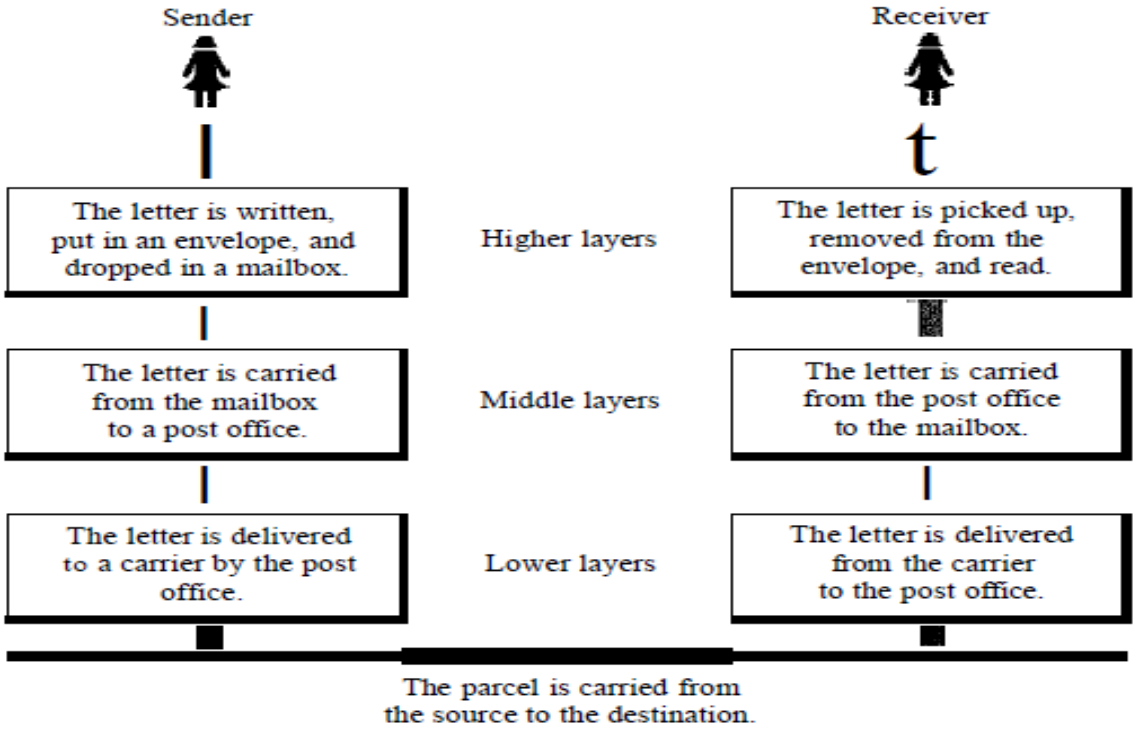
haleluyaluya@yahoo.com

Communication and Layer Architecture

- A network is a combination of hardware and software that sends data from one location to another.
- The hardware consists of the physical equipment that carries signals from one point of the network to another.
- The software consists of instruction sets that make possible the services that we expect from a network
- For example, the task of sending an e-mail from one point in the world to another can be broken into several tasks, each performed by a separate software package.
- Each software package uses the services of another software package.
- At the lowest layer, a signal, or a set of signals, is sent from the source computer to the destination computer.

Layered Tasks

- We use the concept of layers in our daily life.
  - Eg. let us consider two friends who communicate through postal mail.
- The process of sending a letter to a friend would be complex if there were no services available from the post office.



Contd.

- A communication architecture is a strategy for connecting host computers and other communicating equipment.
- It defines necessary elements for data communication between devices.
- A communication architecture, therefore, defines a standard for the communicating hosts.
- A programmer formats data in a manner defined by the communication architecture and passes it on to the communication software.
- Separating communication functions adds flexibility, for example, we do not need to modify the entire host software to include more communication devices.

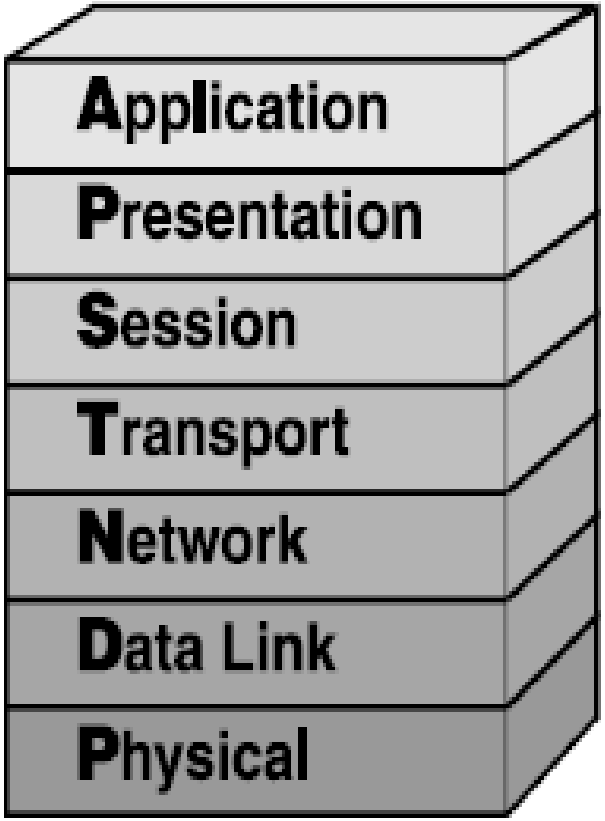
Contd.

- Layer architecture simplifies the network design.
- It is easy to debug network applications in a layered architecture network.
- The network management is easier due to the layered architecture.
- Network layers follow a set of rules, called protocol.
- The protocol defines the format of the data being exchanged, and the control and timing for the handshake between layers.

Open Systems Interconnection (OSI)

- 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.

The Seven Layers



All
People
Seem
To
Need
Data
Processing

Please
Do
Not
Throw
Susage
Pizza
Away

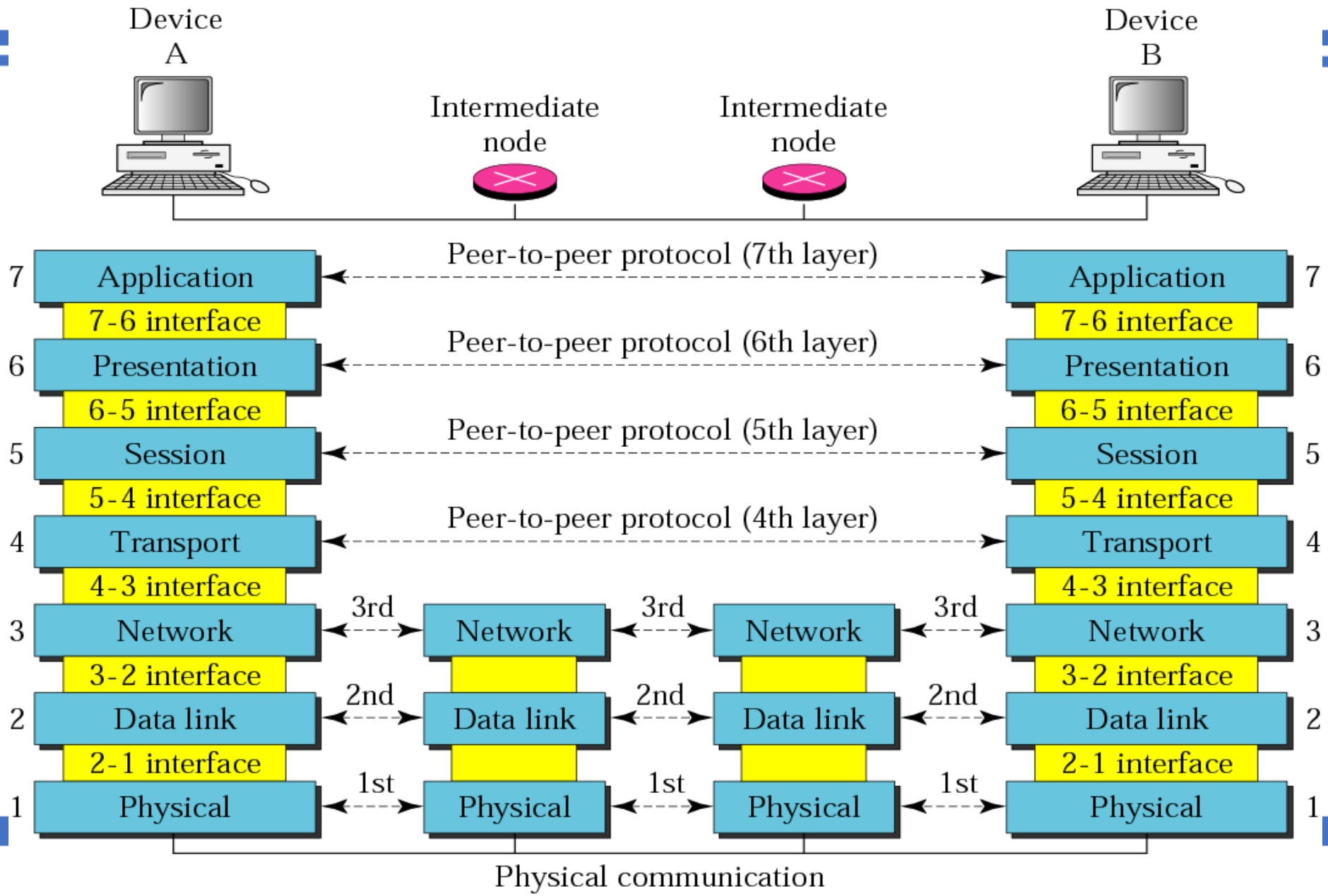
Contd.

Application	• File, print, message, database, and application services
Presentation	• Data encryption, compression, and translation services
Session	• Dialog control
Transport	• End-to-end connection
Network	• Routing
Data Link	• Framing
Physical	• Physical topology

Contd.

- The OSI model is composed of seven ordered layers:
  - Physical (layer 1),
  - Data link (layer 2),
  - Network (layer 3),
  - Transport (layer 4),
  - Session (layer 5),
  - Presentation (layer 6), and
  - Application (layer 7).
- The figure in the next slide shows the layers involved when a message is sent from device A to device B. As the message travels from A to B, it may pass through many intermediate nodes.
- These intermediate nodes usually involve only the first three bottom layers of the OSI model.

Contd.


Device A
Intermediate node
Intermediate node
Device B
Peer-to-peer protocol (7th layer)
Peer-to-peer protocol (6th layer)
Peer-to-peer protocol (5th layer)
Peer-to-peer protocol (4th layer)
7 Application
7-6 interface
6 Presentation
6-5 interface
5 Session
5-4 interface
4 Transport
4-3 interface
3 Network
3-2 interface
2 Data link
2-1 interface
1 Physical
3rd
2nd
1st
Physical communication

Contd.

- In *developing the model, the designers distilled the process of transmitting data to* its most fundamental elements.
- They identified which networking functions had related uses and collected those functions into discrete groups that became the layers.
- Each layer defines a family of functions distinct from those of the other layers.
- By defining and localizing functionality in this fashion, the designers created an architecture that is both comprehensive and flexible.
- Most importantly, the OSI model allows complete interoperability between otherwise incompatible systems.
- Within a single machine, each layer calls upon the services of the layer just below it.

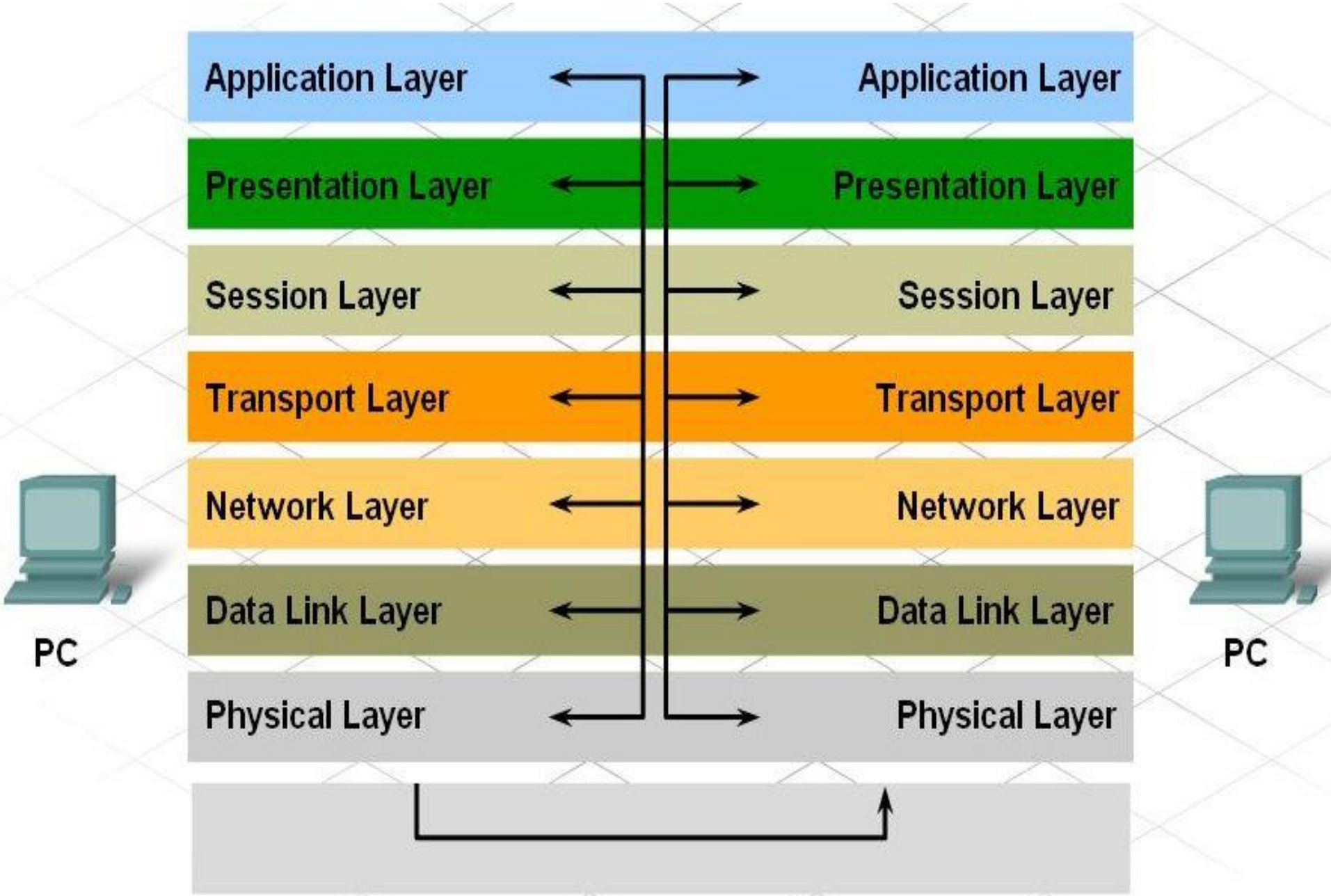
Contd.

- Layer 3, for example, uses the services provided by layer 2 and provides services for layer 4. Between machines, layer *x on one machine communicates with layer x on* another machine.
- This communication is governed by an agreed-upon series of rules and conventions called protocols.
- The processes on each machine that communicate at a given layer are called peer-to-peer processes.
- Communication between machines is therefore a peer-to-peer process using the protocols appropriate to a given layer.

Peer-to-Peer Processes

- At the physical layer, communication is direct: At the higher layers, however, communication must move down through the layers on device A, over to device B, and then back up through the layers.
- Each layer in the sending device adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it.
- At layer 1 the entire package is converted to a form that can be transmitted to the receiving device.
- At the receiving machine, the message is unwrapped layer by layer, with each process receiving and removing the data meant for it.
- For example, layer 2 removes the data meant for it, then passes the rest to layer 3. Layer 3 then removes the data meant for it and passes the rest to layer 4, and so on.

Contd.


Application Layer
Application Layer
Presentation Layer
Presentation Layer
Session Layer
Session Layer
Transport Layer
Transport Layer
Network Layer
Network Layer
Data Link Layer
Data Link Layer
Physical Layer
Physical Layer
PC
PC

Interfaces Between Layers

- The passing of the data and network information down through the layers of the sending device and back up through the layers of the receiving device is made possible by an interface between each pair of adjacent layers.
- Each interface defines the information and services a layer must provide for the layer above it.
- Well-defined interfaces and layer functions provide modularity to a network.
- As long as a layer provides the expected services to the layer above it, the specific implementation of its functions can be modified or replaced without requiring changes to the surrounding layers.

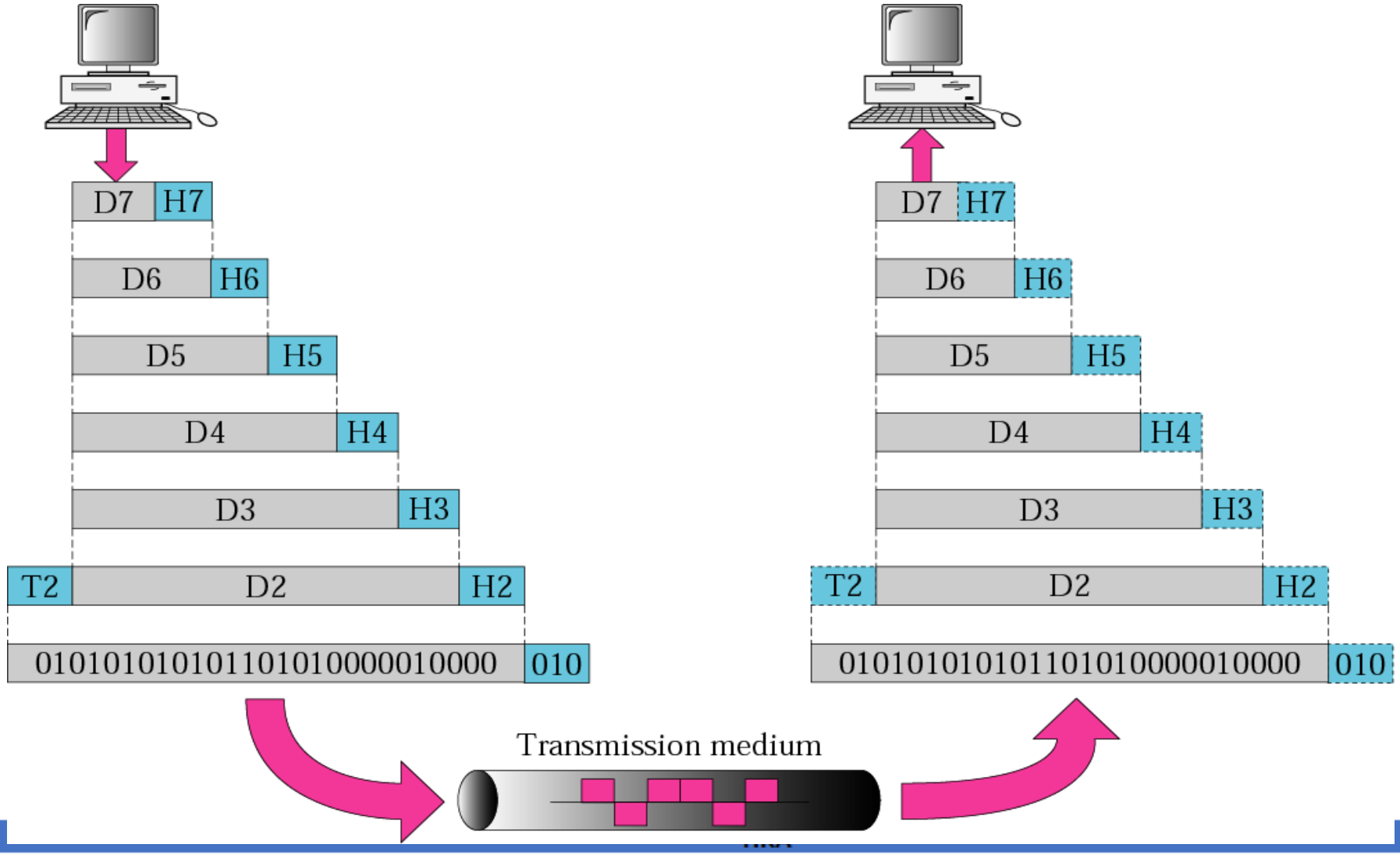
Organization of the Layers

- The seven layers can be thought of as belonging **to three subgroups**.
- Layers 1, 2, and 3 - physical, data link, and network - are the network support layers; they deal with the physical aspects of moving data from one device to another (such as electrical specifications, physical connections, physical addressing, and transport timing and reliability).
- Layers 5, 6, and 7- session, presentation, and application - can be thought of as the user support layers; they allow interoperability among unrelated software systems.
- Layer 4, the transport layer, links the two subgroups and ensures that what the lower layers have transmitted is in a form that the upper layers can use.
- The upper OSI layers are almost always implemented in software; lower layers are a combination of hardware and software, except for the physical layer, which is mostly hardware.

Contd.

- The figure shown in the next slide, gives an overall view of the OSI layers, D7 means the data unit at layer 7, D6 means the data unit at layer 6, and so on. The process starts at layer 7 (the application layer), then moves from layer to layer in descending, sequential order.
- At each layer, a header, or possibly a trailer, can be added to the data unit.
- Commonly, the trailer is added only at layer 2.
- When the formatted data unit passes through the physical layer (layer 1), it is changed into an electromagnetic signal and transported along a physical link.

An exchange using the OSI model



Contd.

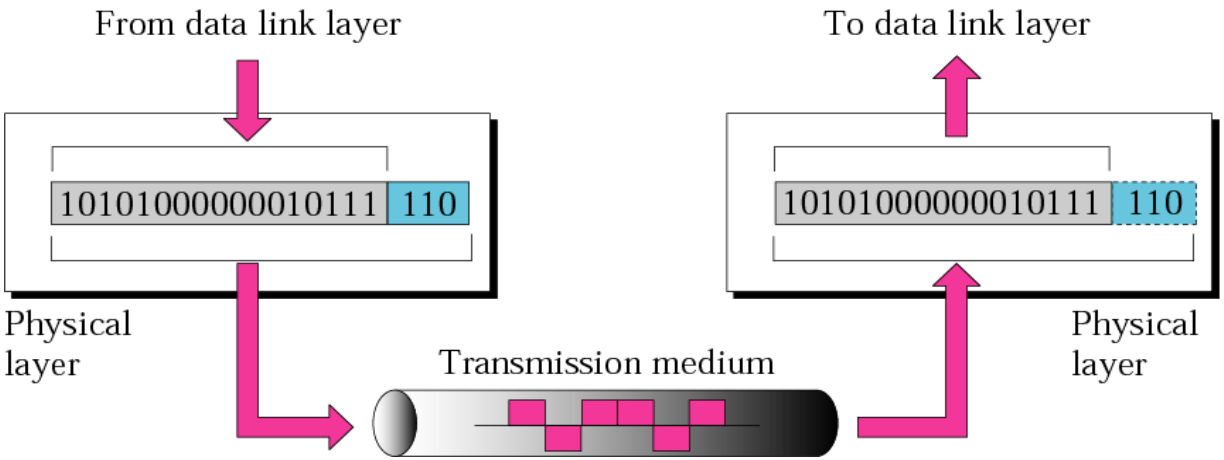
- Upon reaching its destination, the signal passes into layer 1 and is transformed back into digital form. The data units then move back up through the OSI layers.
- As each block of data reaches the next higher layer, the headers and trailers attached to it at the corresponding sending layer are removed, and actions appropriate to that layer are taken.
- By the time it reaches layer 7, the message is again in a form appropriate to the application and is made available to the recipient.

Encapsulation

- A packet (header and data) at level 7 is encapsulated in a packet at level 6. The whole packet at level 6 is encapsulated in a packet at level 5, and so on.
- In other words, the data portion of a packet at level *N - 1 carries the* whole packet (data and header and may be trailer) from level *N. The concept is called encapsulation; level N - 1 is not aware of which part of the encapsulated packet is data and which part* is the header or trailer.
- For level *N - 1, the whole packet coming from level N is treated* as one integral unit.

Physical Layer

- The physical layer coordinates the functions required to carry a bit stream over a physical medium.
- It deals with the mechanical and electrical specifications of the interface and transmission medium.
- It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur.



The physical layer is responsible for movements of individual bits from one hop (node) to the next.

The physical layer is also concerned with the following:

1. Physical characteristics of interfaces and medium. The physical layer defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.
2. Representation of bits. The physical layer data consists of a stream of bits (sequence of 0s or 1s) with no interpretation. To be transmitted, bits must be encoded into signals - electrical or optical. The physical layer defines the type of encoding (how 0s and 1s are changed to signals) (Refer chapter one).
3. Data rate. The transmission rate - the number of bits sent each second - is also defined by the physical layer. In other words, the physical layer defines the duration of a bit, which is how long it lasts.
4. Synchronization of bits. The sender and receiver not only must use the same bit rate but also must be synchronized at the bit level. In other words, the sender and the receiver clocks must be synchronized.

Contd.

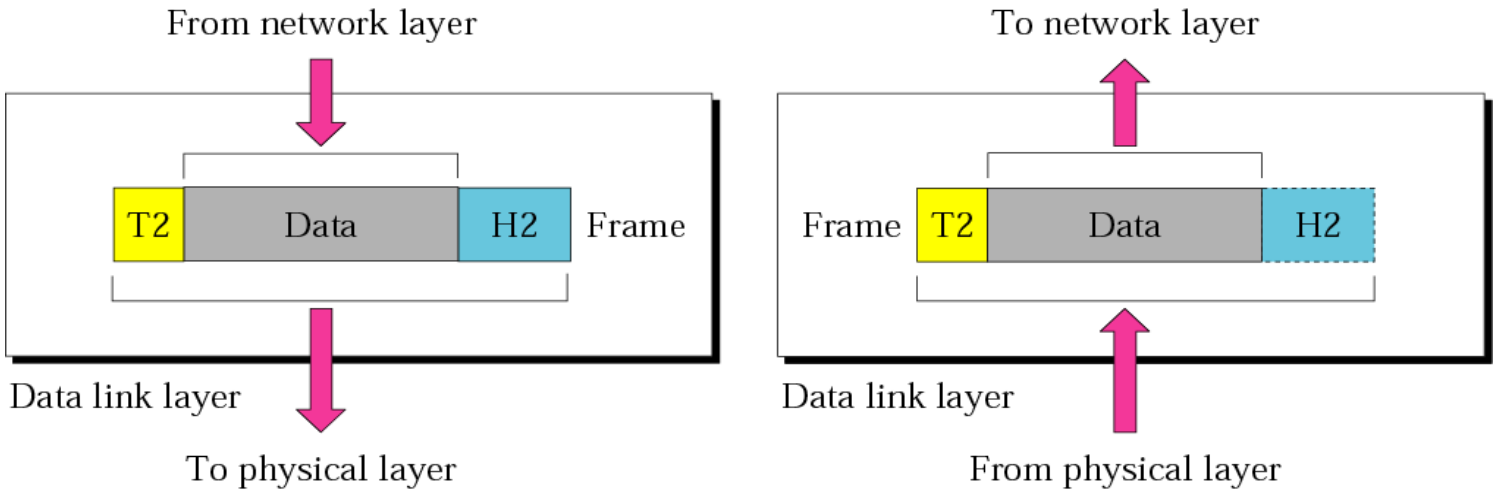
5. **Line configuration**. The physical layer is concerned with the connection of devices to the media (point – to – point or multipoint).

6. **Physical topology**. The physical topology defines how devices are connected to make a network.

6. **Transmission mode**. The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex.

Data Link Layer

- The data link layer transforms the physical layer, a raw transmission facility, to a reliable link.
- It makes the physical layer appear error-free to the upper layer (network layer). The following figure shows the relationship of the data link layer to the network and physical layers.



The data link layer is responsible for moving frames from one hop (node) to the next.

