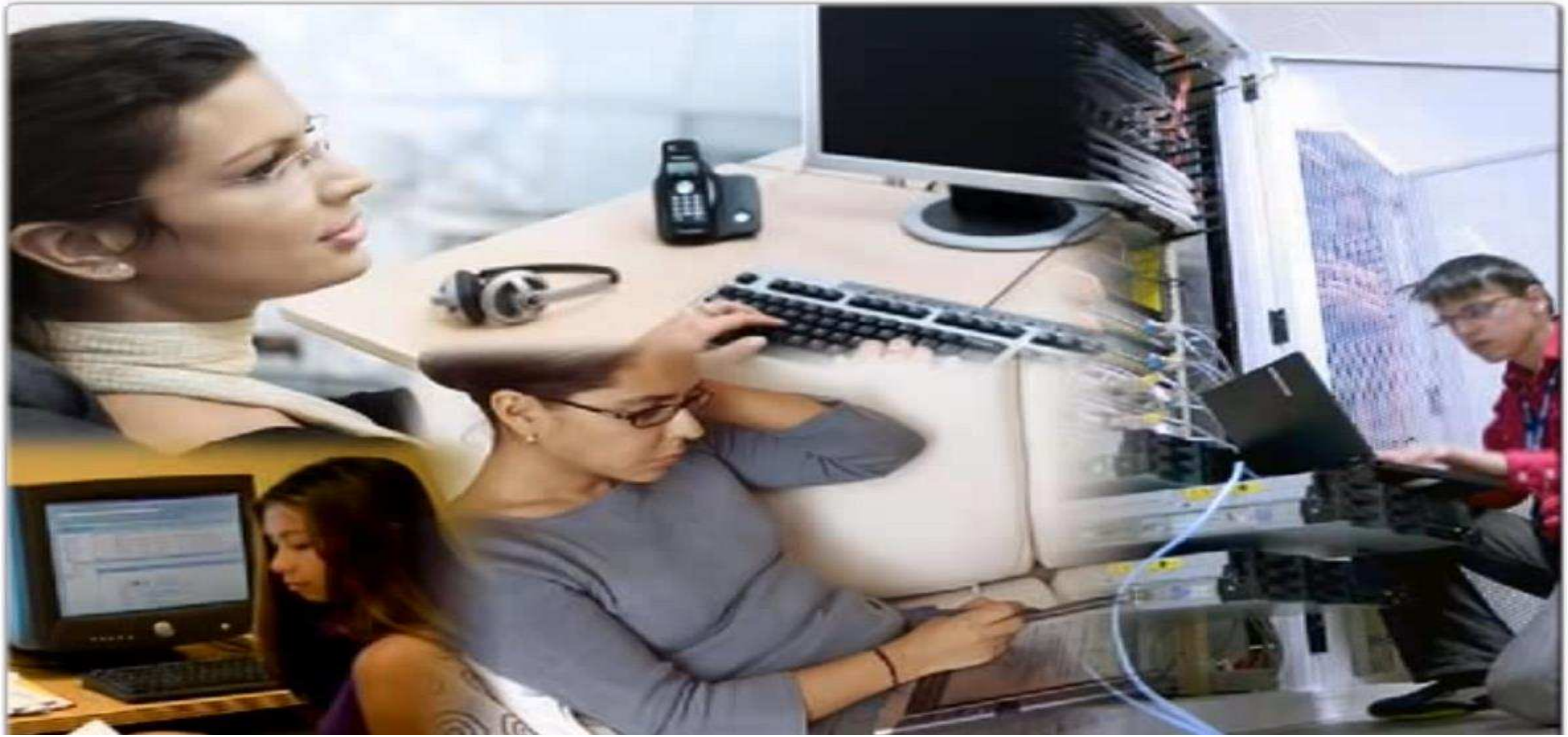
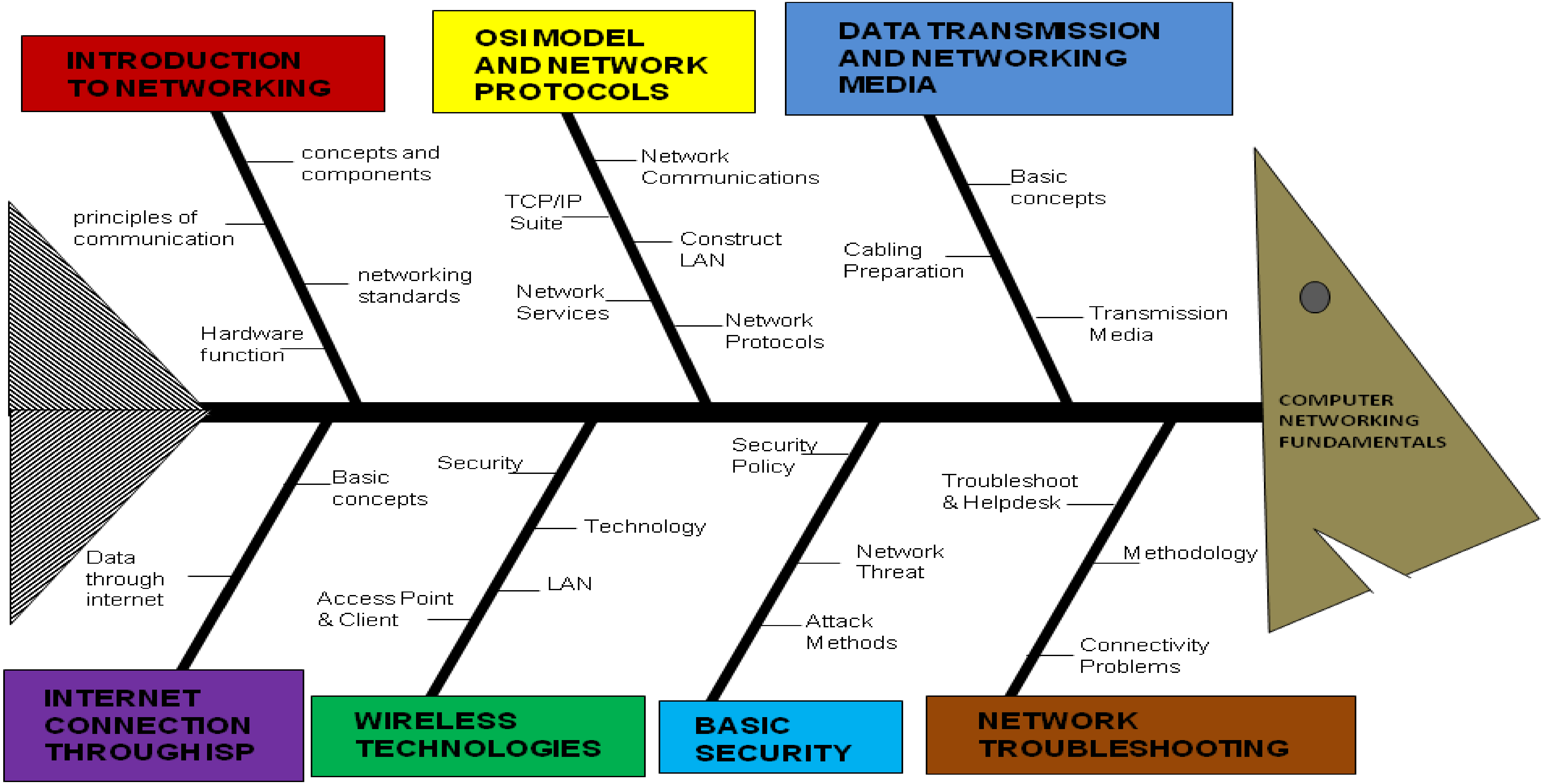
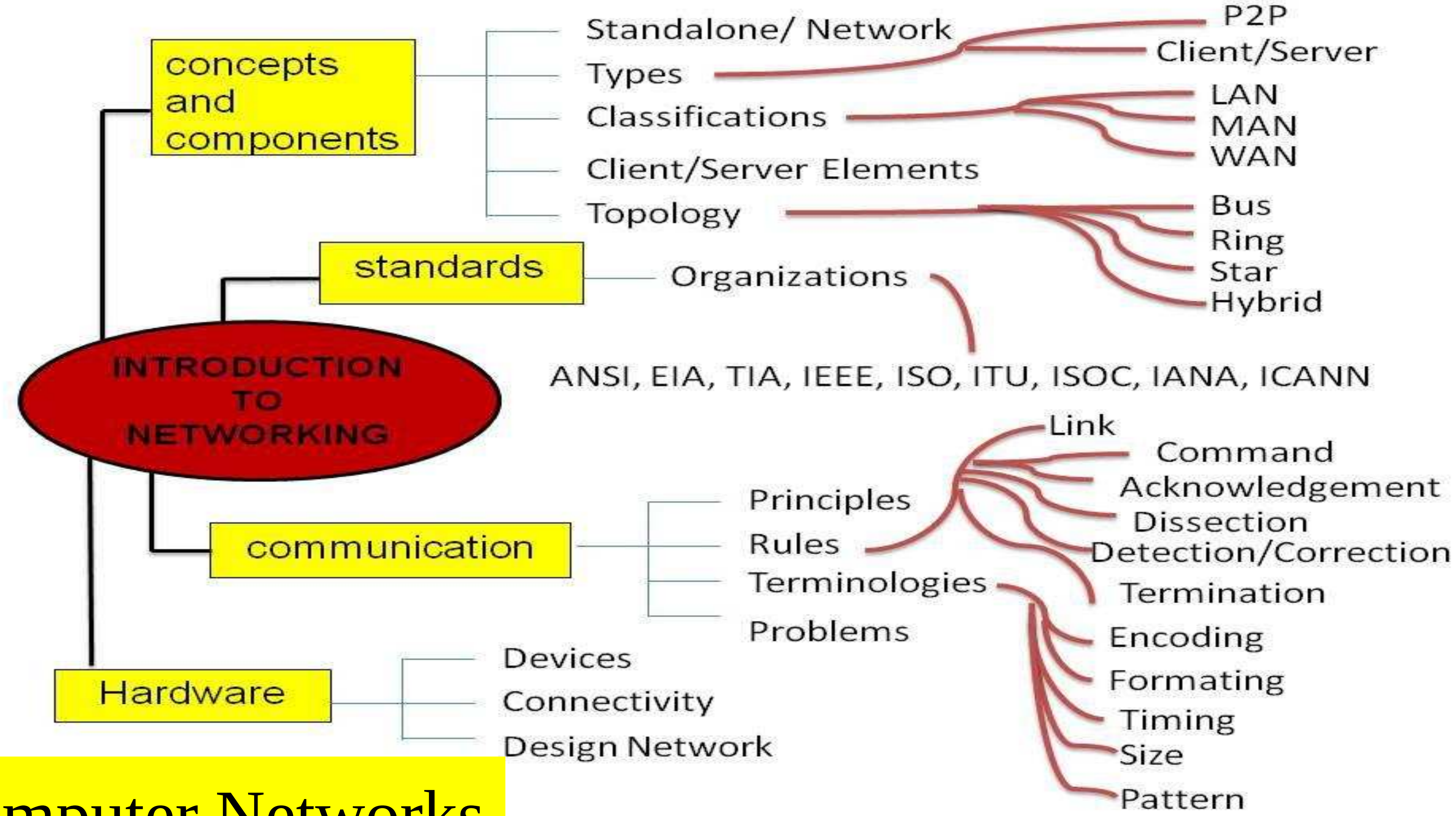
Computer Networks

Unit-1 **DATA COMMUNICATIONS**





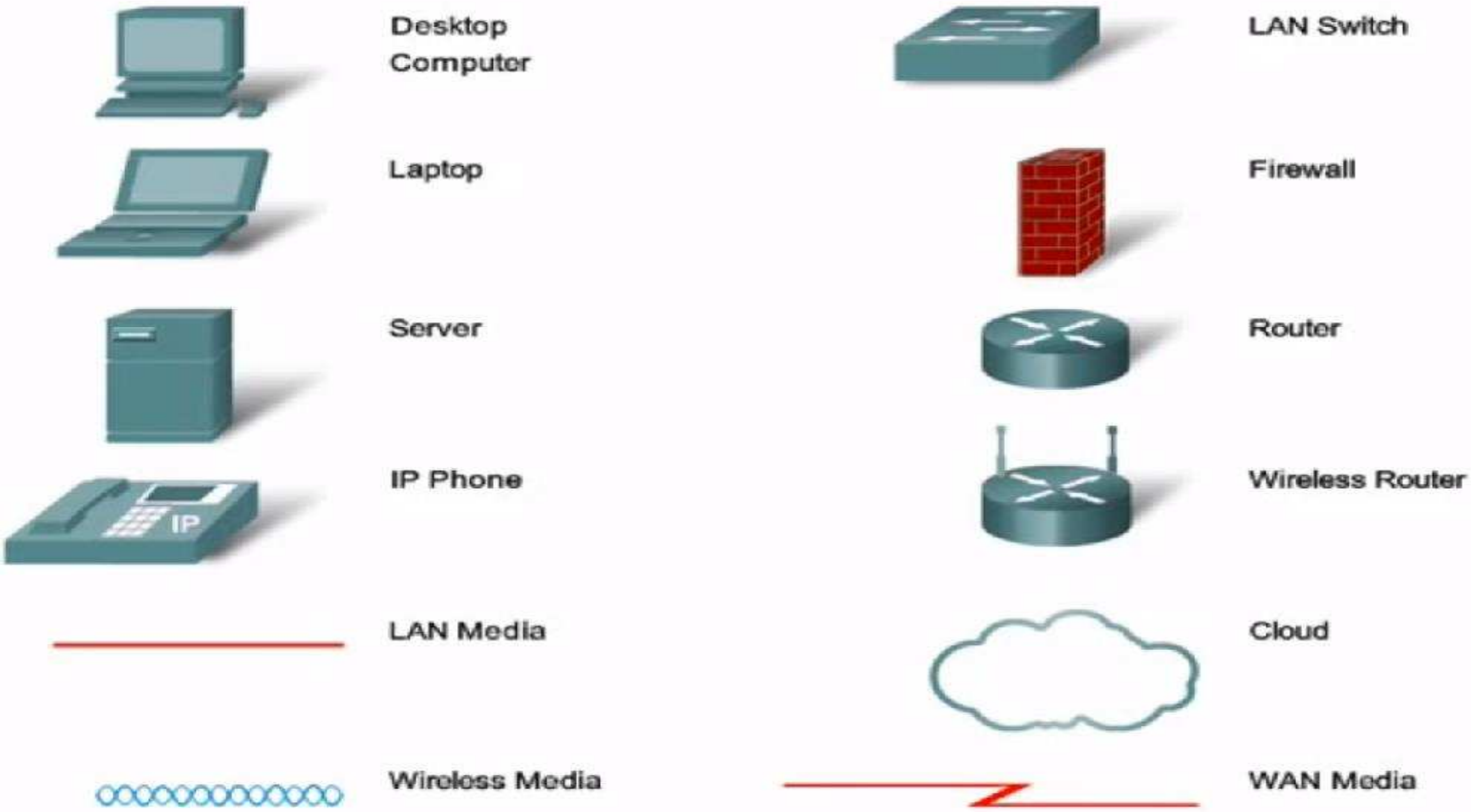
Computer Networks



- INTRODUCTION TO NETWORKING
  - concepts and components
    - Standalone/ Network
    - Types
      - P2P
      - Client/Server
    - Classifications
      - LAN
      - MAN
      - WAN
    - Client/Server Elements
    - Topology
      - Bus
      - Ring
      - Star
      - Hybrid
  - standards
    - Organizations
      - ANSI, EIA, TIA, IEEE, ISO, ITU, ISOC, IANA, ICANN
  - communication
    - Principles
    - Rules
      - Link
      - Command
      - Acknowledgement
      - Dissection
      - Detection/Correction
      - Termination
    - Terminologies
      - Encoding
      - Formating
      - Timing
      - Size
      - Pattern
    - Problems
  - Hardware
    - Devices
    - Connectivity
    - Design Network

Computer Networks

Common Data Network Symbols



Desktop Computer

Laptop

Server

IP Phone

LAN Media

Wireless Media

LAN Switch

Firewall

Router

Wireless Router

Cloud

WAN Media

Why Study Data Communications?

Revolution is occurred in telecommunications networks

Accessibility

– to get accurate information.

- data/information sharing?
- Eg: From one pc – data copied onto a floppy disk and physically reloaded to another pc/remote computer – time consuming, inconveniences.

Technological advances drive communication links to carry more and faster signals.

1. Uses sign language...
2. Writes note: *Sorry I do not understand signing.*
3. Writes note: *Can we use written notes?*
4. Yes, that will be fine.

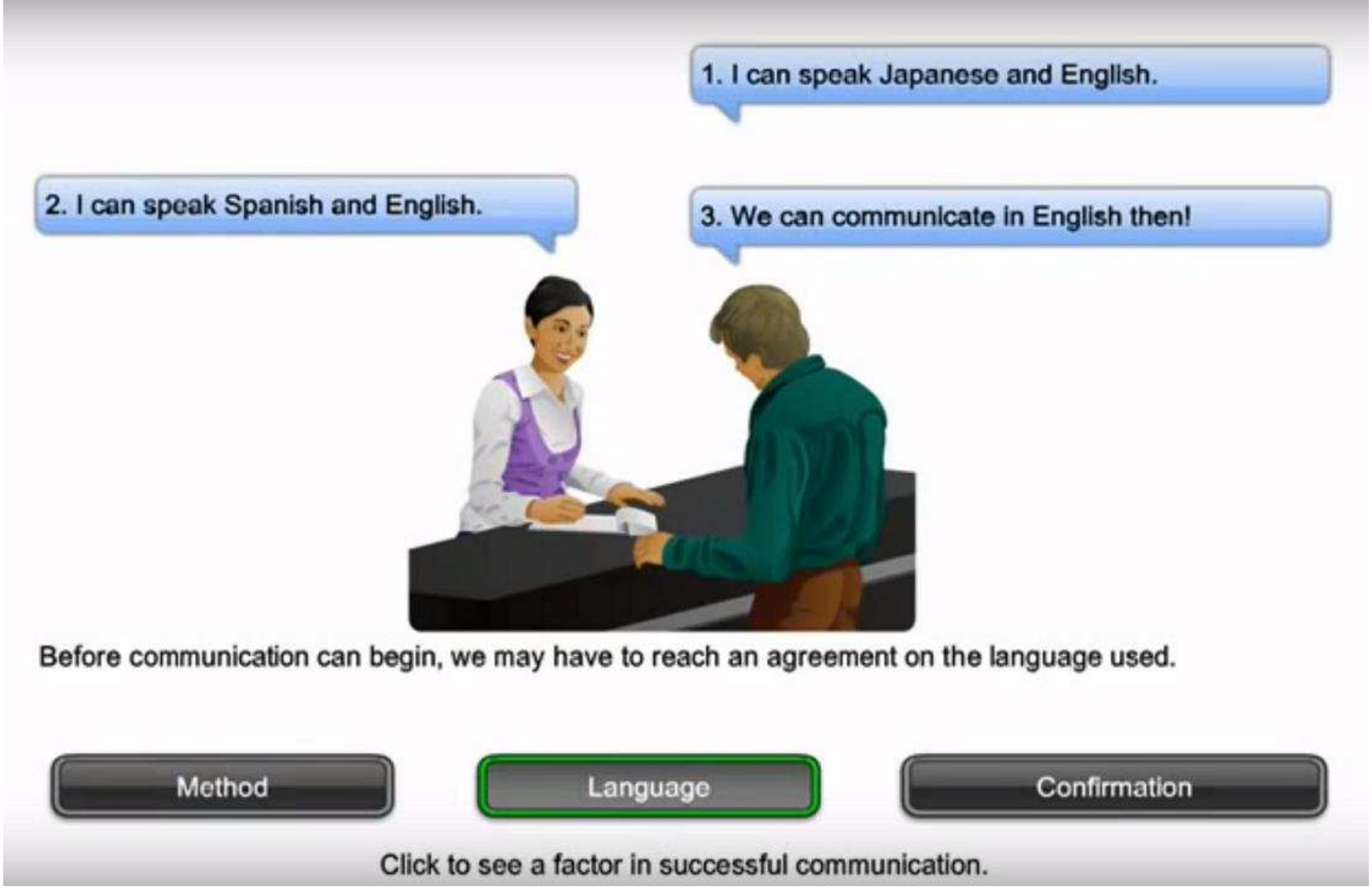
Before communication can begin, we may have to reach an agreement on the method used.

Method

Language

Confirmation

Click to see a factor in successful communication.



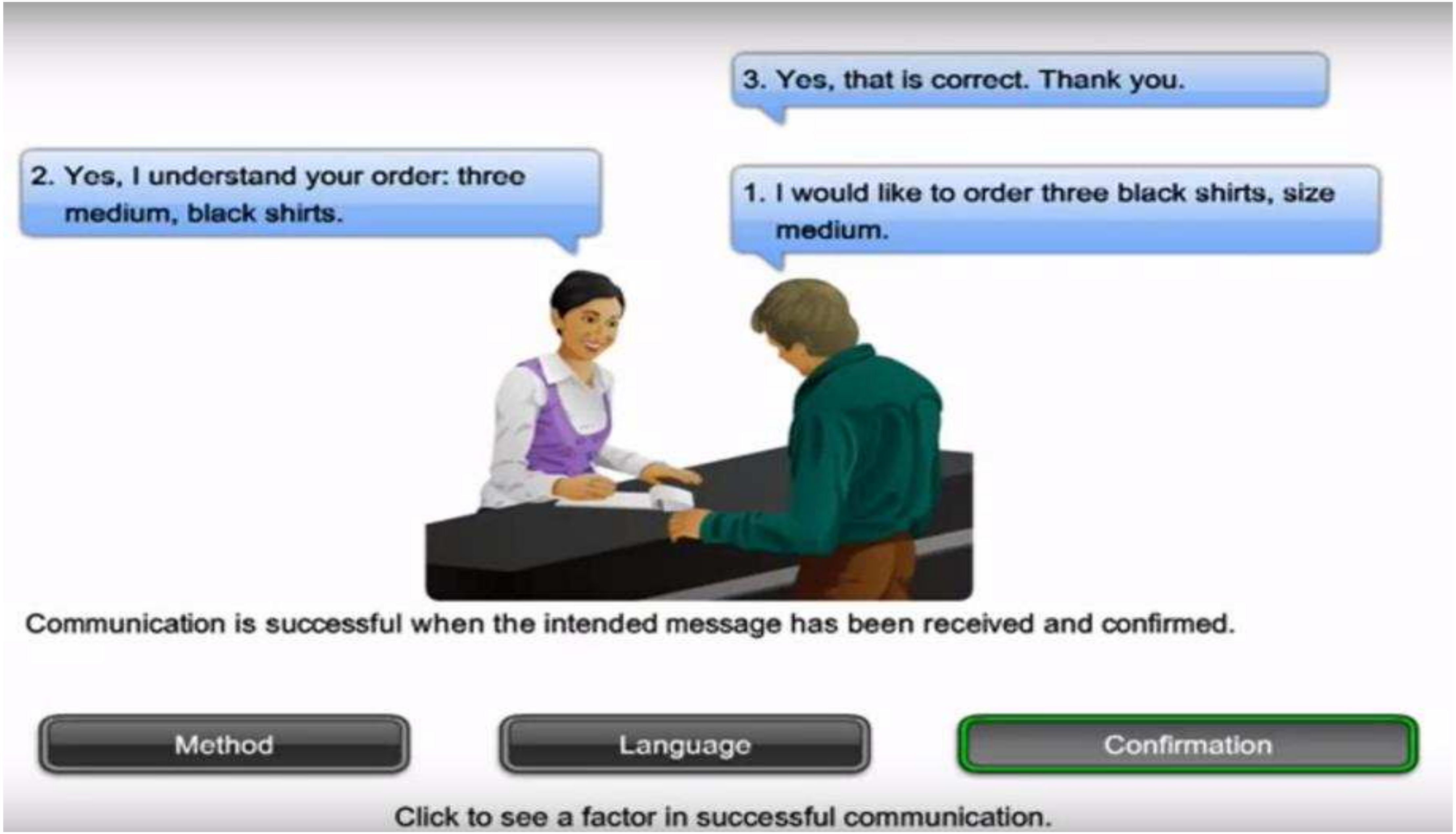
1. I can speak Japanese and English.

2. I can speak Spanish and English.

3. We can communicate in English then!

Before communication can begin, we may have to reach an agreement on the language used.

Click to see a factor in successful communication.



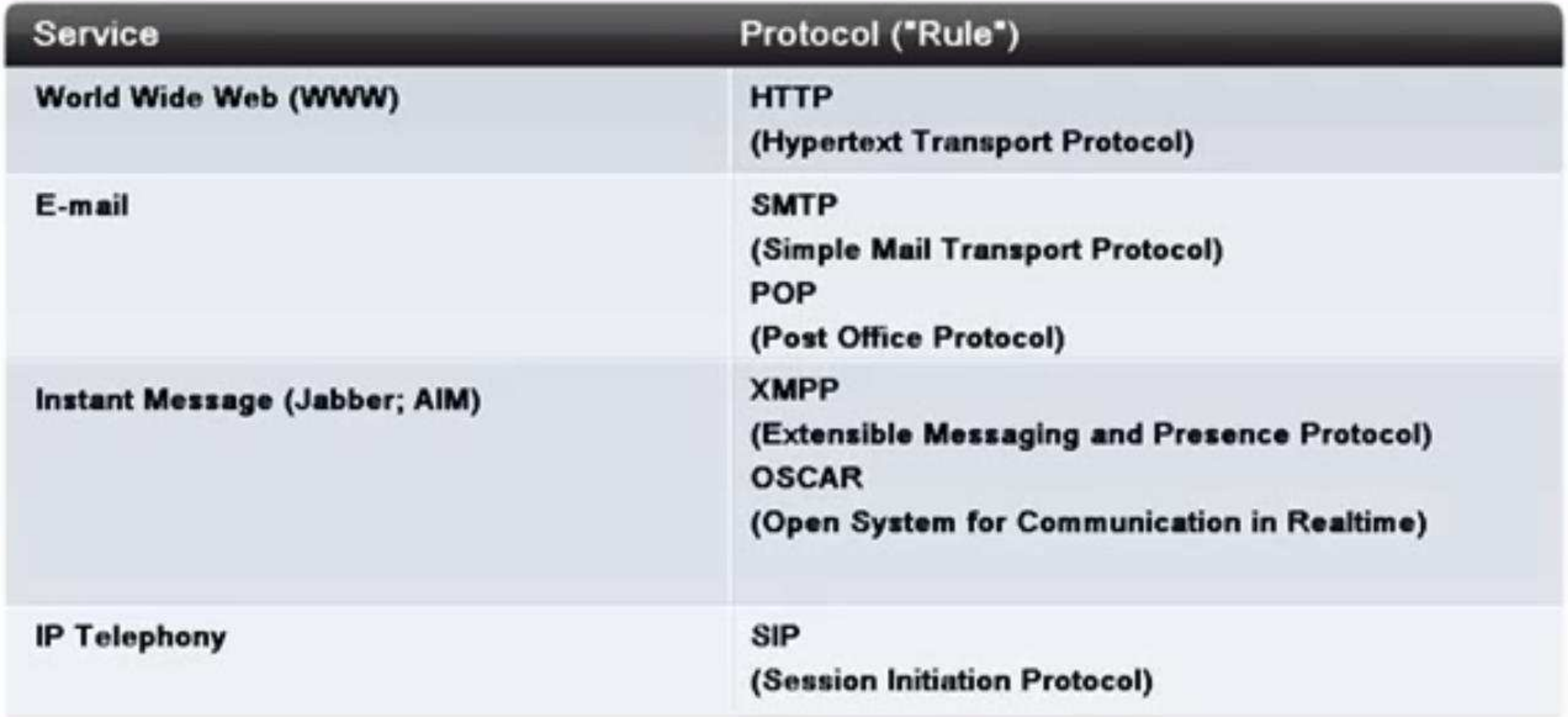
3. Yes, that is correct. Thank you.

2. Yes, I understand your order: three medium, black shirts.

1. I would like to order three black shirts, size medium.

Communication is successful when the intended message has been received and confirmed.

Click to see a factor in successful communication.



Service	Protocol ("Rule")
World Wide Web (WWW)	HTTP (Hypertext Transport Protocol)
E-mail	SMTP (Simple Mail Transport Protocol) POP (Post Office Protocol)
Instant Message (Jabber; AIM)	XMPP (Extensible Messaging and Presence Protocol) OSCAR (Open System for Communication in Realtime)
IP Telephony	SIP (Session Initiation Protocol)

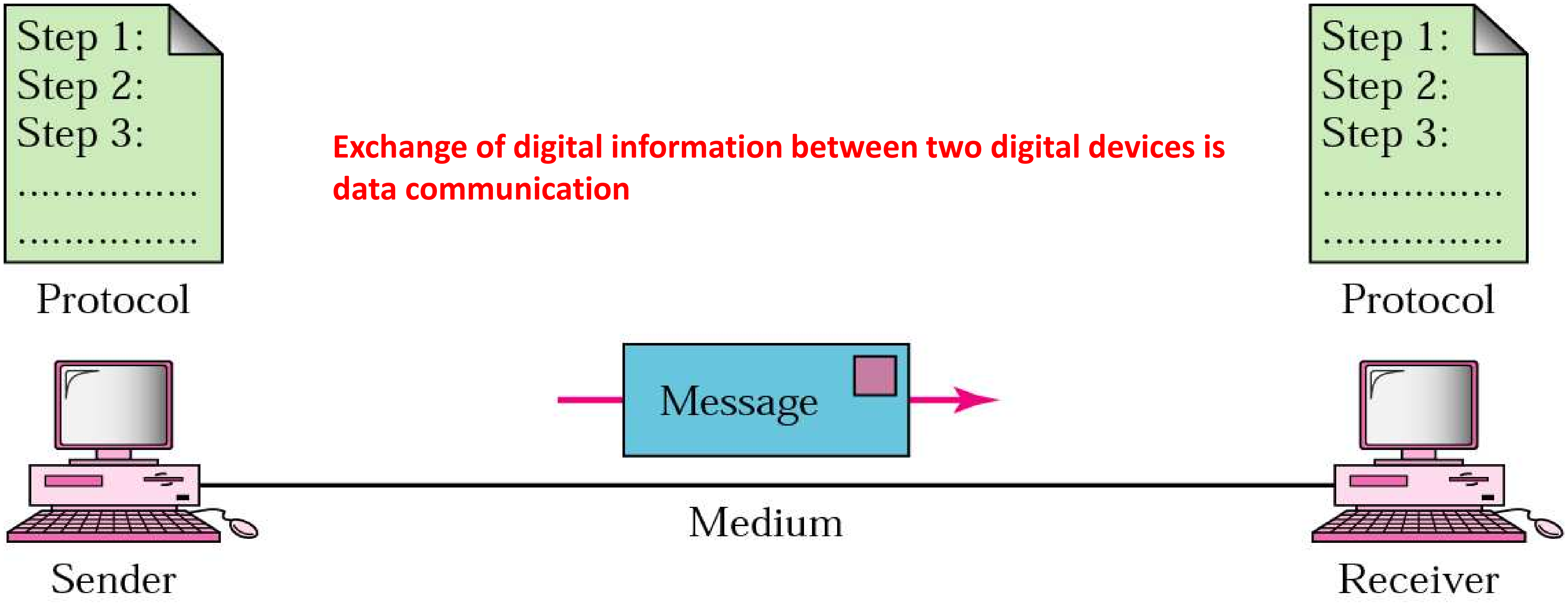
Terminologies of Data communication

- Data- Information that has been processed, organized and stored.
- Data communication-transmission, reception & processing of digital information.
- Network/ nodes/ stations- set of devices interconnected by media links Simple- two computers or a computer with a printer Complex- one or more main frame computers with a thousand remote terminals.

Data Communication

- Data communications (DC) is the process of using computing and communication technologies to transfer data from one place to another, and vice versa.
- It enables the movement of electronic or digital data between two or more nodes, regardless of geographical location, technological medium or data contents.

Basic Components of Data Communication

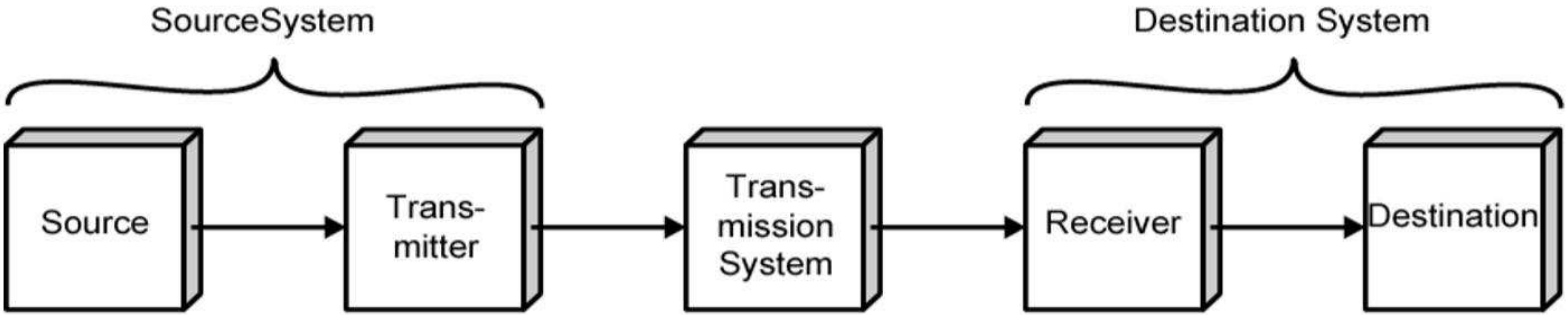


Exchange of digital information between two digital devices is data communication

Five Components :

1. **Message** – the information (data) to be communicated. Can consists of text, numbers, picture, audio, video.
2. **Sender** – the device that sends the data message. Can be a computer, workstation, mobile phone, video cam etc
3. **Receiver** – the device that receives the message. Can be a computer, workstation, mobile phone, tv etc.
4. **Medium** – the physical path by which a message travels from sender to receiver. UTP cable, coaxial, fiber optic, radio wave.
5. **Protocol** – A set of rules that govern data communication. Represent an agreement between the communicating devices.

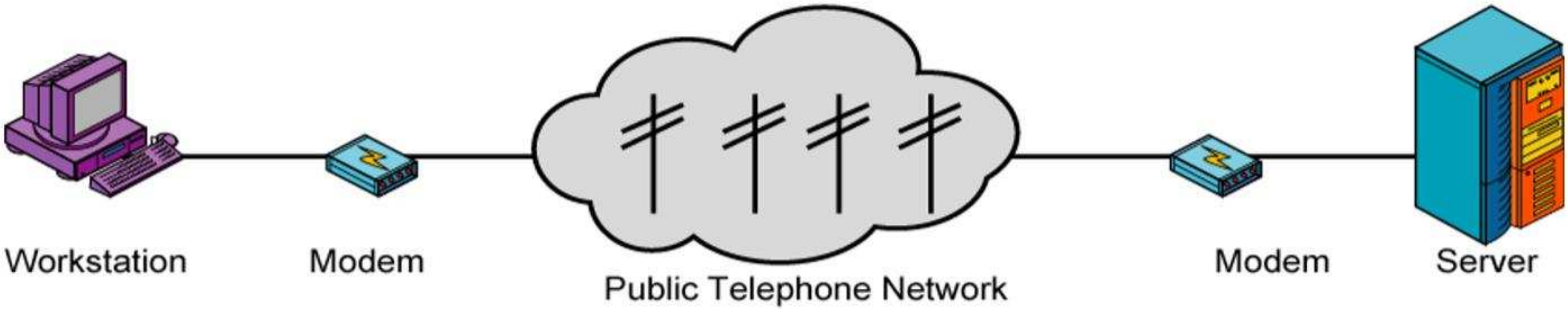
Simplified block diagram of data communication network



Some devices/technologies used in data communications are known as **data communication equipment (DCE)** and **data terminal equipment (DTE)**.

- DCE is used at the sending node
- DTE is used at the receiving node

(a) General block diagram



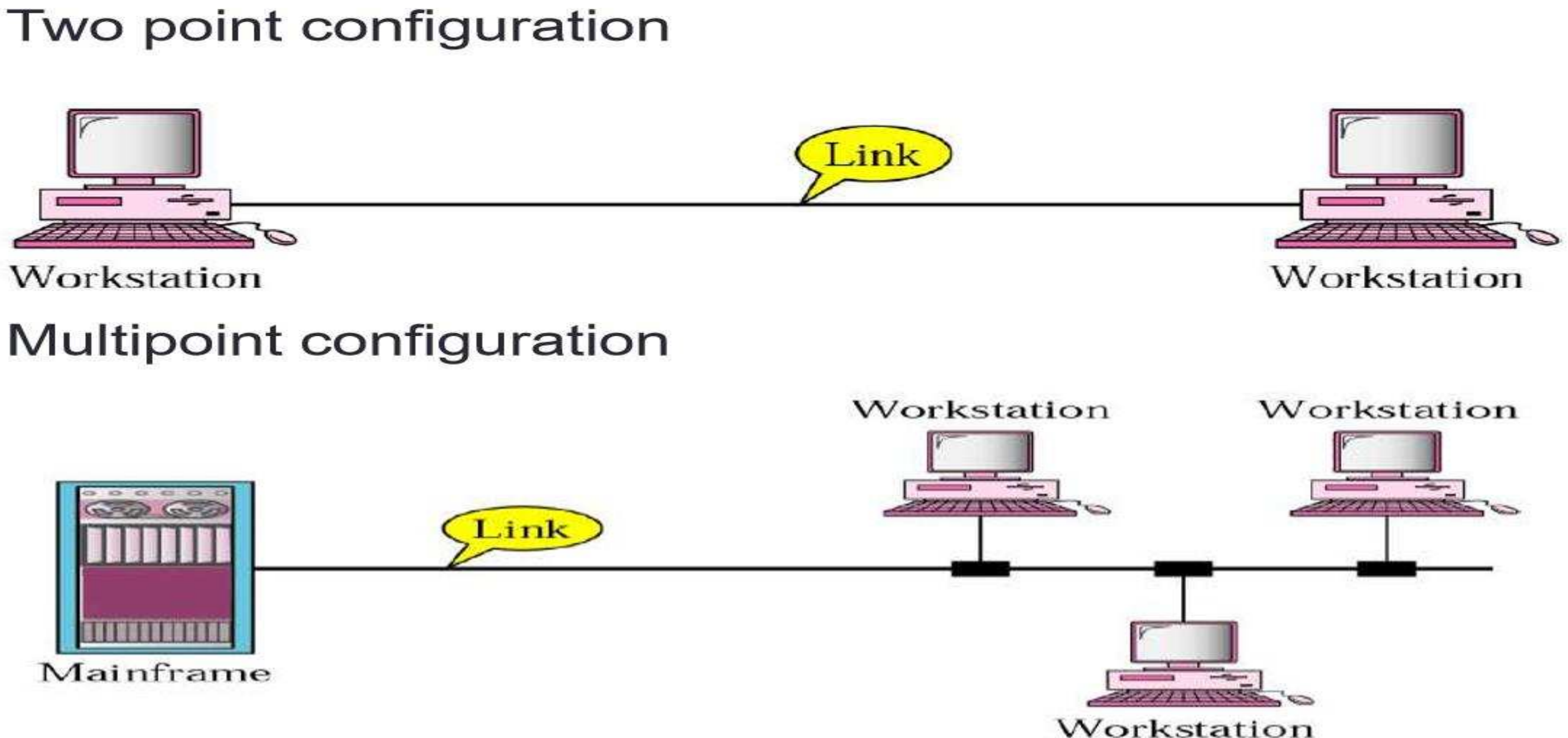
Effectiveness of a data communication system

- The effectiveness of a data communication system depends on 4 fundamental characteristics :

1. **delivery** – the system must deliver data to the correct destination.
2. **accuracy** – the system must deliver data accurately.
3. **timeliness** – The system must deliver data in timely manner.
4. **Jitter** – variation in arrival time

Data Communication circuit arrangements

- **Circuit Configurations**
  - **Point to Point Communication:** Involves only two stations on a circuit.
  - **Multipoint:** Involves more than two stations in a circuit.



Data Transmission

- Data Transmission means movement of the bits over a transmission medium connecting two devices.

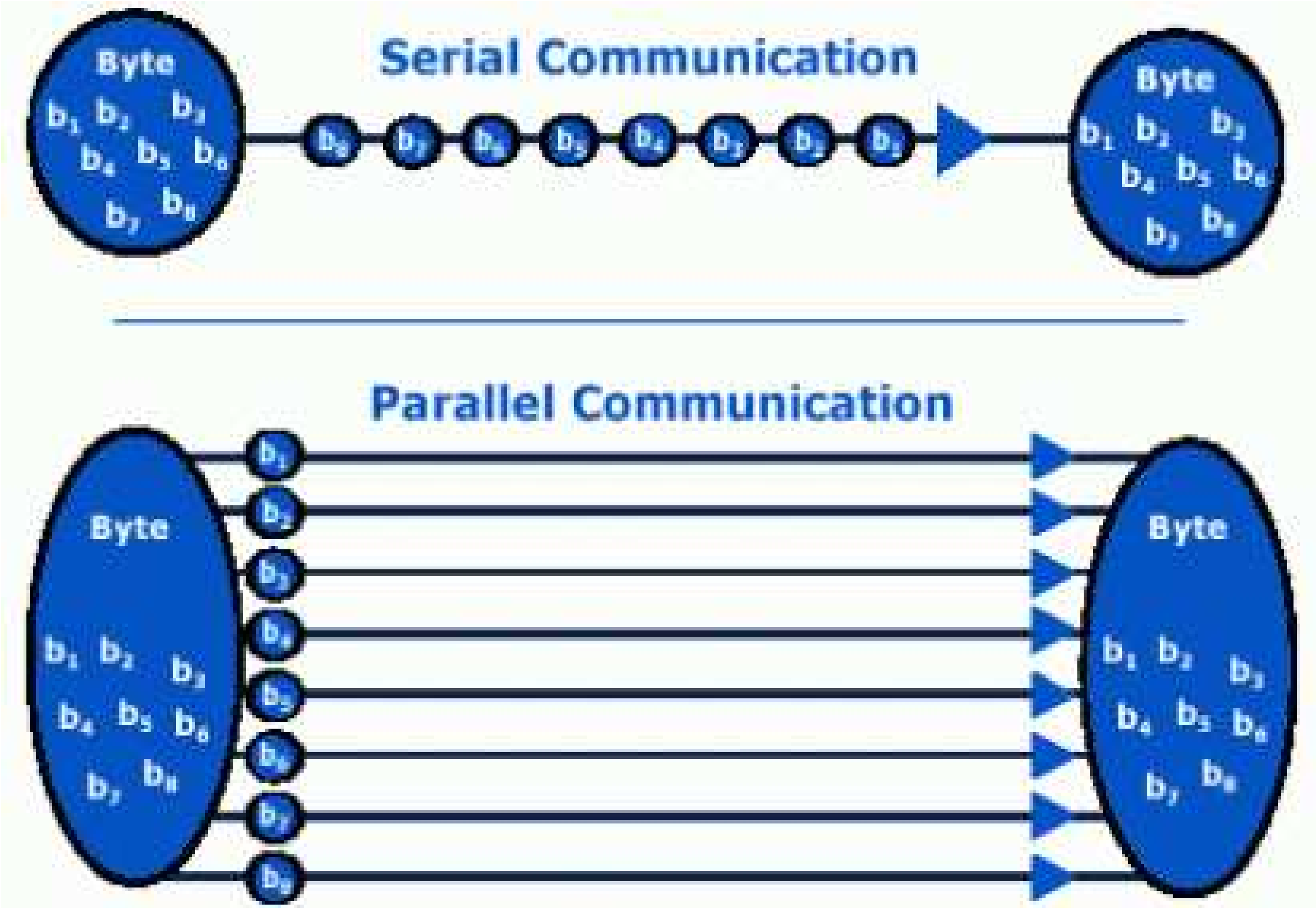
It enables devices or components within devices to speak to each other.

- Two types of Data Transmission are:

Parallel Transmission Serial Transmission

- Serial data transmission sends data bits one after another over a single channel.
- Parallel data transmission sends multiple data bits at the same time over multiple channels.

Serial and Parallel Data Transmission



Types of Serial Transmission

- Serial transmission has two classifications: asynchronous and synchronous.
- **Asynchronous Serial Transmission**

❖Data bits can be sent at any point in time.

❖Stop bits and start bits are used between data bytes to synchronize the transmitter and receiver and to ensure that the data is transmitted correctly.

❖The time between sending and receiving data bits is not constant, so gaps are used to provide time between transmissions.

- **Synchronous Serial Transmission**

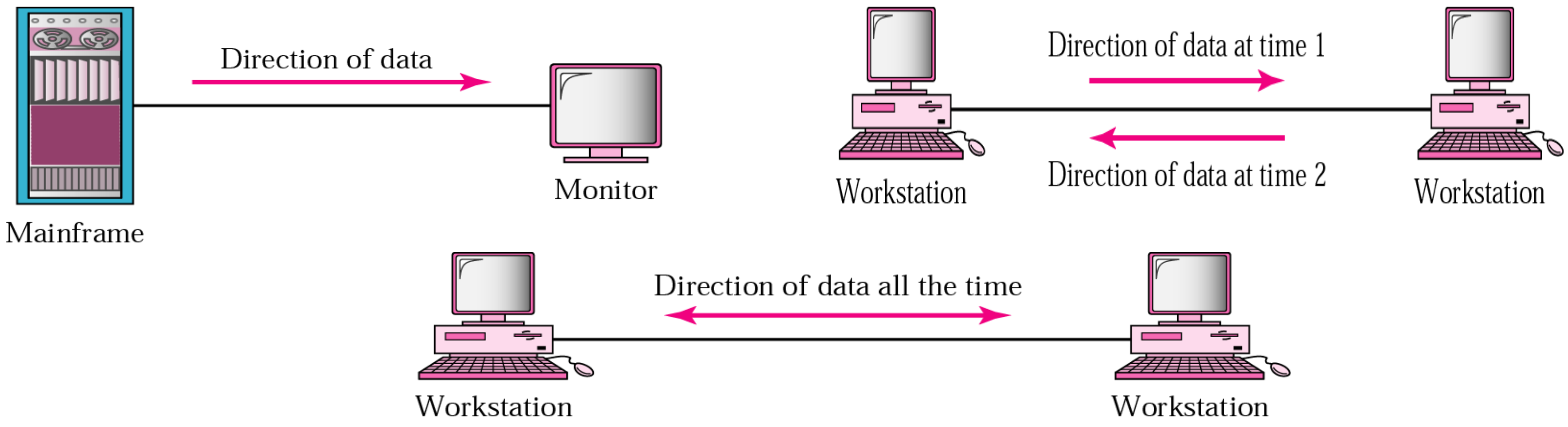
❖Data bits are transmitted as a continuous stream in time with a master clock.

❖The data transmitter and receiver both operate using a synchronized clock frequency; therefore, start bits, stop bits, and gaps are not used.

❖This means that data moves faster and timing errors are less frequent because the transmitter and receiver time is synced. However, data accuracy is highly dependent on timing being synced correctly between devices.

Transmission Modes

- Simplex: Transmit only or receive only or one way only lines. eg. Television


Direction of data
Mainframe
Monitor
Direction of data at time 1
Direction of data at time 2
Workstation
Workstation
Direction of data all the time
Workstation
Workstation

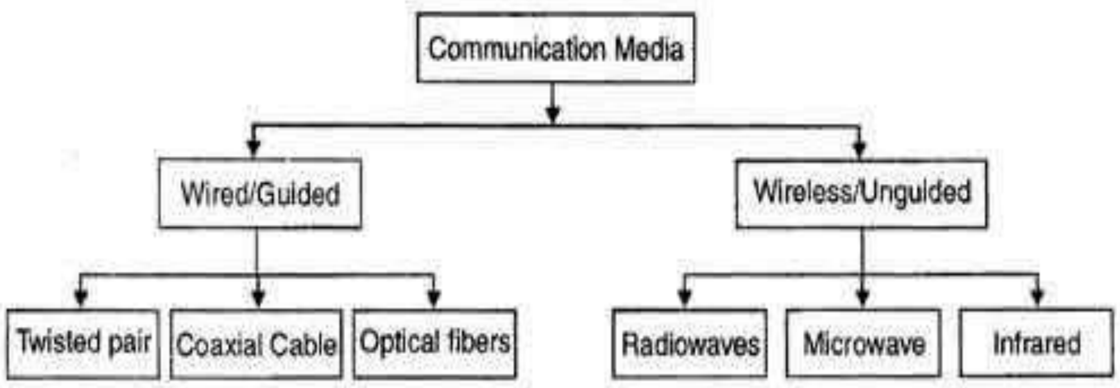
- Half Duplex: Two way alternate or either way lines. eg. police radio
- Full Duplex:Two way simultaneous or both way lines. eg. telephone

FACTORS TO BE CONSIDERED WHILE CHOOSING TRANSMISSION MEDIUM

- Transmission Rate
- Cost and Ease of Installation
- Resistance to Environmental Conditions
- Distances

Transmission Media

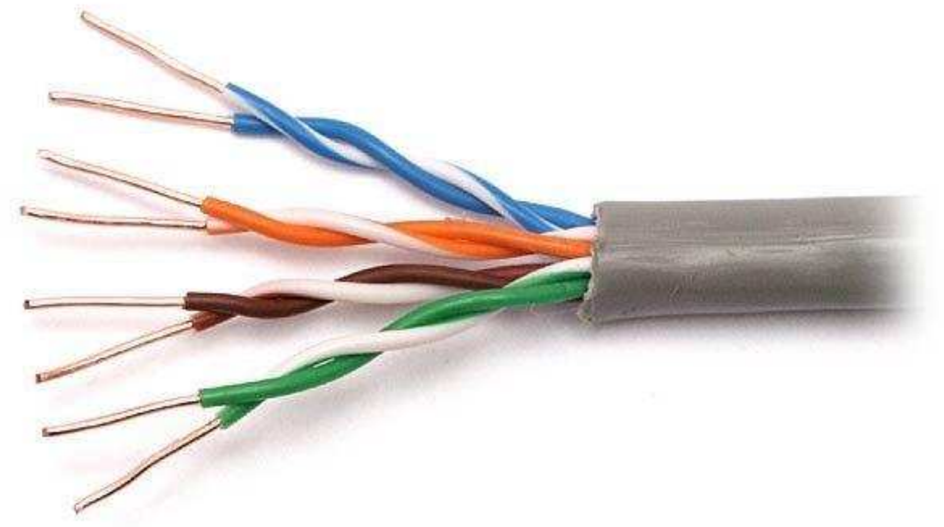
- **Guided Media**
- With guided **transmission media**, the waves are guided along a physical path; examples of guided **media** include phone lines, twisted pair cables, coaxial cables, and optical fibers. Wired
- **Unguided Media**
- Unguided **transmission media** are methods that allow the **transmission** of data without the use of physical means to define the path it takes.