Layer 2 frame structure

<table>
<tr><td rowspan="2">Start Frame (Flag)</td><td colspan="2">Header</td><td rowspan="2">Data</td><td>Trailer</td><td rowspan="2">Stop Frame (Flag)</td></tr>
<tr><td>Address</td><td>Type/Length</td><td>FCS</td></tr>
</table>

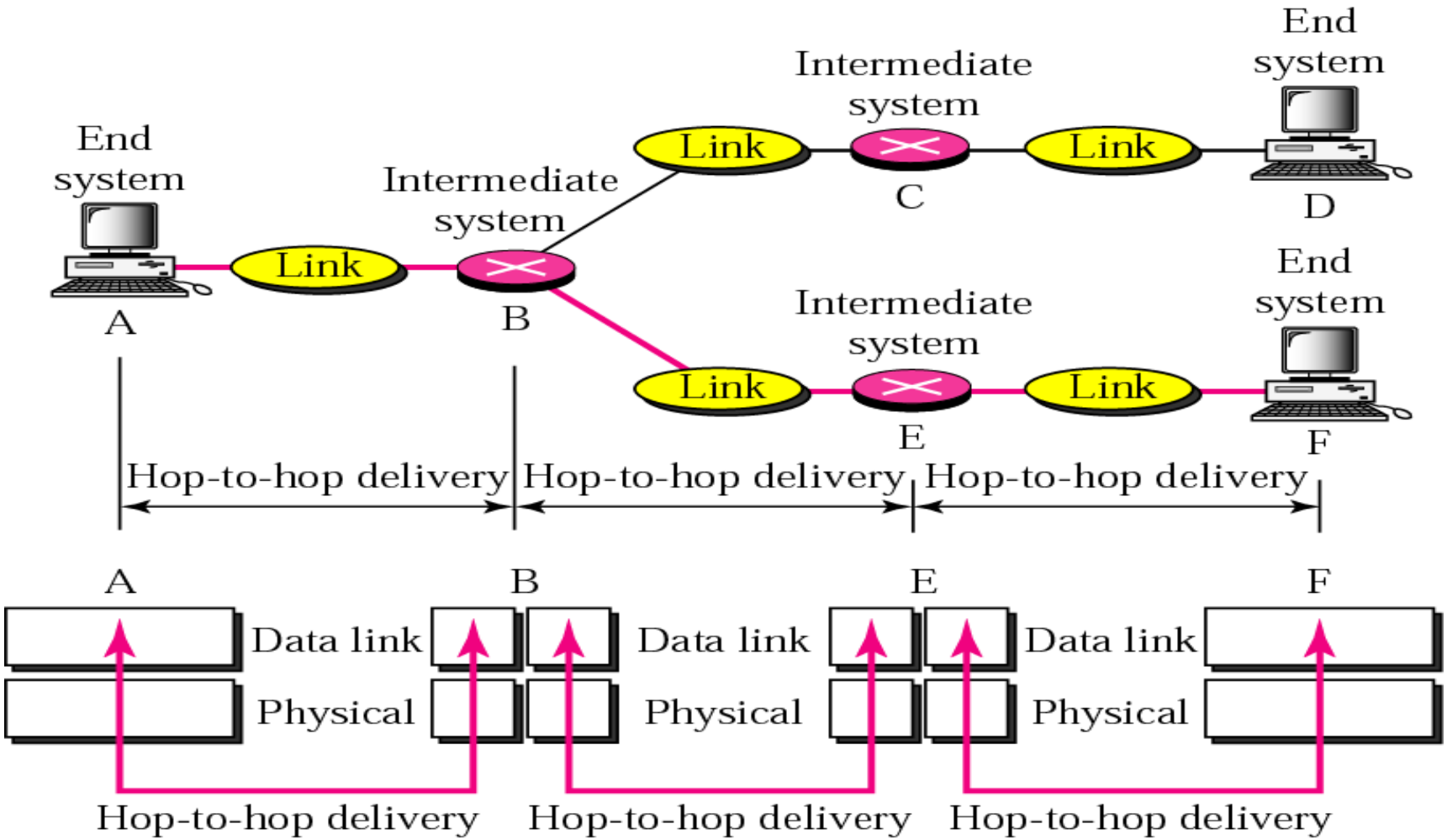
Data Link Layer Responsibilities

1. Framing. The data link layer divides the stream of bits received from the network layer into manageable data units called frames.
2. 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.
   - If the frame is intended for a system outside the sender‘s network, the receiver address is the address of the device that connects the network to the next one.

Contd.

3. 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.
4. 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.
5. 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.

Hop-to-hop (node-to-node) delivery by data link layer



Contd.

- As the figure above shows, communication at the data link layer occurs between two adjacent nodes.
  - To send data from A to F, three partial deliveries are made.
  - First, the data link layer at A sends a frame to the data link layer at B (a router).
  - Second, the data link layer at B sends a new frame to the data link layer at E.
  - Finally, the data link layer at E sends a new frame to the data link layer at F.
- Note that the frames that are exchanged between the three nodes have different values in the headers. The frame from A to B has B as the destination address and A as the source address. The frame from B to E has E as the destination address and B as the source address. The frame from E to F has F as the destination address and E as the source address. The values of the trailers can also be different if error checking includes the header of the frame.

Framing

- The data link layer, needs to pack bits into frames, so that each frame is distinguishable from another. Our postal system practices a type of framing.
- The simple act of inserting a letter into an envelope separates one piece of information from another; the envelope serves as the delimiter.
- In addition, each envelope defines the sender and receiver addresses since the postal system is a many-to-many carrier facility.
- Framing in the data link layer separates a **message** from one source to a destination, or from other messages to other destinations, by adding a sender address and a destination address.
- The destination address defines where the packet is to go; the sender address helps the recipient acknowledge the receipt.

Contd.

- NB: Addressing here is about the next node in the LAN
- Although the whole message could be packed in one frame, that is not normally done.
- One reason is that a frame can be very large, making flow and error control very inefficient.
- When a message is carried in one very large frame, even a single-bit error would require the retransmission of the whole message.
- When a message is divided into smaller frames, a single-bit error affects only that small frame.

Frames can be of fixed or variable size

1. **Fixed-Size Framing:-** In fixed-size framing, there is no need for defining the boundaries of the frames; the size itself can be used as a delimiter. An example of this type of framing is the ATM wide-area network, which uses frames of fixed size called cells.

2. **Variable-Size Framing:-** variable-size framing is prevalent in local area networks. In variable-size framing, we need a way to define the end of the frame and the beginning of the next. Historically, two approaches were used for this purpose: a character-oriented approach and a bit-oriented approach.

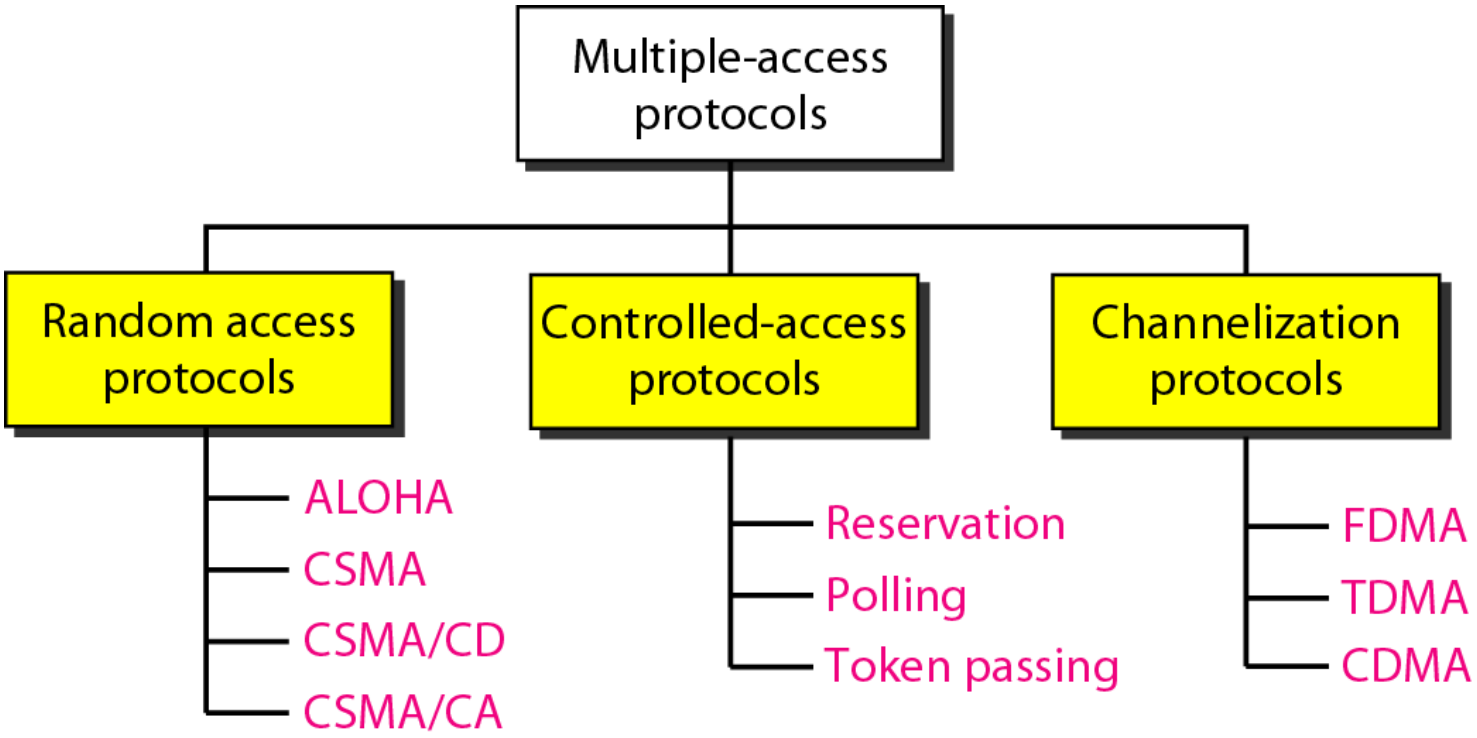
Structure of the Ethernet Frame

Preamble	SFD	Destination MAC Address	Source MAC Address	Length / Type	Encapsulated Data	FCS
7	1	6	6	2	46 to 1500	4

Media Access control

- The data link layer can further be divided in to two layers: the upper sub-layer that is responsible for flow and error control is called the logical link control (LLC) layer; the lower sub-layer that is mostly responsible for multiple access resolution is called the media access control (MAC) layer
- When nodes or stations are connected and use a common link, called a multipoint or broadcast link, we need a multiple-access protocol to coordinate access to the link. The problem of controlling the access to the medium is similar to the rules of speaking in an assembly. The procedures guarantee that the right to speak is upheld and ensure that two people do not speak at the same time, do not interrupt each other, do not monopolize the discussion, and so on.

Contd.



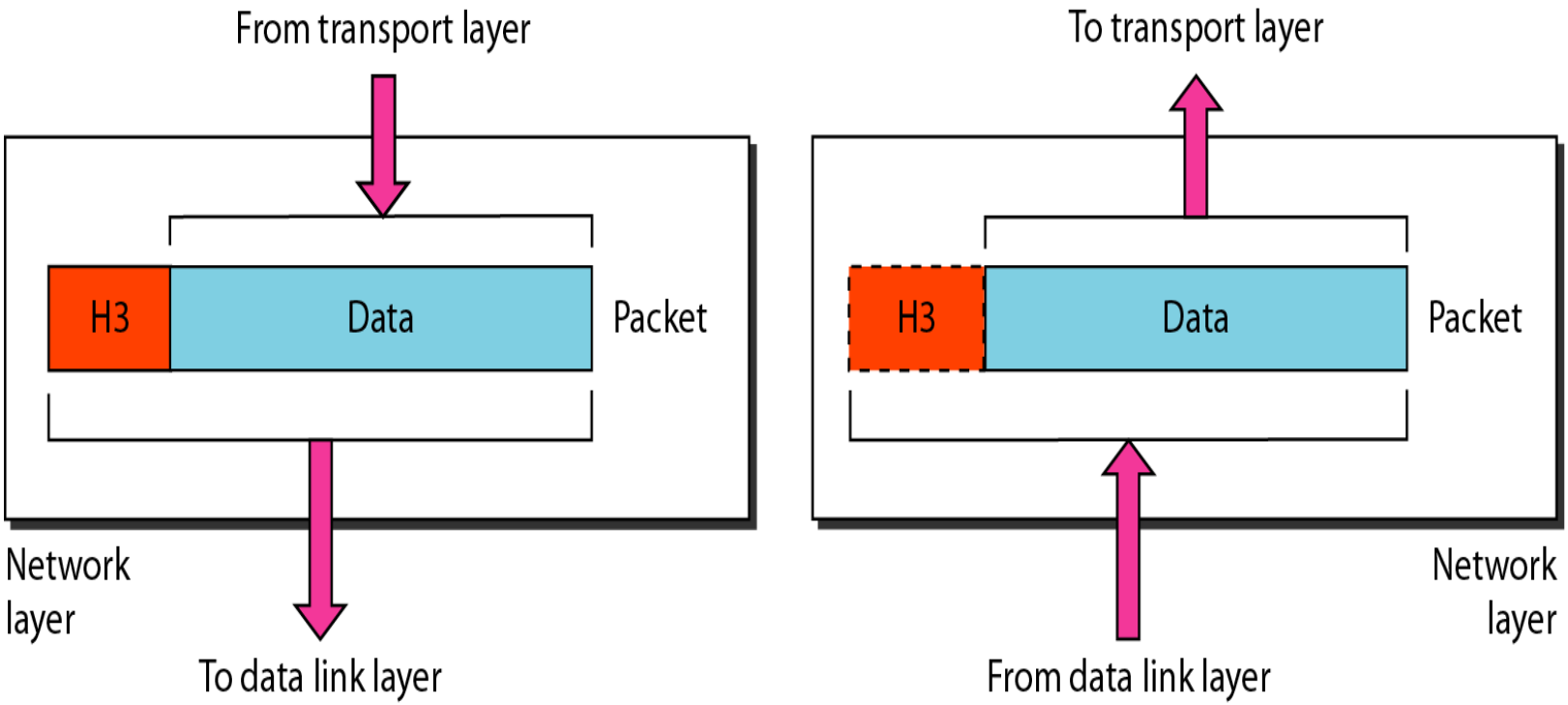
- Read about these?

Network Layer (3rd OSI Layer)

- Concerned with getting packets from source to destination.
- The network layer must know the topology of the subnet and choose appropriate paths through it.
- When source and destination are in *different networks*, the network layer must deal with these differences.
- The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks.
- Whereas the data link layer oversees the delivery of the packet between two systems on the same network, the network layer ensures that each packet gets from its point of origin to its final destination.
- If two systems are connected to the same local network, there is usually no need for a network layer. However, if the two systems are attached to different networks with connecting devices between the networks, there is often a need for the network layer to accomplish source-to-destination delivery.

Contd.

- The network layer is responsible for the delivery of individual packets from the source host to the destination host.

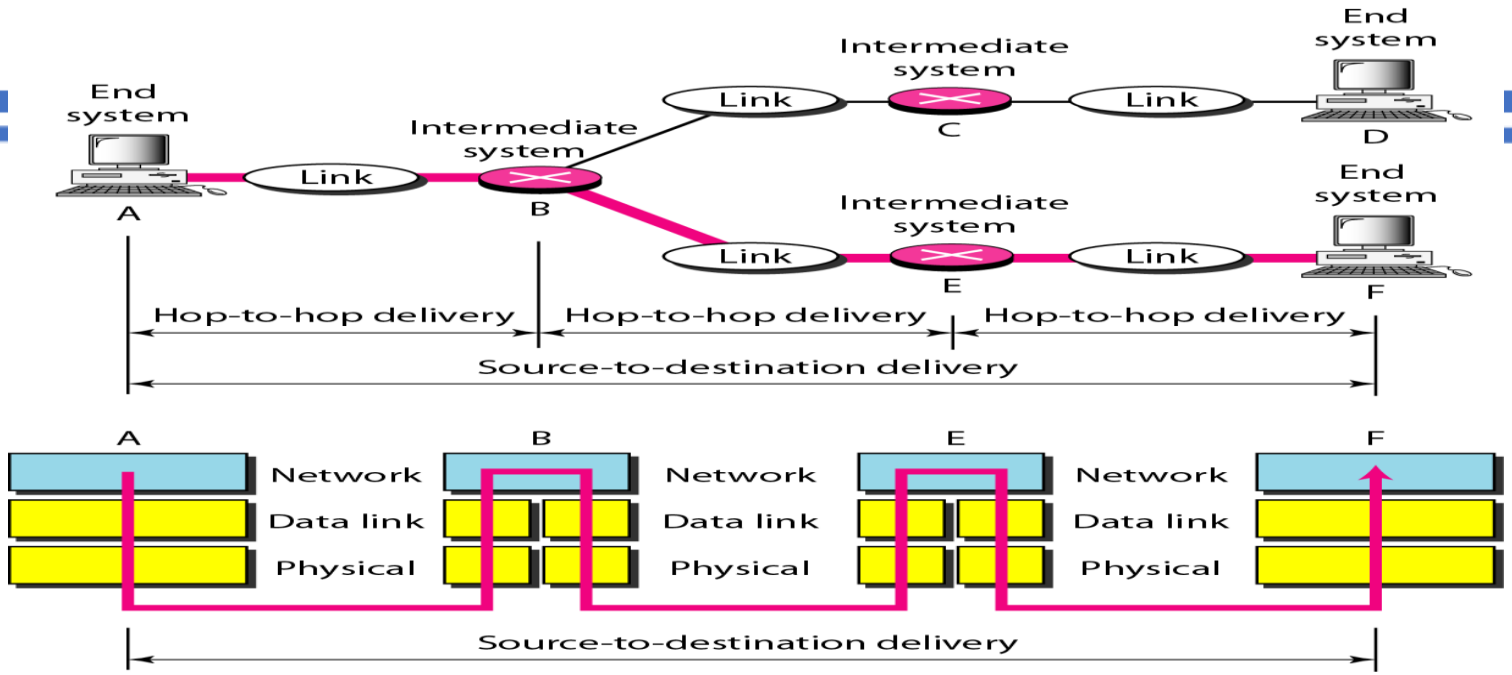


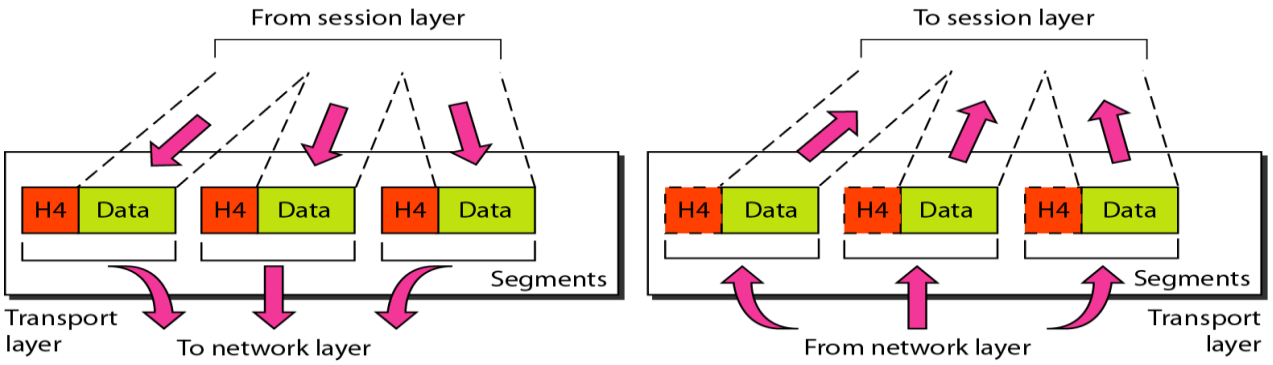
Contd.

Other responsibilities of the network layer include the following:

1. **Logical addressing:-** The physical addressing implemented by the data link layer handles the addressing problem locally.
   - If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems.
   - The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver. We discuss logical addresses later in chapter Six.
2. **Routing:-** When independent networks or links are connected to create *internetworks* (network of networks) or a large network, the connecting devices (called *routers or switches) route or switch the packets to their final destination*.
   - One of the functions of the network layer is to provide this mechanism.

Contd.


End system
A
Link
Intermediate system
B
Link
Intermediate system
C
Link
End system
D
Link
Intermediate system
E
Link
End system
F
Hop-to-hop delivery
Hop-to-hop delivery
Hop-to-hop delivery
Source-to-destination delivery
A
B
E
F
Network
Data link
Physical
Network
Data link
Physical
Network
Data link
Physical
Source-to-destination delivery


From session layer
H4
Data
H4
Data
H4
Data
Segments
Transport layer
To network layer
To session layer
H4
Data
H4
Data
H4
Data
Segments
From network layer
Transport layer

Transport layer (4th OSI layer)

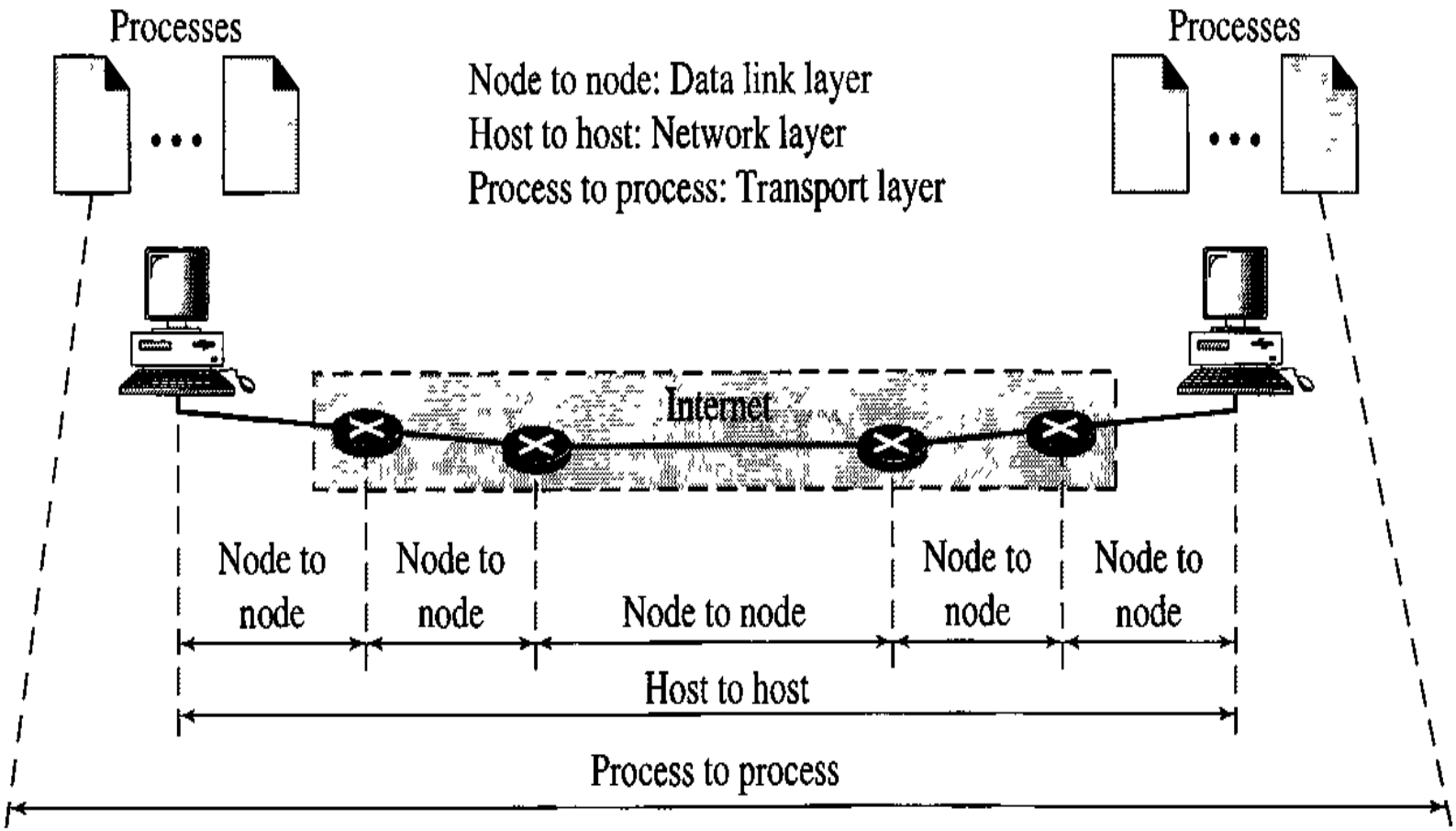
- The transport layer is responsible for process-to-process delivery of the entire message.
- A process is an application program running on a host.
- Whereas the network layer oversees source-to-destination delivery of individual packets, it does not recognize any relationship between those packets.
- The network layer treats each packet independently, as though each piece belonged to a separate message, whether or not it does.
- The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level.

Major functions of the transport layer

- The Transport layer encompasses these functions:

1. **Enables multiple applications to communicate over the network at the same time on a single device**
2. **Ensures that, if required, all the data is received reliably and in order by the correct application**
3. **Employs error handling mechanisms**

Contd.


Processes
Processes
Node to node: Data link layer
Host to host: Network layer
Process to process: Transport layer
Internet
Node to node
Node to node
Node to node
Node to node
Node to node
Host to host
Process to process

Responsibilities of the transport layer include the following:

1. **Service-point addressing:-** Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process on the other. The transport layer header must therefore include a type of address called a **service-point address** *(or* **port address***).*

   - *The network layer gets each packet to the correct computer*; the transport layer gets the entire message to the correct process on that computer.

2. **Segmentation and reassembly:-** A message is divided into transmittable segments, with each segment containing a sequence number.

   - These numbers enable the transport layer to **reassemble** the message correctly upon arriving at the destination and to identify and replace packets that were **lost** in transmission.

Contd.

3. Flow control:- Like the data link layer, the transport layer is responsible for flow control.
   - However, flow control at this layer is performed end to end rather than across a single link.
4. Error control:- Like the data link layer, the transport layer is responsible for error control.
   - However, error control at this layer is performed process-to-process rather than across a single link.
   - The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication).
   - Error correction is usually achieved through retransmission.

Contd.

5. Connection control:- The transport layer can be either connectionless or connection-oriented.

A. **Connectionless** transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine.

B. **Connection-oriented** transport layer makes a connection with the transport layer at the destination machine first before delivering the packets.

- After all the data are transferred, the connection is terminated.

Process-to-Process Delivery

- As a revision, the data link layer is responsible for delivery of frames between two neighboring nodes over a link. This is called *node-to-node delivery*.
- *The network layer is responsible for* delivery of datagrams between two hosts. This is called *host-to-host delivery*.
- *Communication* on the Internet is not defined as the exchange of data between two nodes or between two hosts. Real communication takes place between two processes (application programs). We need process-to-process delivery.
- However, at any moment, **several processes may be running on the source host and several on the destination host. To complete the delivery, we need a mechanism to deliver data from one of these processes running on the source host to the corresponding process running on the destination host**.
- The transport layer is responsible for *process-to-process* delivery-the delivery of a packet, part of a message, from one process to another.
  - Two processes communicate in a client/server relationship.

Transport layer addressing

- Whenever we need to deliver something to one specific destination among many, we need an address.
- At the data link layer, we need a MAC address to choose one node among several nodes if the connection is not point-to-point.
  - A frame in the data link layer needs a destination MAC address for delivery and a source address for the next node's reply.
- At the network layer, we need an IP address to choose one host among millions.
  - A datagram in the network layer needs a destination IP address for delivery and a source IP address for the destination's reply.

Contd.

- At the transport layer, we need a transport layer address, called a port number, to choose among multiple processes running on the destination host.
  - The destination port number is needed for delivery; the source port number is needed for the reply.
  - In the Internet model, the port numbers are 16-bit integers between 0 and 65,535.
  - The client program defines itself with a port number, chosen randomly by the transport layer software running on the client host. This is the ephemeral (temporal) port number. (next slide, more on port number)

Connectionless Versus Connection-Oriented Service

- A transport layer protocol can either be connectionless or connection-oriented.

1. *Connectionless Service*
   - In a connectionless service, the packets are sent from one party to another with no need for connection establishment or connection release.
   - The packets are not numbered; they may be delayed or lost or may arrive out of sequence. There is no acknowledgment either.
   - UDP is connectionless.
2. Connection-Oriented *Service*

   a. In a connection-oriented service, a connection is first established between the sender and the receiver.

   b. Data are transferred. At the end, the connection is released.

   c. TCP and SCTP are connection-oriented protocols.