Guided/Wired Media

- Guided transmission media uses a “Cabling System” that guide the data signal along a specific path.
- The data signals are bounded by cabling system so guided media is also known as bounded media.
- Three basic types of guided media:-
- Twisted Pair Cable
- Coaxial Cable
- Optical Fibre

Guided/Wired

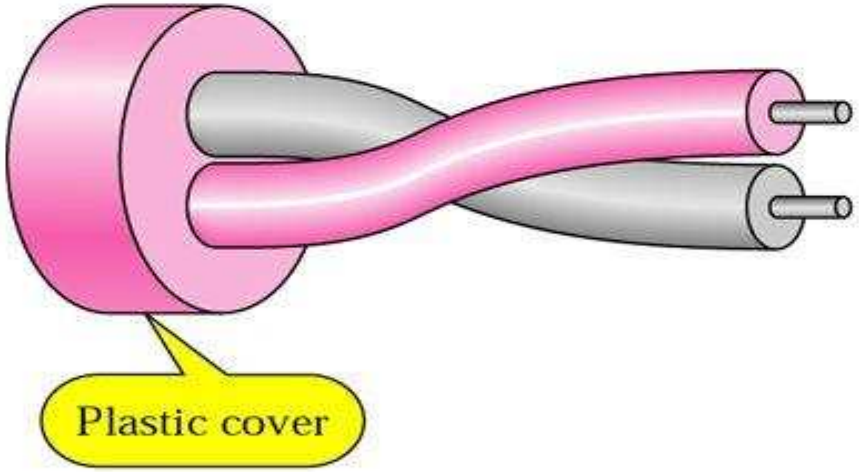


1. Twisted Pair Cable:-

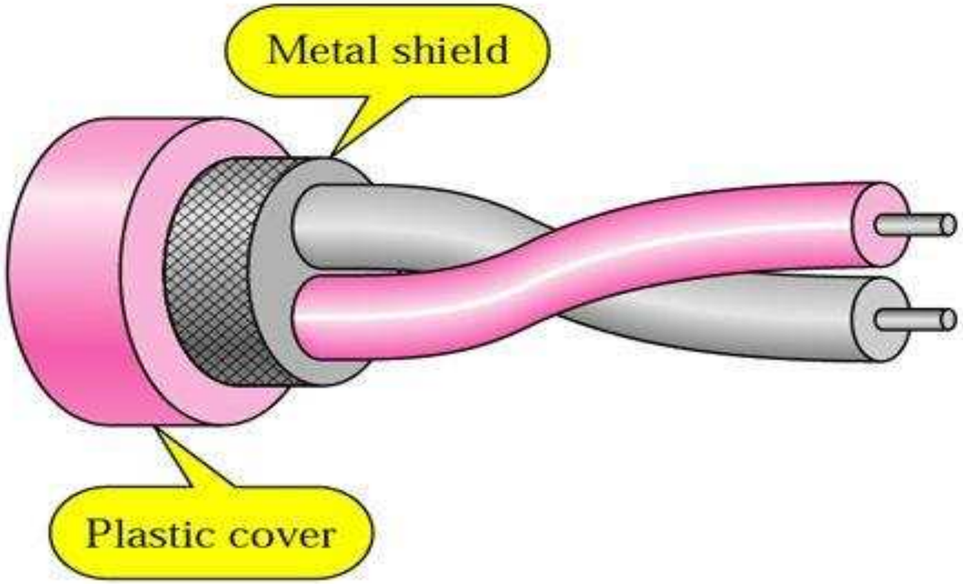
- Most popular communication media
- The wires in twisted pair cable are twisted together in pairs.
- Each pair would consist of a wire used for the positive data signal and a wire for the negative data signal.
- Any noise that appears in the wire of the system creates a disturbance on the other wire.
- It is the cheapest and easily available system which can carry data or information to the destination.
- It is mostly used in telecommunication.

Types of Twisted pair cable

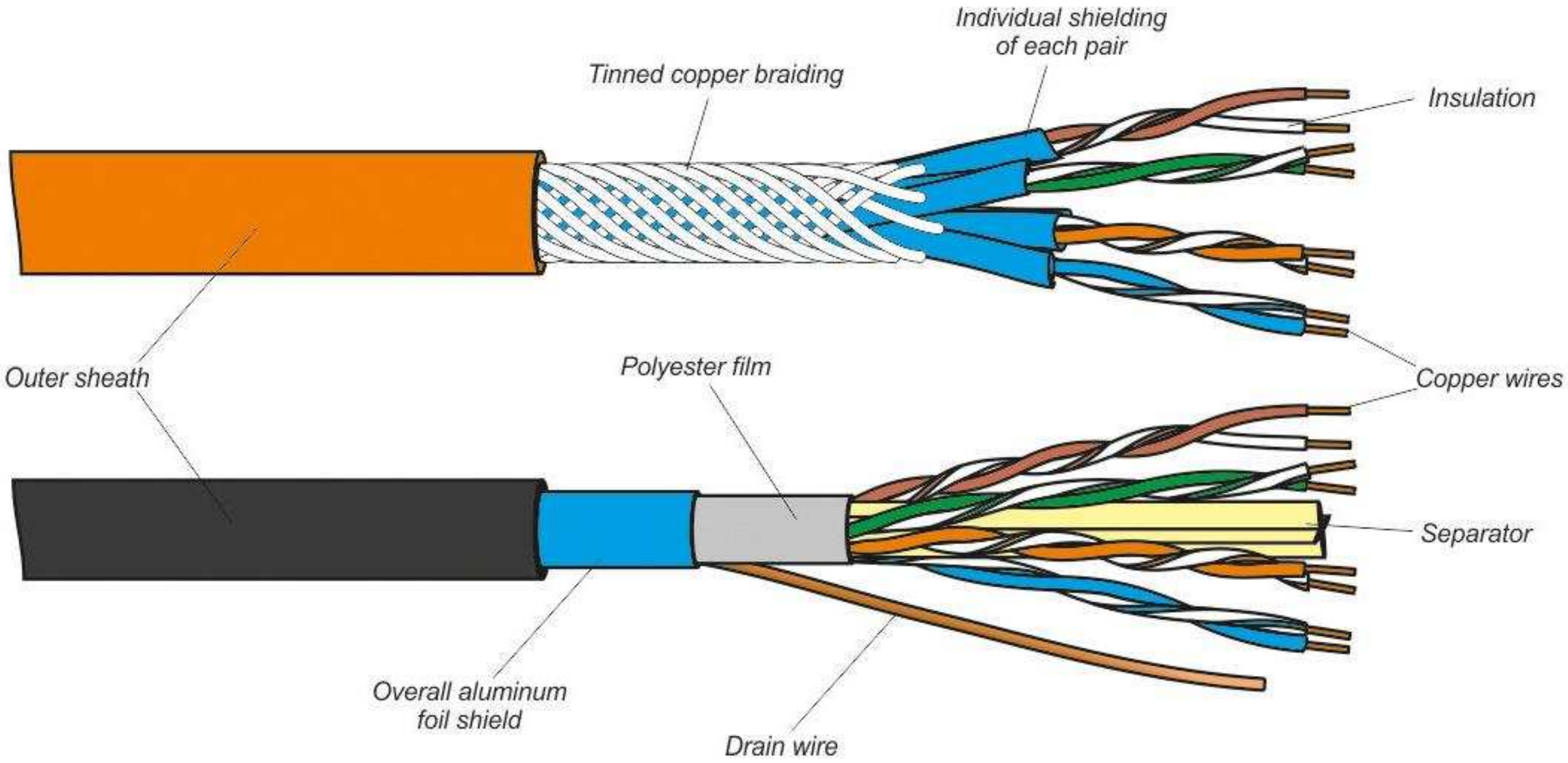
- Unshielded twisted pair cable (UTP).
- Shielded Twisted pair cable (STP).

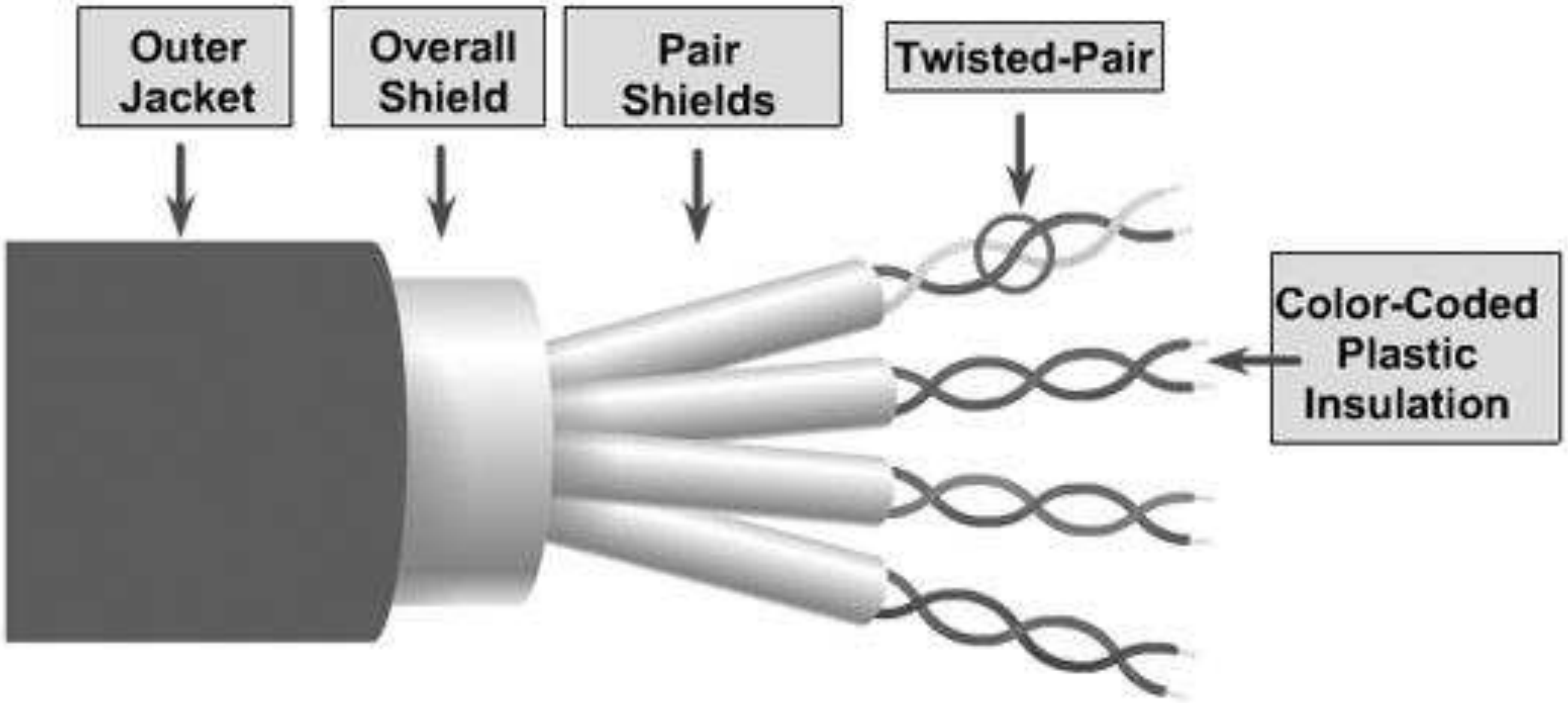


a. UTP

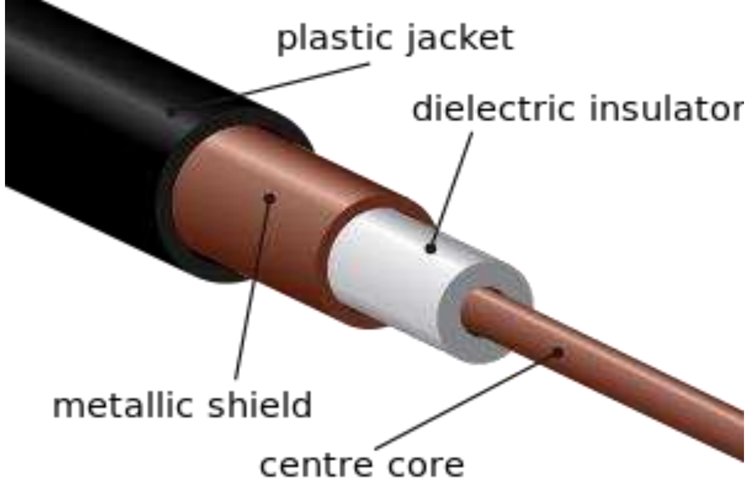


b. STP


Individual shielding of each pair
Tinned copper braiding
Insulation
Outer sheath
Polyester film
Copper wires
Separator
Overall aluminum foil shield
Drain wire


Outer Jacket
Overall Shield
Pair Shields
Twisted-Pair
Color-Coded Plastic Insulation

Guided/Wired



2. Coaxial Cable

A coaxial cable is a type of shielded and insulated copper cable that is used in computer networks and to deliver cable TV services to end users.

It consists of four primary components, as follows:

- A core copper wire, which serves as the primary channel.
- A dielectric insulator, which surrounds the copper.
- Metallic Shield beneath the insulator. This is used to protect from external electromagnetic interference.
- The last layer, which is made of Teflon or plastic jacket, is used to protect the inner layers from physical damage, such as fire and water.

Guided/Wired

3. Optical Fibers

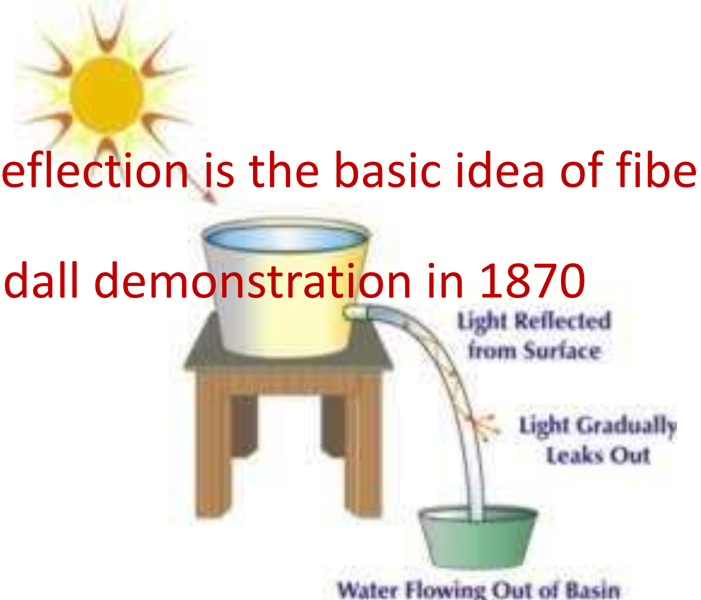
- Fiber-optic cables are now the main way of carrying information over long distances because they have three very big advantages over old-style copper cables:
- **Less attenuation**: (signal loss) Information travels roughly 10 times further before it needs amplifying—which makes fiber networks simpler and cheaper to operate and maintain.
- **No interference**: Unlike with copper cables, there's no "crosstalk" (electromagnetic interference) between optical fibers, so they transmit information more reliably with better signal quality
- **Higher bandwidth**: Fiber-optic cables can carry far more data than copper cables of the same diameter.

Related Videos

https://www.youtube.com/watch?v=aqazAcE19vw

https://www.youtube.com/watch?v=02wPSDOXMhc

https://www.youtube.com/watch?v=MrJswUU143M

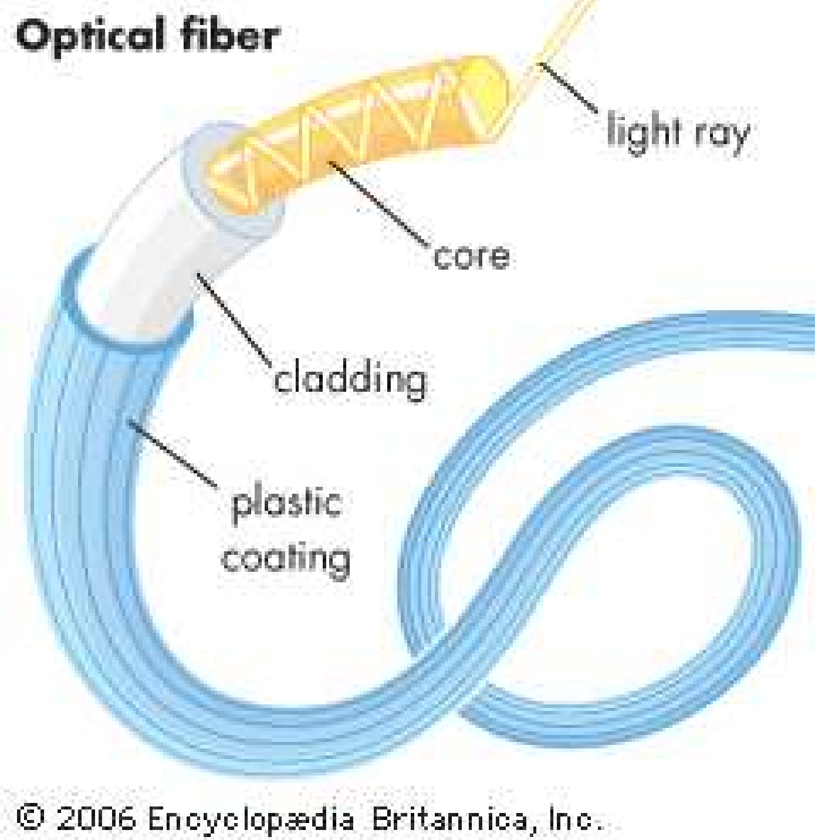

Light Reflected from Surface
Light Gradually Leaks Out
Water Flowing Out of Basin

Total Internal reflection is the basic idea of fiber optic

John Tyndall demonstration in 1870

Fiber optics

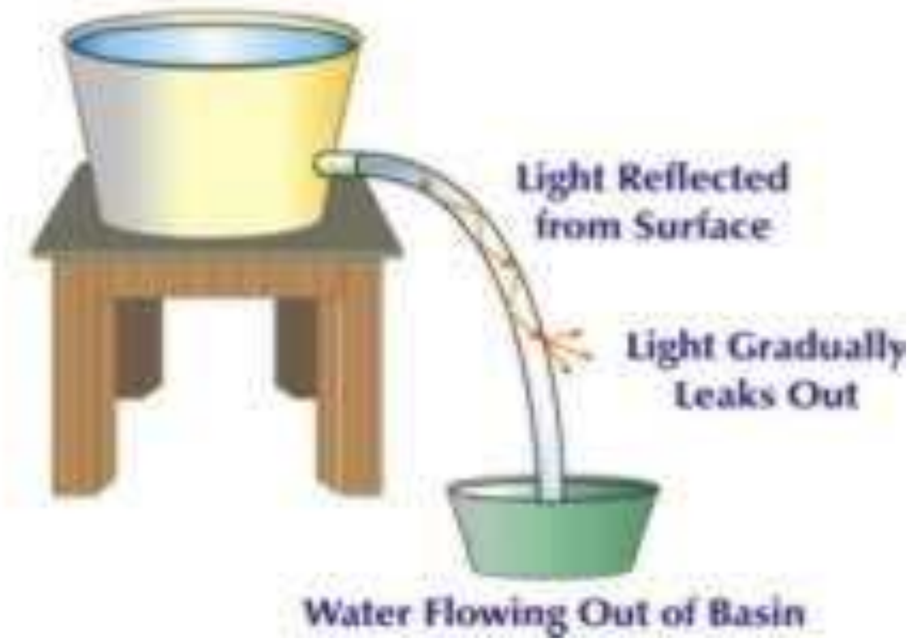
- **Fiber optics**, also spelled **fibre optics**, the science of transmitting data, voice, and images by the passage of light through thin, transparent fibers.
- In telecommunications, fiber optic technology has virtually replaced copper wire in long-distance telephone lines, and it is used to link computers within local area networks.
- Fiber optics is also the basis of the fiberscopes used in examining internal parts of the body (endoscopy) or inspecting the interiors of manufactured structural products.



© 2006 Encyclopædia Britannica, Inc.

History of Fiber Optics

Total Internal reflection is the basic idea of fiber optic


Light Reflected from Surface
Light Gradually Leaks Out
Water Flowing Out of Basin

Unguided/Wireless

- Unguided medium transport electromagnetic waves without using a 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 ahas a device capable of receiving them.
- The below figure shows the part of the electromagnetic spectrum, ranging from 3 kHz to 900 THz, used for wireless communication.

Unguided/Wireless

- **Unguided media** relates to **data transmission** through the **air** and is commonly referred to as **wireless**. The transmission and reception of data is carried out using **antenna**.
- **There are two main ways that antenna work:**
  - Directional (in a beam)
  - Omnidirectional (all around)
- **All unguided media transmission are classified as wireless transmission.**
- This is the wireless media that transport electromagnetic waves without using a physical conductor. Signals are broadcast either through air. This is done through radio communication, satellite communication and cellular telephony.
- Unguided or wireless media sends the data through air (or water), which is available to anyone who has a device capable of receiving them.

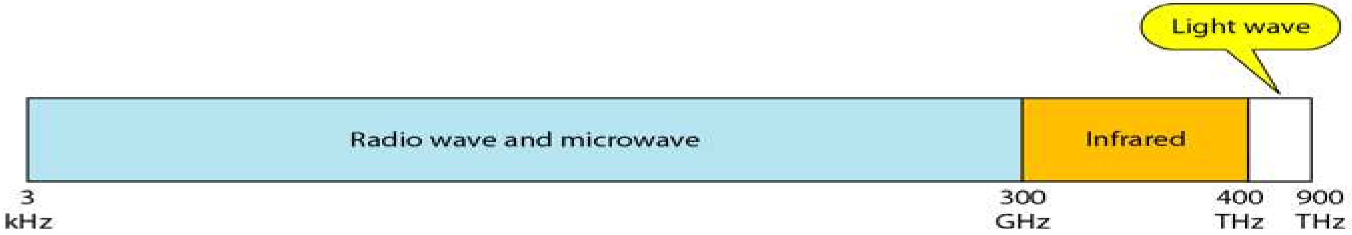
Unguided/Wireless

We can divide wireless transmission into three broad groups:

- **Radio waves:** Electromagnetic waves ranging in frequencies between 3 KHz and 1 GHz are normally called radio waves.

  Radio waves use omnidirectional antennas that send out signals in all directions.

- **Micro waves:** Electromagnetic waves having frequencies between 1 and 300 GHz are called micro waves.
- **Infrared waves:** Infrared waves, with frequencies from 300 GHz to 400 THz, can be used for short-range communication.



Summary

- A **computer network** is a digital telecommunications network for sharing resources between nodes, which are computing devices that use a common telecommunications technology.
- Data transmission between nodes is supported over data links consisting of physical cable media, such as twisted pair or fiber-optic cables, or by wireless methods, such as Wi-Fi.

Networks

- A Network is a set of device (normally called nodes) connected by communication links.
- A node can be computer, printer or any other device capable of sending and receiving data generated by other nodes on the network.
- A network must be able to meet a certain number of criteria:
    - **Performance:**
        - Performance can be measured in many ways, including transmit time and response time:
            - **Transmit time** is the amount of time required for a message to travel from of device to another.
            - **Response time** is the elapsed time between an inquiry and a response
        - The performance of network depends on a number of factors including the number of users, the type of transmission medium, the capabilities of the connected hardware and the efficiency of the software.

Networks

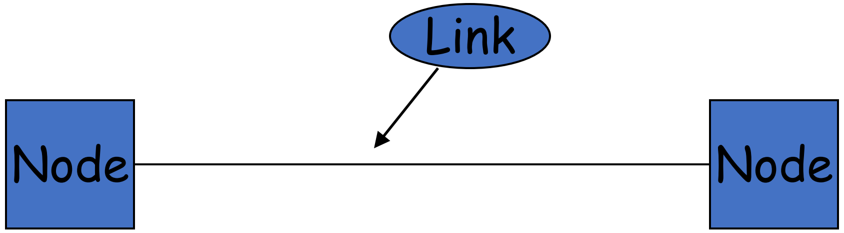
- **Reliability:**
  - In addition to accuracy of delivery, guaranteed delivery, network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure and the network's robustness in a catastrophe.
- **Security:**
  - Network security issues include protecting the data from unauthorized access.
    - Access control.
    - Integrity.
    - Authentication.
    - Confidentiality.
    - Non-repudiation.

Type of Connection.

- A network is two or more devices connected through links.
  - A link is the physical communication path way that transfers data from one device to another.
- For communication to occur, two devices must be connected in some way to the same link at the same time.
- There are two possible types of connections:
  - **Point-to-point.**
  - **Multipoint.**

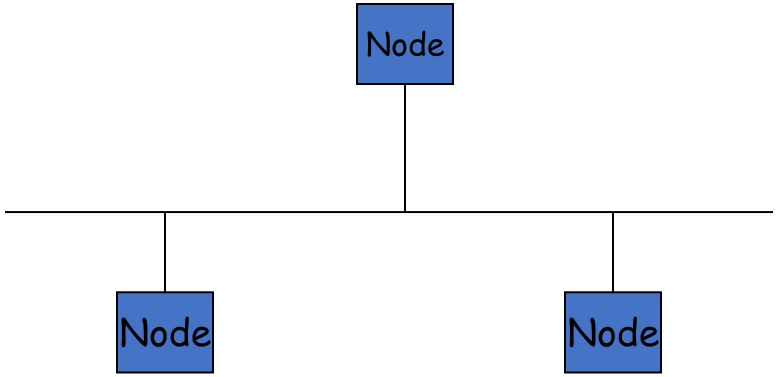
Point-to-Point.

- A point-to-point connection provides a dedicated link between two devices.
- The entire capacity of the link is reserved for transmission between those two devices.
- A point-to-point connection can be established by using both cable or wireless like microwave or satellite links.

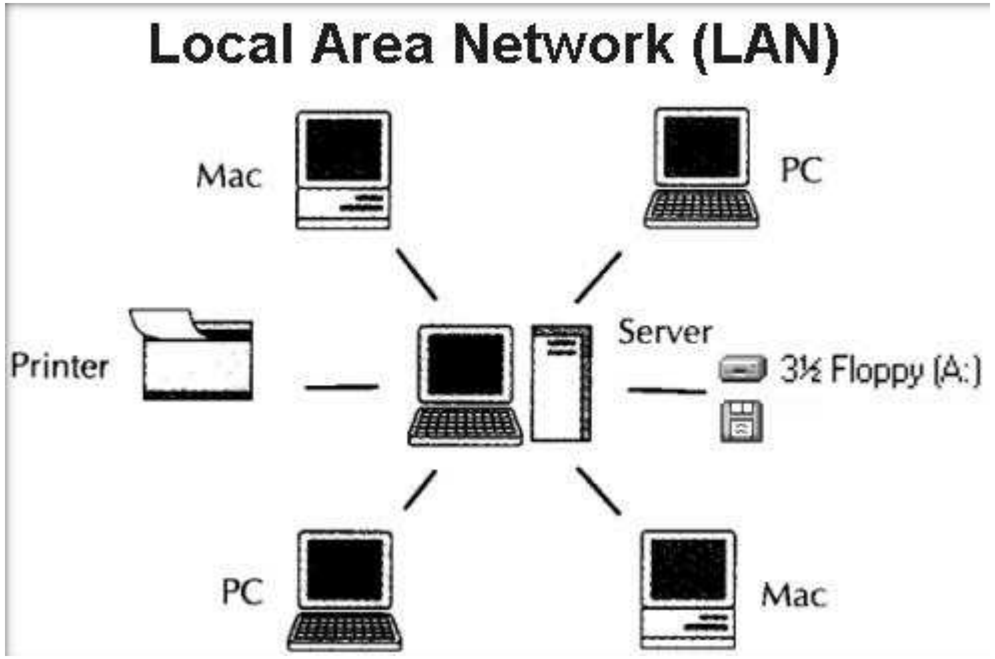


Multipoint.