Reliable Versus Unreliable

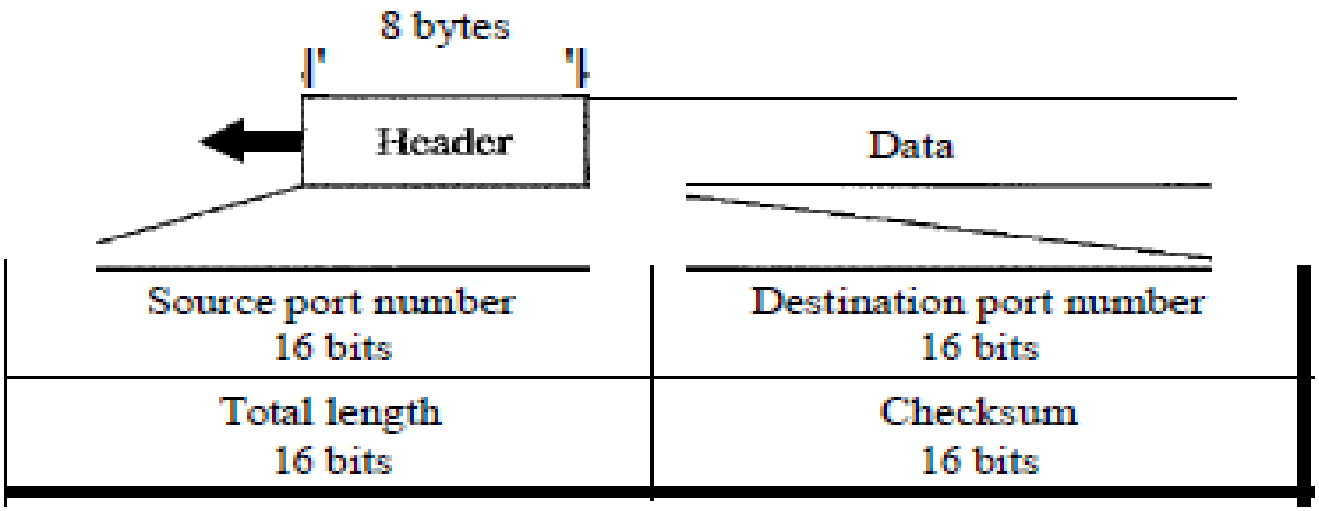
- The transport layer service can be reliable or unreliable.
- If the application layer program needs **reliability**, we use a reliable transport layer protocol by implementing flow and error control at the transport layer.
  - This means a slower and more complex service.
- On the other hand, if the application program does not need **reliability** because it uses its own flow and error control mechanism or it needs fast service or the nature of the service does not demand flow and error control (real-time applications), then an unreliable protocol can be used.
- In the Internet, there are two common different transport layer protocols, as we have already mentioned. UDP is connectionless and unreliable; TCP and SCTP are connection-oriented and reliable protocols. These three can respond to the demands of the application layer programs.

USER DATAGRAM PROTOCOL (UDP)

- The User Datagram Protocol (UDP) is called a **connectionless**, unreliable transport protocol.
  - It does not add anything to the services of IP except to provide process-to-process communication.
- Also, it performs very limited error checking. If UDP is so powerless, why would a process want to use it?
- With the disadvantages come some advantages. UDP is a very simple protocol using a minimum of overhead.
  - If a process wants to send a small message and does not care much about reliability, it can use UDP.
  - Sending a small message by using UDP takes much less interaction between the sender and receiver than using TCP or SCTP.

Contd.

- UDP packets, called user datagrams, have a fixed-size header of 8 bytes
- Source port number. This is the port number used by the process running on the source host.
- Destination port number. This is the port number used by the process running on the destination host.
- Length. This is a 16-bit field that defines the total length of the user datagram, header plus data.



Contd.

- UDP does not perform:
  - Flow control
  - Error control
  - Connection control
    - All these functions are done by the processes (application layer programs) using UDP
  - UDP is **not capable of segmenting and reassembling frames** and **does not implement sequence numbers**
- But UDP, like TCP, performs:
  - Service point addressing
- UDP can transmit only **small portions of data** at a time because it is not capable of segmenting and reassembling frames and does not implement sequence numbers

Use of UDP

1. UDP is suitable for a process that requires simple request-response communication with little concern for flow and error control. It is not usually used for a process such as FTP that needs to send bulk data
2. UDP is suitable for a process with internal flow and error control mechanisms. For example, the Trivial File Transfer Protocol (TFTP) process includes flow and error control. It can easily use UDP.
3. UDP is a suitable transport protocol for multicasting. Multicasting capability is embedded in the UDP software but not in the TCP software.
4. UDP is used for management processes such as SNMP.
5. UDP is used for some route updating protocols such as Routing Information Protocol (RIP).

Transmission Control Protocol (TCP)

- TCP, like UDP, is a process-to-process (program-to-program) protocol.
- TCP, therefore, like UDP, uses port numbers. Unlike UDP, TCP is a connection-oriented protocol; it creates a virtual connection between two TCPs to send data.
- In addition, TCP uses flow and error control mechanisms at the transport level.
- In brief, TCP is called a *connection-oriented, reliable transport protocol. It adds* connection-oriented and reliability features to the services of IP.

TCP Services

1. ***Process-to-Process Communication:-*** Like UDP, TCP provides process-to-process communication using port numbers.
2. ***Stream Delivery Service***
3. ***Full-Duplex Communication***
4. ***Connection-Oriented Service***
5. ***Reliable Service***

Stream Delivery Service

- TCP, unlike UDP, is a stream-oriented protocol.
- In UDP, a process (an application program) sends messages, with predefined boundaries, to UDP for delivery.
- UDP adds its own header to each of these messages and delivers them to IP for transmission.
- Each message from the process is called a user datagram and becomes, eventually, one IP datagram.
- Neither IP nor UDP recognizes any relationship between the datagrams.
- Each application using UDP must send small data to fit into one user datagram as it is. (UDP does not segment/reassemble)

Contd.

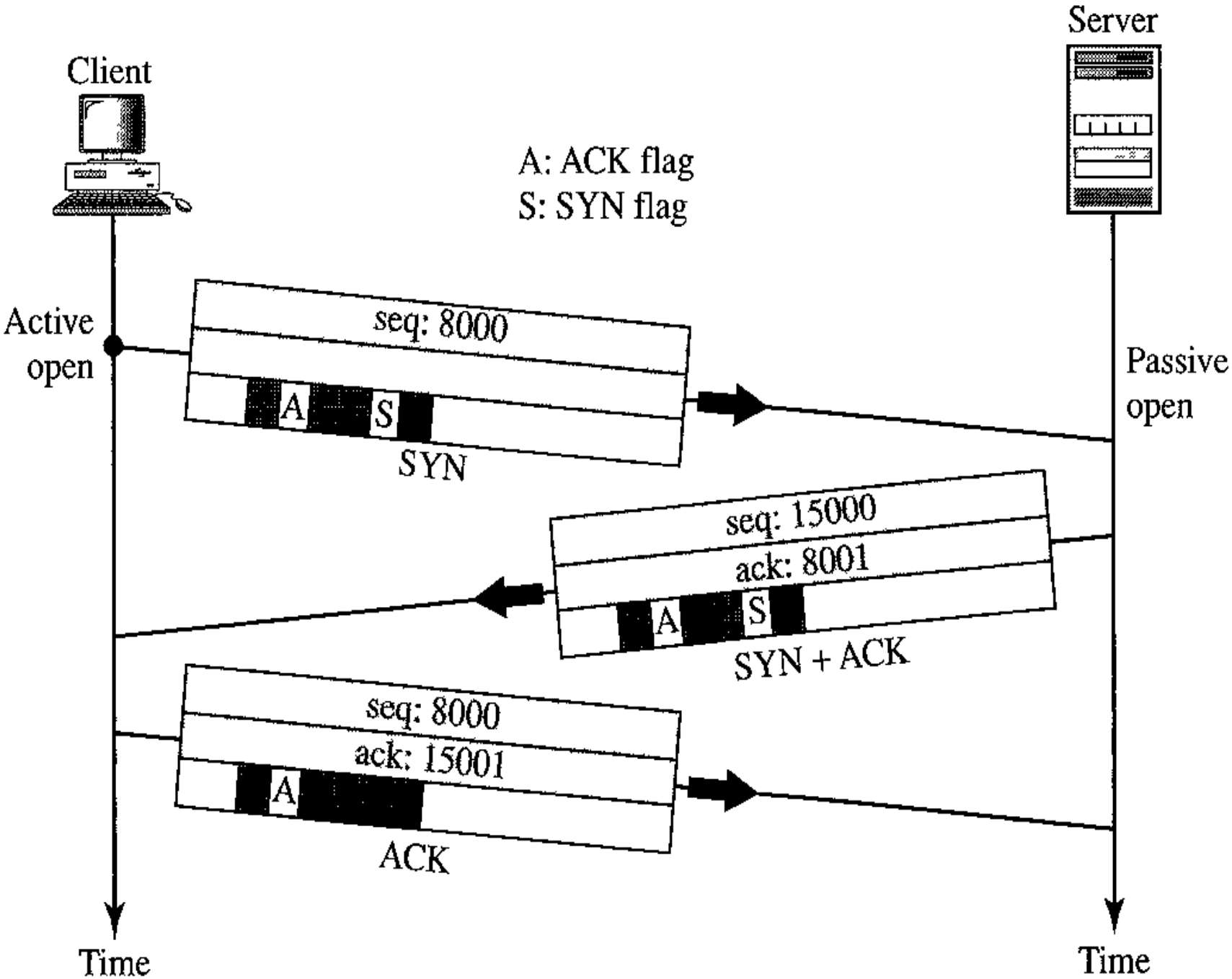
- TCP, on the other hand, allows the sending process to deliver data as a stream of bytes and allows the receiving process to obtain data as a stream of bytes.
- TCP creates an environment in which the two processes seem to be connected by an imaginary "tube" that carries their data across the Internet.
- The sending process produces (writes to) the stream of bytes, and the receiving process consumes (reads from) them (Fig. next slide)

Connection-Oriented Service

- TCP, unlike UDP, is a connection-oriented protocol.
- When a process at site A wants to send and receive data from another process at site B, the following occurs:

  1. **The two TCPs establish a connection between them.**
  2. **Data are exchanged in both directions.**
  3. **The connection is terminated.**

- Note that this is a virtual connection, not a physical connection. The TCP segment is encapsulated in an IP datagram and can be sent out of order, or lost, or corrupted, and then resent.
- Each may use a different path to reach the destination. There is no physical connection.
- TCP creates a stream-oriented environment in which it accepts the responsibility of delivering the bytes in order to the other site.


Client
Server
A: ACK flag
S: SYN flag
Active open
Passive open
seq: 8000
A
S
SYN
seq: 15000
ack: 8001
A
S
SYN + ACK
seq: 8000
ack: 15001
A
ACK
Time
Time

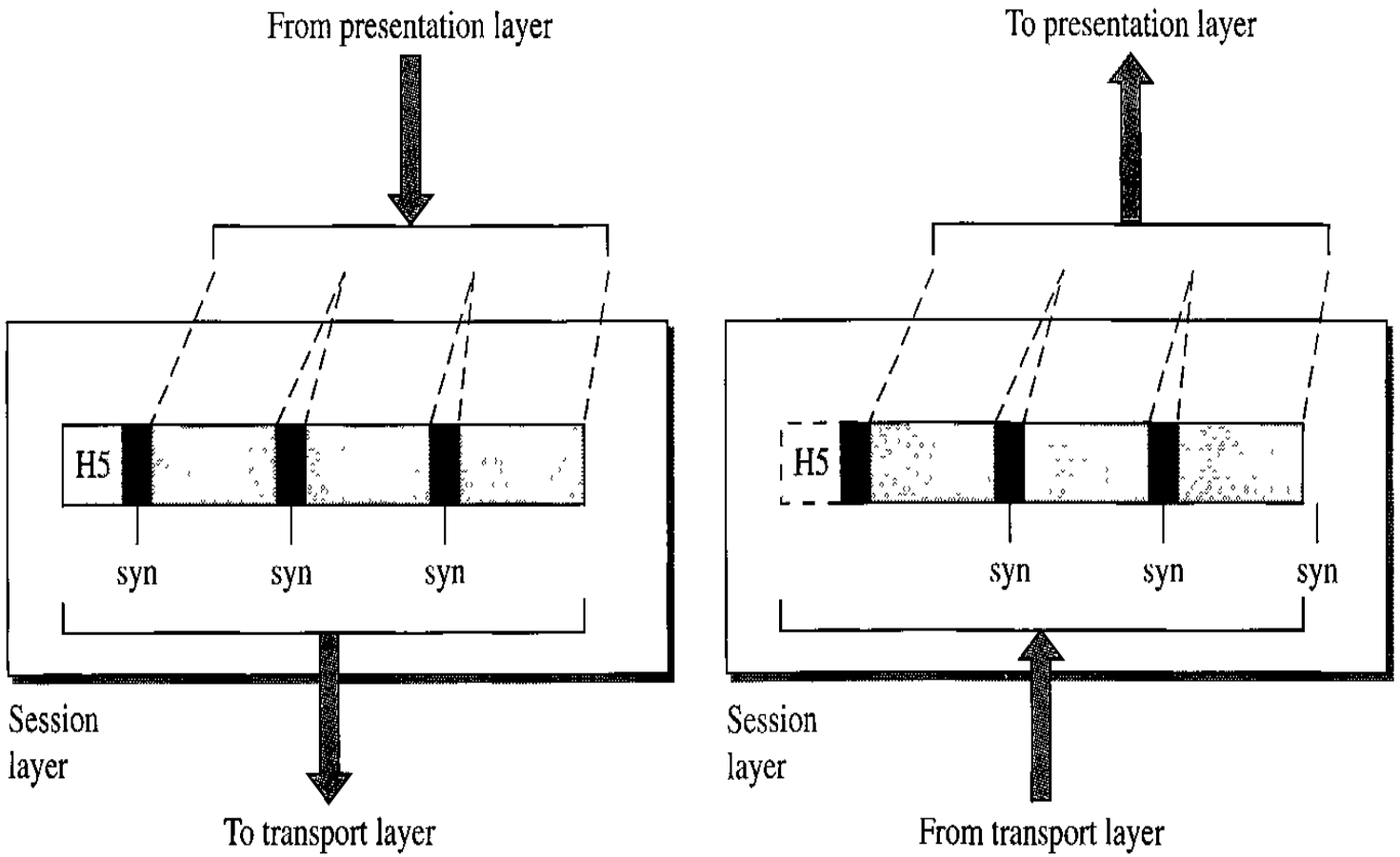
Session Layer

- The lowest four layers of the OSI model (Physical, Data link, Network, and Transport) provide the means for the reliable exchange of data and provide a fast data service.
- For example, a remote terminal access application might require a half-duplex dialogue.
- A transaction-processing application might require checkpoints in the data-transfer stream to permit backup and recovery.
- A message processing application might require the ability to interrupt a dialogue in order to prepare a new portion of a message and later to resume the dialogue where it was left off.

Contd.

- All these capabilities could be embedded in specific applications at layer 7.
- However, because these types of dialogue-structuring tools have widespread applicability, it makes sense to organize them into a separate layer: the session layer.
- The session layer provides the mechanism for controlling the dialogue between applications in end systems.
- In many cases, there will be little or no need for session-layer services, but for some applications, such services are used.

Contd.


From presentation layer
H5
syn
syn
syn
Session
layer
To transport layer
To presentation layer
H5
syn
syn
syn
Session
layer
From transport layer

The key services provided by the session layer include

- The primary job of session layer protocols is to provide the means necessary to **set up, manage, and end sessions**

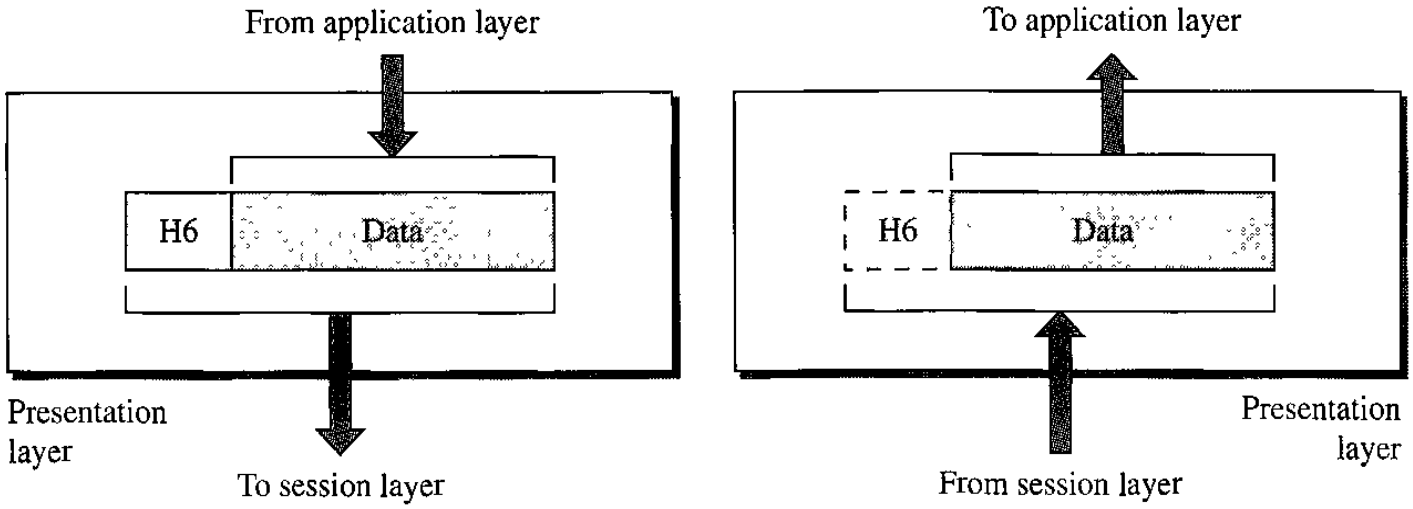
1. **Dialogue discipline.** This can be two-way simultaneous (full duplex) or two way alternate (half duplex) communication between processes.
2. **Grouping.** The flow of data can be marked to define groups of data.
   - For example, if a retail store is transmitting sales data to a regional office, the data can be marked to indicate the end of the sales data for each department; this would signal the host computer to finalize running totals for that department and start new running counts for the next department.

Contd.

3. **Recovery.** The session layer can provide a check pointing mechanism, so that if a failure of some sort occurs between checkpoints, the session entity can retransmit all data since the last checkpoint, as in the example shown below:
   - 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.

Presentation Layer

- The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.



Specific responsibilities of the presentation layer :

1. 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.
   - The presentation layer at the sender changes the information from its **sender-dependent format into a common format**.
   - The presentation layer at the receiving machine changes the common format into its receiver-dependent format.

Contd.

2. 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.
3. 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.

Application Layer

- The application layer enables the user, whether human or software, to access the network.
- It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.
- Application layer is where users actually communicate to the computer.
  - Take the case of Internet Explorer (IE).
- It is also responsible for identifying and establishing the availability of the intended communication partner

Contd.

- Typical application layer protocols
  - Domain Name System (DNS)
  - Hyper Text Transfer Protocol (HTTP)
  - File Transfer Protocol (FTP)
  - E-mail (SMTP,POP,IMAP)

1. Domain Name System (DNS)

- Thousands of servers, installed in many different locations, provide the services we use over the Internet.
- Each of these servers is assigned a unique IP address
- It would be impossible to remember all of the IP addresses

Contd.

- DNS provides a way for hosts to use this name to request the IP address of a specific server.
- DNS names are registered and organized on the Internet within specific high level groups, or domains.
  - Some of the most common high level domains on the Internet are .com, .edu, and .net
- A DNS server contains a table that associates hostnames in a domain with corresponding IP addresses

2. Web client and web server

- A web client first receives the IP address of a web server from DNS server
- Then the client browser uses that IP address and port 80 to request web services
- This request is sent to the server using the Hypertext Transfer Protocol (HTTP)
- The information content of a web page is encoded using specialized 'mark-up' languages.
  - E.g. HTML (Hypertext Mark-up Language)
- Many different web servers and web clients from many different manufactures work together seamlessly because of HTTP and HTML

3. File Transfer Protocol (FTP)

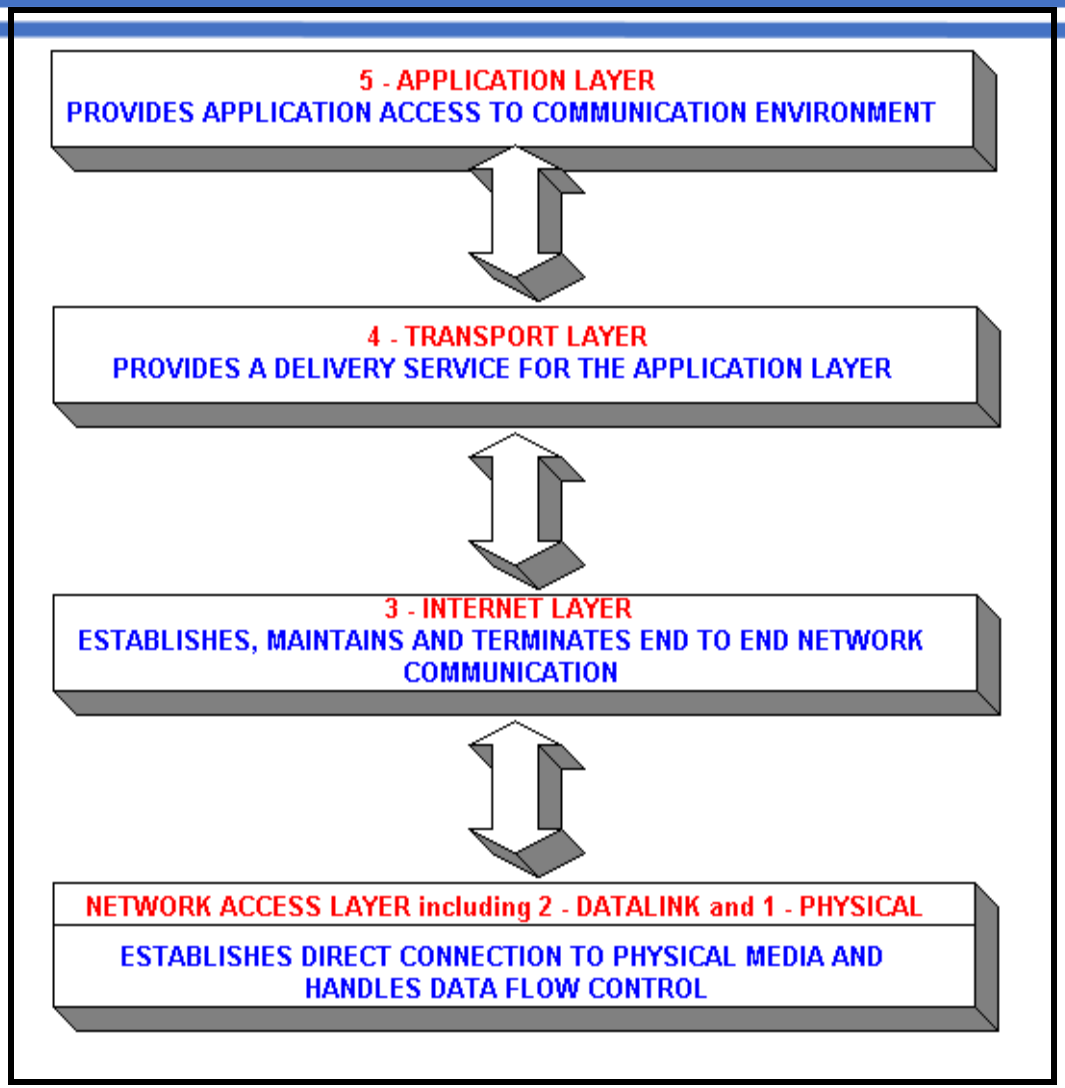
- FTP is another common service used across the Internet that allows users to transfer files
- A host running FTP client software can access an FTP server to perform various file management functions including file uploads and downloads
- FTP service uses two different ports to communicate between client and server
  - Requests to begin an FTP session are sent to the server using destination port 21.
  - Once the session is opened, the server will change to port 20 to transfer the data files
- FTP client software is built into computer operating systems and into most web browsers

4. Email Servers (SMTP, POP3 and IMAP4)

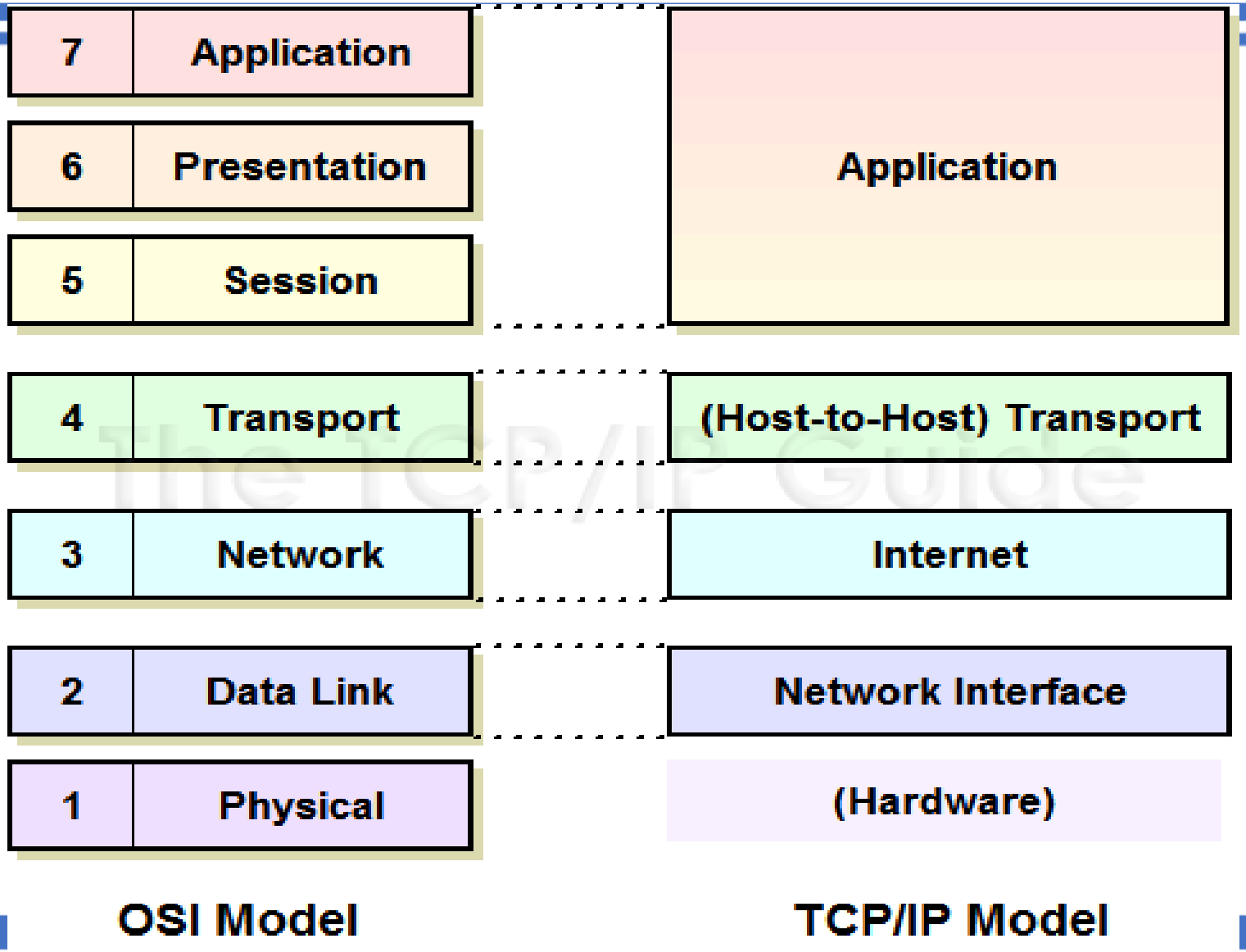
- Each mail server receives and stores mail for users who have mailboxes configured on the mail server
- Each user with a mailbox must then use an email client to access the mail server and read these messages
  - Mailboxes are identified by the format: **user@company.domain**
- Three application protocols used in processing email include
  1. **Simple Mail Transfer Protocol (SMTP):-** to send mail from client to server or server to server
  2. **Post Office Protocol (POP3):-** to download email from server to client, and the server deletes the mail
  3. **Internet Message Access Protocol (IMAP4):-** to download email from server to client, and the server does not delete (keeps) the mail

TCP/IP Network Model Layers

- As with the OSI model, the TCP/IP suite uses a layered model.
- TCP/IP model has four or five - depending on who you talk to and which books you read!
- Some people call it a four layer suite - **Application**, **Transport**, **Internet** and **Network Access**, others split the **Network Access** layer into its **Physical** and **Datalink** components.