- A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link.
- In a multipoint environment, the capacity of the channel is shared either permanently or temporally.

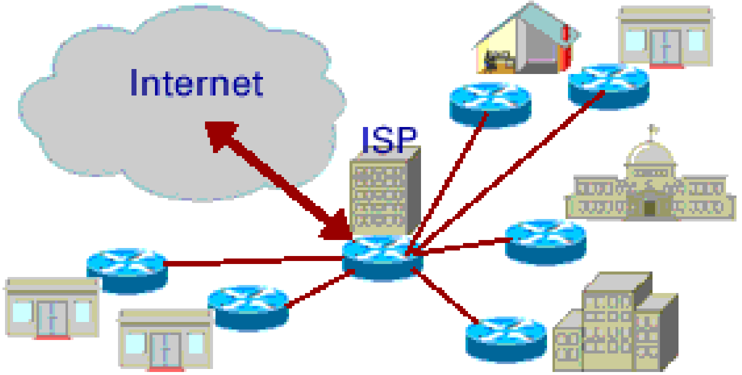


Categories of Network.



- Three categories of network.
  - **Local Area Network.**
  - **Metropolitan Area Network.**
  - **Wide Area Network.**
- **Local Area Network:**
  - A LAN is usually owned and links the devices in a single office, building or campus.
  - A LAN can be as simple as two PC's and a printer in someone home office or it can be extend throughout a company an include connecting several office together.
  - LANs are designed to share resource between personal computers.
    - The resources to be shared can include hardware .i.e. printer, software .i.e. application program or data.

Categories of Network.

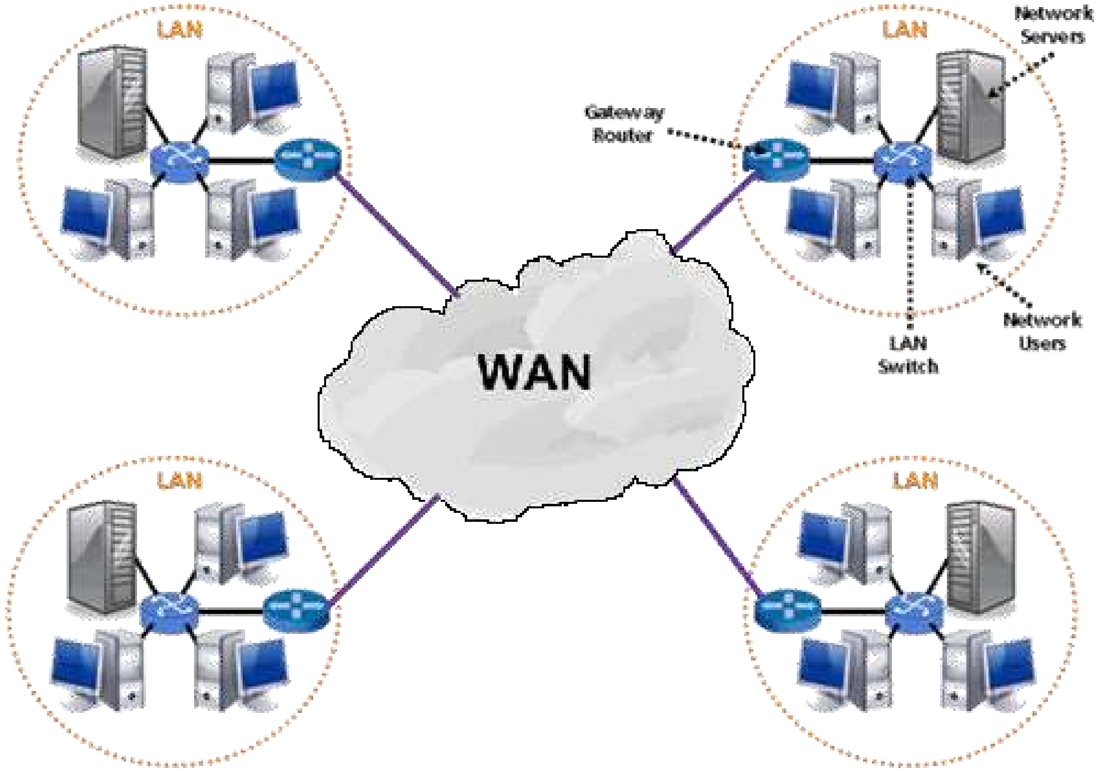


Metropolitan Area Network (MAN)

- **Metropolitan Area Network:**
  - A MAN is designed to extend over an entire city.
  - It may be a single network such as a cable television network or it may be a means of connecting a number of LANs into a larger network so that resources may be shared LAN to LAN.
  - For example, a company can use a MAN to connect the LANs in all its offices throughout a city.
  - A MAN may be wholly owned and operated by a private company, or it may be a service provided by a public company such as local telephone company.

Categories of Network.

- **Wide Area Network:**
  - A WAN provides long-distance transmission of data, voice, image and video information over larger geographic areas that may comprise a country, a continent or even the whole world.
  - Internet is an example of WAN.



WAN Types

- **Point to Point WAN**

Connects two communicating devices through a transmission media(cable or air).

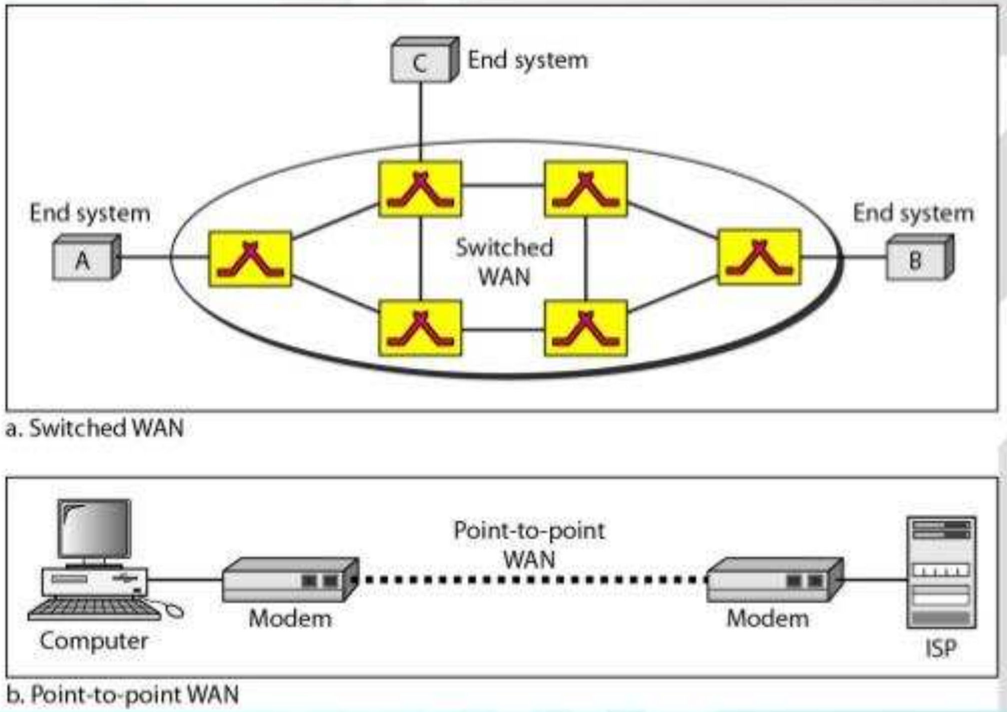
- **A Switched WAN**

Backbone of global communication.

It is a network with more than two ends.

Note: when two or more networks are connected, they make an internetwork or internet.

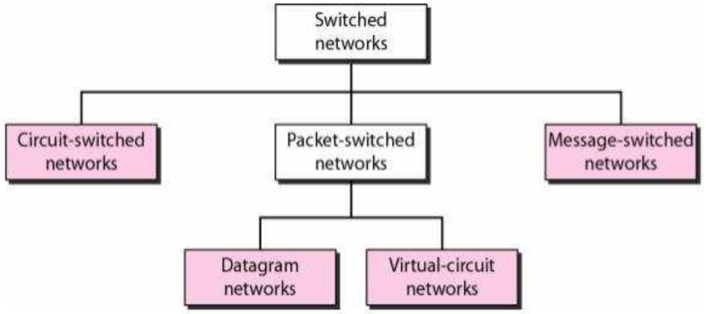
Example : *WANs: a switched WAN and a point-to-point WAN*



a. Switched WAN

b. Point-to-point WAN

Switched networks


Switched networks

Circuit-switched networks

Packet-switched networks

Message-switched networks

Datagram networks

Virtual-circuit networks

An internet is Switched Network in which a switch connects at least two links together.
A Switch needs to forward data from a network to another network when required.

Additional building blocks of transmission media

Network interfaces

- **A Network Interface Controller (NIC)** is computer hardware that provides a computer with the ability to access the transmission media, and has the ability to process low-level network information.

  For example, the NIC may have a connector for accepting a cable.

- **Repeater** – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network.

  An important point to be noted about repeaters is that they do no amplify the signal.

- **Hub** – A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices.

Repeater

Hub

Network Interface Controller

Additional building blocks of transmission media

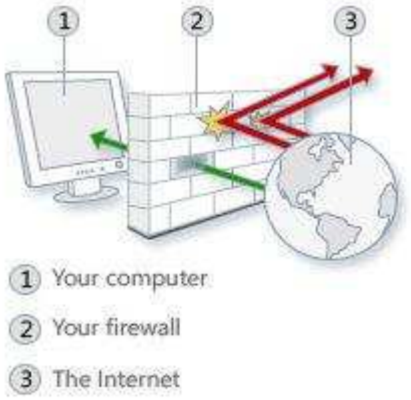
- **Routers**

- A **router** is a networking device that forwards data packets between **computer** networks.
- It determines the best way for a packet to be forwarded to its destination.
- A data packet is typically forwarded from one **router** to another **router** through the networks that constitute an internetwork until it reaches its destination node.

Note: The **router** is wired to the **modem**, and the **modem** is wired to the cable company's coaxial cable.

- **Firewalls**

- Control network security and access rules.
- Typically configured to reject access requests from unrecognized sources while allowing actions from recognized ones.
- The vital role firewalls play in network security grows in parallel with the constant increase in cyber attacks.

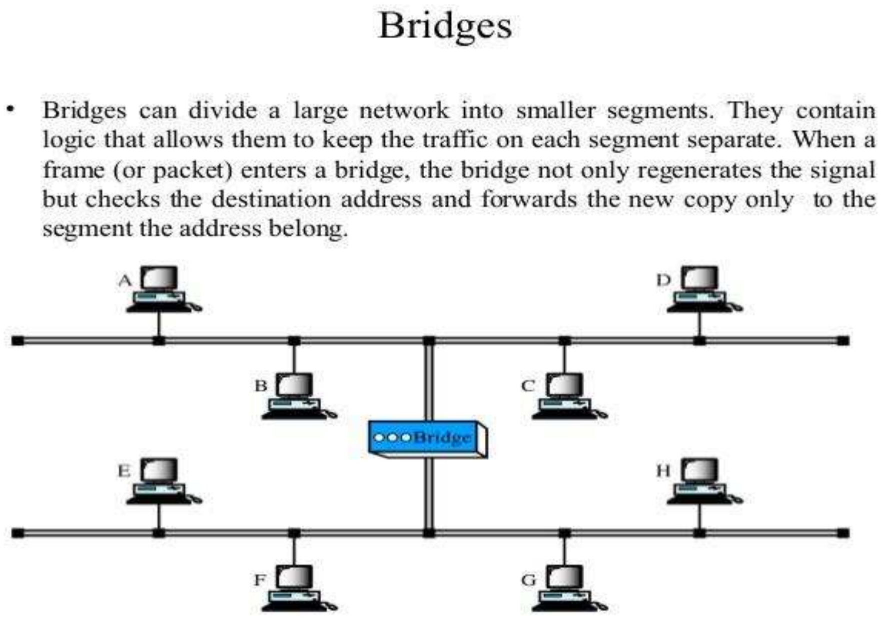


Additional building blocks of transmission media

Bridges: A **bridge** is a type of **computer network** device that provides interconnection with other **bridge networks** that use the same protocol.

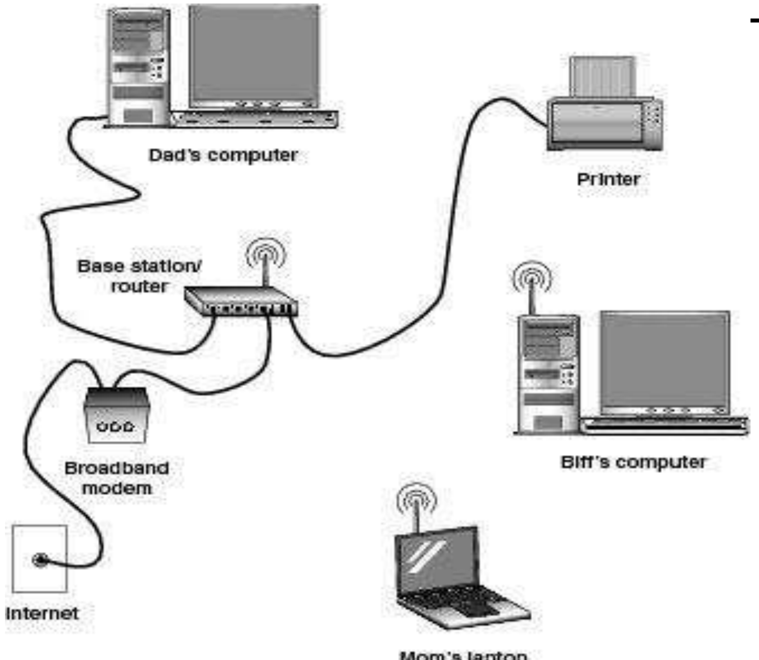
Switches: A **switch** is **used** in a wired network to connect Ethernet cables from a number of devices together. The **switch** allows each device to talk to the others. **Switches** allow dozens of devices to connect.

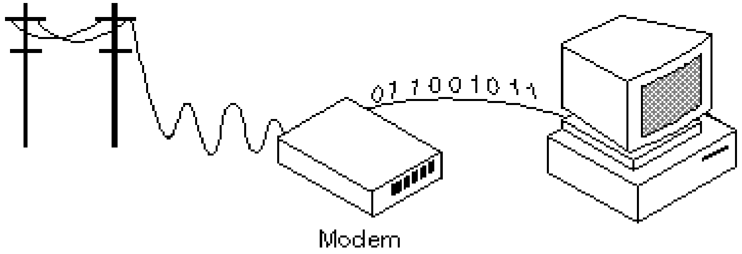
Modem: A **modem** is a hardware device that allows a computer to send and receive data over a telephone line or a cable or satellite connection.



Bridges

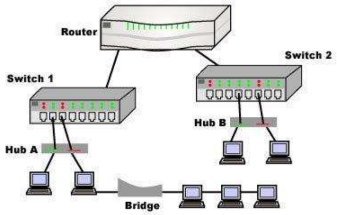
- Bridges can divide a large network into smaller segments. They contain logic that allows them to keep the traffic on each segment separate. When a frame (or packet) enters a bridge, the bridge not only regenerates the signal but checks the destination address and forwards the new copy only to the segment the address belong.





Switch

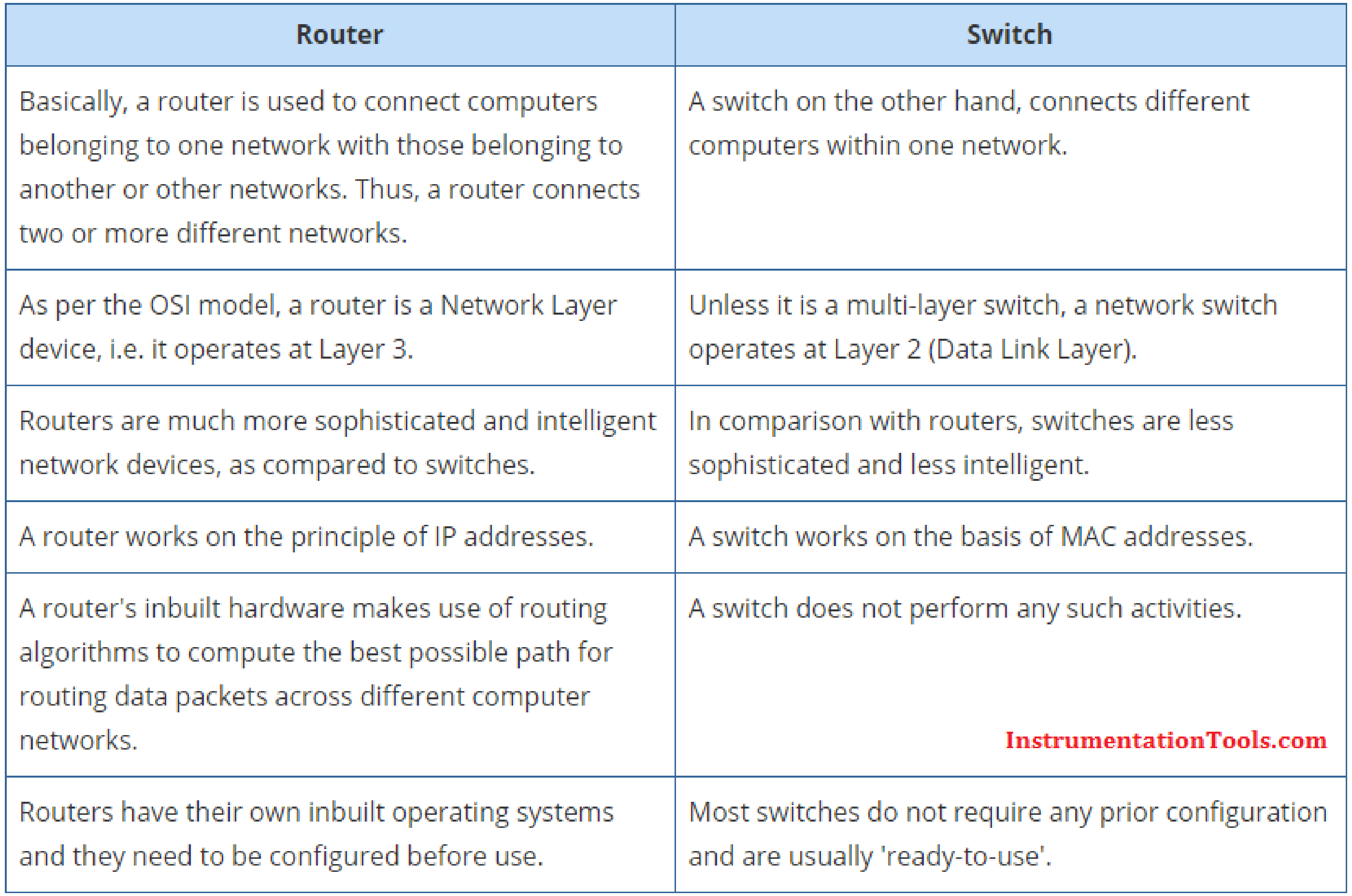
S.NO	HUB	SWITCH
1.	Hub is operated on **Physical layer**.	While switch is operated on **Data link layer**.
2.	Hub is a broadcast type transmission.	While switch is a Unicast, multicast and broadcast type transmission.
3.	Hub have maximum 4 ports.	While switch can have 24 to 28 ports.
4.	In hub, there is only one collision domain.	While in switch, different ports have own collision domain.
5.	Hub is a half duplex transmission mode.	While switch is a full duplex transmission mode.



•**Hubs** are “dumb” devices that pass on anything received on one connection to all other connections.

•**Switches** are semi-intelligent devices that learn which devices are on which connection.

•**Routers** are essentially small computers that perform a variety of intelligent tasks.



Router	Switch
Basically, a router is used to connect computers belonging to one network with those belonging to another or other networks. Thus, a router connects two or more different networks.	A switch on the other hand, connects different computers within one network.
As per the OSI model, a router is a Network Layer device, i.e. it operates at Layer 3.	Unless it is a multi-layer switch, a network switch operates at Layer 2 (Data Link Layer).
Routers are much more sophisticated and intelligent network devices, as compared to switches.	In comparison with routers, switches are less sophisticated and less intelligent.
A router works on the principle of IP addresses.	A switch works on the basis of MAC addresses.
A router's inbuilt hardware makes use of routing algorithms to compute the best possible path for routing data packets across different computer networks.	A switch does not perform any such activities. InstrumentationTools.com
Routers have their own inbuilt operating systems and they need to be configured before use.	Most switches do not require any prior configuration and are usually 'ready-to-use'.

Network Topology

- The topology of a network defines how the nodes of a network are connected.
- There are two basic categories of network topologies:

(To define The network)

- Physical topology: defines how the nodes of the network are physically connected.
- Logical topology: How data is transmitted between nodes.

(dedicated connections between certain selected source-destination pairs using the underlying physical topology.)

  - the logical topology should be chosen such that either the average hop distance or the packet delay or the maximum flow on any link must be minimal.

Physical

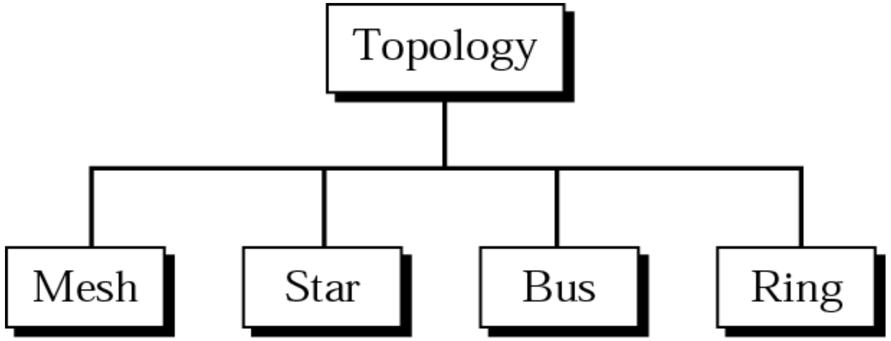
➢Describes the geometric arrangement of components that make up the LAN

Logical

➢Describes the possible connections between pairs of networked end-points that can communicate

Physical Network Topology

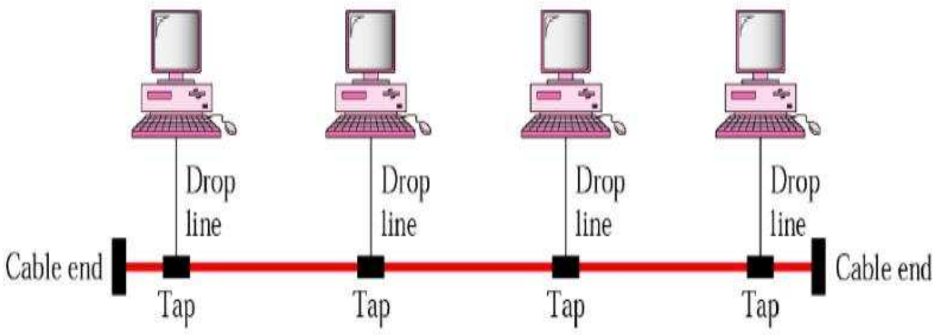
- The shape of the cabling layout used to link devices is called the physical topology of the network.
- This refers to the layout of cabling, the locations of nodes, and the interconnections between the nodes and the cabling
- It describes the layout or appearance of a network
- A multi point topology connects 3 or more stations through a single transmission medium
- Eg: star, bus, ring, mesh & hybrid

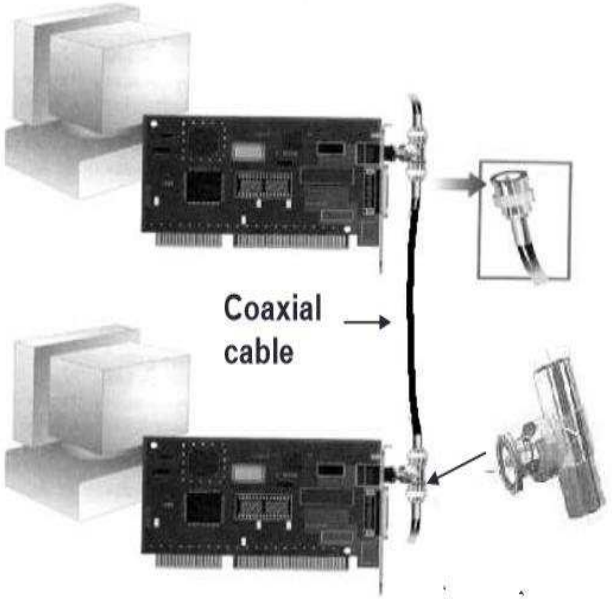


Bus topology-

Simple and low-cost

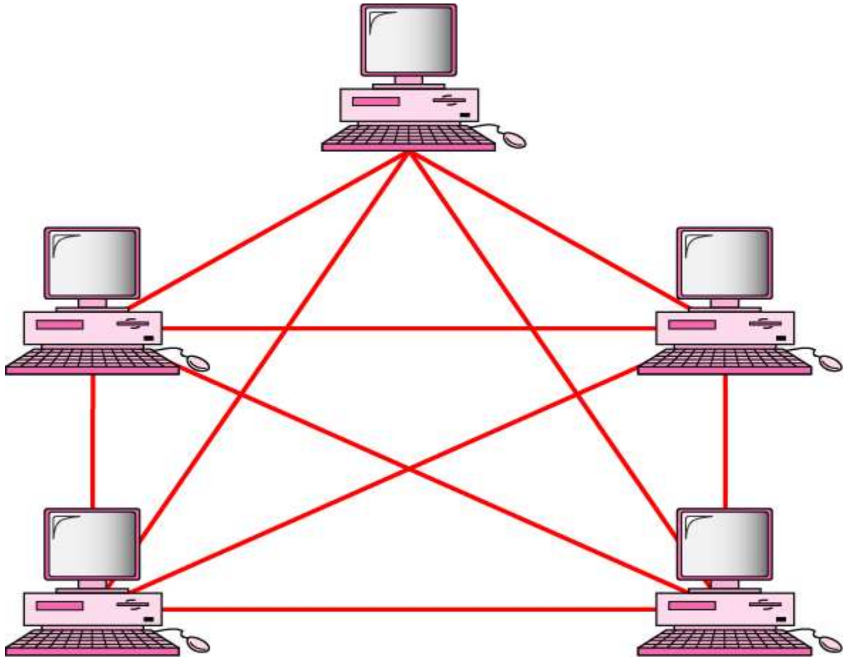
A single cable called a trunk (backbone, segment)





- Each node is connected to a single cable, by the help of interface connectors.
- This central cable is the backbone of the network and is known as the bus (thus the name).
- A signal from the source travels in both directions to all machines connected on the bus cable until it finds the intended recipient.
- If the machine address does not match the intended address for the data, the machine ignores the data.
- Alternatively, if the data matches the machine address, the data is accepted.
- Because the bus topology consists of only one wire, it is rather inexpensive to implement when compared to other topologies.

Fully Connected Mesh Topology



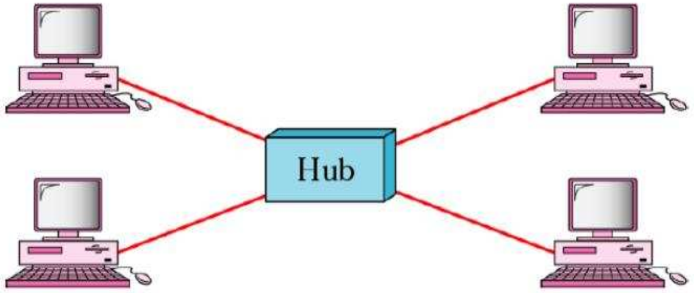
- In a fully connected network, all nodes are interconnected. (In graph theory this is called a complete graph.)
- The simplest fully connected network is a two-node network.
- A fully connected network doesn't need to use packet switching or broadcasting.
- However, since the number of connections grows quadratically with the number of nodes: This kind of topology does not trip and affect other nodes in the network.

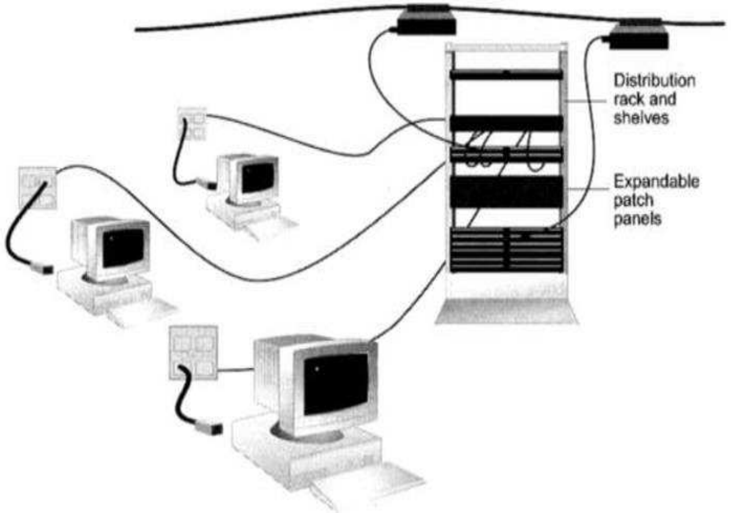
- **C=n(n-1)/2**

This makes it impractical for large networks.

Star topology-

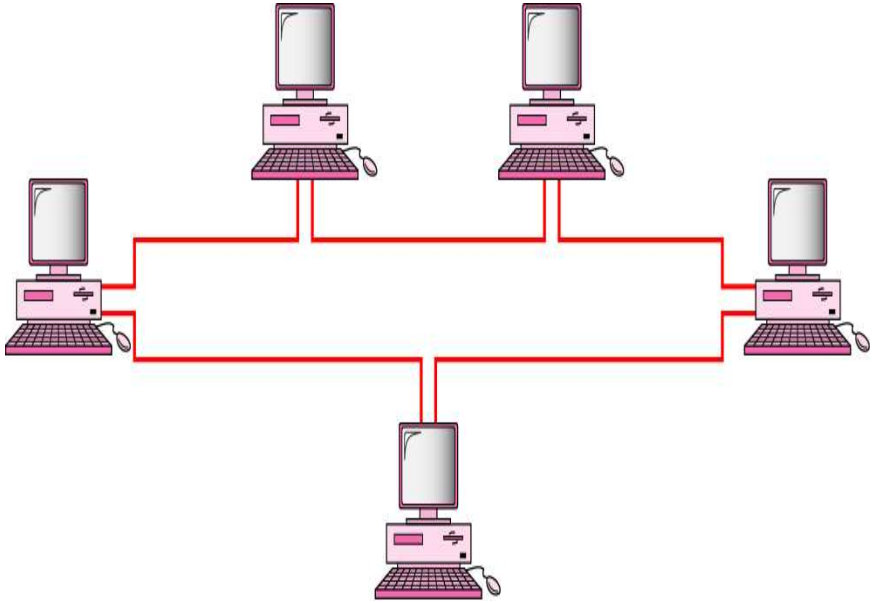
Each computer has a cable connected to a single point
More cabling, hence higher cost
All signals transmission through the hub; if down, entire network down





- Each network host is connected to a central hub with a point-to-point connection.
- Every computer is indirectly connected to every other node with the help of the hub.
- In Star topology, every node (computer workstation or any other peripheral) is connected to a central node called hub, router or switch.
- The switch is the server and the peripherals are the clients.
- The network does not necessarily have to resemble a star to be classified as a star network, but all of the nodes on the network must be connected to one central device.
- All traffic that traverses the network passes through the central hub.
- The star topology is considered the easiest topology to design and implement.
- An advantage of the star topology is the simplicity of adding additional nodes.
- The primary disadvantage of the star topology is that the hub represents a single point of failure.

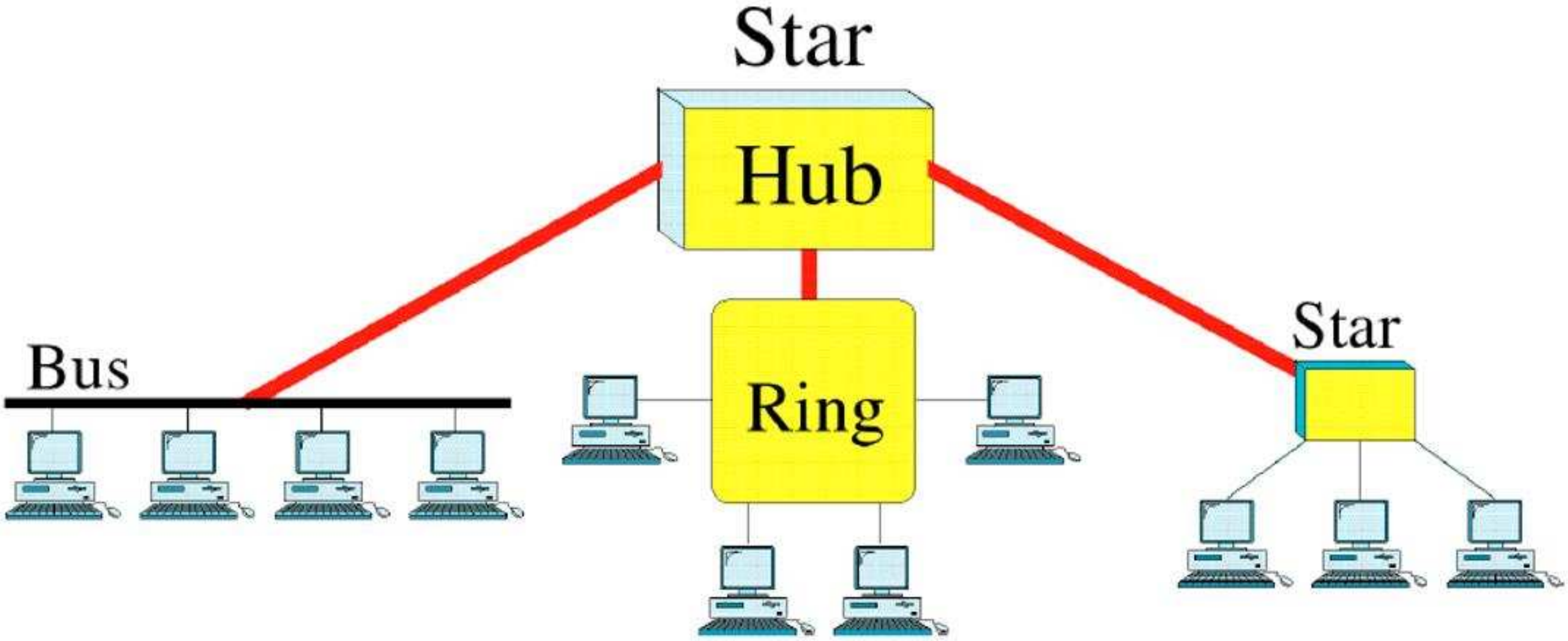
Ring Topology



- A ring topology is a bus topology in a closed loop.
- Data travels around the ring in one direction. When one node sends data to another, the data passes through each intermediate node on the ring until it reaches its destination.
- The intermediate nodes repeat (re transmit) the data to keep the signal strong.
- Every node is a peer; there is no hierarchical relationship of clients and servers.
- If one node is unable to re transmit data, it severs communication between the nodes before and after it in the bus.

Hybrid topology

- Combination of two or more topologies



Logical Topology

- The logical topology, in contrast, is the way that the signals act on the network media, or the way that the data passes through the network from one device to the next without regard to the physical interconnection of the devices.
- A network's logical topology is not necessarily the same as its physical topology.

Protocols.

- Two communicating entities cannot simply send bit streams to each other and expect to understand.
- For communication to occur, the entities must agree on a protocol.
- A protocol is a set of rules that governs data communication.
- A protocol defines what is communicated, how it is communicated and when it is communicated.
- The key elements of a protocol are Syntax, Semantics and Timing.

Protocols.

- **Syntax:**
  - Syntax refers to the format of the data, meaning the order in which they are presented.
  - For example, a simple protocol might expect the first 8-bits of data to be the address of the sender, the second 8-bits to be the address of the receiver and the rest of the stream to be the message itself.
- **Semantics:**
  - Semantics refers to the meaning of each section of bits.
  - How a particular pattern to interpreted and what action to be taken based on the interpretation.
  - For example, an address identify the route to be take or the final destination of the message.

Protocols.

- **Timing:**
  - Timing refers to two characteristics: when data should be sent and how fast they can be sent.
  - For example, if a sender produces data at 100Mbps but he receiver can process data at only 1Mbps, the transmission will overload the receiver and data will be largely lost.

The Need For Standards.

- Over the past couple of decades many of the networks that were built used different hardware and software implementations, as a result:
  - They were incompatible and it became difficult for networks using different specifications to communicate with each other.
- The companies involved in networks development realized that they needed to move from proprietary networking system into open system.
- Proprietary systems are privately developed, owned and controlled.
  - Disadvantages are:
    - Leads to monopolistic environment.
    - Slows down the development of networking products.
- Open system is the opposite of proprietary systems.
  - Advantages are:
    - Leads to competitive environment.
    - Accelerates the development of networking products.

The Need for Standards.

- To address the problem of networks being incompatible and unable to communicate with each other, the International Organisation for Standardisation (ISO) created a NETWORK MODEL.
- This NETWORK MODEL would help the vendor to create interoperable network implementations.
- This NETWORK MODEL is called OSI Reference Model.

ISO - Organization for Standardization.

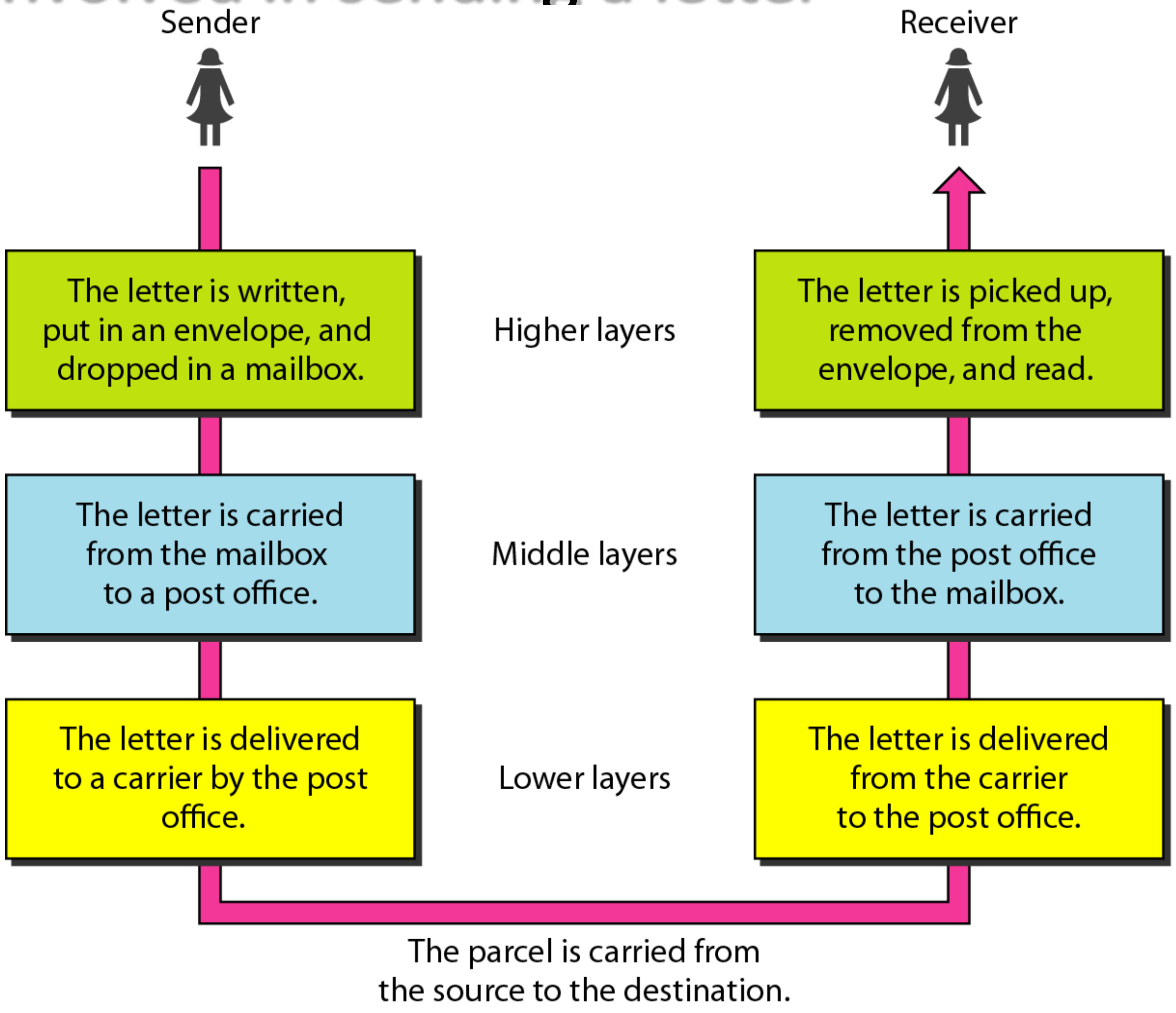
- The International Organisation for Standardisation (ISO) is an International standards organisation responsible for a wide range of standards, including many that are relevant to computer networking.
- In 1984 , the Open Systems Interconnection (OSI) Reference Model was approved as an international standard for communications architecture.

International Organization for Standardization

Layered Tasks.

- We use the concept of ***layers*** in our daily life.
- As an example, 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.
  - This process of sending mail can be divided into several phases/activities and each phase/activities is called layer.

Figure. Tasks involved in sending a letter



Sender
Receiver
The letter is written, put in an envelope, and dropped in a mailbox.
Higher layers
The letter is picked up, removed from the envelope, and read.
The letter is carried from the mailbox to a post office.
Middle layers
The letter is carried from the post office to the mailbox.
The letter is delivered to a carrier by the post office.
Lower layers
The letter is delivered from the carrier to the post office.
The parcel is carried from the source to the destination.

Hierarchy.

- In the previous mail communication example, we saw that three activities were performed at the sender side and another three activities were preformed at the receiver side.
- The task of transporting the mail between the sender and receiver is done by the carrier.
- On important thing is that tasks must be done in the order given in the hierarchy.
  - At the sender side, the letter must be written and dropped into the mailbox before being picked up by the mail carrier and delivered to the post office.
  - At the receiver side, the letter must be dropped in the recipient mailbox before being picked up and read by the recipient.

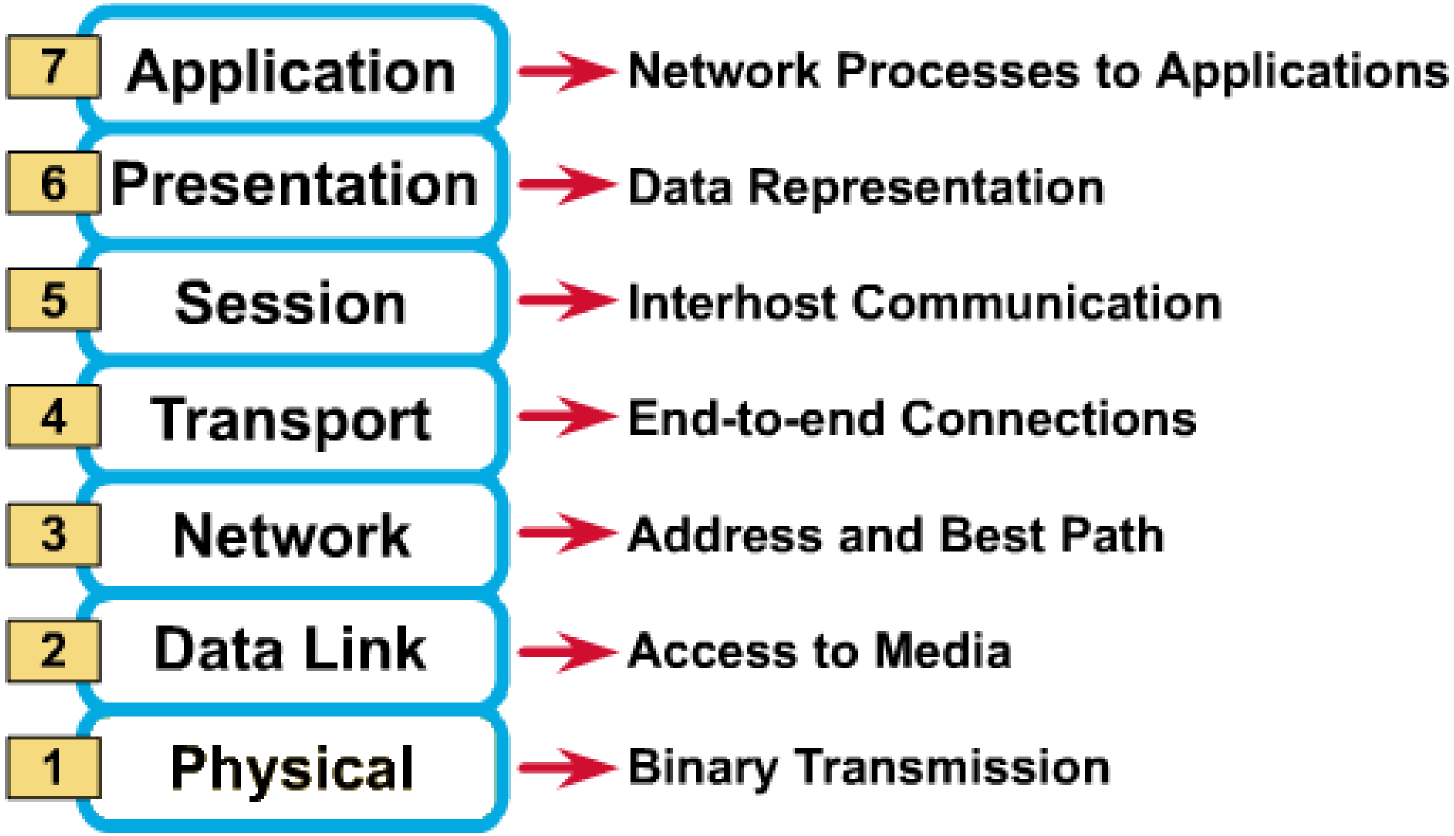
The OSI Reference Model.

- The model was developed by the International Organisation for Standardisation (ISO) in 1984. It is now considered the primary architectural model for inter-computer communications.
- The Open Systems Interconnection (OSI) reference model is a descriptive network scheme. It ensures greater compatibility and interoperability between various types of network technologies.
- 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.

A Layered Network Model.

- The OSI Reference Model is composed of seven layers, each specifying particular network functions.
  - The process of breaking up the functions or tasks of networking into layers reduces complexity and makes learning easier to understand.
  - It breaks the network communication into smaller, simpler parts that are easier to develop.
  - It allows different types of hardware and software to communicate with each other.
  - It prevents changes in one layer from affecting the other layers.

Layers of OSI Reference Model.



7 Application → Network Processes to Applications

6 Presentation → Data Representation

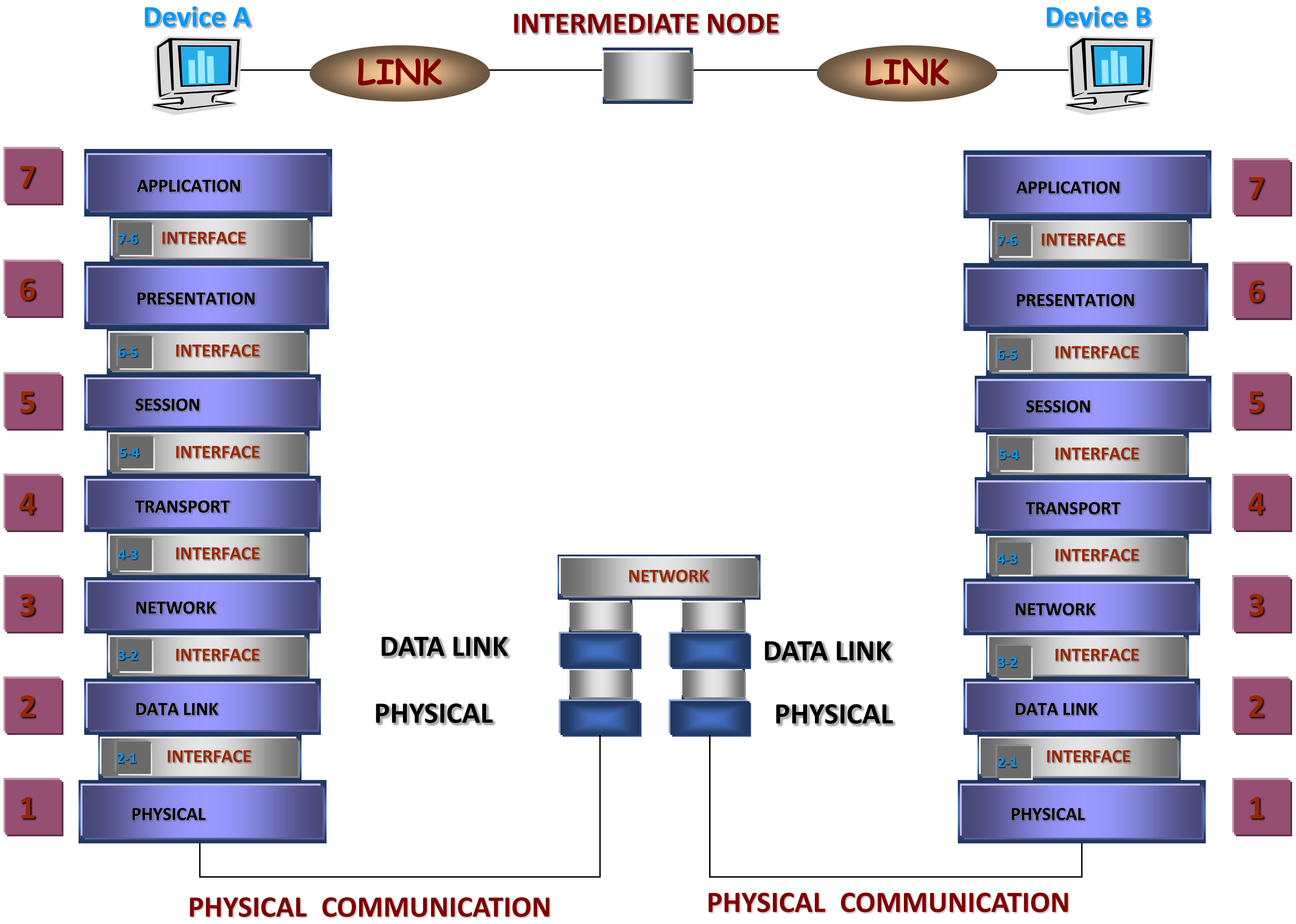
5 Session → Interhost Communication

4 Transport → End-to-end Connections

3 Network → Address and Best Path

2 Data Link → Access to Media

1 Physical → Binary Transmission

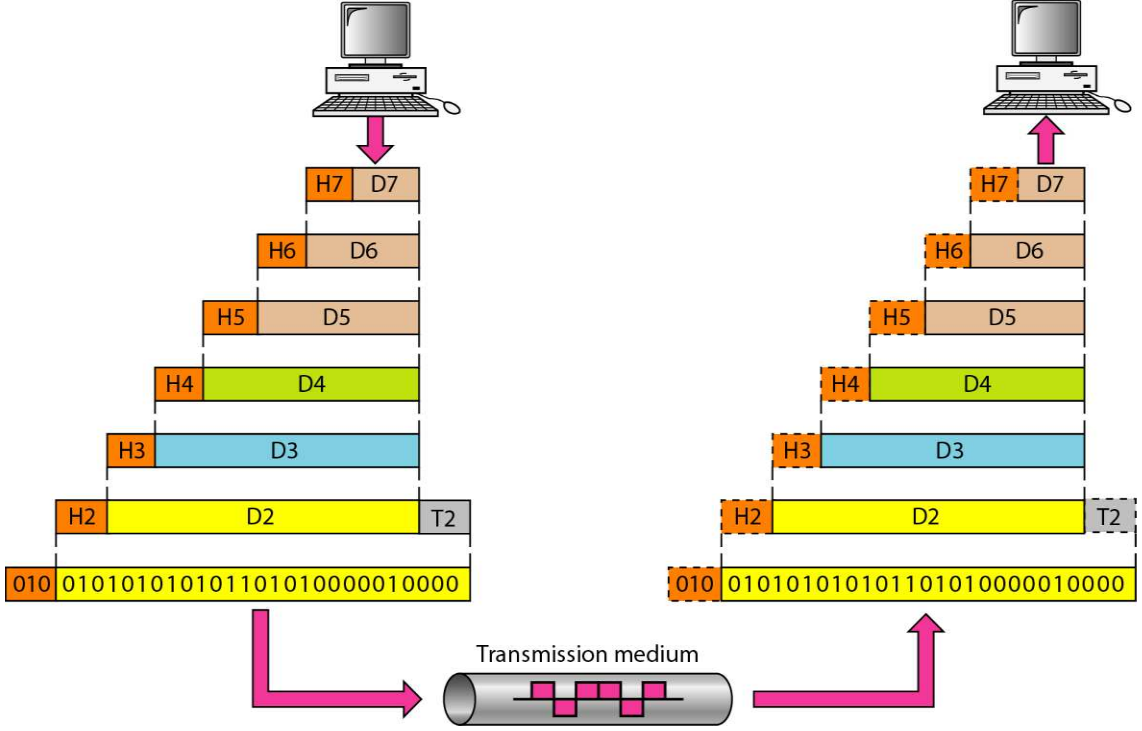

Device A
LINK
INTERMEDIATE NODE
LINK
Device B
7
APPLICATION
7-6
INTERFACE
6
PRESENTATION
6-5
INTERFACE
5
SESSION
5-4
INTERFACE
4
TRANSPORT
4-3
INTERFACE
3
NETWORK
3-2
INTERFACE
2
DATA LINK
2-1
INTERFACE
1
PHYSICAL
NETWORK
DATA LINK
PHYSICAL
DATA LINK
PHYSICAL
APPLICATION
7
7-6
INTERFACE
PRESENTATION
6
6-5
INTERFACE
SESSION
5
5-4
INTERFACE
TRANSPORT
4
4-3
INTERFACE
NETWORK
3
3-2
INTERFACE
DATA LINK
2
2-1
INTERFACE
PHYSICAL
1
PHYSICAL COMMUNICATION
PHYSICAL COMMUNICATION