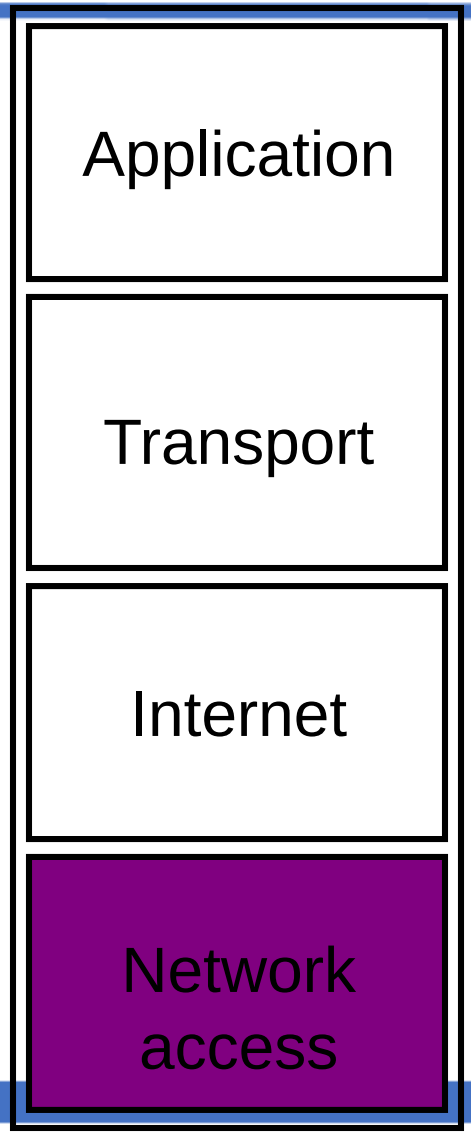


OSI Model Vs. TCP/IP Model Layers



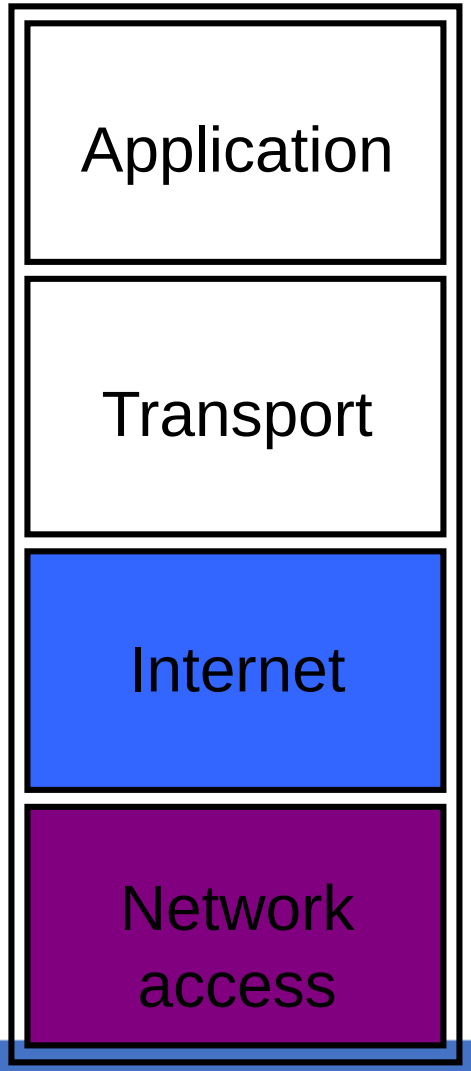
The TCP/IP Guide

TCP/IP Layers- What does each layer do?



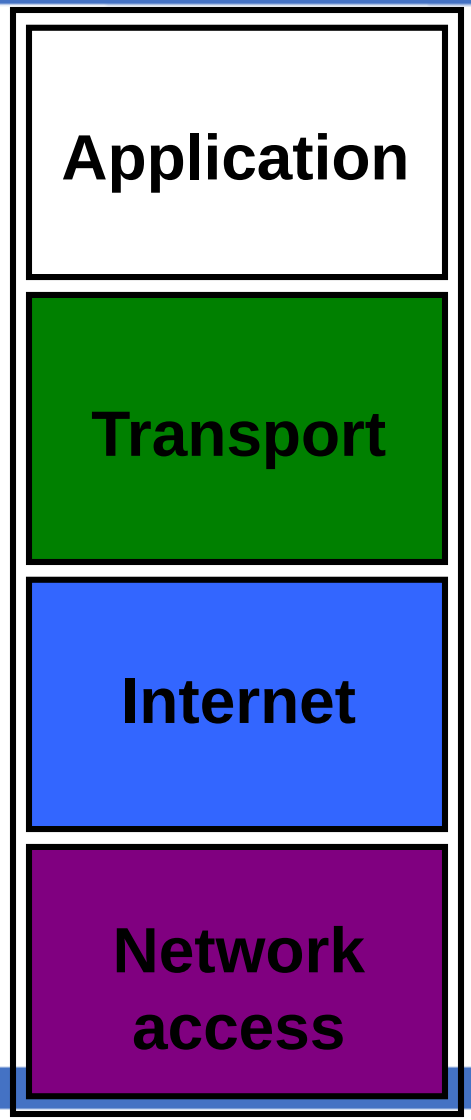
- Network access layer is the combination of data link and physical layers and it deals with pure hardware issues (wires, satellite links, network interface cards, etc.)
- Access methods such as **CSMA/CD** (carrier sensed multiple access with collision detection)
- Ethernet exists at the network access layer - its hardware operates at the physical layer and its medium access control method (CSMA/CD) operates at the data link layer.

TCP/IP Layers- What does each layer do?



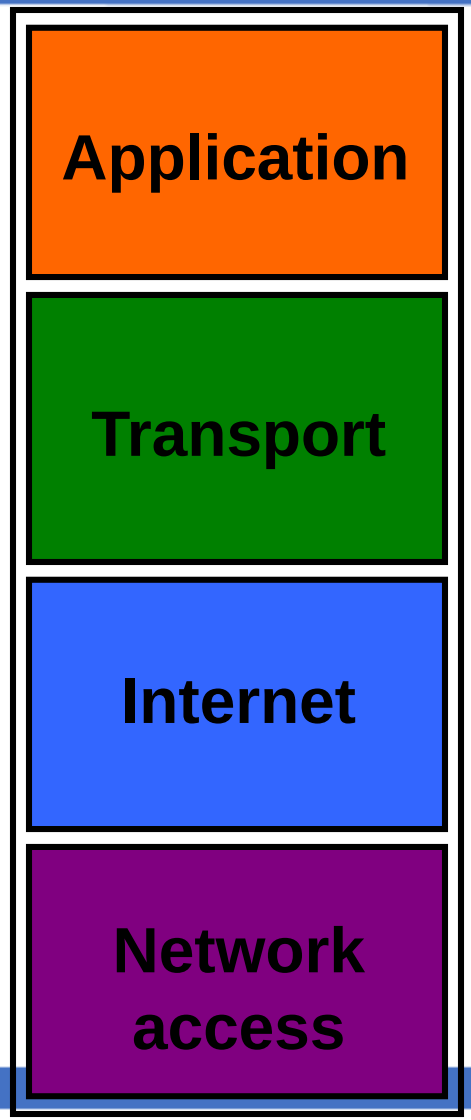
- The Internet layer is responsible for the routing and delivery of data across networks.
- It allows communication across networks of the same and different types and carries out translations to deal with dissimilar data addressing schemes.
- IP (Internet Protocol) and ARP (Address Resolution Protocol) are both to be found at the Internet layer.

TCP/IP Layers- What does each layer do?



- The Transport layer is similar to the OSI transport model, but with elements of the OSI session layer functionality.
- The two protocols found at the transport layer are:
  A. TCP (Transmission Control Protocol): reliable, connection-oriented protocol that provides error checking and flow control through a virtual link that it establishes and finally terminates. Examples include FTP and Email
  B. UDP (User Datagram Protocol): unreliable, connectionless protocol that not error check or offer any flow control. Examples include SNMP

TCP/IP Layers- What does each layer do?



- The Application layer is broadly equivalent to the application, presentation and session layers of the OSI model.
- It gives an application access to the communication environment.
- Some examples: FTP, HTTP, SMTP

?

Debre Markos University
Institute of Technology
Information Technology Academy Program

Course Title: Data Communication and Computer Networks ()

Chapter: Three

Transmission Medias

Transmission medium

- The transmission medium is the physical **path** between transmitter and receiver in a data transmission system.
- Transmission media are actually located **below** the physical layer of the OSI model
- Types of Transmission media (path):
  - **Guided**: the waves are guided along a solid medium, such as TP, Coaxial, and Optical fiber.
    - this form of transmission is usually referred to as wired transmission.
  - **UnGuided**: The atmosphere and outer space are used to trnamit data;
    - This form of transmission is usually referred to as wireless transmission.

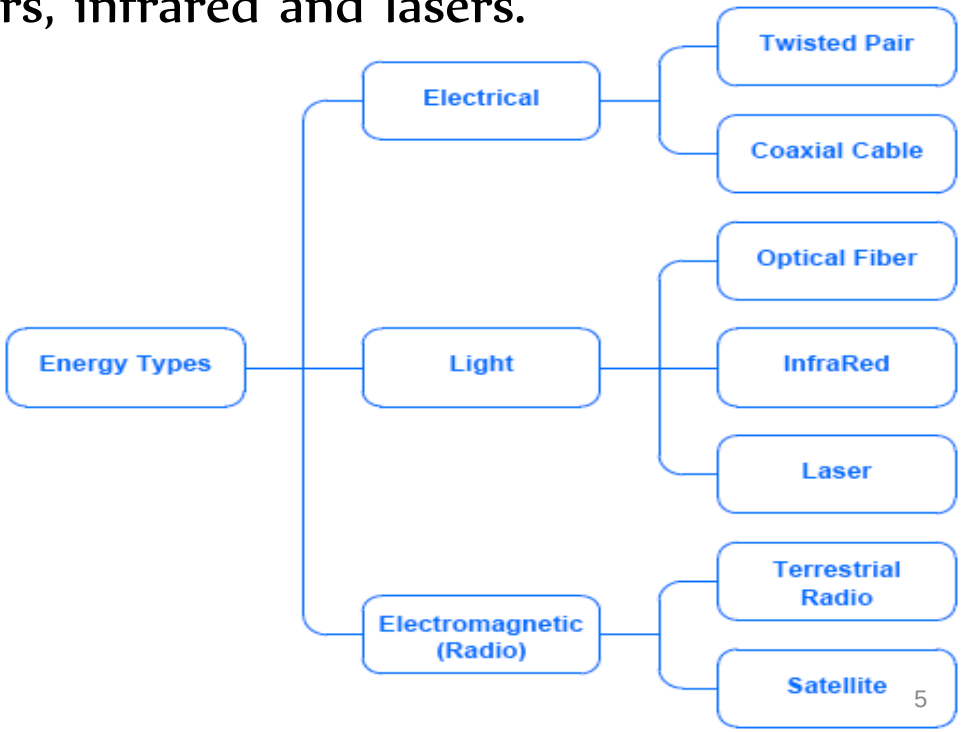
- In considering the design of data transmission systems, a key concern, generally, is data rate and distance: the greater the data rate and distance, the better.
- A number of design factors - determine the **data rate** and **distance**:

Contd.

- **Some of the design factors**
  - **Bandwidth:-** the greater the bandwidth of a signal, the higher the data rate that can be achieved.
  - **Transmission impairments:-** Impairments, such as attenuation, limit the distance. For guided media, twisted pair generally suffer much impairment then coaxial cable, then optical fiber.
  - **Interference:-** overlapping frequency bands. it is also a problem for unguided media, and guided media.
  - **A Number of receivers:-** A guided medium can be used to construct a point-to-point link or a shared link with multiple attachments. If multiple attachments, each attachment introduces some attenuation and distortion on the line, limiting distance and/or data rate.

Contd.

- Types of Transmission Medium (**energy**):
  - ***Electrical Energy*** is used on wires (TP and Coaxial),
  - ***Radio Frequency Transmission*** is used for wireless(Terrestrial Radio and Satellite),
  - ***Light*** is used for optical fibers, infrared and lasers.

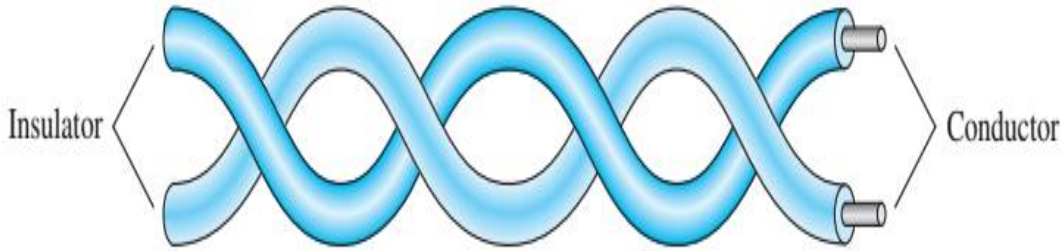


GUIDED TRANSMSSION MEDIA

- Provide a conduit/pipe from one device to another:
  - twisted-pair cable, coaxial cable, and fiber-optic cable.
- The signal is directed & contained by the physical limits of the medium.
  - Metallic (copper) conductors
    - Twisted-pair and coaxial cable use electric current.
  - Glass or Plastic
    - Optical fiber use light.

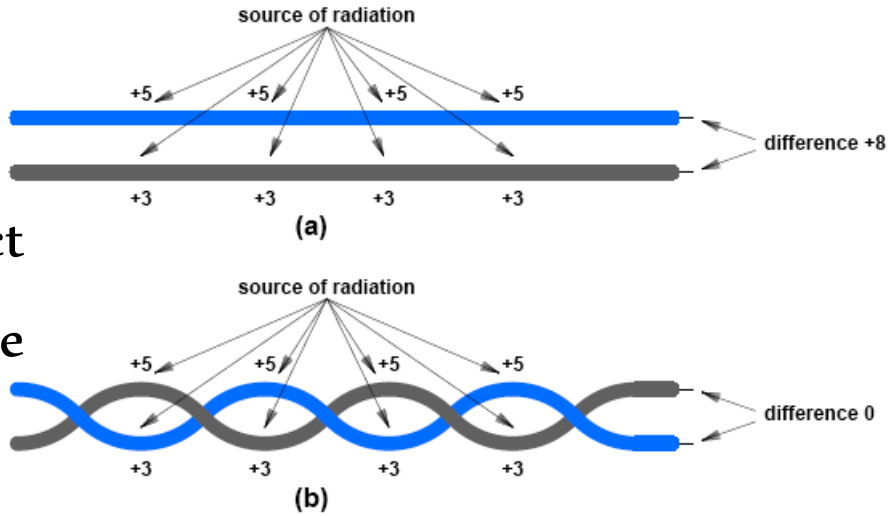
Twisted-Pair Cable (TP)

- A TP consists of two conductors (normally copper), each with its own **plastic insulation**, **twisted together**



- **One of the wires** is used to carry signals to the **receiver**, and the **other** is used only as a **ground reference**.
- The receiver uses the difference between the two.
- **interference** (noise) and **crosstalk** may affect both wires and create **unwanted signals**.

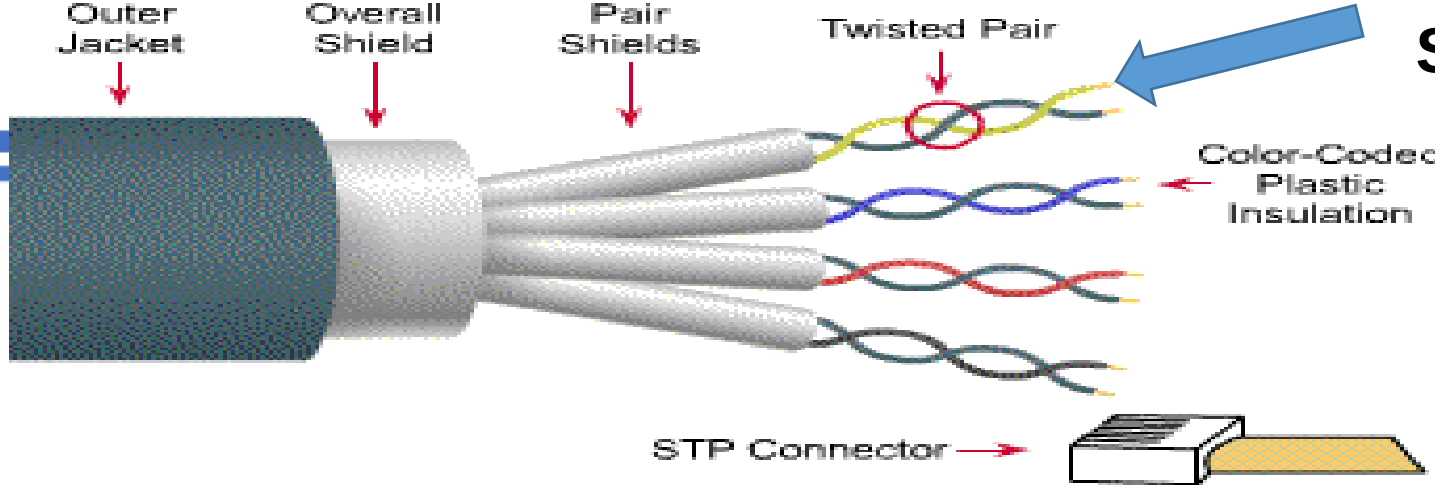
Contd.



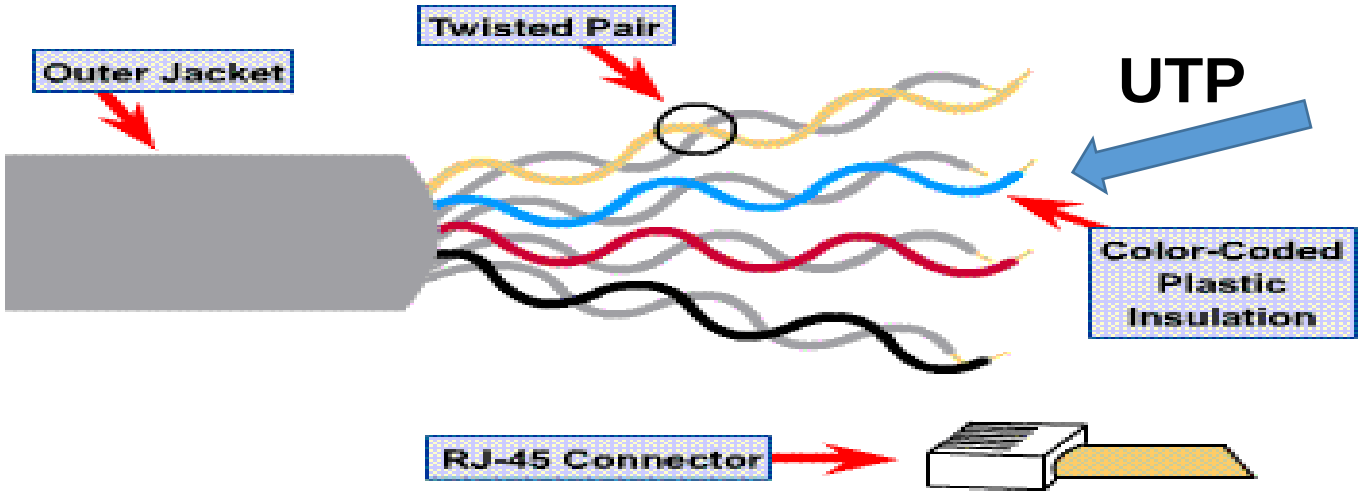
- If the two wires are parallel, the effect of these unwanted signals is not the same
  - Crosstalk,
  - Electromagnetic interference (EMI),
  - Radio frequency interference (RFI).
- **By twisting the pairs, a balance is maintained.** b/cs both wires are equally affected
  - i.e when the receiver, which calculates the difference between the two, receives no **unwanted signals**. The unwanted signals are **mostly canceled out.**
- The **number of twists per unit of length** (e.g., inch) has some effect on the **quality of the cable**.

Types of Twisted-Pair Cable

- Types of twisted-pair cable
  - Unshielded Twisted-Pair Cable
  - Shielded Twisted-Pair Cable
- unshielded twisted-pair (UTP)- most common.
  - IBM has also produced a version of twisted-pair cable for its use called shielded twisted-pair (STP).
- STP cable has a metal foil or braided mesh covering that encases each pair of insulated conductors.
  - Metal casing improves the **quality** of cable by preventing the penetration of noise or crosstalk, But bulkier and more expensive.
- STP is seldom used outside of IBM.



- Speed and throughput: 10-100 Mbps
- Cost per node: Moderately expensive
- Media and connector size: Medium to Large
- Maximum cable length: 100m (short)



- Speed and throughput: 10-100 Mbps
- Cost per node: Least Expensive
- Media and connector size: Small
- Maximum cable length: 100m (short)

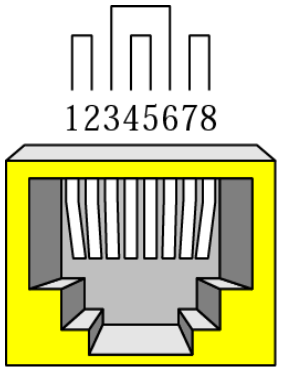
UTP Categories

- The Electronic Industries Association (EIA) has developed standards to classify unshielded twisted-pair cable into **seven categories**.
- Categories are determined by cable quality, with **1** as the lowest and **7** as the highest.
- Each EIA category is suitable for specific uses.

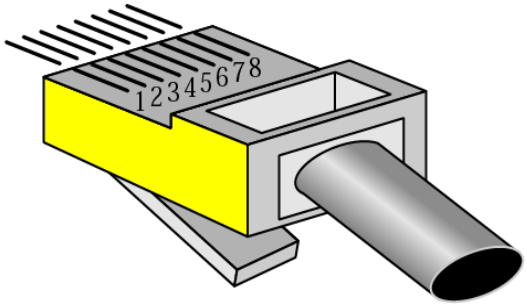
Category	*Specification*	*Data Rate (Mbps)*	*Use*
1	Unshielded twisted-pair used in telephone	< 0.1	Telephone
2	Unshielded twisted-pair originally used in T-lines	2	T-llines
3	Improved CAT 2 used in LANs	10	LANs
4	Improved CAT 3 used in Token Ring networks	20	LANs
5	Cable wire is normally 24 AWG with a jacket and outside sheath	100	LANs
SE	An extension to category 5 that includes extra features to minimize the crosstalk and electromagnetic interference	125	LANs
6	A new category with matched components coming from the same manufacturer. The cable must be tested at a 200-Mbps data rate.	200	LANs
7	Sometimes called SSTP (shielded screen twisted-pair). Each pair is individually wrapped in a helical metallic foil followed by a metallic foil shield in addition to the outside sheath. The shield decreases the effect of crosstalk: and increases the data rate.	600	LANs

Connectors

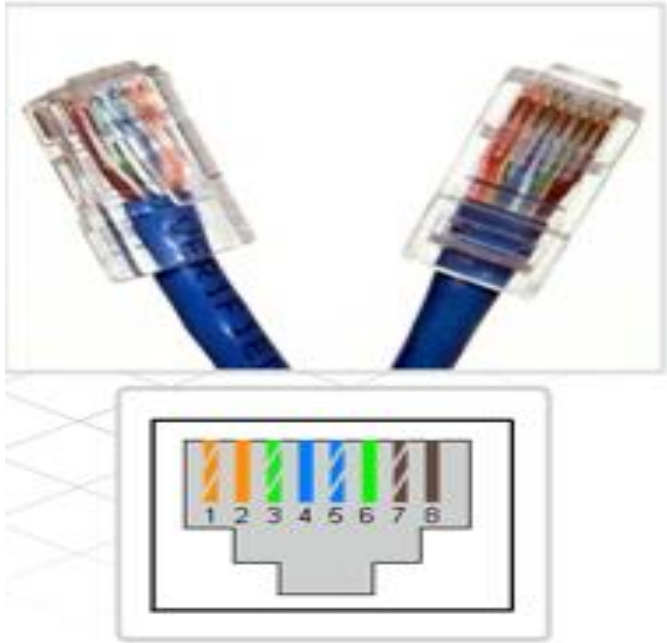
- The most common UTP connector is **RJ45** (RJ stands for registered jack).
- The RJ45 is a keyed connector, meaning the connector can be inserted in only one way.



RJ-45 Female



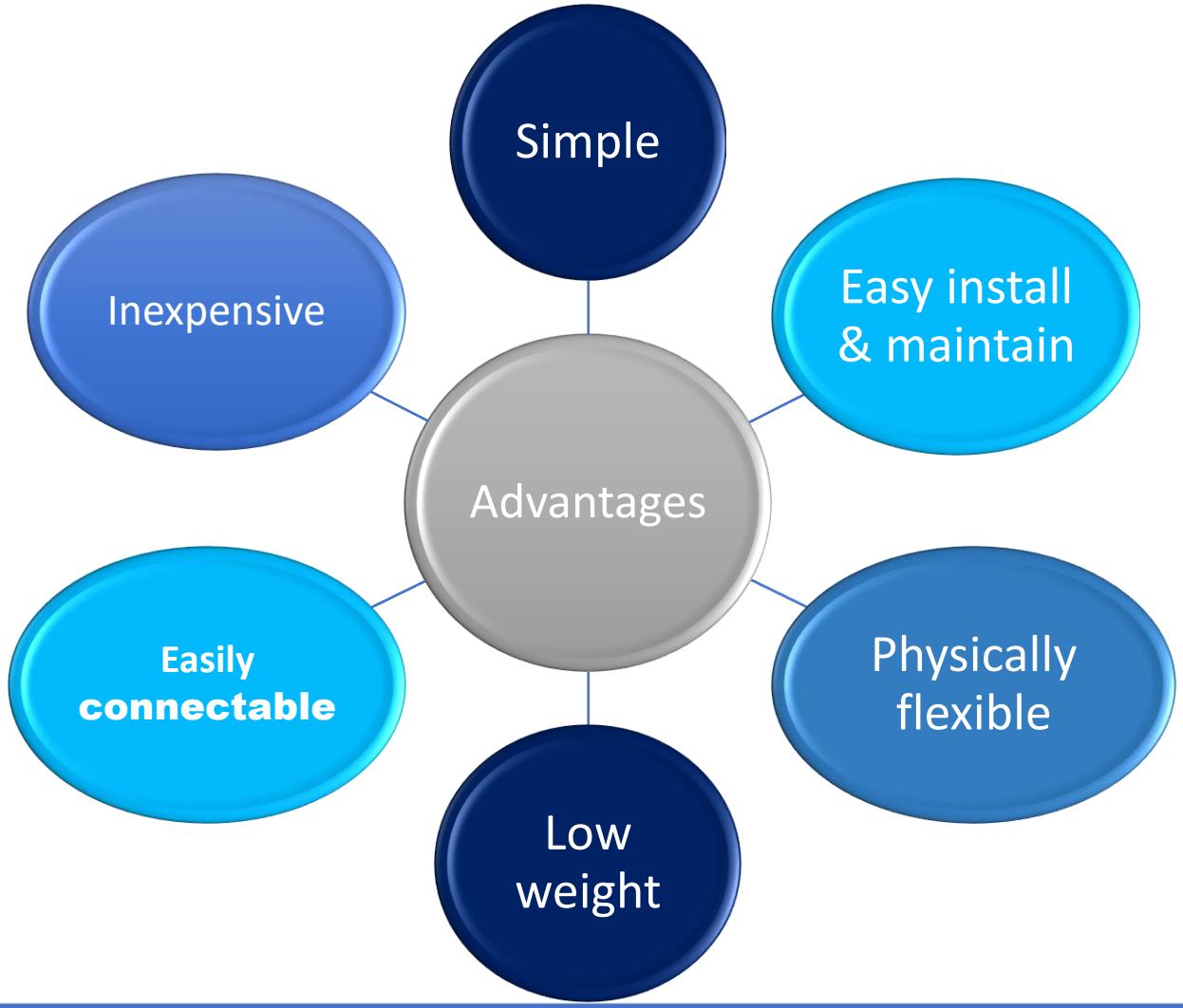
RJ-45 Male



Twisted-pair cable Applications

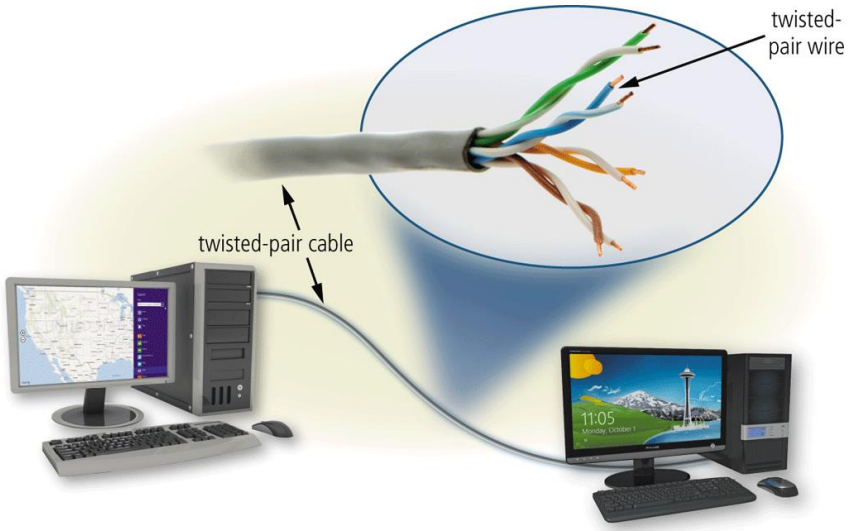
- Most common medium
  - Within buildings
  - For **telephones lines** to provide voice and data channels.
    - The **DSL lines** that are used by the telephone companies to provide high data rate connections also use the high-bandwidth capability of unshielded twisted-pair cables.
  - **Local area networks**, such as 10Base-T and 100Base-T, also used UTP cables.