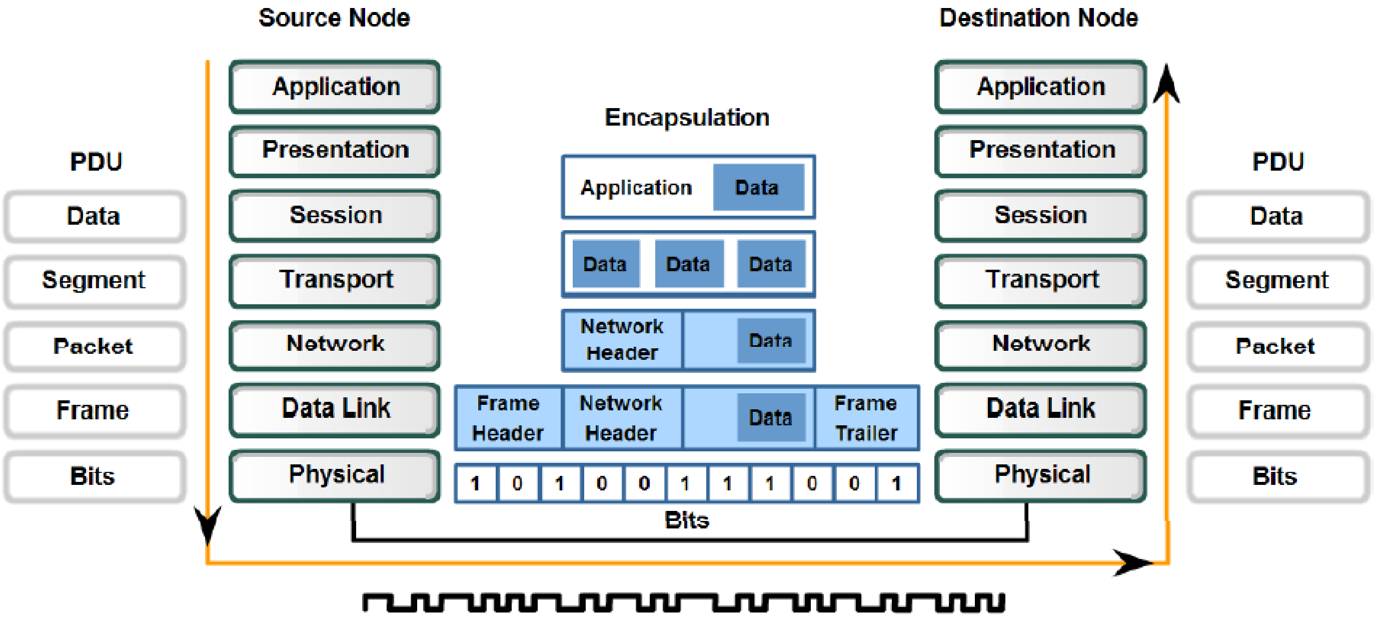
Encapsulation.

- As the data flows down through the layers in the hierarchy, each layer adds some extra information to the data in the form of headers or tailors.
- This process of wrapping data with headers and tailors is called encapsulation.
- These extra information are added for:
  - To enable the opposite corresponding layer to take the right operation on the data (to facilitate his work).
  - To enable the network to transfer the data accurately from the source to the destination.
- Through these information each layer actually communicates with the opposite corresponding layer and this is called peer-to-peer communication.
- At the receiver side De-Encapsulation take place.

encapsulation is a process of adding protocol specific information as well as converting a protocol data unit (PDU) into a form that conforms into the layer it is in. in this case, the PDU at the transport layer is the segment.

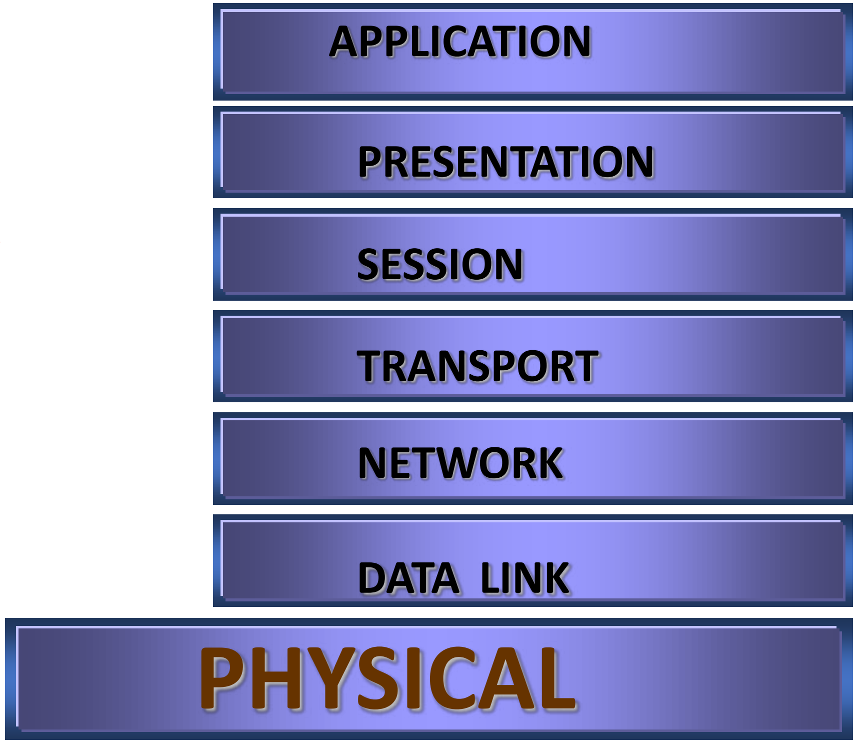
Encapsulation.





PHYSICAL

- Physical characteristics of interfaces and media
- Representation of bits
- Data rate
- Synchronization of bits
- Line configuration
- Physical topology
- Transmission mode



APPLICATION

PRESENTATION

SESSION

TRANSPORT

NETWORK

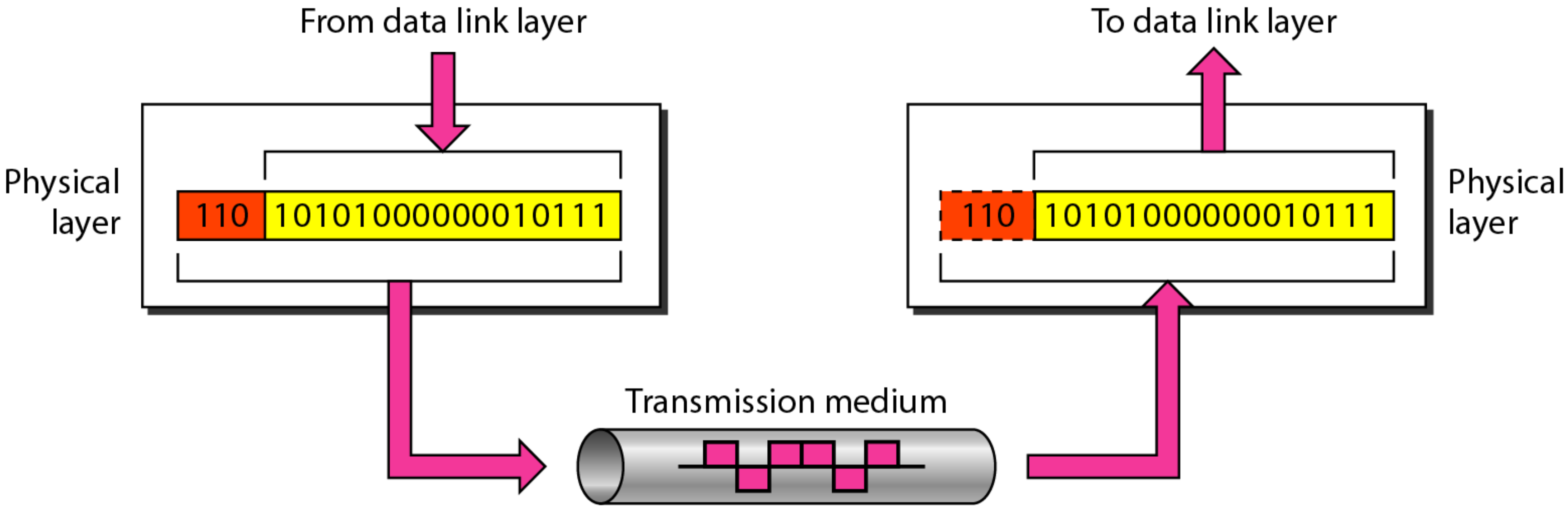
DATA LINK

PHYSICAL

Physical Layer.

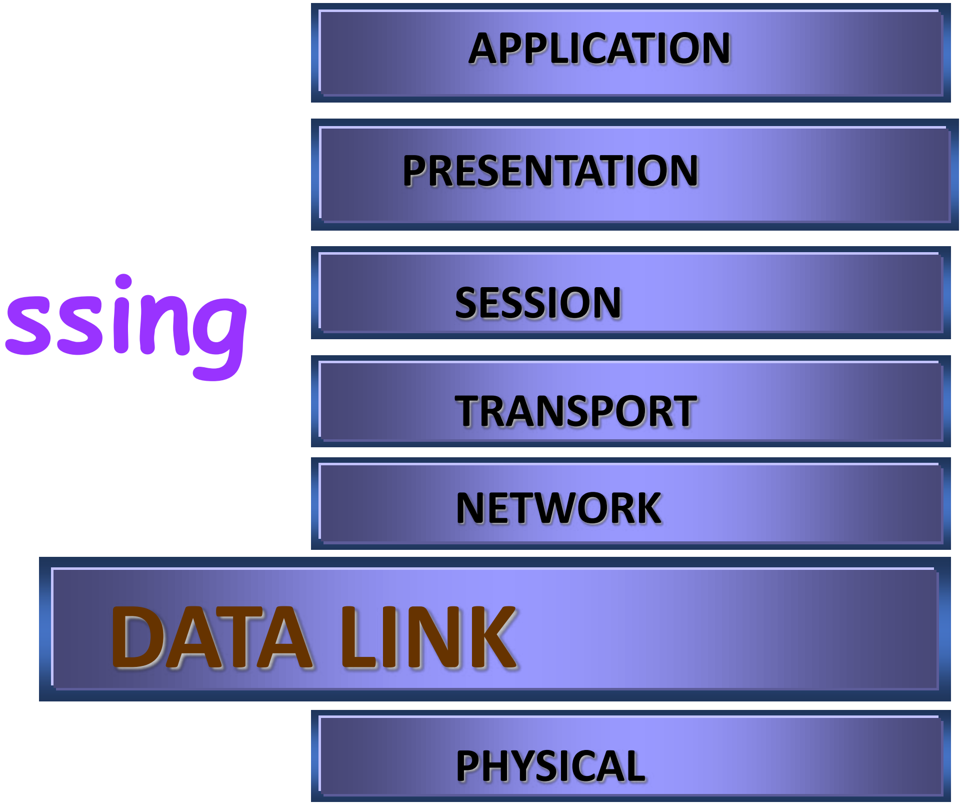
- The physical layer performs the functions required to transmit a bit stream over a physical medium.
- It deals with the mechanical and electrical specification of the transmission media.
- The major duties performed by physical layer are:
  - **Physical characteristics of interface and media.**
    - Defines the characteristics of the interface between the devices and the transmission media.
    - It also defines the type of transmission medium.
  - **Representation of bits:**
    - Physical layer receives a steam of bits (sequence of 0s and 1s) without any interruption.
    - To be transmitted, bits must be encoded into a signals – electrical or optical.
    - The physical layer defined the type of representation (how 0s and 1s are changed into signals).
  - **Data rate:**
    - The transmission rate – the number of bit per second- is also defined by the physical layer.
- Repeater is a device of the physical layer.
- Physical layer protocols are encoding techniques (RZ, NRZ, Manchester etc).

Physical Layer.



DATA LINK

- Framing
- Physical addressing
- Flow control
- Error control
- Access control



APPLICATION

PRESENTATION

SESSION

TRANSPORT

NETWORK

DATA LINK

PHYSICAL

Data Link Layer.

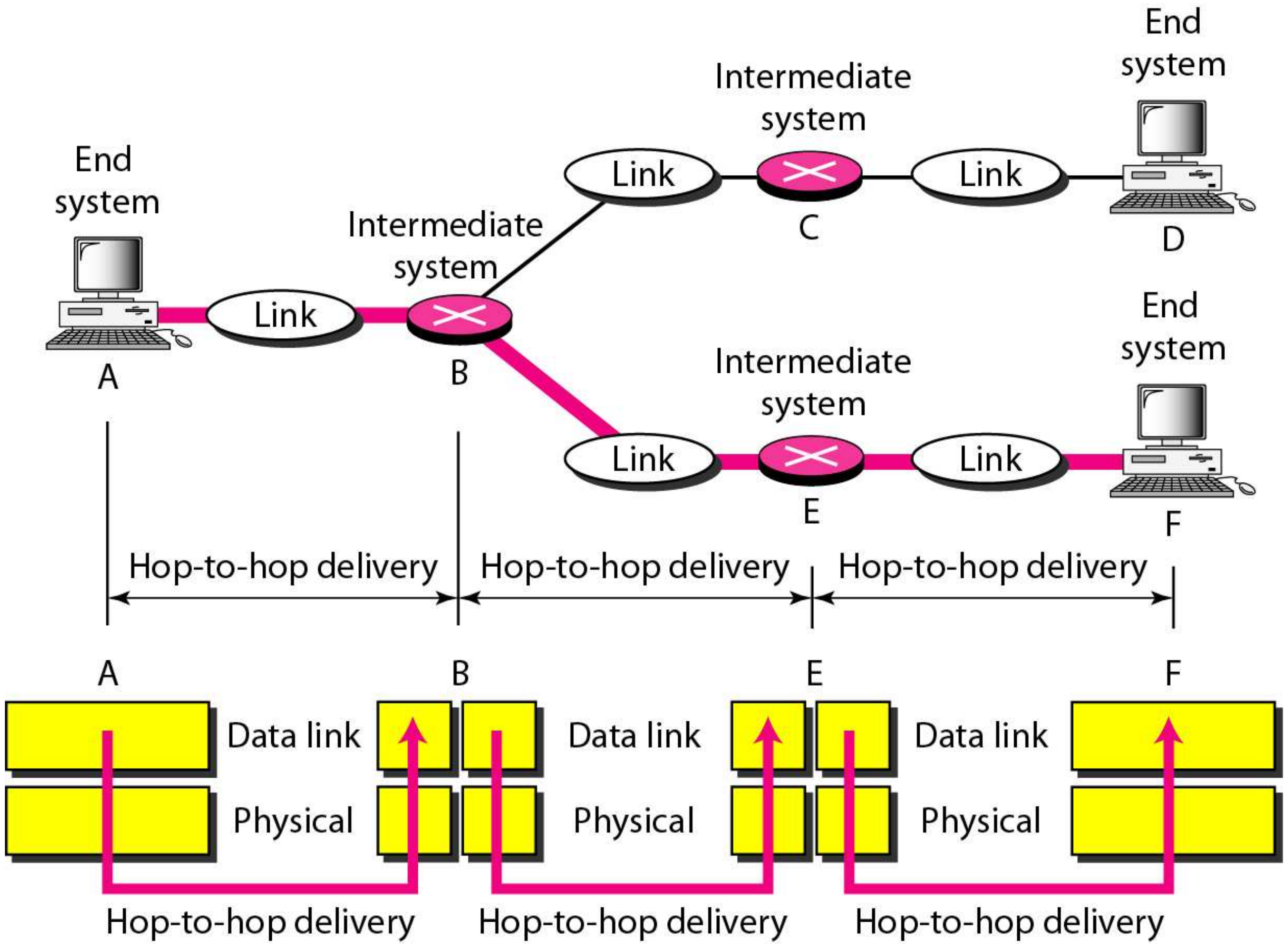
- The data link layer is responsible for moving frames from one hop (node) to the next.
- The major duties of the data link layer are:
  - **Framing:**
    - The data link layer divides the stream of bits steam from the network layer into manageable data units called frames.
  - **Physical addressing:**
    - If frame is to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and receiver of the frame.
    - Physical address is the MAC address, which is hard coded into NIC and is of 48-bit represented by Hexadecimal format.
  - **Flow control:**
    - If the rate at which the data are absorbed by the receiver is less than the rate produced in the sender, the data link layer imposes a flow control mechanism to prevent overwhelming the receiver.

Data Link Layer.

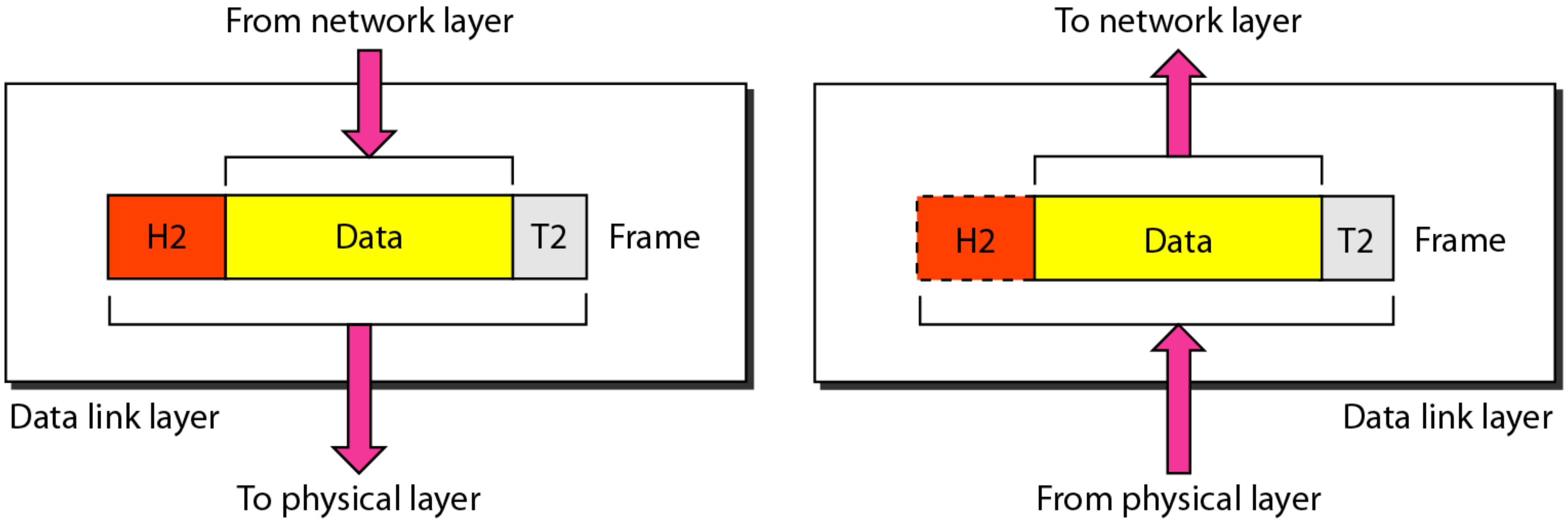
- **Error control:**
  - The data link layer adds reliability to the physical layer by adding mechanism to detect and retransmit damaged or lost frames.
  - It also uses a mechanism to prevent duplication of frames.
  - Error control is normally achieved through a trailer added to the end of the frame.
- **Access control:**
  - The data link layer protocol has to determine that how to get access to the link in case when two or more devices are connected to the same link.

- The PDU of the data link layer is called frame.
- Data Link layer protocols are CSMA/CD, CSMA/CA, Token Passing etc.

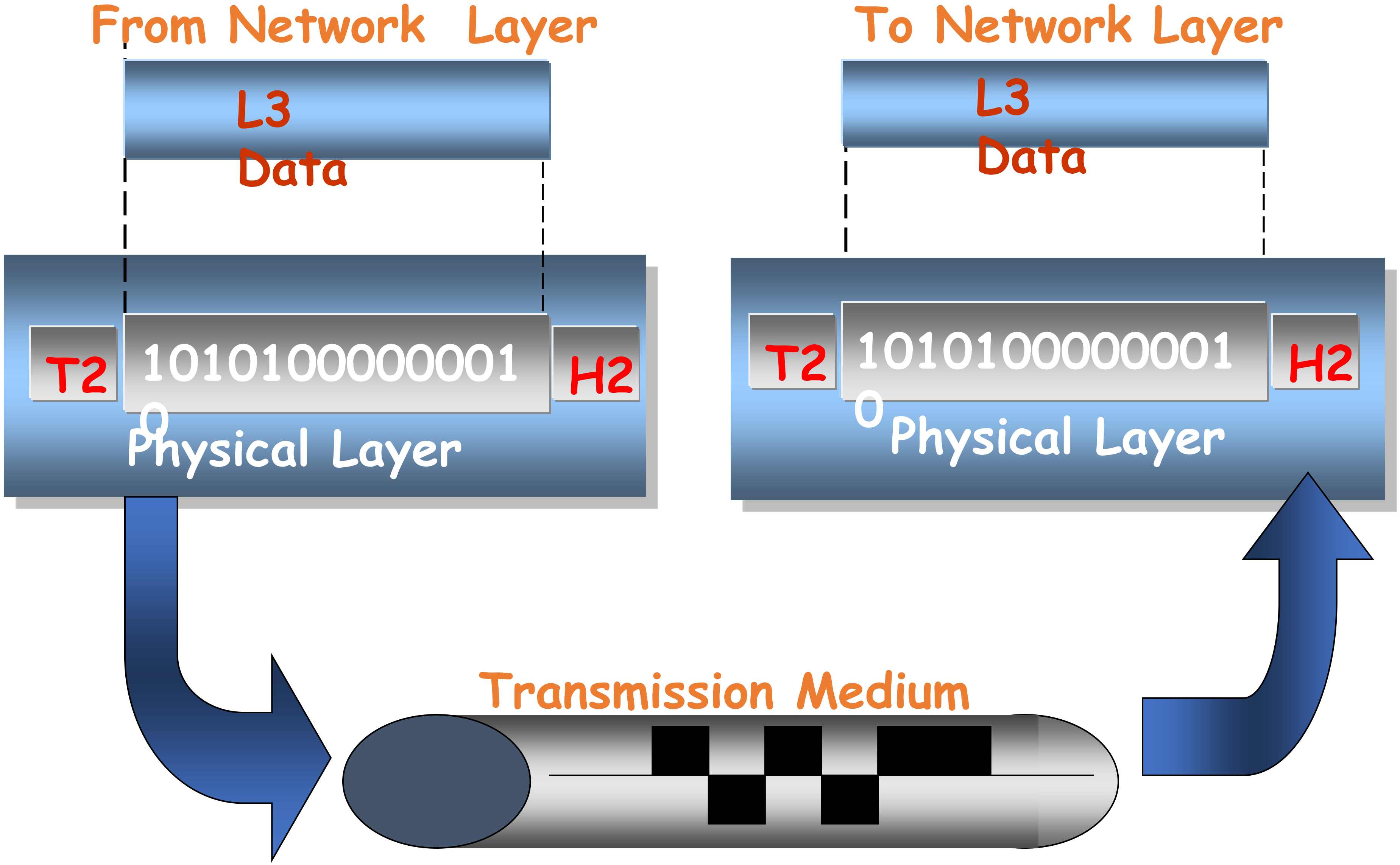
Node-to-Node Delivery.