Advantages


Simple
Inexpensive
Easy install & maintain
Advantages
Easily connectable
Physically flexible
Low weight

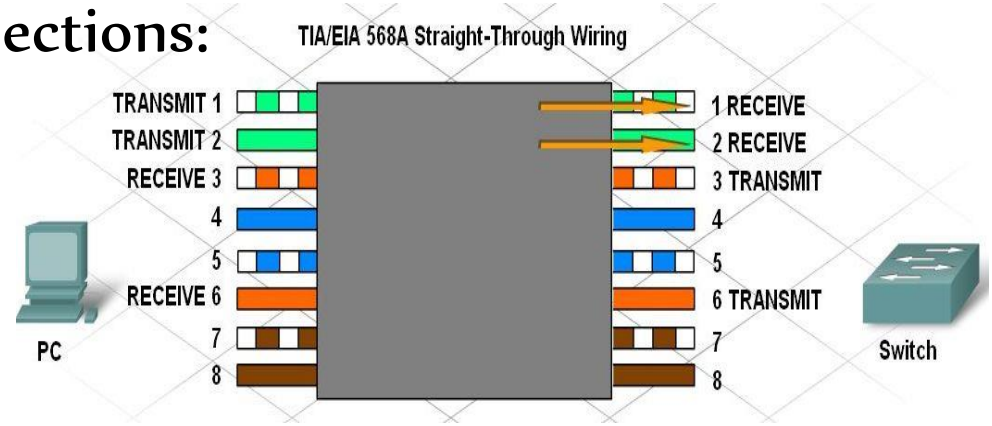
Disadvantages

- **Incapable** of carrying signal over long distances due to high attenuation.
- Low **bandwidth** capabilities-unsuitable for broadband applications.
- max. data rates is
  - 1 Mbps- without conditioning
  - 10 Mbps with conditioning



UTP connections

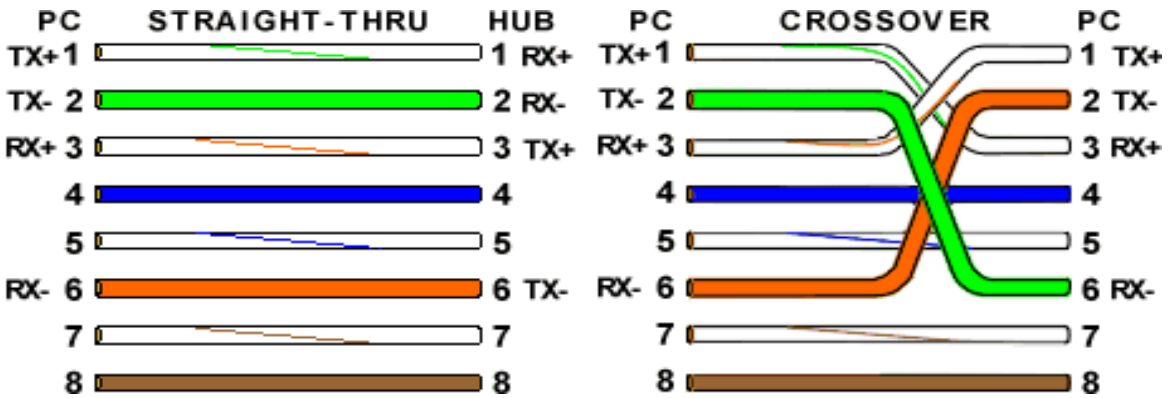
- **Pin of the source device vs pin of the destination device.**
- There are three types of connections:
  - Straight through cables
  - Crossover Cables
  - Rollover cables



- **Straight through cables**
  - They are used to connect dissimilar devices.
  - Switch/Hub to PC
  - Switch/Hub to Router

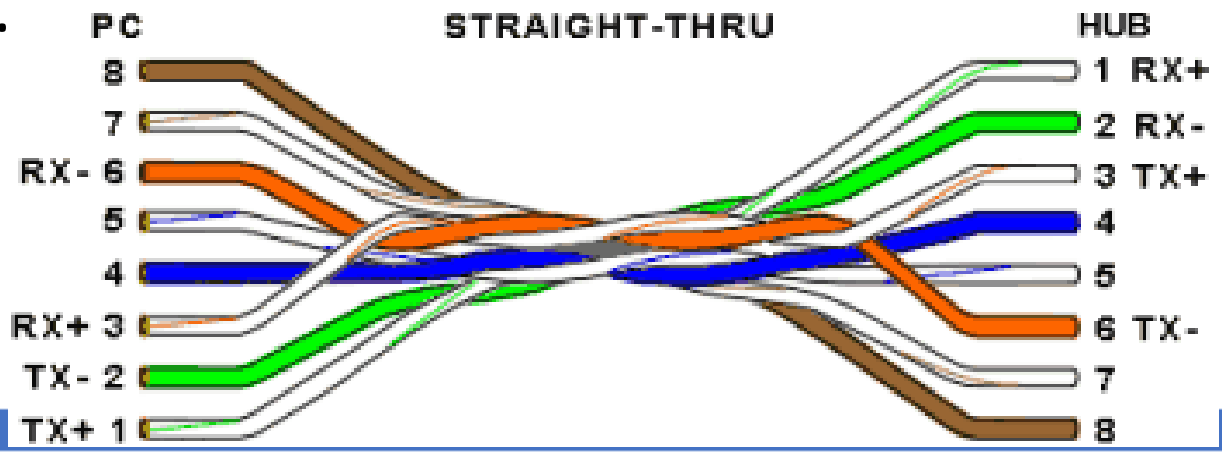
UTP connections

- **Cross over cable**
  - The crossover cable can be used to connect similar devices
    - Hub to hub
    - Switch to switch
    - Hub to switch
    - PC to PC
    - PC to Router



UTP connections

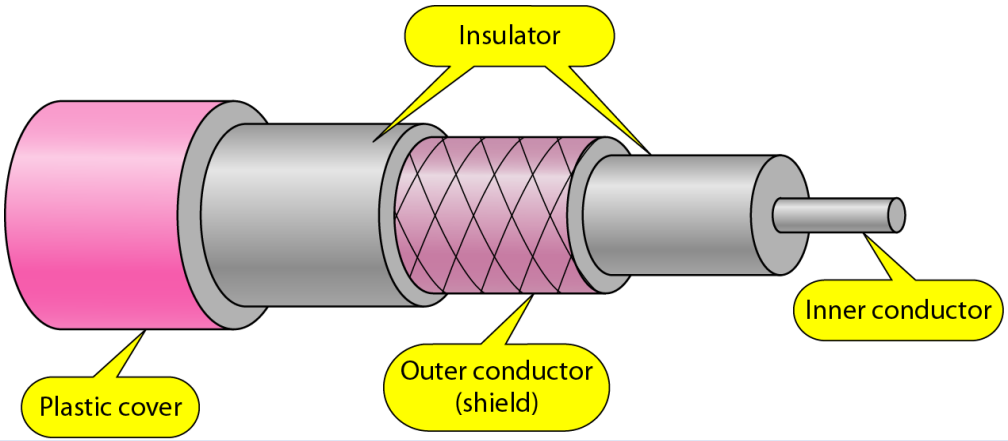
- **Console (Rolled) Cable**
  - Although rolled cable isn't used to connect any Ethernet connections together, you can use a rolled Ethernet cable to connect a **PC to a router console** serial communication (com) port.
  - If you have a Cisco router or switch, you would use this cable to connect your PC running HyperTerminal to the Cisco hardware.



Unshielded Twisted Pair	Shielded Twisted Pair
UTP Advantages: • Least expensive • Easy to install • High speed capacity **UTP Disadvantages:** • Susceptible to external interference • Lower capacity & performance in comparison to STP • Short distance transmission due to attenuation	**STP Advantages:** • Better performance at a higher data rate in comparison to UTP • Eliminates crosstalk • Comparitively faster **STP Disadvantages:** • Comparitively difficult to install & manufacture • More expensive • Bulky

Coaxial Cable

- **Coaxial cable (or *coax*)** *carries signals of* ***higher frequency ranges*** *than twisted pair* cable.
- Has a central core conductor of **solid or stranded wire (usually copper)** enclosed in an insulating sheath, which is, in turn, encased in an **outer conductor of metal foil, braid**, or a combination of the two.
- **The outer metallic wrapping** serves both as a **shield against noise** and as the **second conductor**, which completes the circuit.
- This outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover



Coax Contd.

- coaxial cable **was** the **most widely used** network cabling.
- Reasons for coaxial cable's wide usage: it was relatively **inexpensive**, and it was **light**, **flexible**, and **easy to work with**.
- The term **shielding** refers to the **woven or stranded metal mesh** (or other material) that surrounds some types of cabling.
- **Shielding protects transmitted** data by **absorbing stray electronic signals**, called **noise**, so that they do not get onto the cable and distort the data.
- Cable that contains one layer of foil insulation and one layer of braided metal shielding is referred to as **dual shielded**.
- For environments that are subject to **higher interference**, **quad shielding** is available.
- **Quad shielding** consists of two layers of foil insulation and two layers of braided metal shielding.

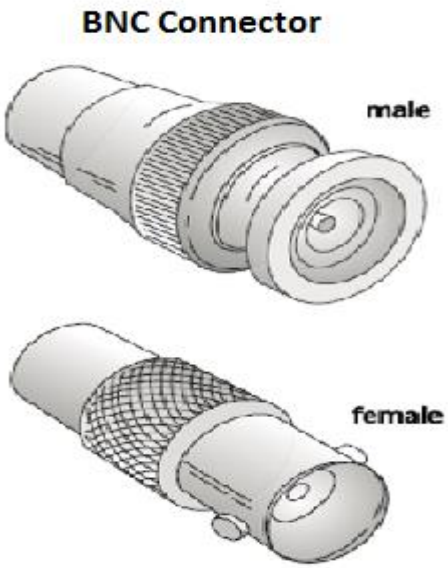
Types of Coaxial Cable

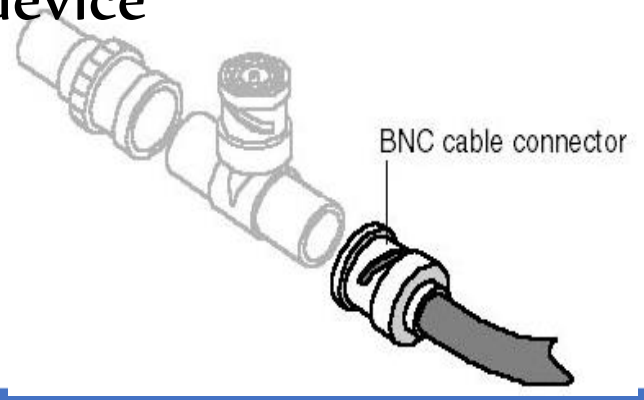
1. **Thin (thinnet) cable**
2. **Thick (thicknet) cable**

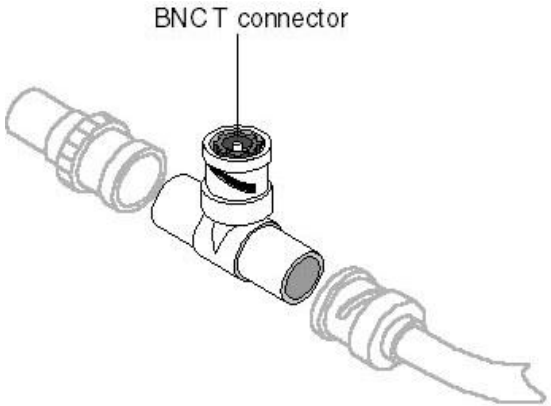
1. **Thinnet(10Base2):-** is a flexible coaxial cable about **0.64** centimeters (0.25 inches) thick.
   - Because this type of coaxial cable is **flexible** and easy to work with, it can be used in **almost any type** of network installation.
2. **Thicknet(10Base5):-** is a relatively rigid coaxial cable about **1.27** centimeters (0.5 inches) in diameter.
   - Thicknet cable is referred to as **Standard Ethernet** b/cs it was the **first type** of cable used with the popular network architecture Ethernet.
   - Thicknet cable's copper core is thicker, and carry signal farther.
   - Thicknet cable can carry a signal for 500 meters (about 1640 feet).
   - it is sometimes used as a **backbone** to connect several smaller thinnet-based networks

Connector

- The BNC connector is used to connect the end of the cable to a device, such as a TV set.
- The BNC T connector is used in Ethernet networks to branch out to a connection to a computer or other device

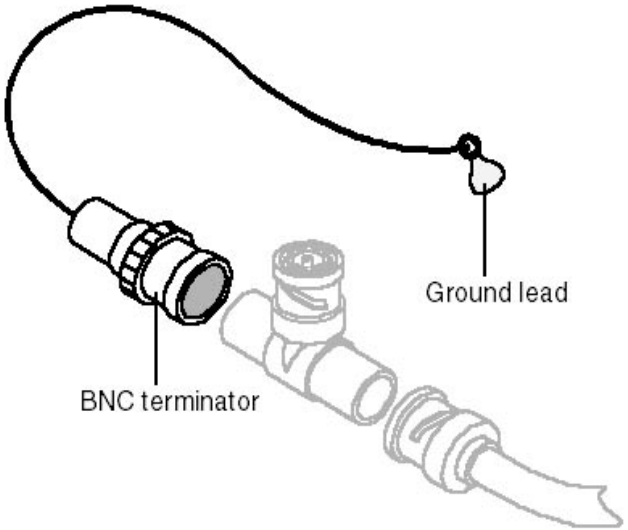


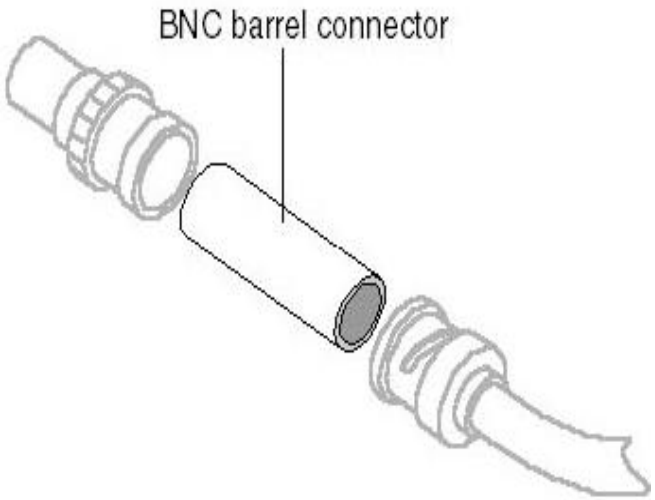




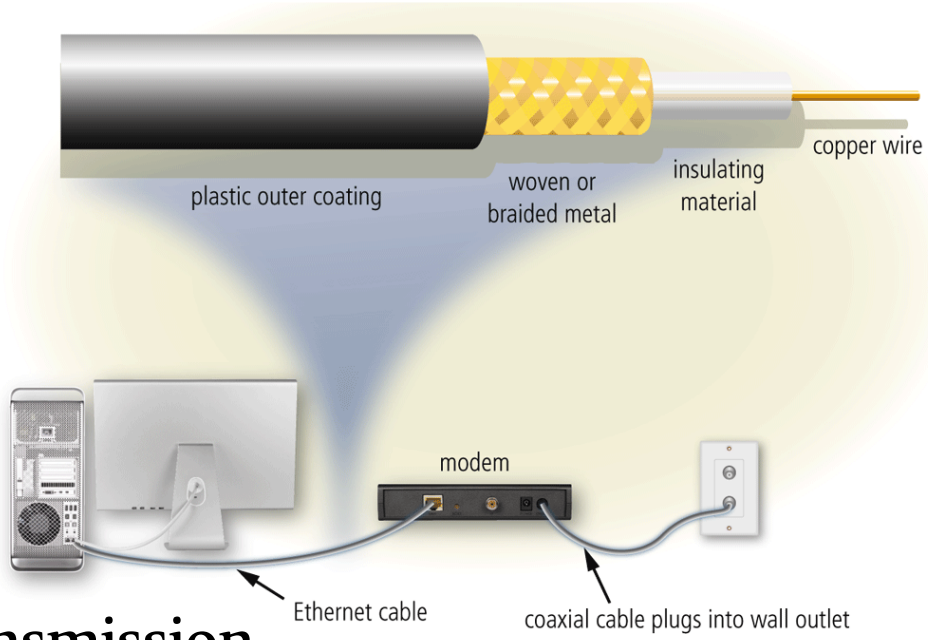
Connector Contd.

- The **BNC terminator** is used at the end of the cable to prevent the reflection of the signal
- **BNC barrel connector** is used to join two lengths of thinnet cable to make one longer length.

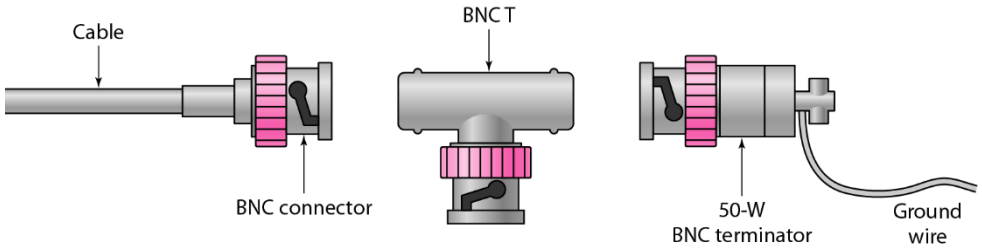




Coaxial Cable Applications



- Most versatile medium
- Television distribution
  - Ariel to TV
  - Cable TV
- Long distance telephone transmission
  - Can carry 10,000 voice calls simultaneously
  - Being replaced by fiber optic
- Short distance computer systems links
  - Local area networks

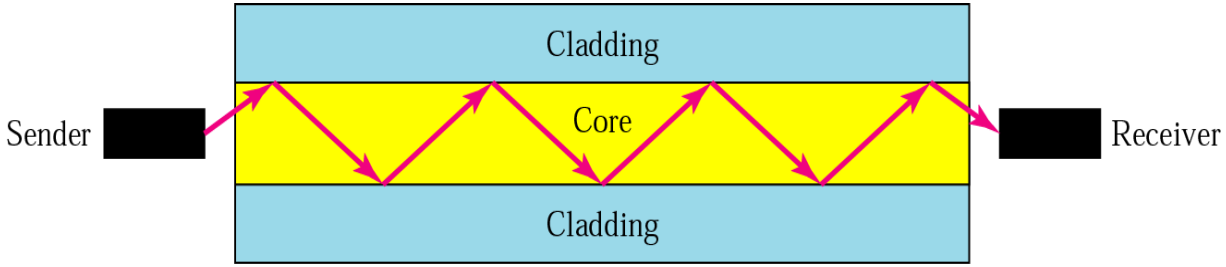


Fiber-Optic Cable

- A fiber-optic cable is made of **glass** or **plastic** and transmits signals in the form **of light**.
- Fiber-optic cabling consists of a signal-carrying glass core of **5 to 100 microns** in diameter (a sheet of paper is about 25 microns thick and a human hair about 75 microns thick), surrounded by a layer of pure silica called **cladding**, which prevents light from escaping.
- Surrounding the cladding are **protective layers** of acrylic plastic coating, **Kevlar fibers** for additional strength, and a PVC (polyvinyl chloride) jacket (usually colored a distinctive orange).

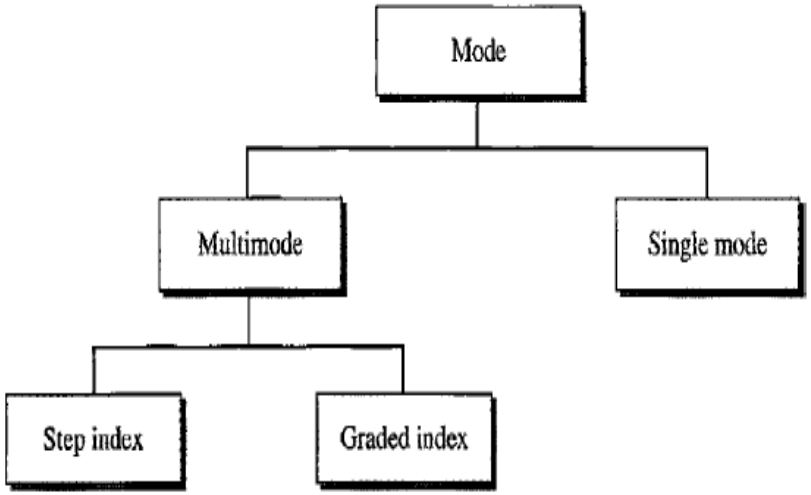
Fiber Contd.

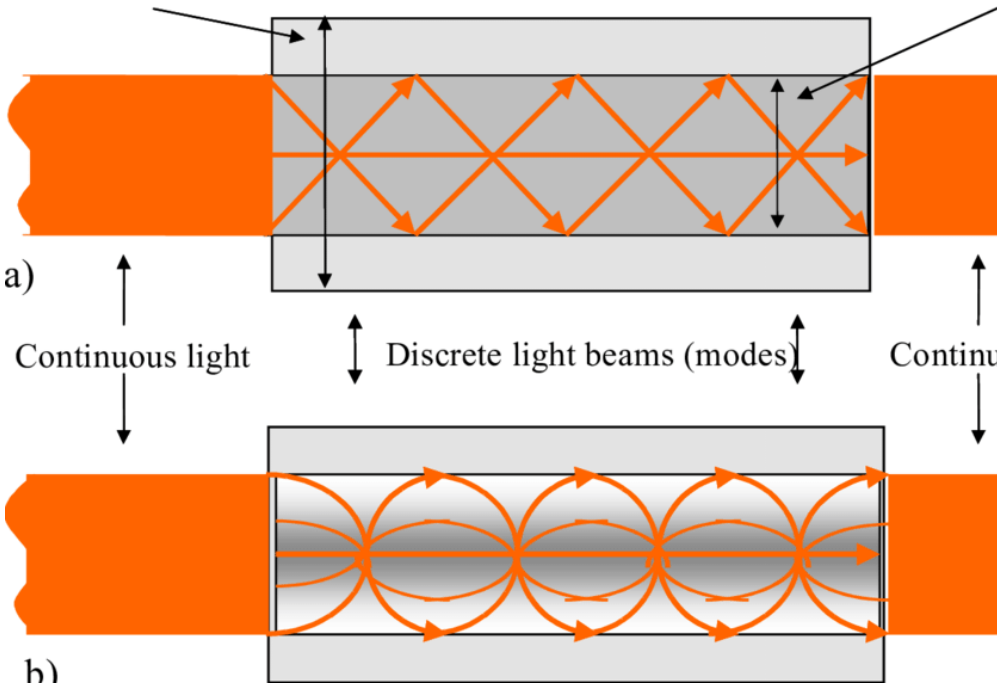
- Network components use **LED or laser diodes** to convert electrical signals into light pulses for transmission on fiber-optic cables.
- An **optical detector** is used to convert the light pulses back into electrical signals.
- Optical fibers use **reflection** to guide light through a channel.
- A glass or plastic core is surrounded by a cladding of less dense glass or plastic.



Propagation Modes

- Current technology supports two modes (**multimode** and **single mode**) for propagating light along optical channels.
- Multimode can be implemented in two forms: **step-index** or **graded-index**





Single-mode fiber-optic cabling

- Has a **narrow core** (5 or 10 microns in diameter) and allows **only one signal** to be sent or received at a time over very long distances [**about 50 kms**](up to 50 times farther than multimode fiber-optic cabling).
- Single-mode fiber-optic cabling uses **laser-emitting diodes** to introduce signals into the fiber and can transmit only one signal (light beam) at a time.
- Signal transmission is clear for approximately 30 miles (50 kilometers) before dispersion will distort signals, which means that single-mode fiber is **ideal for long cable runs**.
- Is suitable for **long-distance telephony** and **multichannel television broadcast systems**

Multimode fiber-optic cabling:

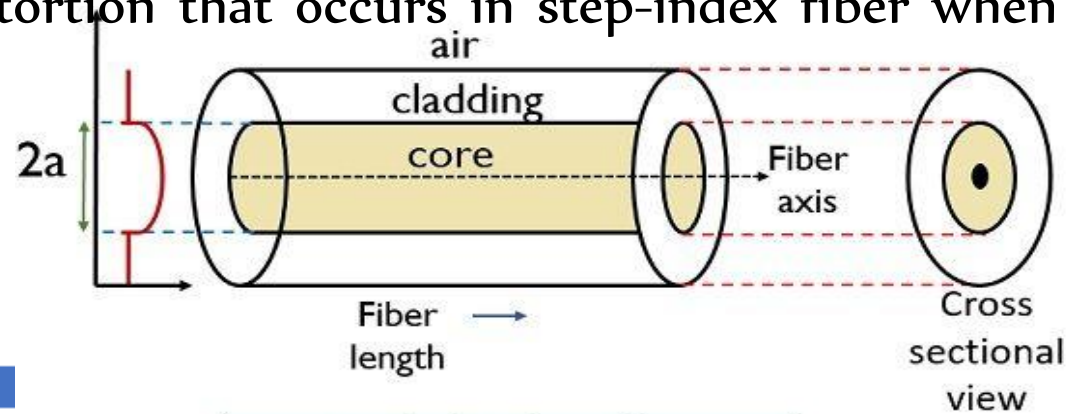
- Has a **thicker core** (50, 62.5, or 100 microns in diameter) and has sufficient bandwidth to allow multiple signals to be simultaneously transmitted or received;
- Each signal follows a different path or mode through the fiber.
- Signal transmission is clear for approximately 3000 feet (**almost 1km**), but longer cable runs can distort signals through modal dispersion.
- There are two types of multimode fiber:
  1. **Step-index multimode fiber**
  2. **Graded-index multimode fiber**
- is suited for use in **LAN systems** and **video surveillance**.

A. Step-index multimode fiber

- Less costly variety of multimode fiber, uses a **wide core with a constant density** from the center to the edges, causing the light beams to reflect **in mirror fashion** off the inside surface of the core by the process of total internal reflection
- At the interface there is an abrupt change to a lower density that alters the angle of the beam's motion.
- Because light can take many different paths down the cable and each path takes a different amount of time, signal distortion can result when step-index fiber is used for long cable runs.
- Used only for short cable runs.

B. Graded-index multimode fiber

- The **more expensive** type of multimode fiber.
- A graded-index fiber is one with **varying densities**.
- Density is highest at the center of the core and decreases gradually to its lowest at the edge.
- Therefore, light beams follow curved paths and all rays reach the end of the fiber simultaneously
- This reduces the signal distortion that occurs in step-index fiber when long cable runs are used.



Graded Index Fiber

Circuit Globe

Types of Optical Fiber

Multimode stepped index

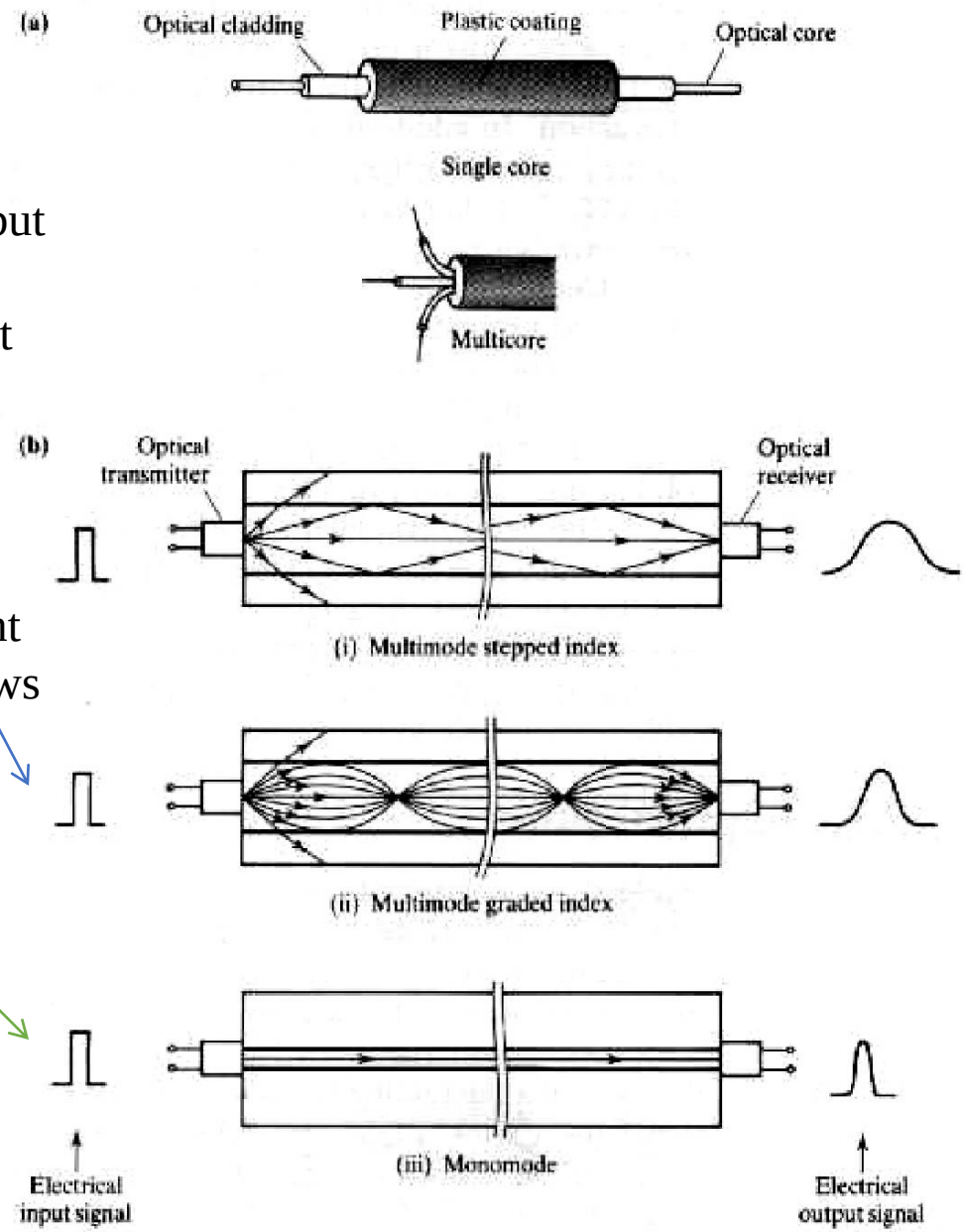
- Cladding and core each have a different but uniform refractive index
- Signal has a wider pulse width => modest bit rates

Multimode graded index

- Core material has a variable refractive index
- Light is refracted by an increasing amount as it moves away from the core => narrows pulse width

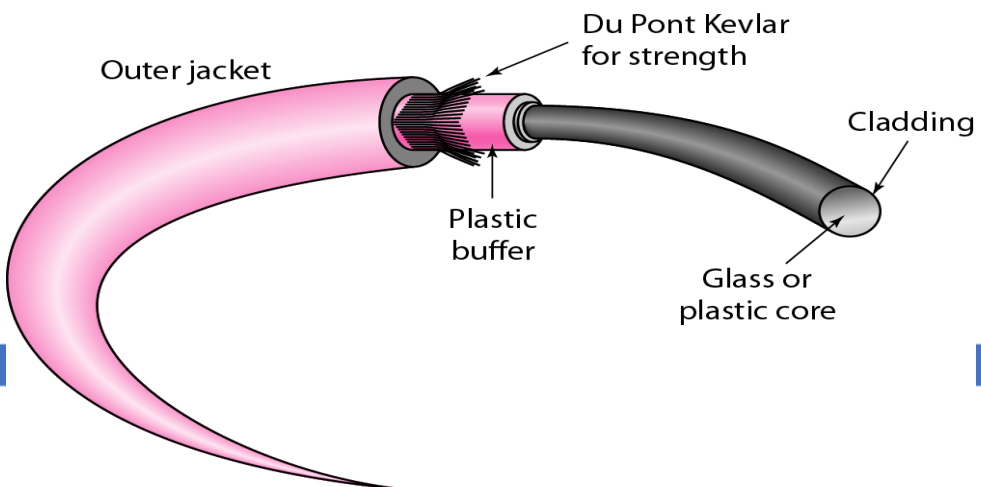
Monomode

- Reduces core diameter to that of a single wavelength (3-10 micrometers)
- Light propagates along a single path => width of output signal = width of input signal



Cable Composition

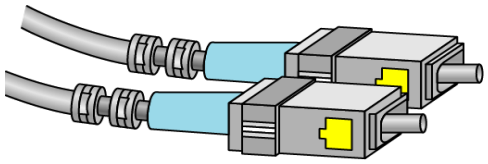
- The outer jacket is made of either **PVC (polymer of vinyl chloride) or Teflon**.
- Inside the jacket are **Kevlar strands** to strengthen the cable.
- **Kevlar** is a strong material used in the fabrication of bulletproof vests.
- Below the Kevlar is another **plastic coating** to cushion the fiber.
- The fiber is at the center of the cable, and it consists of **cladding** and **core**.



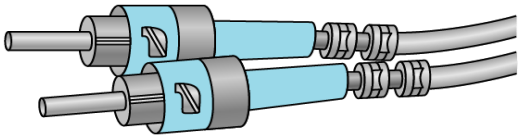
Fiber-Optic Cable Connectors

There are three types of connectors for fiber-optic cables.

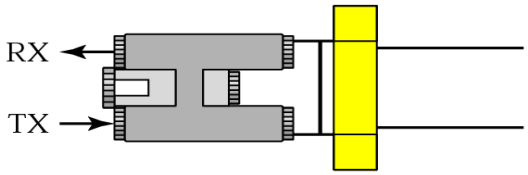
1. **Subscriber channel (SC) connector:-** is used for cable TV. It uses a push/pull locking system.
2. **Straight-tip (ST) connector:-** is used for connecting cable to networking devices. It uses a bayonet locking system and is more reliable than SC.
3. **MT-RJ is a connector:-** that is the same size as RJ45.



SC connector



ST connector



MT-RJ connector

Optical Fiber - Applications

- Long-haul trunks
- Metropolitan trunks
- Rural exchange trunks
- Subscriber loops
- LANs

Advantages of Optical Fiber

- Advantages of fiber-optic over twisted-pair and coaxial cable are:

1. **Noise Resistance**: Because fiber-optic transmission uses light rather than electricity, noise is not a factor. External light, the only possible interference, is blocked from the channel by the outer jacket.
2. **Less signal attenuation:-** Fiber-optic transmission distance is significantly greater than that of other guided media. A signal can run for miles without requiring regeneration.
3. **Higher bandwidth:-** Currently, data rates and bandwidth utilization over fiber-optic cable are limited not by the medium but by the signal generation and reception technology available.

Disadvantages of Optical Fiber

- The main disadvantages of fiber optics are:

1. **Cost:-** Fiber-optic cable is expensive. Also, a laser light source can cost thousands of dollars, compared to hundreds of dollars for electrical signal generators.

2. **Installation/maintenance**

3. **Fragility:-** Glass fiber is more easily broken than wire, making it less useful for applications where hardware portability is required.

Cautions about Optical Fiber

- ✓ **Warning:** The laser light used with single-mode has a longer wavelength than can be seen. The laser is so strong that it can seriously damage eyes.

- ✓ **Never** look at the near end of a fiber that is connected to a device at the far end.

- ✓ **Never** look into the transmit port on a NIC, switch, or router. Remember to keep protective covers over the ends of fiber and inserted into the fiber-optic ports of switches and routers.

- ✓ **Be very careful.**

Optical Fiber - Transmission Characteristics

- Act as wave guide for 10^{14} to 10^{15} Hz
  - Portions of infrared and visible spectrum
- Light Emitting Diode (LED)
  - Cheaper
  - Wider operating temp range
  - Last longer
- Injection Laser Diode (ILD)
  - More efficient
  - Greater data rate
- Wavelength Division Multiplexing

Comparison Table

Type	Type Sub type	Max.Segment Length	Bandwidth supported	installation	cost	Interference
Twisted pair cable	UTP STP	100 mts 100 mts	100 Mbps 500 Mbps	Easy moderate	Cheapest moderate	High moderate
Coaxial cable	Thinnet Thicknet	185 mts 500 mts	10 Mbps 10 Mbps	Easy hard	Cheap moderate	Moderate Low
Fiber optic cable	Multimode Singlemode	2 kms 100 kms	100 Mbps 2 Gbps	Very hard Very hard	Expensive Expensive	None None

Unguided (Wireless) Media

- Unguided media transport electromagnetic waves without using any **physical conductor**.
- This type of communication is often referred to as **wireless communication**.
- Signals are normally broadcast through **free space** and thus are available to **anyone** who has a device capable of receiving them.
- Unguided signals can travel from the source to destination in several ways: **ground propagation**, **sky propagation**, and **line-of-sight propagation**.

Ground propagation (below 2 MHz)

Sky propagation (2-30 MHz)

Line-af-sight propagation (above 30 MHz)

Contd.

1. **In ground propagation**, radio waves travel through the lowest portion of the atmosphere, hugging the earth.
   - These low-frequency signals emanate in all directions from the transmitting antenna and follow the curvature of the planet.
   - **Distance depends** on the amount of power in the signal: The greater the power, the greater the distance.
2. **In sky propagation**, higher-frequency radio waves radiate upward into the ionosphere (the layer of atmosphere where particles exist as ions) where they are **reflected back to earth**.
   - This type of transmission allows for greater distances with lower output power.

Contd.

3. **In line-of-sight** propagation, very high-frequency signals are transmitted in straight lines directly from **antenna to antenna**.
   - Antennas must be directional, facing each other, and either tall enough or close enough together not to be affected by the curvature of the earth.
   - Line-of-sight propagation is tricky because radio transmissions cannot be completely focused.

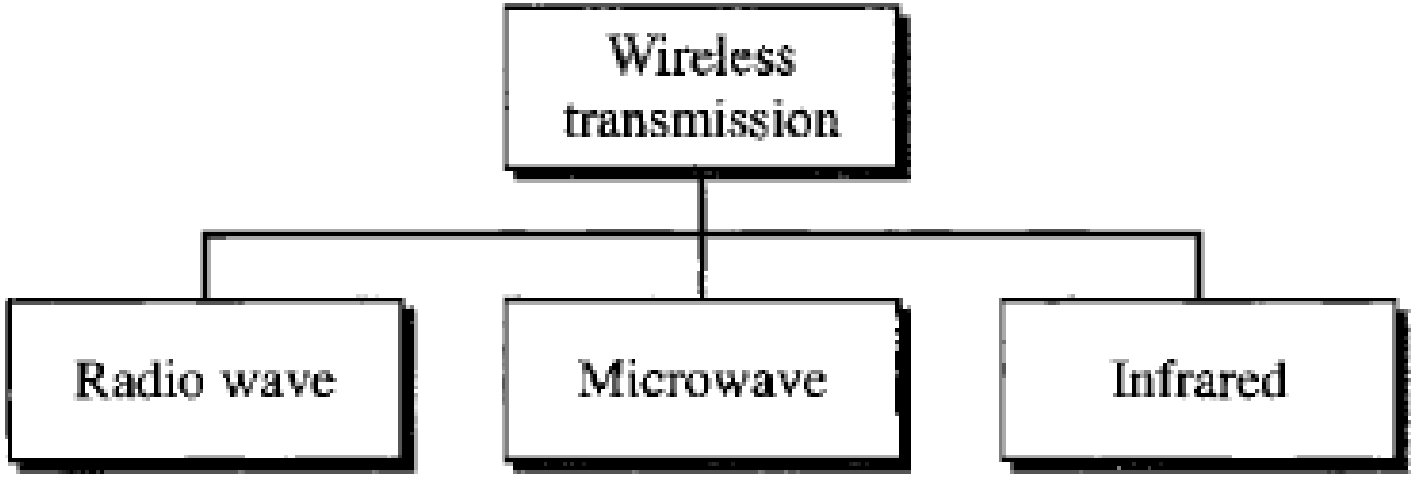
- These bands are rated from *very* ***low frequency (VLF) to extremely high frequency (EHF).***

Contd.

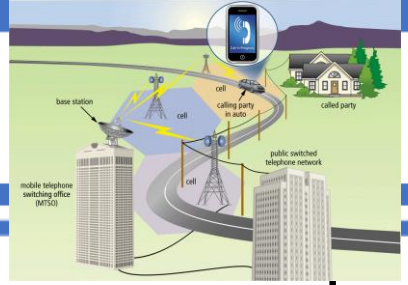
Band	*Range*	*Propagation*	*Application*
VLF (very low frequency)	3-30 kHz	Ground	Long-range radio navigation
LF (low frequency)	30-300 kHz	Ground	Radio beacons and navigational locators
MF (middle frequency)	300 kHz-3 MHz	Sky	AM radio
HF (high frequency)	3-30 MHz	Sky	Citizens band (CB), ship/aircraft communication
VHF (very high frequency)	30-300 MHz	Sky and line-of-sight	VHF TV, FM radio
UHF (ultrahigh frequency)	300 MHz-3 GHz	Line-of-sight	UHF TV, cellular phones, paging, satellite
SHF (superhigh frequency)	3-30 GHz	Line-of-sight	Satellite communication
EHF (extremely high frequency)	30-300 GHz	Line-of-sight	Radar, satellite

Wireless Transmission Types

- We can divide wireless transmission into three broad groups: radio waves, microwaves, and infrared waves.



Radio Waves



- No clear-cut demarcation between radio waves and microwaves,
- electromagnetic waves 3 kHz and 1 GHz are normally called radio waves; 1 and 300 GHz are called microwaves.
- **Bbehavior**: Radio waves, for the most part, are Omni-directional, antenna propagated in all directions.
- This means that the sending and receiving antennas do not have to be aligned. A sending antenna sends waves that can be received by any receiving antenna.

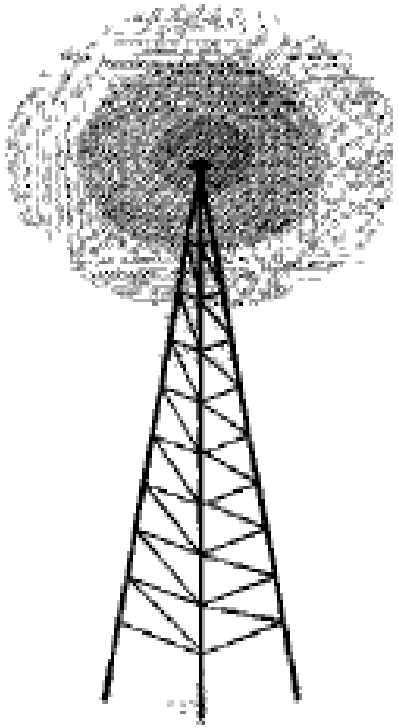
Contd.

- Radio waves, that propagate in the sky mode, can travel **long distances**. This makes radio waves a good candidate for long-distance broadcasting such as AM radio.
- Radio waves, particularly those of **low and medium frequencies**, can penetrate walls.
- This characteristic can be both an advantage and a disadvantage.
- It is an **advantage** because, for example, an AM radio can receive signals inside a building.
- It is a **disadvantage** because we cannot isolate a communication to just inside or outside a building.

Contd.

Applications

- The unidirectional characteristics of radio waves make them useful for **multicasting**, in which there is one sender but many receivers.



- **AM and FM radio, television, maritime radio, cordless phones, etc** are examples of multicasting.

Microwaves

- Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves.
- Microwaves are unidirectional. When an antenna transmits microwave waves, they can be narrowly focused. The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas.
- some characteristics of microwave propagation:
  - Microwave propagation is line-of-sight. So need to be very tall.

Contd.

- The curvature of the earth as well as other blocking obstacles do not allow to communicate by using microwaves.
- Repeaters are often needed for long distance communication.
- Very high-frequency microwaves cannot penetrate walls.
  - Is a disadvantage, if receivers are inside buildings.
- The microwave band is **relatively wide**, almost 299 GHz.
  - wider subbands can be assigned, and a high data rate is possible

Unidirectional Antenna

- Microwaves need unidirectional antennas that send out signals in one direction.
- Two types of antennas: the **parabolic dish** and the **horn**.

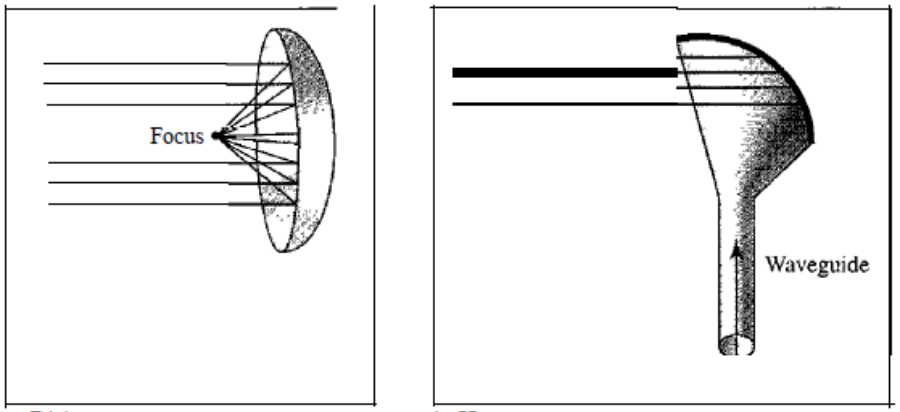
1. **A parabolic dish antenna** :

   - Every line parallel to the line of sight reflects off the curve at angles such that all the lines intersect in a common point called **the focus**.
   - The parabolic dish works as a funnel, catching a wide range of waves and directing them to a common point.
   - More of the signal is recovered than would be possible with a single-point receiver.
   - The microwaves hit the dish and are deflected outward in a reversal of the receipt path.

Contd.

2. **A horn antenna** looks like a gigantic scoop.

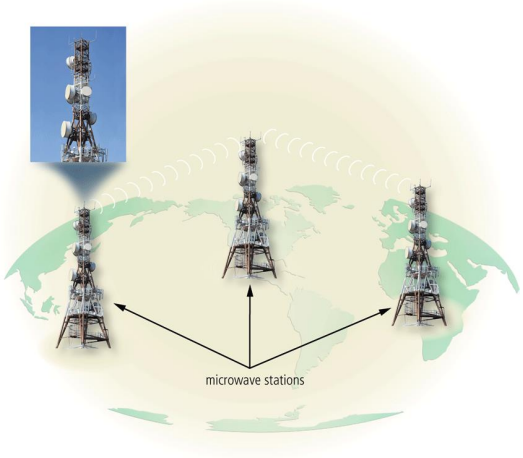
- Outgoing transmissions are broadcast up a stem (resembling a handle) and deflected outward in a series of narrow parallel beams by the curved head.
- Received transmissions are collected by the scooped shape of the horn, in a manner similar to the parabolic dish, and are deflected down into the stem.



a. Dish antenna b. Horn antenna

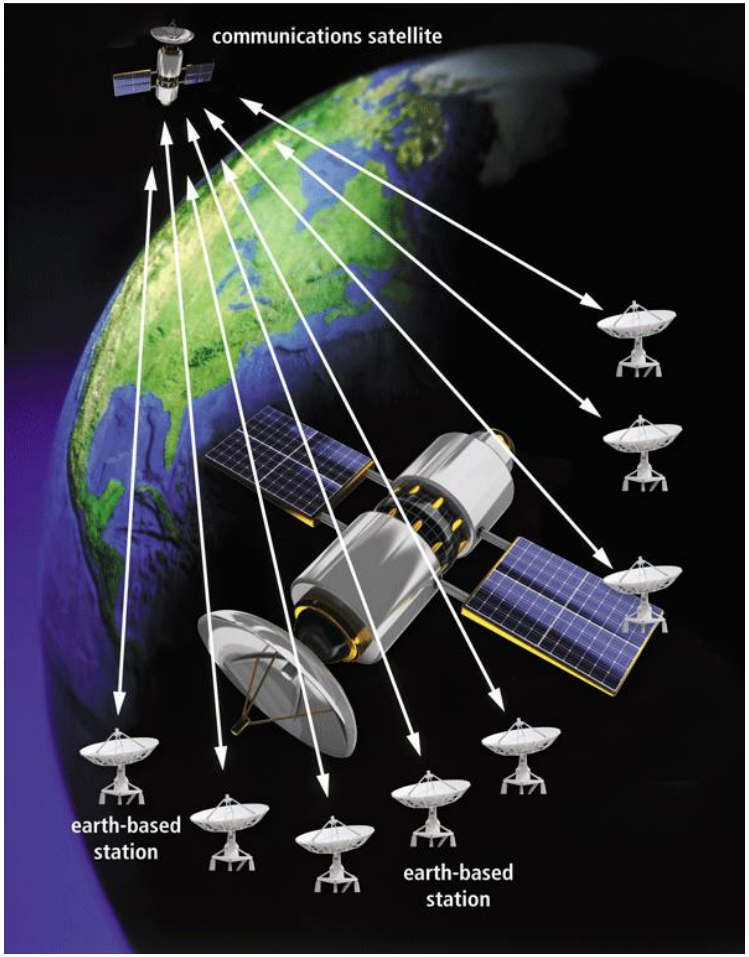
Applications

- Microwaves, due to their unidirectional properties, are very useful when **unicast (one-to-one) communication** is needed between the sender and the receiver.
- They are used in **cellular phones**, **satellite networks** , and **wireless LANs.**

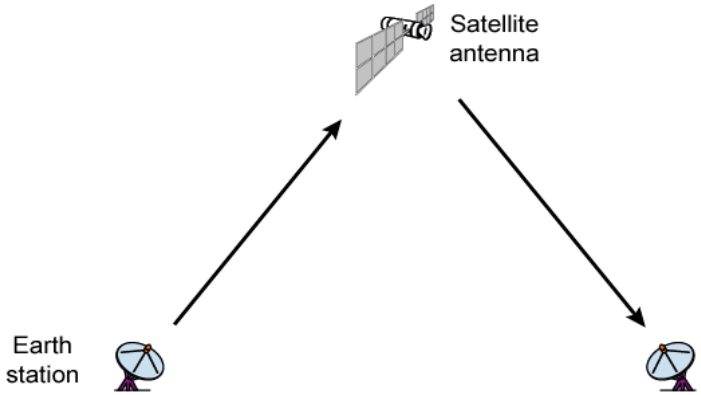


Satellite

- A **communications satellite** is a space station that receives microwave signals from an earth-based station, amplifies it, and broadcasts the signal over a wide area

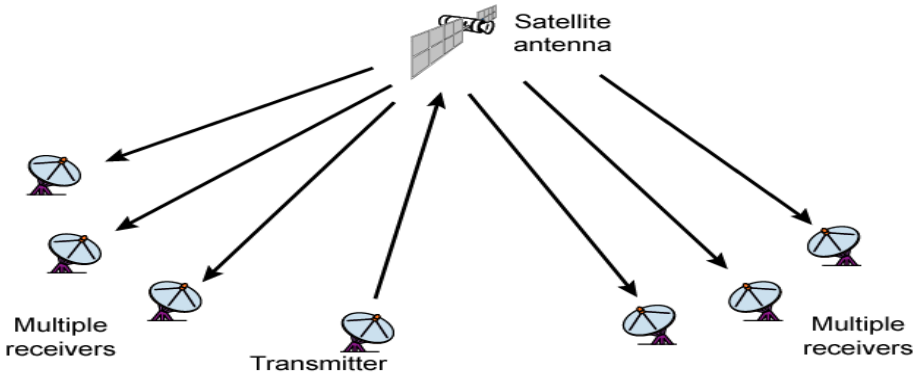


Satellite Point to Point Link



(a) Point-to-point link

Satellite Broadcast Link



(b) Broadcast link

Infrared

- Frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 nm), can be used for short-range communication.
- cannot penetrate walls.
- This advantageous characteristic prevents interference between one system and another; a short-range communication system in one room cannot be affected by another system in the next room.
- However, useless for long-range communication.
- We cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication.

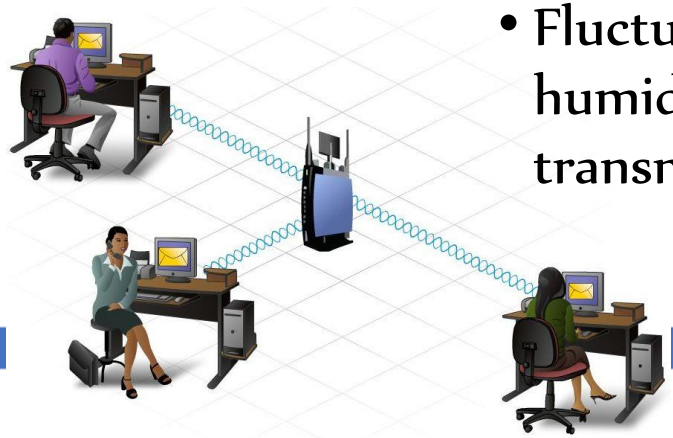
Applications

- The infrared band, almost 400 THz, has an excellent potential for data transmission.
  - Such a wide bandwidth can be used to transmit digital data with a very high data rate.
- The ***Infrared Data Association (IrDA)***, *an association for sponsoring the use of infrared* waves, has established standards for using these signals for communication between devices such as keyboards, mice, PCs, and printers.
- The standard originally defined a data rate of 75 kbps for a distance up to 8 m. The recent standard defines a data rate of 4 Mbps.
- Infrared signals defined by IrDA transmit through line of sight; the IrDA port on the keyboard needs to point to the PC for transmission to occur.

Wireless Technologies

- **Pros**
  - Anytime, anywhere connectivity with hotspots
  - Easy and cheap installation
  - Device prices dropping
  - Data rate capabilities increasing
  - Easy expansion

- **Cons**
  - Unlicensed RF which is crowded with other devices
    - Bluetooth
    - Microwaves
    - Cordless phones
  - Security is difficult
    - Encryption helps, but can be defeated
  - Fluctuations in temperature and humidity can really affect transmission range.



?

Chapter Four

Internet Protocol (IP) and IP Addressing

Data Communication and Computer Networks

haleluyaluya@yahoo.com

Internet Protocol (IP)

- The **Internet Protocol** (**IP**) is a protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as **TCP/IP.**
- IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of:
  - delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.
- IP version
  - Internet Protocol Version 4 (IPv4) is still the dominant protocol
  - Internet Protocol Version 6 (IPv6), is being deployed actively worldwide.

Contd.

- Communication at the network layer is host-to-host (computer-to-computer);
  - a computer communicate with any computer anywhere else in the world.
- Usually, computers communicate through the Internet.
- The packet transmitted by the sending computer may pass through several LANs or WANs before reaching the destination computer.
- For this level of communication, we need a global addressing scheme; we use the term IP address to mean a logical address in the network layer of the TCP/IP protocol suite. (What is phisical address?)