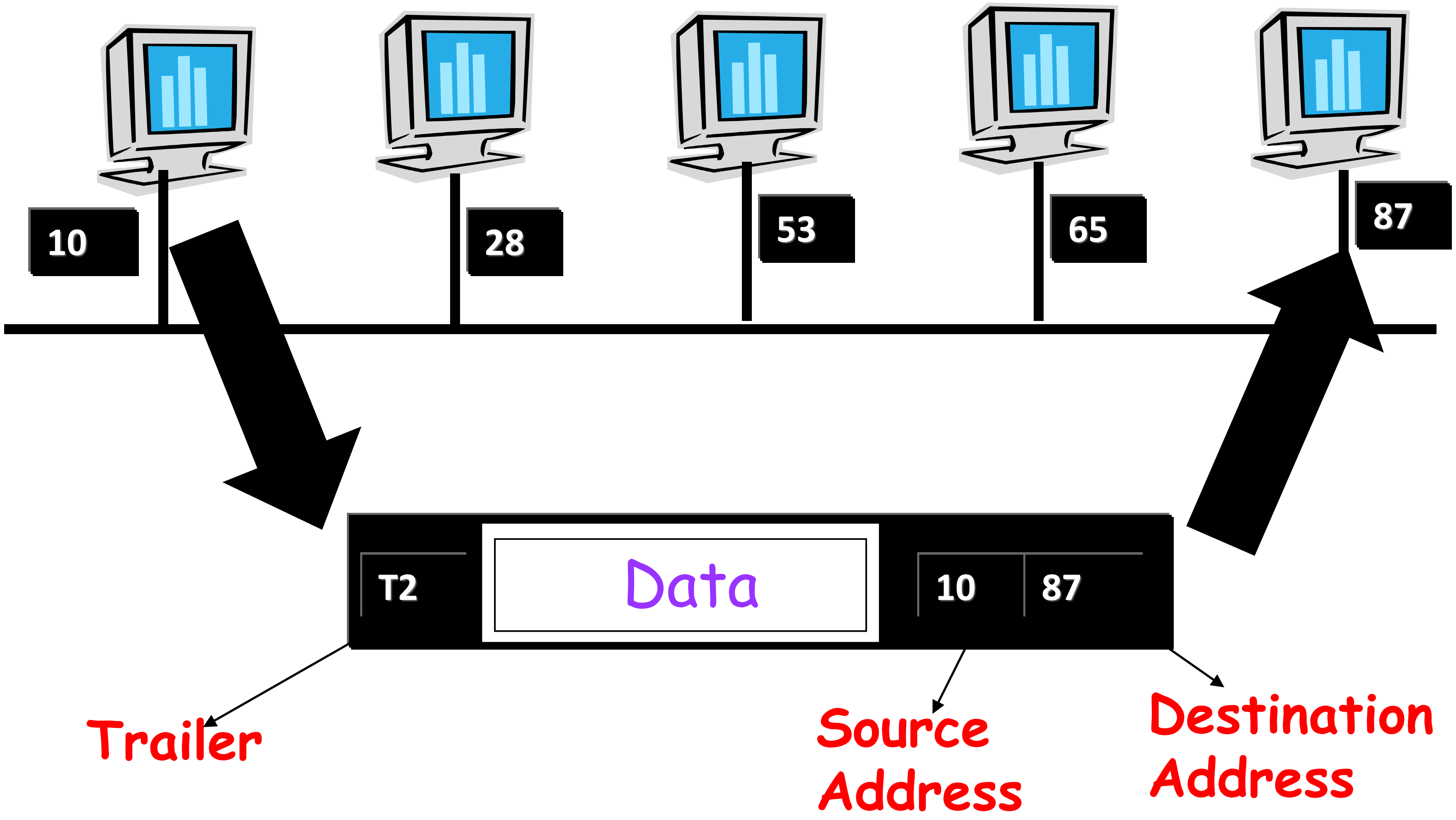
Data Link Layer.



Data Link Layer

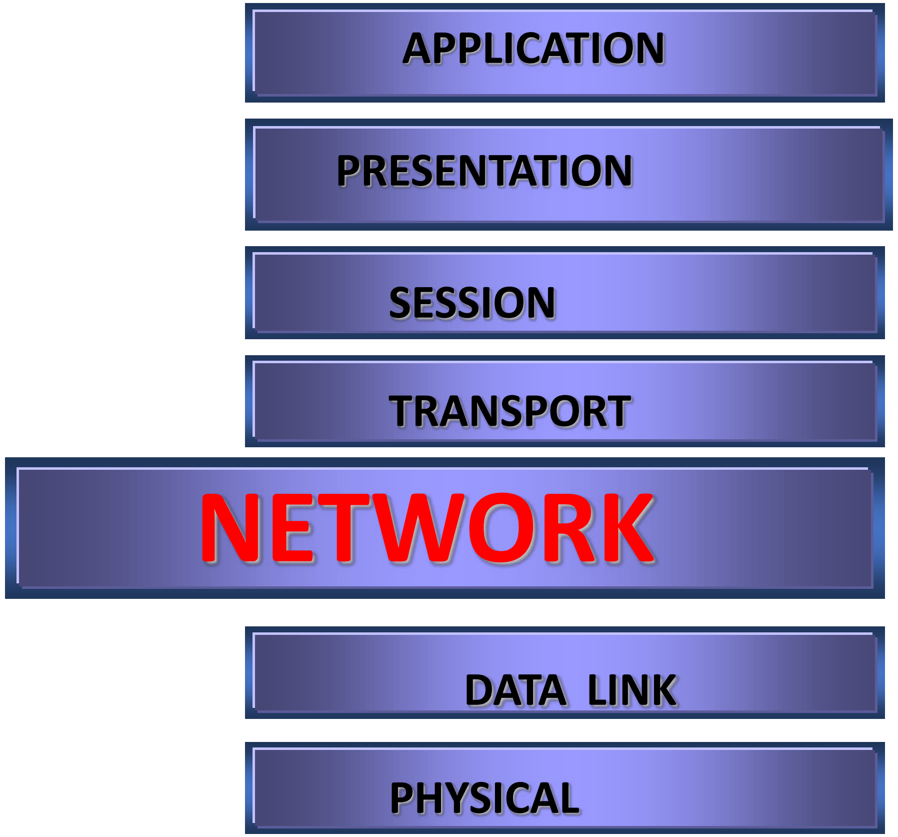


Data Link Layer



NETWORK

The network layer is responsible for the source-to-destination delivery of a packet possibly across multiple networks (links).



APPLICATION

PRESENTATION

SESSION

TRANSPORT

NETWORK

DATA LINK

PHYSICAL

Network Layer.

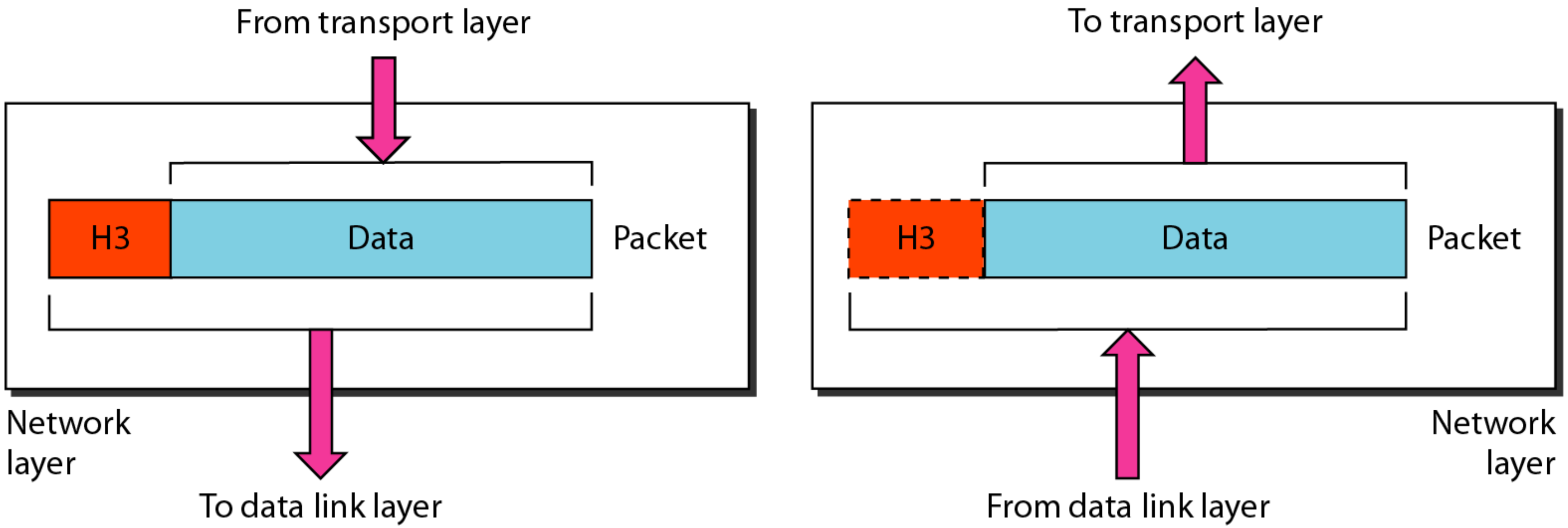
- The network layer is responsible for the source -to-destination delivery of a packet possibly across multiple networks.
  - It two systems are connected to the same link, there is usually no need for a network layer.
  - However, if the two systems are attached to different networks with connecting devices between the networks, there is need for the network layer to accomplish the delivery.
- The major duties performed by the network layer are:

Network Layer.

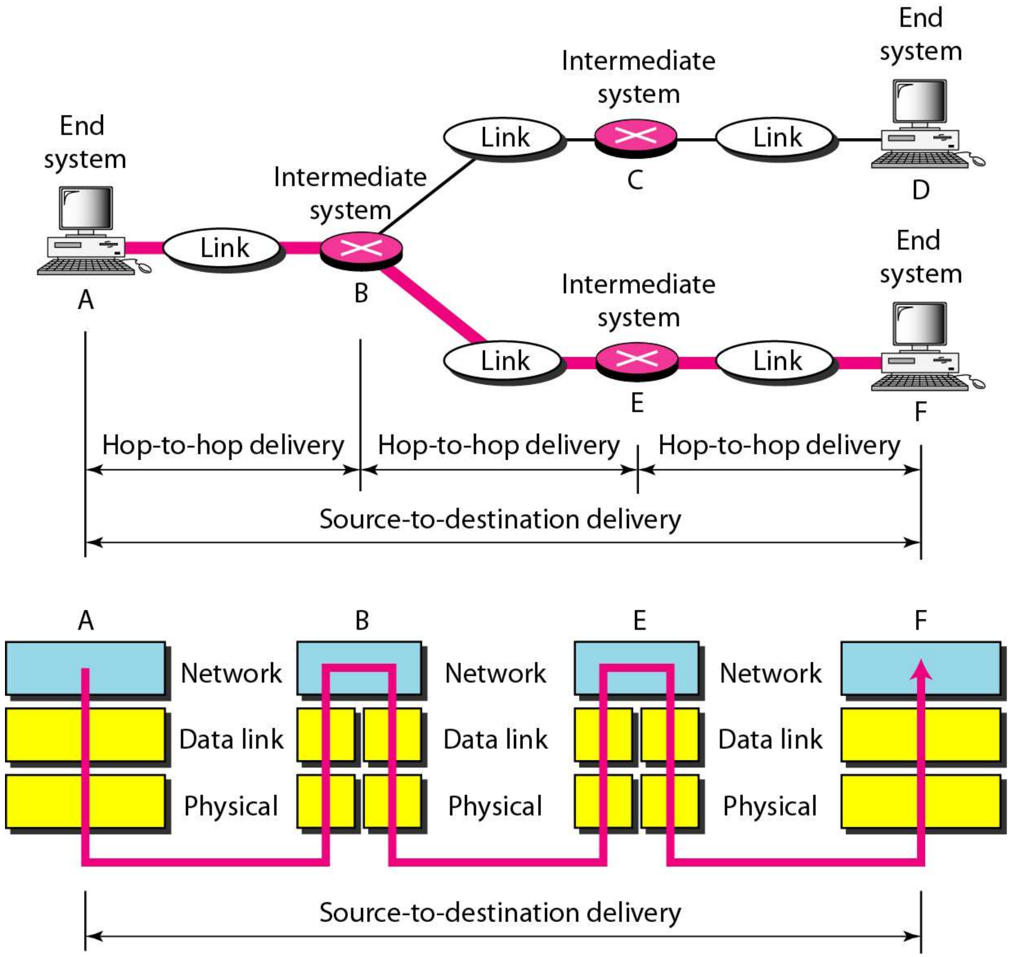
- **Logical addressing:**
  - The physical addressing implemented by the data link layer handles the addressing problem locally.
  - If a packet passes the network boundary, we need another addressing system to perform the source and destination delivery.
  - The network layer adds a header to the segment received from the session containing the logical addresses of the sender and receiver.
  - Logical address is also called IP address which is of 32-bits and represented in decimal format.
- **Routing:**
  - To route the packets from the source to destination in an internetwork, the router uses network layer information.

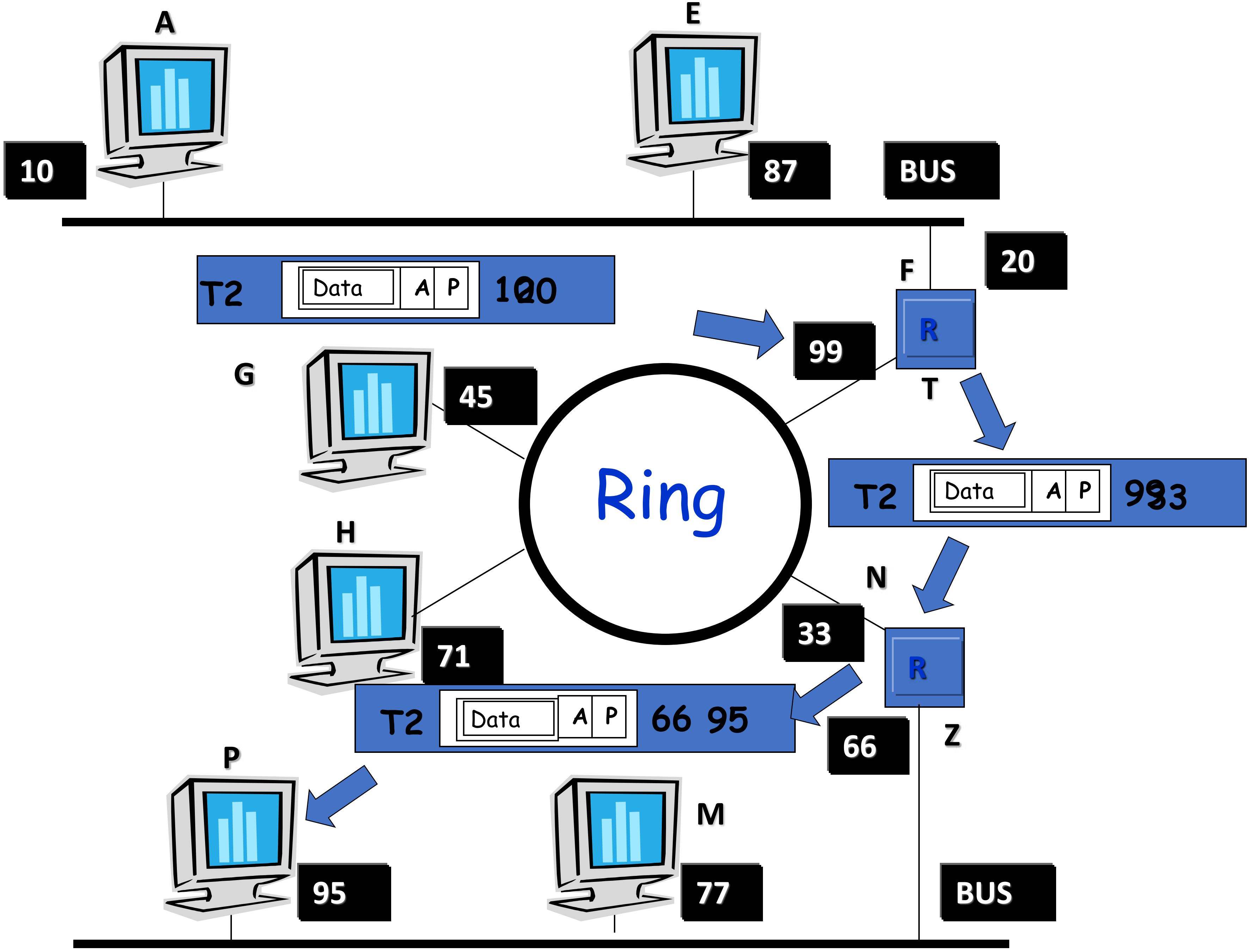
- The PDU of network layer is packet.
- Network layer protocols are IP, IPX, AppleTalk.

Network Layer.



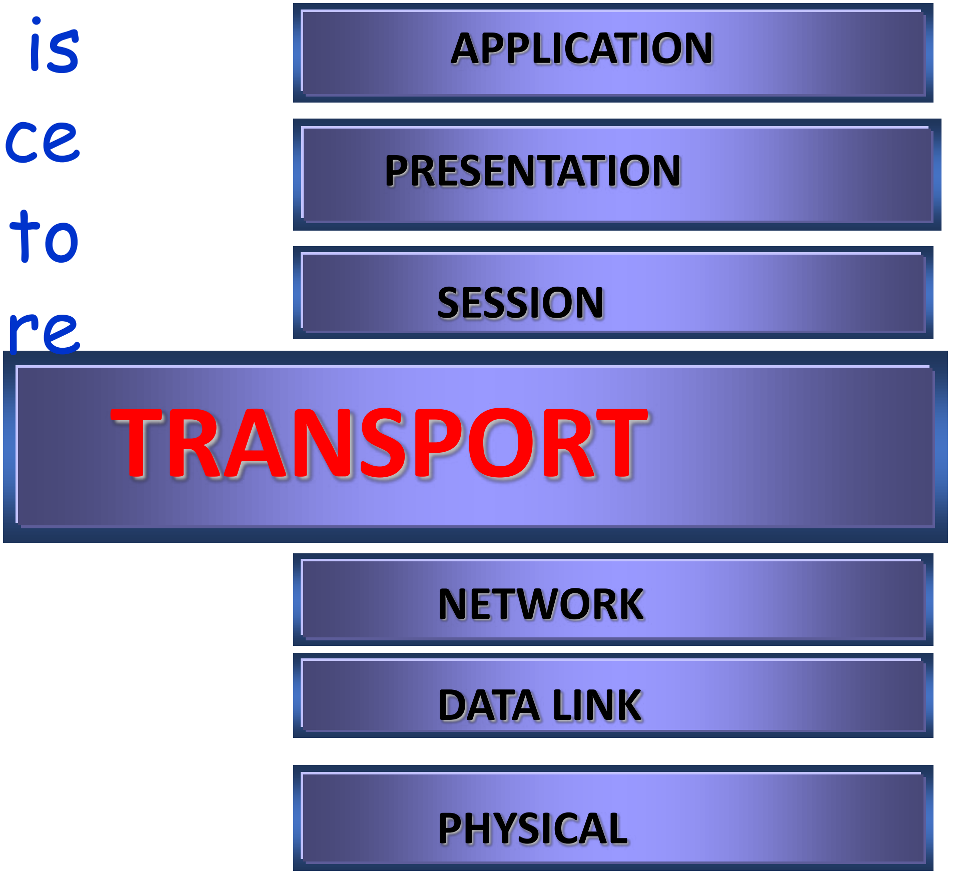
Source-to-Destination Delivery.




A
10
E
87
BUS
T2
Data
A
P
100
F
20
R
99
G
45
T
Ring
T2
Data
A
P
993
H
71
N
33
R
T2
Data
A
P
66 95
66
Z
P
95
M
77
BUS

TRANSPORT

- The transport layer is responsible for source to destination (end to end) delivery of entire message .



APPLICATION

PRESENTATION

SESSION

TRANSPORT

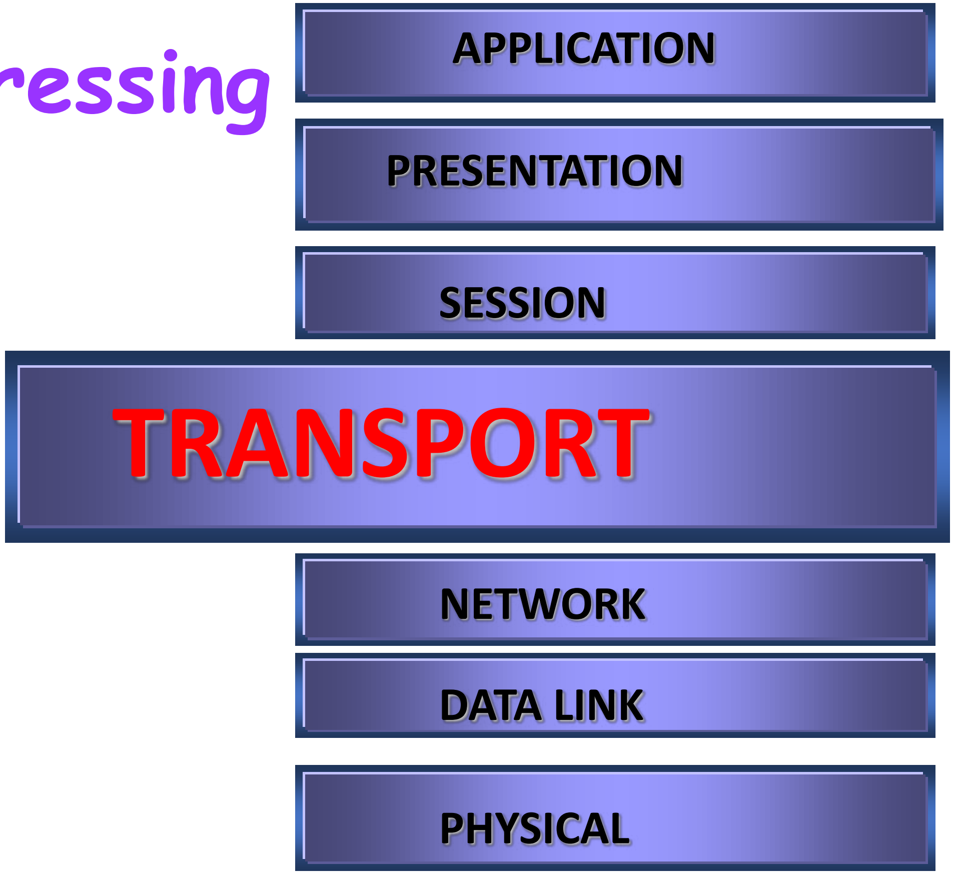
NETWORK

DATA LINK

PHYSICAL

TRANSPORT

- Service point addressing
- Segmentation and reassembly
- Connection control
- Flow control
- Error control