IPv4 Addresses

- An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a device (a computer or a router) to the Internet.
- IPv4 addresses are unique and universal.
- They are unique in the sense that each address defines one, and only one, connection to the Internet.
- Two devices on the Internet can never have the same address at the same time.

Address Space

- A protocol such as IPv4 that defines addresses has an address space.
- An address space is the total number of addresses used by the protocol.
- If a protocol uses N bits to define an address, the address space is 2^N because each bit can have two different values (0 or 1) and N bits can have 2^N values.
- IPv4 uses 32-bit addresses, which means that the address space is 2^{32} or 4,294,967,296 (more than 4 billion). This means that, theoretically, if there were no restrictions, more than 4 billion devices could be connected to the Internet.
- The actual number is much less because of the restrictions imposed on the addresses.

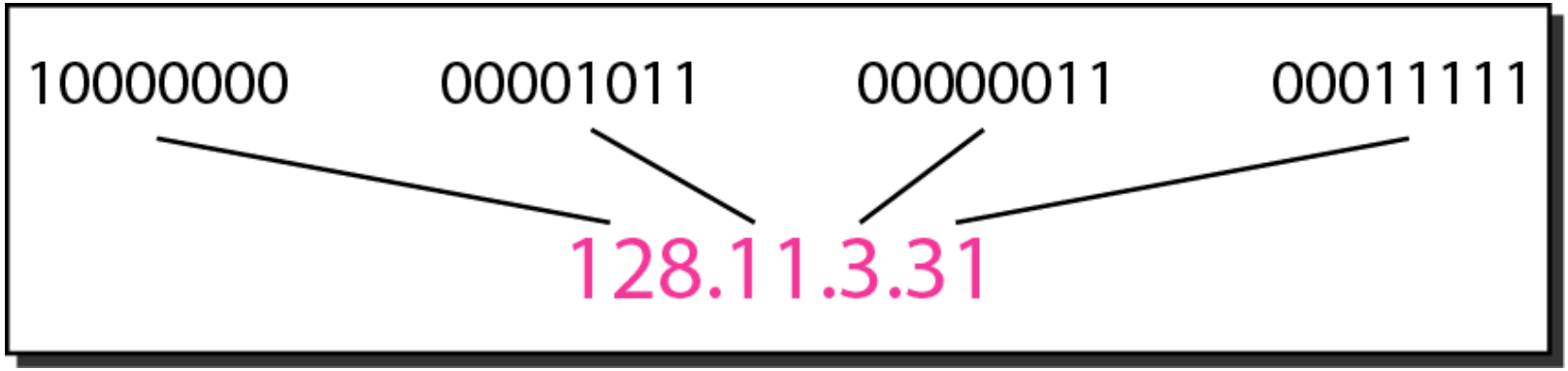
Notations

- There are two prevalent notations to show an IPv4 address: binary notation and dotted-decimal notation.
- Binary Notation
  - In binary notation, the IPv4 address is displayed as 32 bits, 4 Octets, Each octet is often referred to as a byte (4-byte address). Eg.:

    01110101 10010101 00011101 00000010
- Dotted-Decimal Notation
  - Internet addresses are usually written in decimal form with a decimal point (dot) separating the bytes. Eg:

    117.149.29.2

Example: *Dotted-decimal notation and binary notation for an IPv4 address*



Example 1

Change the following IPv4 addresses from binary notation to dotted-decimal notation.

a. 10000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

Solution

We replace each group of 8 bits with its equivalent decimal number and add dots for separation.

a. 129.11.11.239

b. 193.131.27.255

Example 2

Change the following IPv4 addresses from dotted-decimal notation to binary notation.

a. 111.56.45.78

b. 221.34.7.82

Solution

We replace each decimal number with its binary equivalent.

a. 01101111 00111000 00101101 01001110

b. 11011101 00100010 00000111 01010010

Example 3

Find the error, if any, in the following IPv4 addresses.

a. 111.56.045.78

b. 221.34.7.8.20

c. 75.45.301.14

d. 11100010.23.14.67

Solution

a. There must be no leading zero (045).

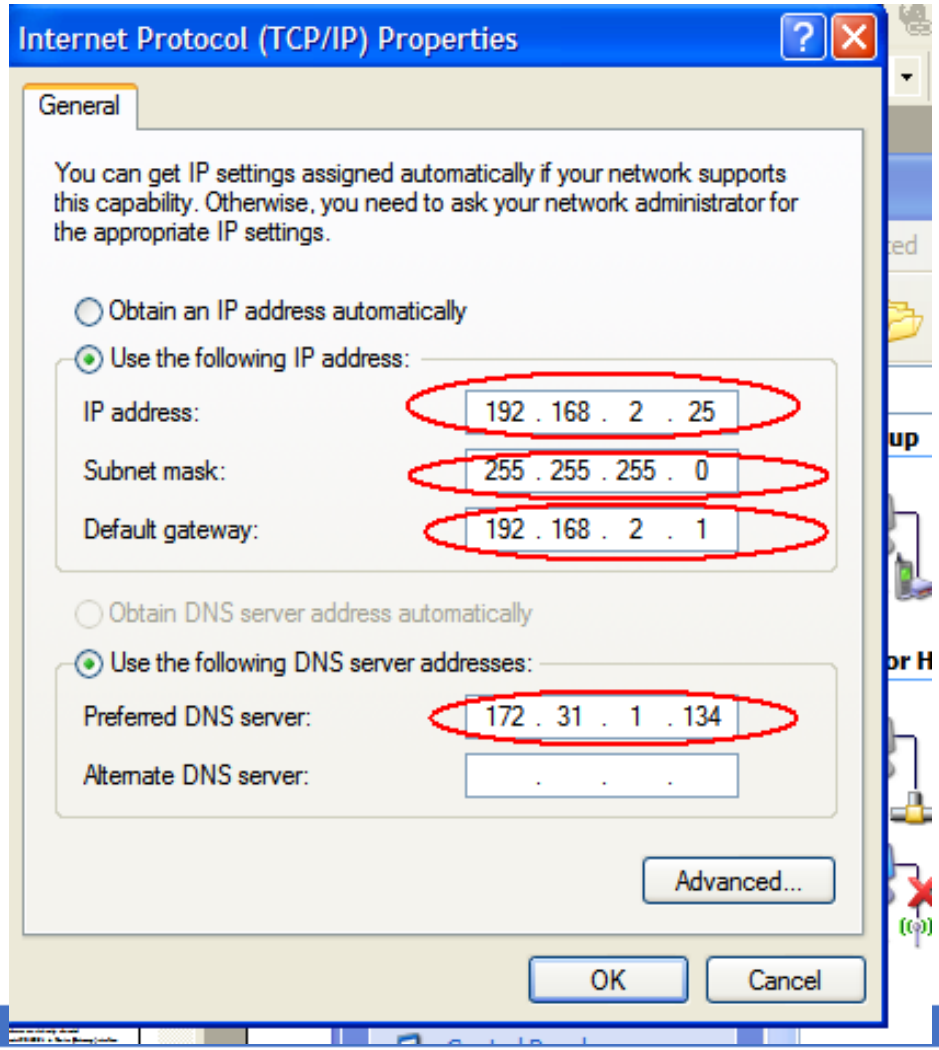
b. There can be no more than four numbers.

c. Each number needs to be less than or equal to 255.

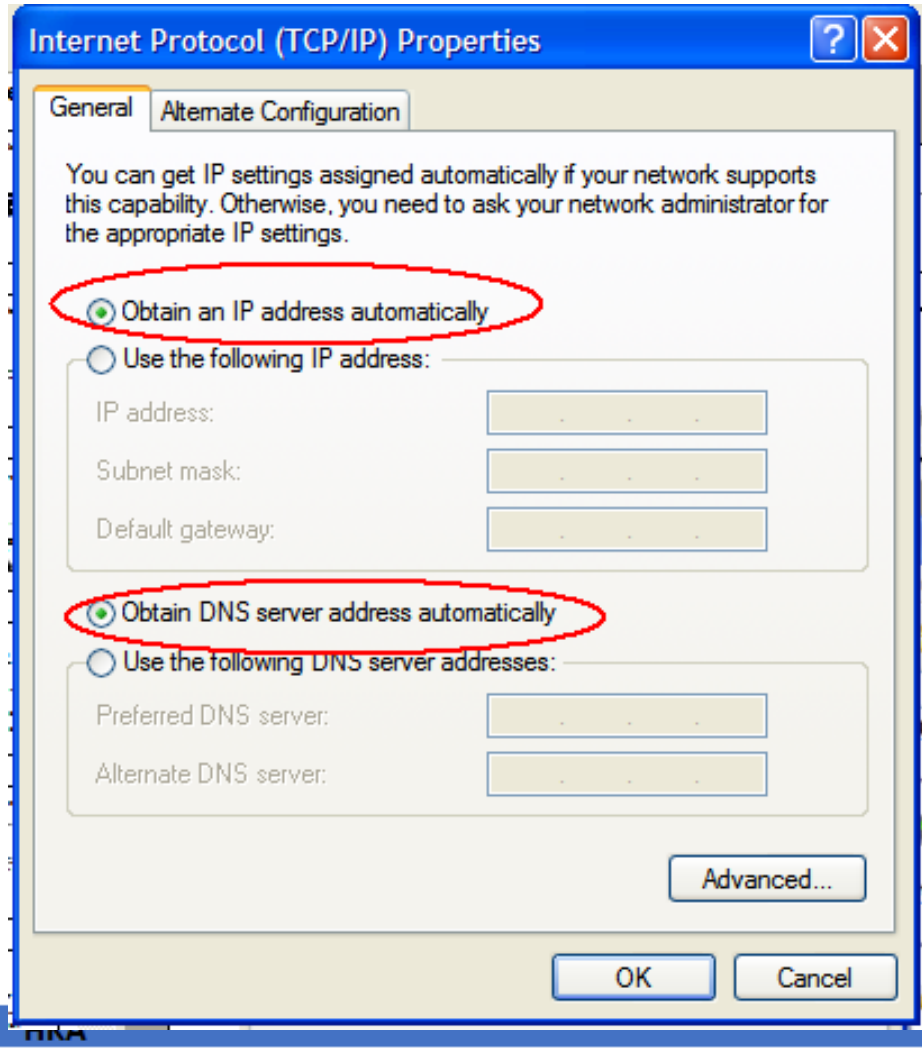
d. A mixture of binary notation and dotted-decimal notation is not allowed.

IP Configuration of an Interface

Static



DHCP



Classful Addressing

- IPv4 addressing, at its inception, used the concept of classes. This architecture is called classful addressing.
- In classful addressing, the address space is divided into five classes: A, B, C, D, and E. Each class occupies some part of the address space.

	First byte	Second byte	Third byte	Fourth byte
Class A	0			
Class B	10			
Class C	110			
Class D	1110			
Class E	1111			

a. Binary notation

	First byte	Second byte	Third byte	Fourth byte
Class A	0–127			
Class B	128–191			
Class C	192–223			
Class D	224–239			
Class E	240–255			

b. Dotted-decimal notation

Example 4

Find the class of each address.

a. 00000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

c. 14.23.120.8

d. 252.5.15.111

Solution

a. The first bit is 0. This is a class A address.

b. The first 2 bits are 1; the third bit is 0. This is a class C address.

c. The first byte is 14; the class is A.

d. The first byte is 252; the class is E.

Classes and Blocks

- One problem with classful addressing is that each class is divided into a fixed number of blocks with each block having a fixed size

Class	*Number of Blocks*	*Block Size*	*Application*
A	128	16,777,216	Unicast
B	16,384	65,536	Unicast
C	2,097,152	256	Unicast
D	1	268,435,456	Multicast
E	1	268,435,456	Reserved

Number of Blocks for class A = 2^7
Number of Blocks for class B = 2^{14}
Number of Blocks for class C = 2^{21}

Block size for class A = 2^{24}
Block size for class B = 2^{16}
Block size for class C = 2^8

Class A

- If the **first bit** of an IP address is **0**, it is the address of a class A network.
- The **first bit** of a class a address identifies the address class.
- The **next seven** bits identify the **network**, and
- The **last 24** bits identify the **host**.
- There are fewer than 128 class a network numbers, but in each class a network can have millions of hosts.

Class A

- |_| first one bit is used to determine the class to which an address belongs to for Class **A** address.
- |_____| 7 bits are used for Network address.Therefore, number of class A networks can be $2^{7} = 128$. Number 0 is not used, and number 127 is used for testing loopback for each host. There **are 126** potential Class A **network** numbers, which have a first dotted decimal number in the range 1 to 126.
- |_____| 24 bits are used for host address. Therefore, each Class A network can have $\mathbf{2}^{24} = 16{,}777{,}216$ **hosts**.
- Class A is **not** available to the **general public**, and it is restricted to special uses.
- ***Class A final format:***
- |/|_____/|/|_____/
- *7 bits* *24 bits*

  Network *Host*

  Part *Part*

Class A

Summary:

- If the the first decimal number in IP address is 1 to 126, then it is a class A address.
- The **first byte** is for the network number, and the **next three bytes** are for the host addresses.

Class B

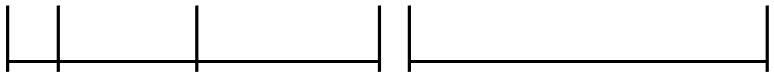
- If the **first two bits** of the address are **1** and **0**, it is a class B network address.
  - The first **two** bits identify class;
  - The next **fourteen** bits identify the network,
  - The last **sixteen** bits identify the host.
- There are thousands of class B network numbers.
- Each class B network can have thousands of hosts.

Class B

- first two bits are used to determine the class to which an address belongs to for class B address.
- 14 (6 + 8) bits are used for network address. Therefore, the number of class B networks can be **2^{14} = 16,384.** There are 16,384 potential Class B network numbers, which have a first dotted decimal number in the range 128 to 191.
- 16 bits are used for host address. Therefore, each Class B network can have **2^{16} = 65,536 hosts**.

Class B

- ***Class B final format***

- 

Summary:

- If the the first decimal number in IP address is 128 to 191, then it is a class B address.
- The first two bytes identify the network.
- The last two bytes identify the host.

Class C

- If the **first three** bits of the address are **1 1 0**, it is a class C network address.
- The first three bits are class identifiers.
- The **next 21** bits are for the network address.
- The **last eight** bits identify the host.
- There are millions of class C network numbers.
- However, each class C network can have **254 hosts**.

Class C

- |__| first three bits are used to determine the class to which an address belongs to for class C address.
- |____|_____|_____| 21 (5 + 16) bits are used for network address. Therefore, the number of class C networks can be **2^{21} = 2, 097,152**. There are 2,097,152 potential Class C network numbers, which have a first dotted decimal number in the range 192 to 223.
- |_____| 8 bits are used for host address. Therefore, each Class C network can have **2^{8} = 256 hosts**.

Class C

Class C final format

|___|_____| |_____| |_____| |_____|
21 bits Network part 8 bits host part

Summary:

- If the the first decimal number in IP address is 192 to 223, then it is a class C address.
- The first three bytes are for the network address.
- The last byte is for the host number.

Summary

- **Class A**:Few networks, each with many hosts.
- **Class B**: Medium number of networks, each with a medium number of hosts
- **Class C**: Many networks, each with a few hosts.

Summary.

- Previously, when an organization requested a block of addresses, it was granted one in class A, B, or C.
- Class A addresses were designed for large organizations with a large number of attached hosts or routers.
- Class B addresses were designed for midsize organizations with tens of thousands of attached hosts or routers.
- Class C addresses were designed for small organizations with a small number of attached hosts or routers.
- A block in class A address is too large for almost any organization. This means most of the addresses in class A were **wasted & were not used**.
- A block in class B is also very large, probably too large for many of the organizations that received a class B block.
- A block in class C is probably too small for many organizations.

Summary

- In classful addressing, an IP address in class A, B, or C is divided into network ID and host ID.
- These parts are of varying lengths, depending on the class of the address.
- In class A, one byte defines the network ID and three bytes define the host ID.
- In class B, two bytes define the network ID and two bytes define the host ID.
- In class C, three bytes define the network ID and one byte defines the host ID.

Loopback Address

- IP defines a loopback address used to test network applications.
- Programmers often use loopback testing for preliminary debugging after a network application has been created.
- To perform a loopback test, a programmer must have two application programs that are intended to communicate across a network.
- Each application includes the code needed to interact with TCP/IP protocol software.
- Instead of executing each program on a separate computer, the programmer runs both programs on a single computer and instructs them to use a loopback IP address when communicating.

Default subnet Mask

- Although the length of the network ID and host ID (in bits) is predetermined in classful addressing, we can also use a mask (also called the default mask), a 32-bit number made of contiguous 1s followed by contiguous 0s. The masks for classes A, B, and C are shown below
- The mask can help us to find the network ID and the host ID. For example, the mask for a class A address has eight 1 s, which means the first 8 bits of any address in class A define the network ID; the next 24 bits define the host ID

Class	*Binary*	*Dotted-Decimal*	*CIDR*
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	/24

SPECIAL IP ADDRESSES

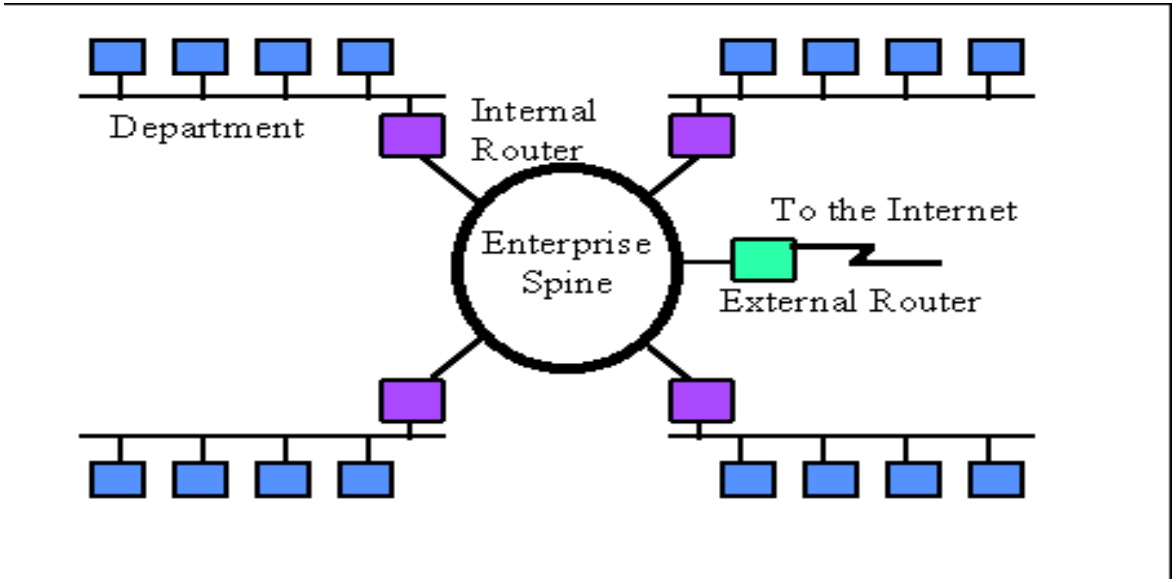
IP addresses	also called	Description
0.0.0.0 /0	Default route	
0.0.0.0/32	This host	
10.0.0.0-10.255.255.255	Private IP address	Used for LAN in a private network
127.0.0.0-127.255.255.255	Loopback address	Used for loopback addresses
169.254.0.0-169.254.255.255	APIPA (Automatic Private IP Addressing)	Assigned automatically if the host does not get an IP from a DHCP server
172.16.0.0-172.31.255.255	Private IP Address	Used for LAN in a private network
192.168.0.0-192.168.255.255	Private IP Address	Used for LAN in a private network
224-239	Class D	Reserved for multicast assignments
240-255	Class E	Reserved for future use
Network Addresses and Broadcast Addresses in a subnet		

Subnetting

- During the era of classful addressing, subnetting was introduced.
- Classful IP addressing **does not provide any flexibility** of having less number of Hosts per Network or more Networks per IP Class.
- If an organization was granted a large block in class A or B, it could divide the addresses into several contiguous groups and assign each group to smaller networks (called subnets) or, in rare cases, share part of the addresses with neighbors.
- Subnetting increases the number of 1s in the mask.
- Allocating a part of the host address space to network addresses, which will let you have more networks

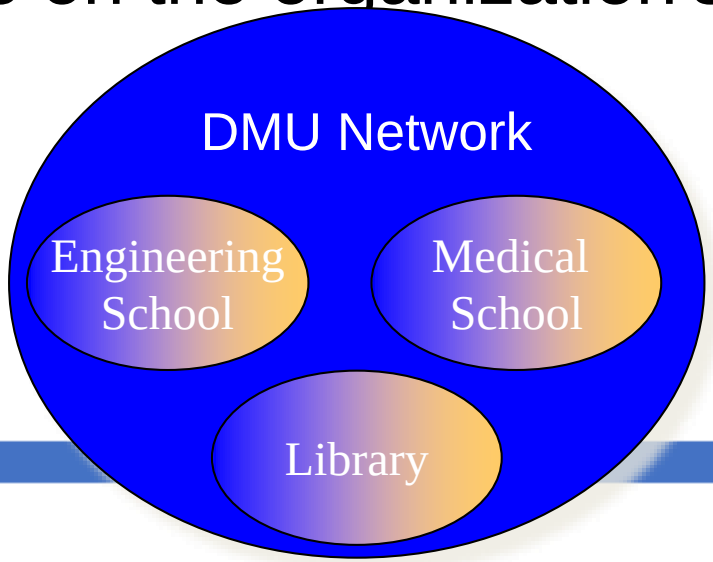
Why subnetting?

- Preservation of address space
- Control network traffic, avoid collisions
- Reduce the routing complexity
- Improve network performance
- Security



Subnet Design Considerations

1. How many total subnets does the organization need today?
2. How many total subnets will the organization need in the future?
3. How many hosts are there on the organization's largest subnet today?
4. How many hosts will there be on the organization's largest subnet in the future?



Subnetting

- The subnet mask is used to determine the bits of the network identifier.
- All **hosts on the same network** should have the **same subnet mask**.
- **Steps:**
  - Determine the number of networks required and convert it into binary.
  - Reserve bits in the mask and find the increment
  - Find the network ranges based on the increment
- Assume that the organization has a network address of 192.168.100.0/24 and if this organization asks you to make this a Class C address in to nine valid networks, show that how you do the subnetting.

Subnetting - soln

- **Solution**
  - Determine the number of networks required and convert it into binary
    - 9 networks= 0000**1001**
    - We need only **4 bits** to denote 9 in binary.
  - Reserve bits in the mask and find the increment
    - Default mask: /24=255.255.255.0=11111111.11111111.11111111.00000000
    - Reserve bits in the mask: 11111111.11111111.11111111.**1117**0000
    - New subnet mask: 255.255.255.240 or /28
    - Increment=lowest bit in the network portion (Italic one) i.e. **16.**
  - Find the network ranges based on the increment

Quiz

- Abaytana private company has bought an IP address of 216.10.180.0/24 from Ethiotelecom. Abaytana has six different branches in Ethiopia.
  - 1st Addis Ababa, 2nd Bhirdar, 3rd Mekele, 4th Jimma, 5th Awasa, and 6th Harer
- How many bits you borrow to create subnets for this network?
- How many network addresses you created for Abaytana
- How many hosts exist in each branch of Abaytana company
- How many total IP addresses are lost due to sub netting
- Where does the following IP address belong to?
  - 216.10.180.89
  - 216.10.180.133
  - 216.10.180.184
  - 216.10.180.230
  - 216.10.180.246

VLSM (Variable Length Subnet Masks)

- VLSM simply means that the subnet design uses more than one mask in the same classful network.
- VLSMs allow you to use different masks for each subnet, Use VLSM to:
  - Create a larger subnet of more than 255 host addresses
  - Create very small subnets for WAN links
- ***Example:*** Given the 172.16.0.0/16 network and requirements below, develop a subnetting scheme with the use of VLSM:
  - LAN1 must support 330 hosts
  - WAN must support 2 hosts for a T1 circuit to a remote site
  - LAN3 must support 6 hosts

VLSM (Variable Length Subnet Masks)

- The first step is to determine what mask allows the required number of hosts.
  - LAN1 requires a /23 (255.255.254.0) mask to support 510 hosts
  - WAN requires a /30 (255.255.255.252) mask to support 2 hosts
  - LAN3 requires a /29 (255.255.255.248) mask to support 6 hosts
- The easiest way to assign the subnets is to assign the largest first.
- For example: You can assign the subnets in this manner:
  - LAN1 —172.16.0.0/23 address range 0.0 to 1.255
  - LAN3 —172.16.2.0/29 address range 0 to 7
  - WAN —172.16.2.8/30 address range 8 to 11

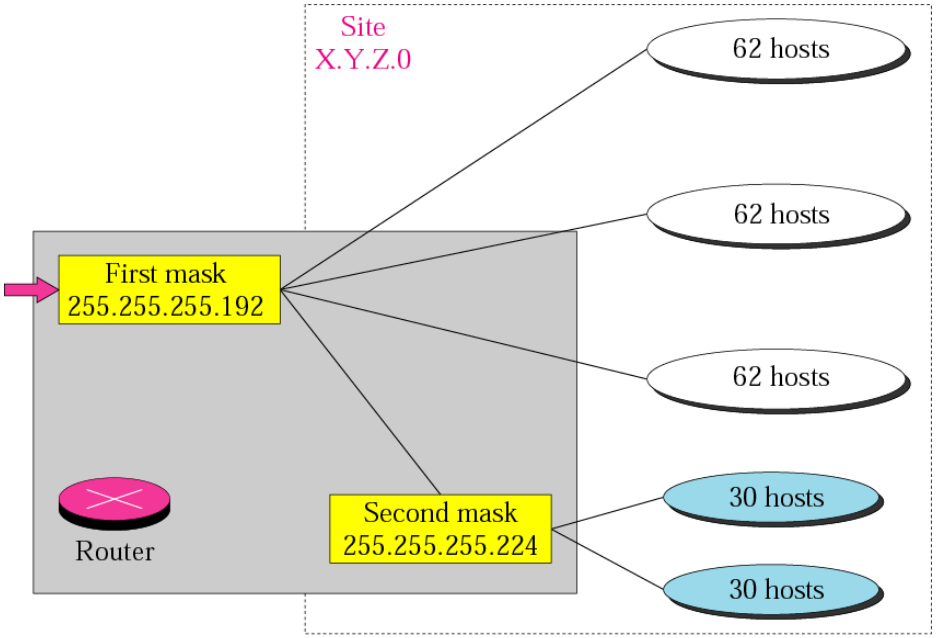
VLSM (Variable Length Subnet Masks)

- A company is granted the site address 181.56.0.0 (class B). The company needs 1000 subnets. Design the subnets.
- But, what if it has two departments with 30 computers.

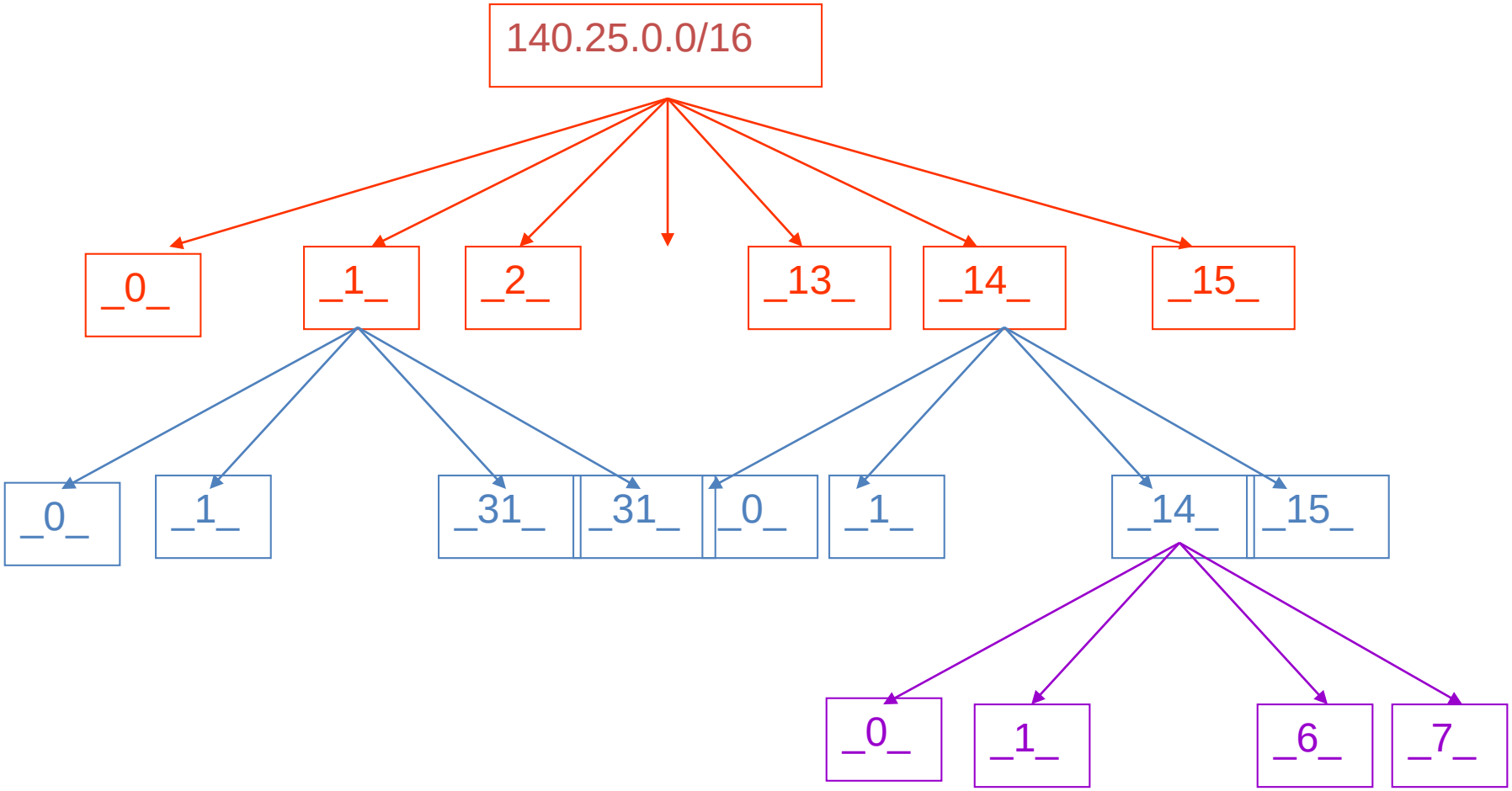
The number of 1s in the default mask is 16 (class B).

Number of bits borrowed 1024 (2^{10}).

The total number of 1s in the subnet mask is 26 (16 + 10).



VLSM Example



Excercise 1:

- ABC Mobile softwre develpemnt companhy which provides application develoopment for users on different parts of the world. This company has bought an ip address of 140.10.0.0 from an ISP. The companhy has 14 departments on different basic sales branches where it has about 2000 computers each. This company also has other 14 departments on medium income countries with about 250 computers each. Besides the compay opened new sales on 7 low income countries where each of them accomodate about 25 computers.
- Do you think the ipaddress can afford all the 35 departments and the computers on each department?
- If not what will be the solution you provide for this company?

Solution for excercise One

- **Define the 16 subnets of 140.25.0.0/16 to accoodate the first 14 departments with 2000 computer each**

  Base Network:10001100.00011001.***0000***0000.00000000=140.25.0.0/16
  SN #0: 10001100.00011001.***0000*** 0000.00000000=140.25.0.0/20
  SN #1: 10001100.00011001.***0001*** 0000.00000000 = 140.25.16.0/20
  SN #15: 10001100.00011001.***1111*** 0000.00000000 = 140.25.240.0/20

- **Define the sub-subnets for Subnet #14 for the next 14 departments with 250 computers each**

  SN#14: 10001100.00011001.1110 0000.00000000 = 140.25.224.0/20
  SN #14-0: 10001100.00011001.1110 ***0000*** .00000000 = 140.25.224.0/24
  SN #14-1: 10001100.00011001.1110 ***0001*** .00000000 = 140.25.225.0/24
  SN #14-15: 10001100.00011001.1110 ***1111*** .00000000=140.25.239.0/24

- **Define the sub 2 -subnets for Subnet #14-14 for the seven departments each with 25 computers**

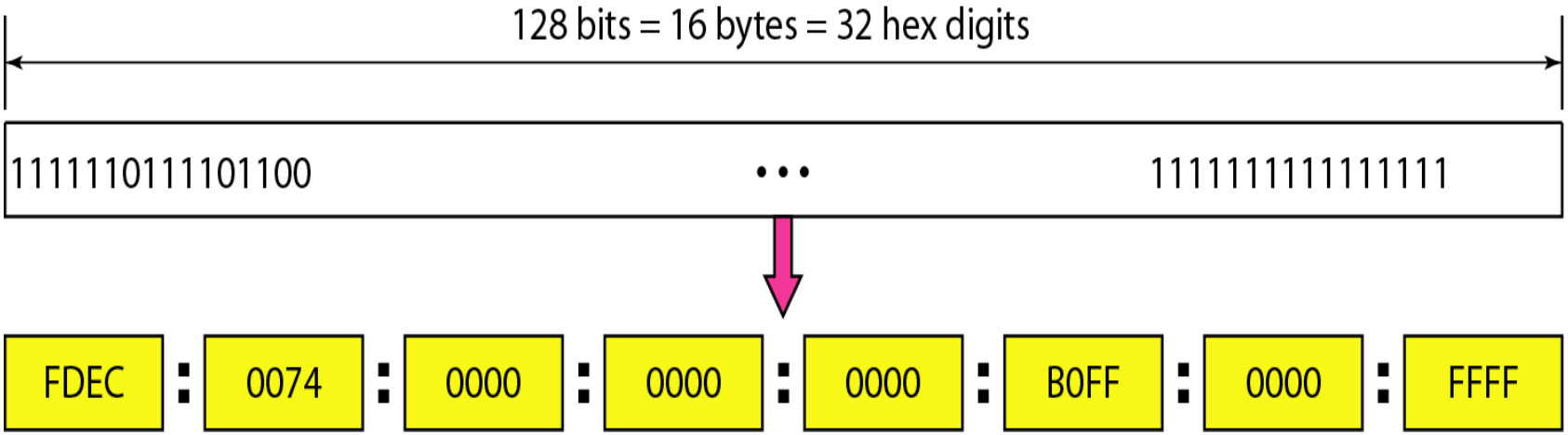
  SN #14-14:10001100.00011001.11101110.***000***00000=140.25.238.0/24
  SN14-14-0:10001100.00011001.11101110.***000***00000=140.25.238.0/27
  SN14-14-1:10001100.00011001.11101110.***001***00000=140.25.238.32/27
  SN14-14-7:10001100.00011001.11101110.***111***00000=140.25.238.224/27

IPv6 ADDRESSES

- Major points that played a key role in the birth of IPv6:
  - Internet has **grown** exponentially and IPv4 address is saturating.
    - Future Internet addresses
  - IPv4 on its own does not provide any **security** features.
    - Data has to be encrypted with some other security application before being sent on the Internet.
  - Data prioritization in IPv4 is not up-to-date. Though IPv4 has a **few bits reserved** for Type of Service or Quality of Service, but they do not provide much functionality.
  - IPv4 enabled clients can be **configured manually** or they need some address configuration mechanism.
  - It does not have a mechanism to configure a device to **have globally unique IP address**.

IPv6 ADDRESSES

- An IPv6 address is **128** bits or **32** hexadecimal digits long.



IPv6 ADDRESSES

- The Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for the assignment of IPv6 addresses. ICANN assigns a range of IP addresses to Regional Internet Registry (RIR) organizations.
- The size of address range assigned to the RIR may vary but with a minimum prefix of /12 and belong to the following range: 2000::/12 to 200F:FFFF:FFFF:FFFF::/64.
- Each **ISP** receives a /32 address from a given RIR and provid/es a /48 address for each site. Every ISP can provide $2^{(48-32)}$ = 65,536 site addresses (note: each network organized by a single entity is often called a site).
- Each **site** provides /64 address for each LAN and each site can provide $2^{(64-48)}$ = 65,536 LAN addresses for use in their private networks.
- So each **LAN** can provide 2^{64} interface addresses for hosts.

IPv6 Provider-Based Addresses

- The first IPv6 addresses will be allocated to a provider-based plan

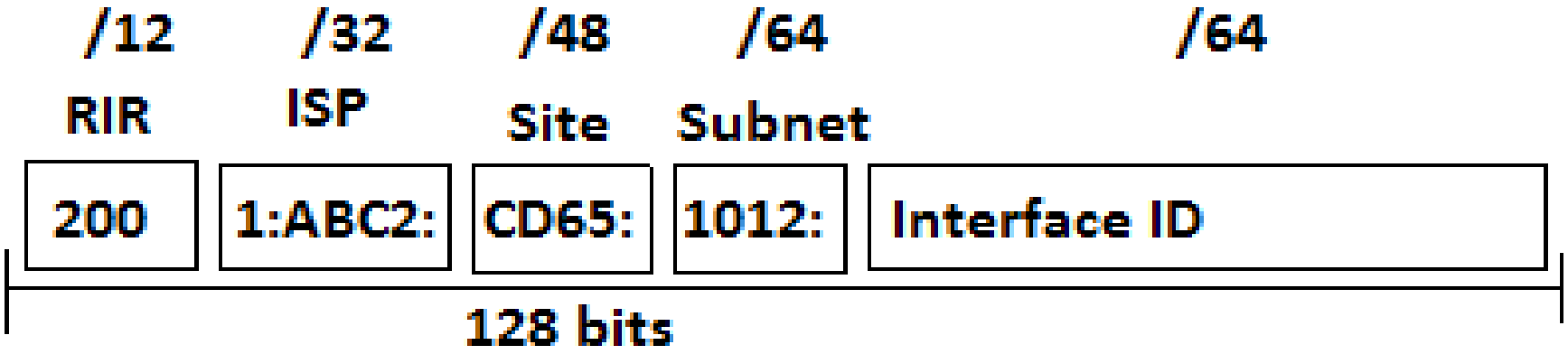
010	Registry ID	Provider ID	Subscriber ID	Subnetwork ID	Interface ID

- Type: Set to "010" for provider-based addresses
- Registry: identifies the agency that registered the address

The following fields have a variable length (recommeded length in "()")

- Provider: Id of Internet access provider *(16 bits)*
- Subscriber: Id of the organization at provider *(24 bits)*
- Subnetwork: Id of subnet within organization *(32 bits)*
- Interface: identifies an interface at a node *(48 bits)*

IPv6 ADDRESSES



0010000000000001 0000000000000000 **0011001000111000** 1101111111100001 **000000 0001100011** 0000000000000000 **0000000000000000** 1111111011111011

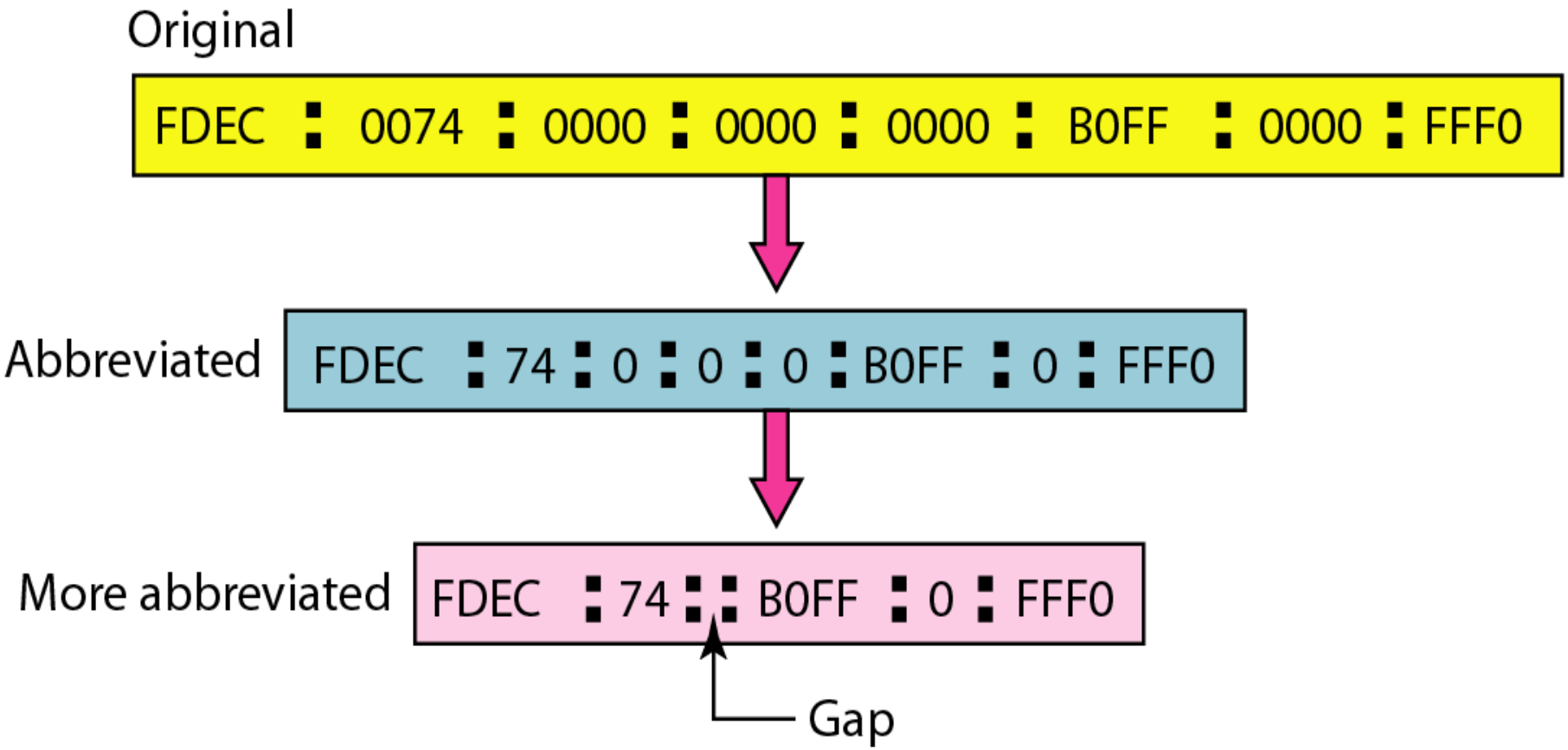
Each block is then converted into Hexadecimal and separated by ':' symbol:

2001:0000:3238:DFE1:0063:0000:0000:FEFB

IPv6 ADDRESSES

- IPv6 address In Hexadecimal format, remains long. 2001:0000:3238:DFE1:0063:0000:0000:FEFB
- Some rules to shorten the address.
  - **Rule 1:** Discard leading Zero(es):
    - In Block 5, 0063, the leading two 0s can be omitted, such as (5th block):
    - 2001:0000:3238:DFE1:63:0000:0000:FEFB
  - **Rule 2:** If two or more blocks contain consecutive zeroes, omit all of them and replace with double colon sign **::**, such as (6th and 7th block):
    - 2001:0000:3238:DFE1:63::FEFB
  - **Rule 3:** If there are still blocks of zeroes in the address, they can be shrunk down to a single zero, such as (2nd block):
    - 2001:0:3238:DFE1:63::FEFB

Abbreviated IPv6 addresses



More on IPv6 Addresses

- The provider-based addresses have a similar flavor as Classless Interdomain Routing CIDR addresses
- IPv6 provides address formats for:
  - Unicast – identifies a single interface
  - Multicast – identifies a group. Datagrams sent to a multicast address are sent to all members of the group
  - Anycast – identifies a group. Datagrams sent to an anycast address are sent to one of the members in the group.

IPv6 Address types

- In IPv6, a destination address can belong to one of three categories:
- ***Unicast Address***
  - A unicast address defines a single interface (computer or router). The packet sent to a unicast address will be routed to the intended recipient.
- ***Anycast Address***
  - An anycast address defines a group of computers that all share a single address. A packet with an anycast address is delivered to only one member of the group, the most reachable one.
- ***Multicast Address***
  - A multicast address also defines a group of computers. However, there is a difference between anycasting and multicasting. In anycasting, only one copy of the packet is sent to one of the members of the group; in multicasting each member of the group receives a copy. It is interesting that IPv6 does not define broadcasting, even in a limited version. IPv6 considers broadcasting as a special case of multicasting.

Special IPv6 Addresses

Reserved Address	Description
FF02::1	A multicast address to all nodes on a link (link-local scope)
FF02::2	A multicast address to all routers on a link
FF02::5	OSPFv3 All SPF routers
FF02::6	OSPFv3 All DR routers
FF02::9	A multicast address to all routing information protocol (RIP) routers on a link
FF02::A	EIGRP routers
FF02::1:FFxx:xxxx	All solicited-node multicast addresses used for host auto-configuration and neighbor discovery (similar to ARP in IPv4)
FF05::101	A multicast address to all Network Time Protocol (NTP) servers

TRANSITION FROM IPv4 TO IPv6

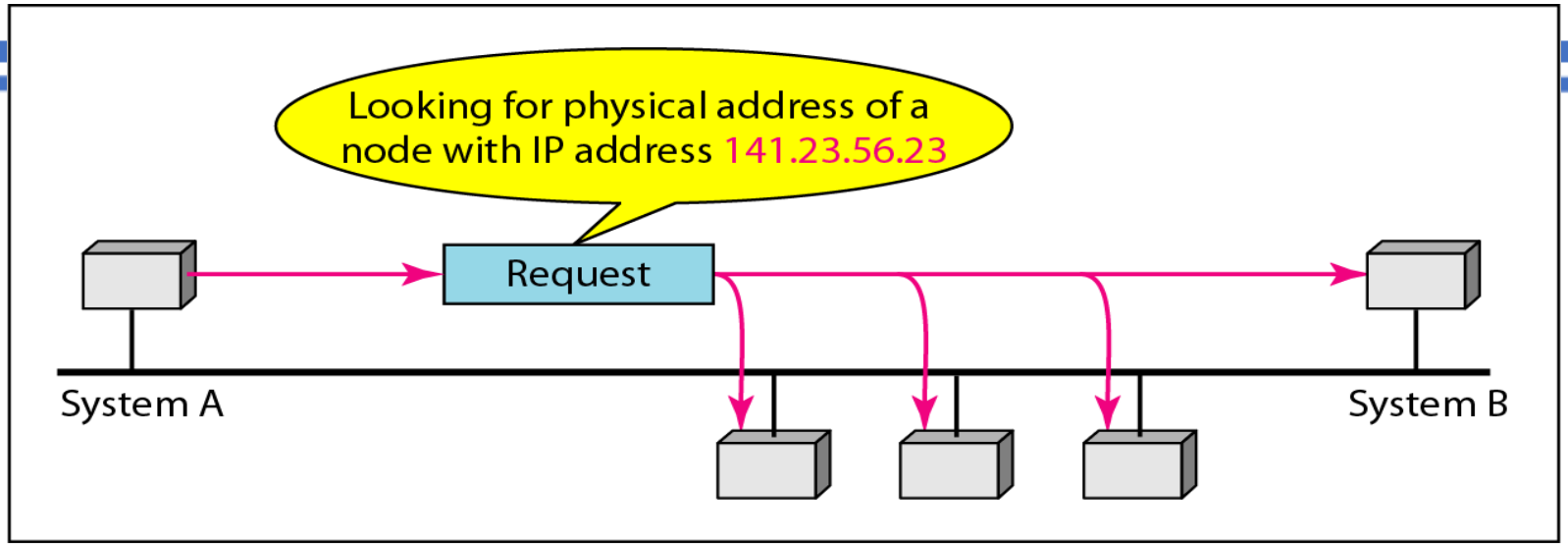
- Three strategies have been devised for transition:
  - ***Dual Stack***
    - It is recommended that all hosts, before migrating completely to version 6, have a dual stack of protocols during the transition. In other words, a station must run IPv4 and IPv6 simultaneously until all the Internet uses IPv6.
  - ***Tunneling***
    - When two computers using IPv6 want to communicate with each other and the packet must pass through a region that uses IPv4. To pass through this region, the packet must have an IPv4 address. So the IPv6 packet is encapsulated in an IPv4 packet when it enters the region, and it leaves its capsule when it exits the region.
  - ***Header Translation***
    - Is necessary when the majority of the Internet has moved to IPv6 but some systems still use IPv4. The sender wants to use IPv6, but the receiver does not understand IPv6. In this case, the header format must be totally changed through header translation. The header of the IPv6 packet is converted to an IPv4 header.

ADDRESS MAPPING

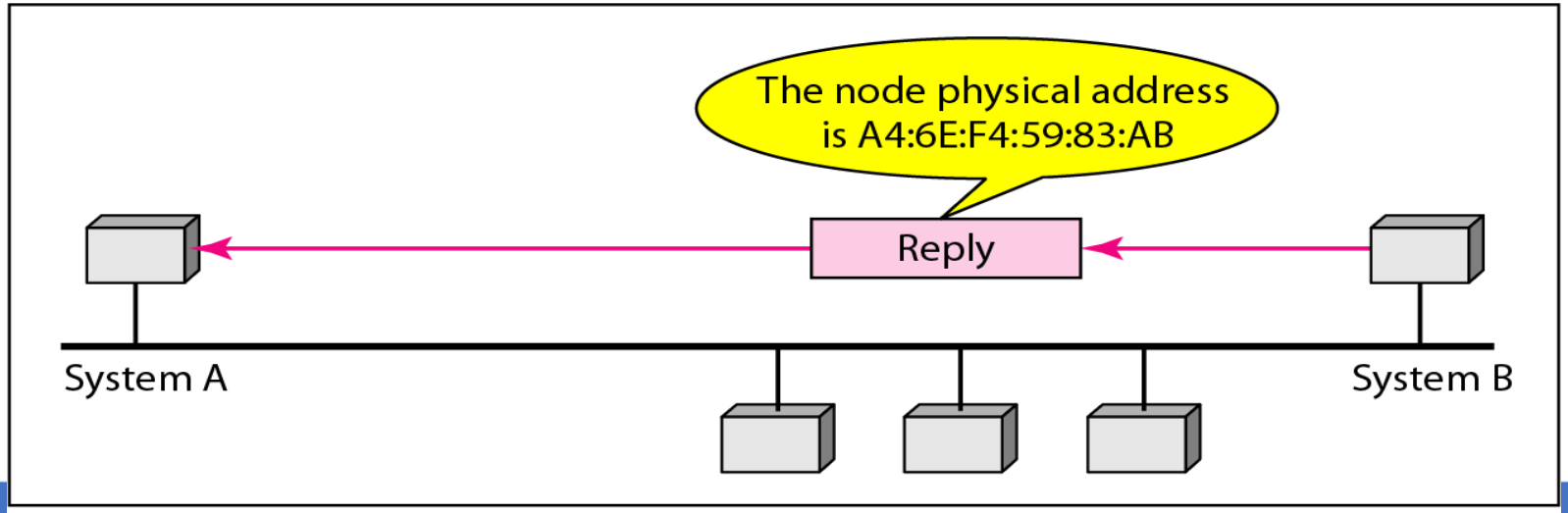
- The delivery of a packet to a host or a router requires two levels of addressing: logical and physical. We need to be able to map a logical address to its corresponding physical address and vice versa. This can be done by using either static or dynamic mapping.
- IP is used for logical addressing
- MAC is used for physical addressing in a local network such as Ethernet

Mapping Logical to Physical Address: ARP

- Anytime a host or a router has an IP datagram to send to another host or router, it has the logical (IP) address of the receiver.
- The logical (IP) address is obtained from the DNS if the sender is the host or it is found in a routing table if the sender is a router.
- But the IP datagram must be encapsulated in a frame to be able to pass through the physical network. This means that the sender needs the physical address of the receiver. The host or the router sends an ARP query packet.
- The packet includes the physical and IP addresses of the sender and the IP address of the receiver. Because the sender does not know the physical address of the receiver, the query is broadcast over the network



a. ARP request is broadcast



b. ARP reply is unicast

Mapping Physical to Logical Address: RARP

- There are occasions in which a host knows its physical address, but needs to know its logical address. This may happen in two cases:

1. A diskless station is just booted. The station can find its physical address by checking its interface, but it does not know its IP address.
2. An organization does not have enough IP addresses to assign to each station; it needs to assign IP addresses on demand. The station can send its physical address and ask for a short time lease.

Reverse Address Resolution Protocol (RARP)

- RARP finds the logical address for a machine that knows only its physical address. Each host or router is assigned one or more logical (IP) addresses, which are unique and independent of the physical (hardware) address of the machine. To create an IP datagram, a host or a router needs to know its own IP address or addresses. The IP address of a machine is usually read from its configuration file stored on a disk file.
- The machine can get its physical address (by reading its NIC, for example), which is unique locally. It can then use the physical address to get the logical address by using the RARP protocol. A RARP request is created and broadcast on the local network. Another machine on the local network that knows all the IP addresses will respond with a RARP reply.

ICMP

- The IP protocol has no error-reporting or error-correcting mechanism. The IP protocol also lacks a mechanism for host and management queries. The Internet Control Message Protocol (ICMP) has been designed to compensate for the above two deficiencies. It is a companion to the IP protocol.
- PING and TRACEROUTE are two tools for ICMP

Vlsm example

- *A company called XYZ needs to interconnect its 25 offices located around the World. In order to do that, it requires 25 public IP addresses that are requested to the ICANN. Without CIDR/VLSM, the obvious choice would be the use of a Class C address. By default a Class C address offers 8 bits for the host part, so up to 254 devices can be uniquely identified and connected to the network.*
- ***195.1.1.0/24***
- *It's clear that the company needs to pay for 254 public IP addresses (range from 195.1.1.1 to 195.1.1.254) even though it is only using 25 of them. What happens to the remaining 232 IP addresses?*
- *The introduction of CIDR/VLSM allowed the allocation of a smaller block of IP addresses:*
- ***195.1.1.0/27***
- The Subnet Mask was /24 (Class C) but is now /27 and that means 3 bits have been stolen to create the subnet field. The range of public IP assigned to the XYZ company is now from *195.1.1.1 to 195.1.1.30, a total of 30 IP addresses. This means having all 25 offices connected to the network, with a minimum waste of 5 IP addresses (while before it was 232).*

VLSM EXAMPLE

- Given the same network and requirements as in Sample Exercise 2 develop a subnetting scheme with the use of VLSM, given:
  - netA: must support 14 hosts
  - netB: must support 28 hosts
  - netC: must support 2 hosts
  - netD: must support 7 hosts
  - netE: must support 28 host
- 204.15.5.0 can be broken down into 5 different networks given the example requirement above into:
  - netB: 204.15.5.0/27 host address range 1 to 30
  - netE: 204.15.5.32/27 host address range 33 to 62
  - netA: 204.15.5.64/28 host address range 65 to 78
  - netD: 204.15.5.80/28 host address range 81 to 94
  - netC: 204.15.5.96/30 host address range 97 to 98

Vlsm eXAMPLE

- We want to divide 192.168.10.0, which is a Class C network, into four networks, each with unequal number of IPv4 addresses requirements as shown below.
  - Subnet A : 126 IPv4 Addresses.
    Subnet B : 62 IPv4 Addresses.
    Subnet C : 30 IPv4 Addresses.
    Subnet D : 30 IPv4 Addresses.
- 1) 192.168.10.0/25, which can be represented in binaries as below.
  - 11000000.10101000.00001010.00000000
    11111111.11111111.11111111.10000000
- 2) 192.168.10.128/25, which can be represented in binaries as below.
  - 11000000.10101000.00001010.10000000
    11111111.11111111.11111111.1000000
- 1) 192.168.10.128/26, which can be represented in binaries as below.
  - 11000000.10101000.00001010.10000000
    11111111.11111111.11111111.11000000
- 2) 192.168.10.192/26
  - 11000000.10101000.00001010.11 000000
    11111111.11111111.11111111.11000000
- 1) 192.168.10.192/27, which can be represented in binaries as below.
  - 11000000.10101000.00001010.11000000
    11111111.11111111.11111111.11100000
- 2) 192.168.10.224/27, which can be represented in binaries as below.
  - 11000000.10101000.00001010.11100000
    11111111.11111111.11111111.11100000

- For example, consider a traditional Class C address space like 192.168.1.0 and an organization with four groups of computers:
  - The data center with 75 hosts;
  - The call center with 50;
  - The operations floor with 25; and
  - The executive floor with 20.

?