APPLICATION

PRESENTATION

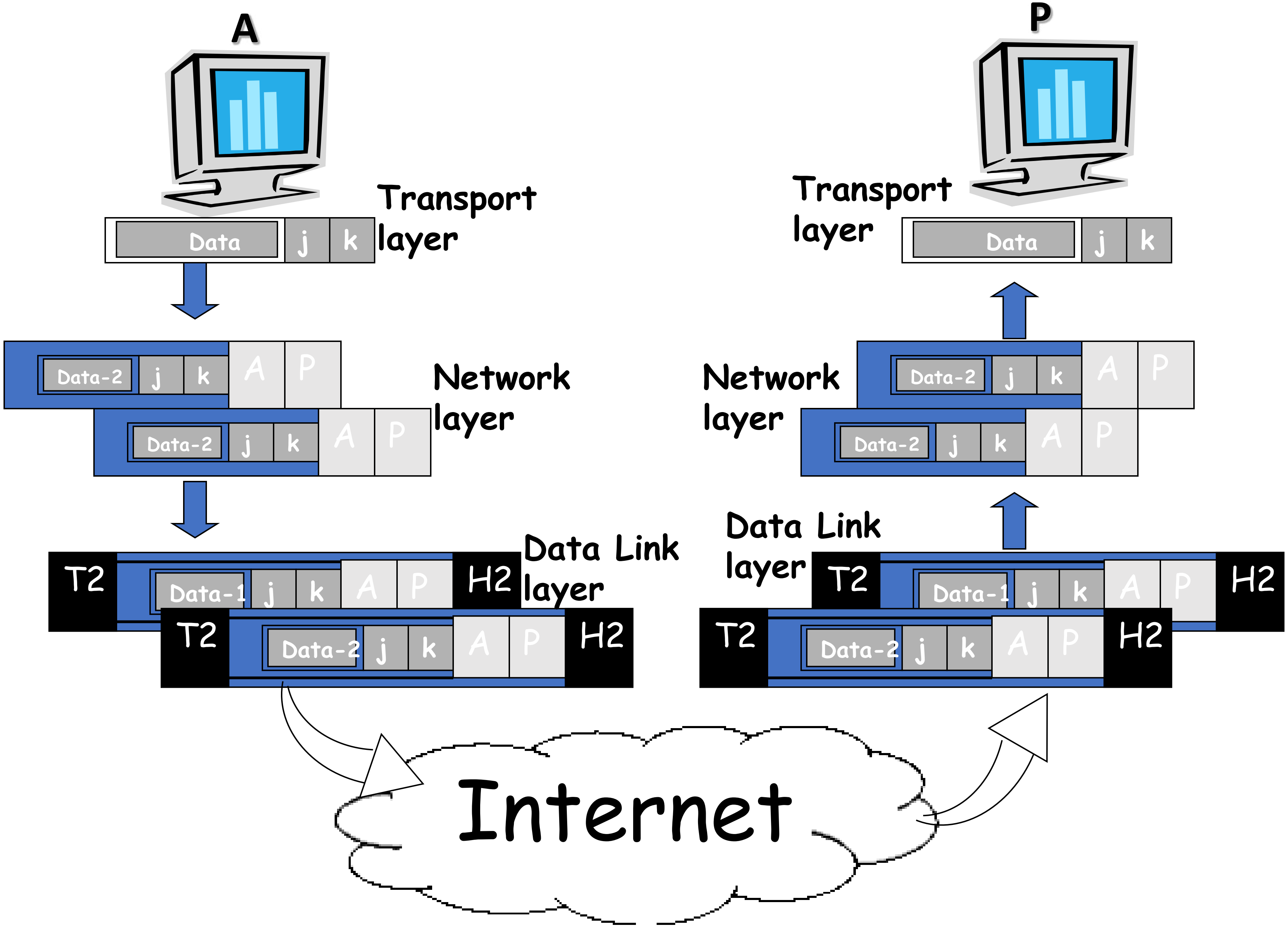
SESSION

TRANSPORT

NETWORK

DATA LINK

PHYSICAL



A

P

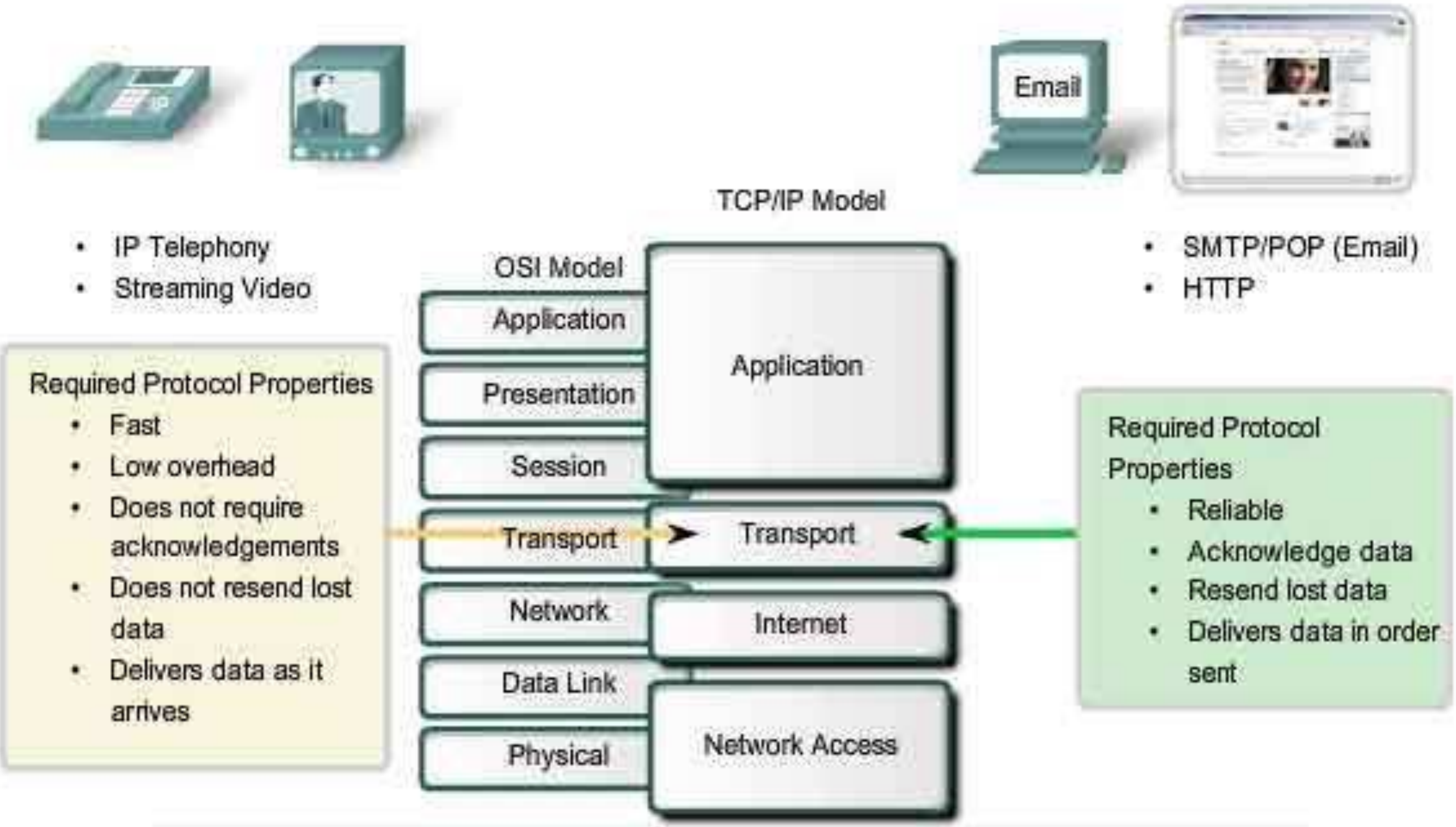
Transport layer

Network layer

Data Link layer

Internet

Transport Layer Protocols



- IP Telephony
- Streaming Video

Required Protocol Properties

- Fast
- Low overhead
- Does not require acknowledgements
- Does not resend lost data
- Delivers data as it arrives

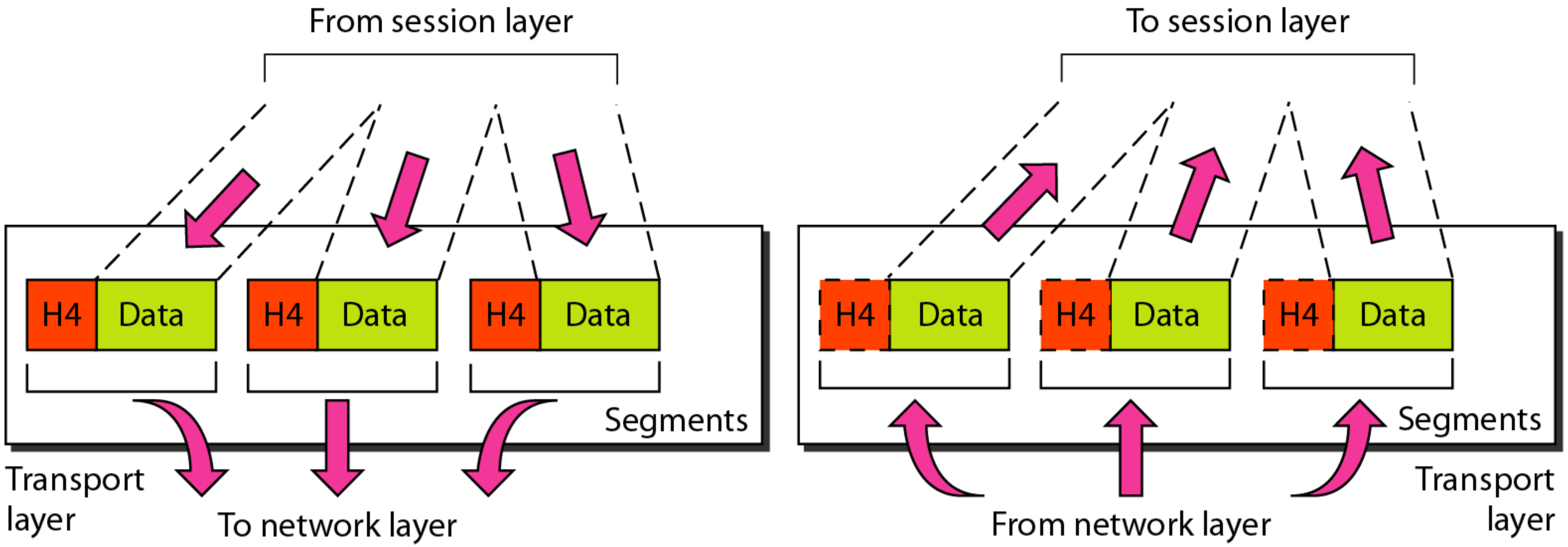
- SMTP/POP (Email)
- HTTP

Required Protocol Properties

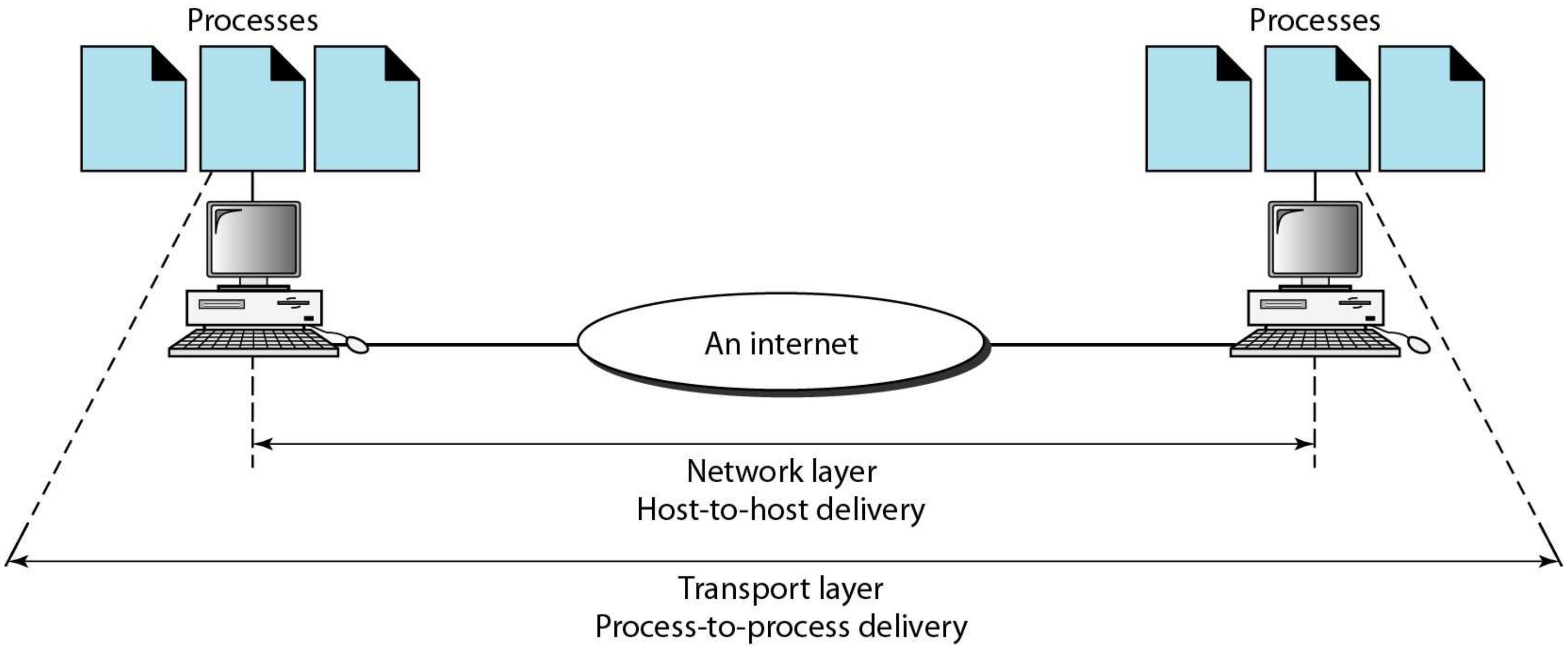
- Reliable
- Acknowledge data
- Resend lost data
- Delivers data in order sent

Application developers choose the appropriate Transport Layer protocol based on the nature of the application.

Transport Layer.



Reliable Process-to-Process Delivery.



Transport Layer.

- The transport layer is responsible for process-to-process delivery of the entire message.
- The major duties performed by the transport layer are:
  - **Port address:**
    - Computers often running several processes (running programs) at the same time:
    - Each running process open a logical port on the computer.
    - The transport layer header must therefore include a type of address called port address.
    - The network layer gets each packet to the correct computer, the transport layer get the entire message to the correct process on that computer.
  - **Segmentation and reassembly:**
    - A message received form the upper layers is divided into transmittable segments, each segment contains a sequence number.
    - These number enables the transport layer to reassemble the message correctly upon arrival at the destination and to identify and replace packets that were lost in the transmission.

Port No:

A port number is the logical address of each application or process that uses a network or the Internet to communicate.

A port number uniquely identifies a network-based application on a computer.

A port number is a way to identify a specific process to which an Internet or other network message is to be forwarded when it arrives at a server.

For the Transmission Control Protocol and the User Datagram Protocol, a port number is a 16-bit integer that is put in the header appended to a message unit.

This port number is passed logically between client and server transport layers and physically between the transport layer and the Internet Protocol layer and forwarded on.

For example, a request from a client (perhaps on behalf of you at your PC) to a server on the Internet may request a file be served from that host's File Transfer Protocol (FTP) server or process.

In order to pass your request to the FTP process in the remote server, the Transmission Control Protocol (TCP) software layer in your computer identifies the port number of 21 (which by convention is associated with an FTP request) in the 16-bit port number integer that is appended to your request. At the server, the TCP layer will read the port number of 21 and forward your request to the FTP program at the server.

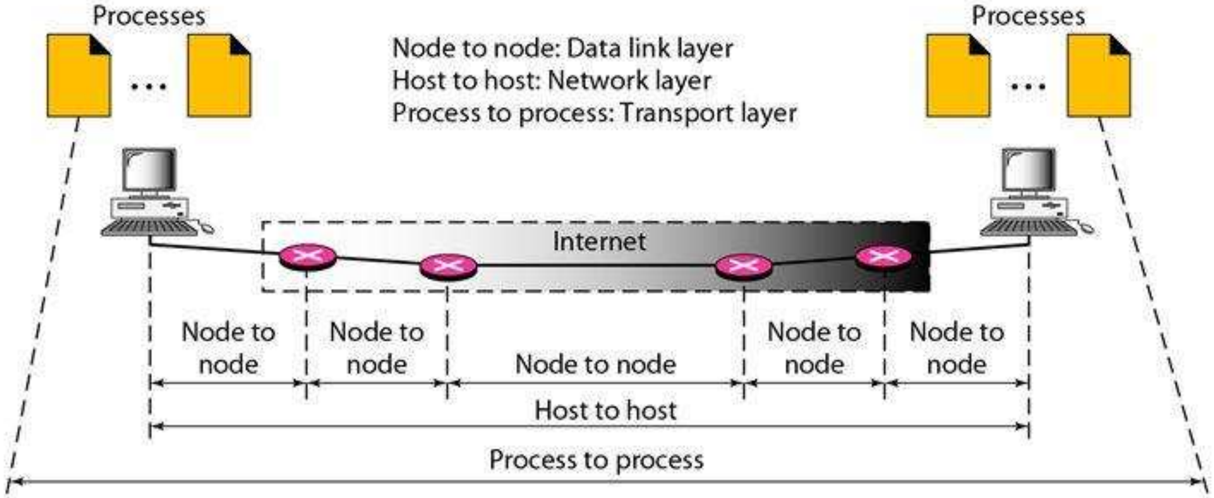
Some services or processes have conventionally assigned permanent port numbers.

These are known as well-known port numbers. In other cases, a port number is assigned temporarily (for the duration of the request and its completion) from a range of assigned port numbers.

This is called an ephemeral port number.

Important to Remember!!

- The Internet model has three protocols at the transport layer: UDP, TCP, and SCTP.
- 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. So that 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. The following figure shows these three types of deliveries and their domains.



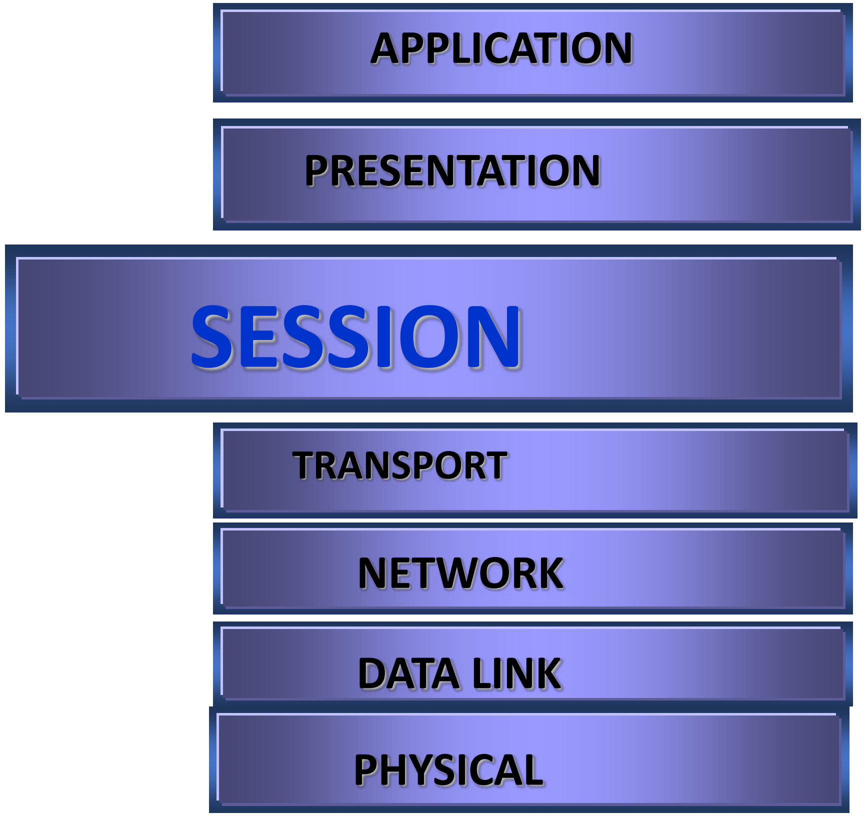
Transport Layer.

- **Connection Control:**
    - The transport layer can be either connectionless or connection oriented.
    - A connection oriented transport layer makes a logical connection with the transport layer at the destination machine first before delivering the packets.
    - After all the data are transferred, the connection is terminated.
- **Flow control:**
    - Like data link layer, the transport layer is resposnsible for flow control.
    - However, flow control at this layer is performed end to end rather than across a single link.
- **Error control:**
    - Like data link layer, the transport layer is responsible for error control.
    - However, error control at this layer is performed end to end rather than across a single link.

- Transport layer 4 protocols include TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

SESSION

- The session layer is the network dialog controller .It establishes ,maintains ,and ,synchronizes the interaction between communicating systems.



APPLICATION

PRESENTATION

SESSION

TRANSPORT

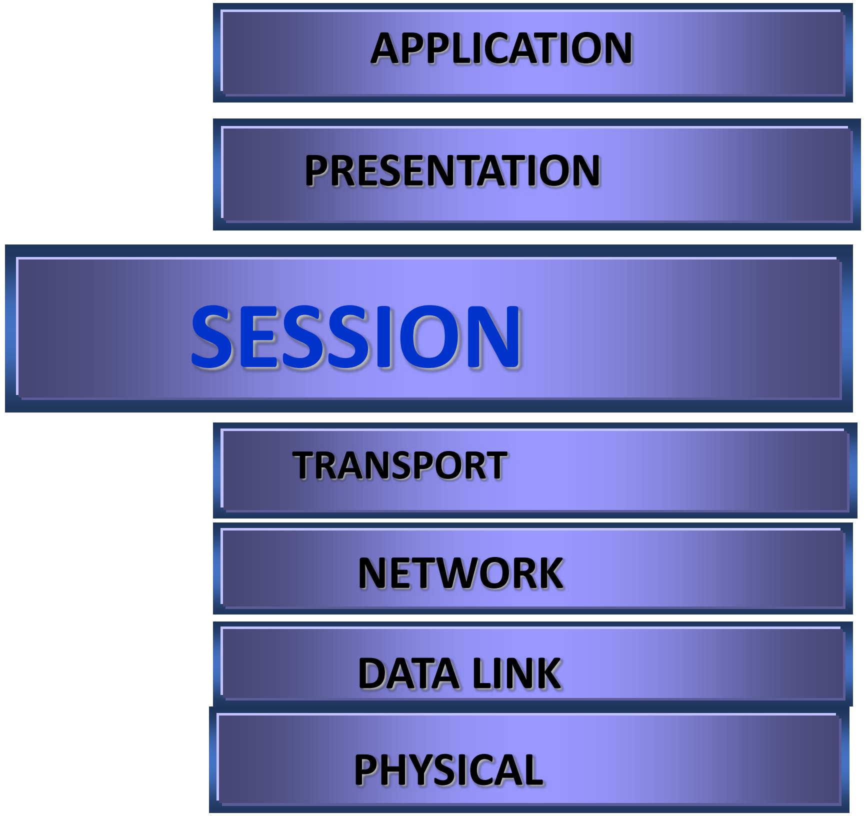
NETWORK

DATA LINK

PHYSICAL

SESSION

- Dialog control
- Synchronization



APPLICATION

PRESENTATION

SESSION

TRANSPORT

NETWORK

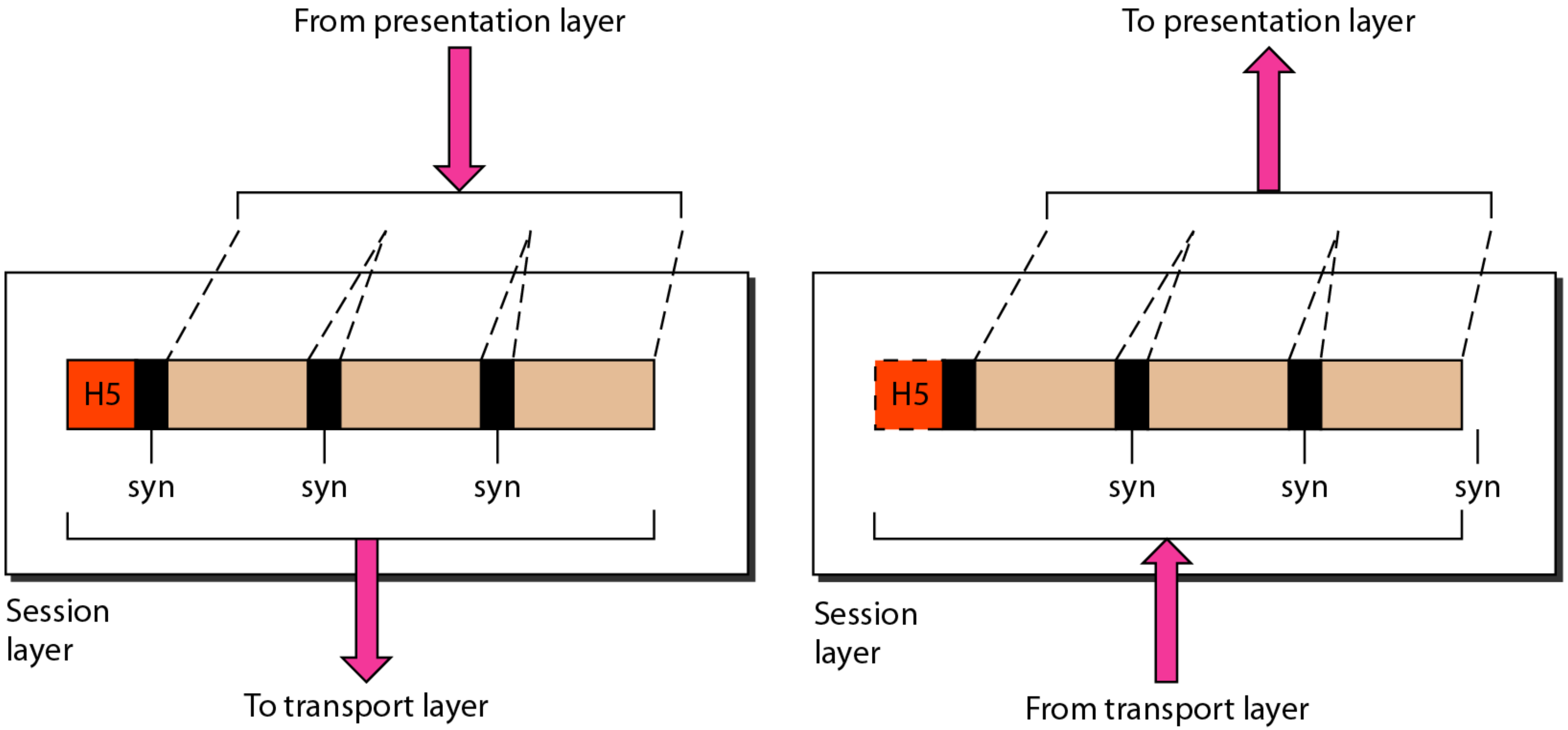
DATA LINK

PHYSICAL

Session Layer.

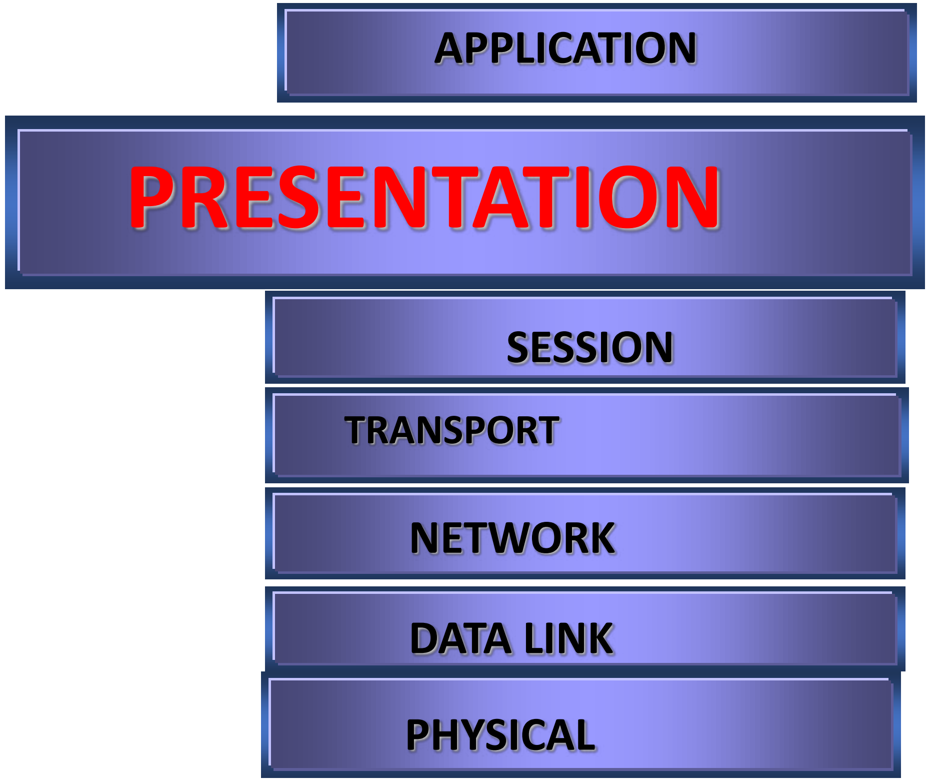
- The session layer defines how to establish, maintaining and terminates session between two communication hosts.
- The major duties of the session layer are:
  - **Synchronization:**
    - For lengthy transaction (file transfer), the user may choose to establish synchronization points associated with the transfer. If a fault develops during a transaction, the dialog may be restarted at an agreed synchronization point.
  - **Dialog control:**
    - Session layer determines that which role is to be played at any given time by a host.
      - **Duplex:** Two-way simultaneous.
      - **Half-Duplex:** Two-way alternate.
      - **Simplex:** One-way.
- Session layer protocols are SQL, ASP(AppleTalk Session Protocol), Remote Procedure Call (RPC), X Window System.

Session Layer.



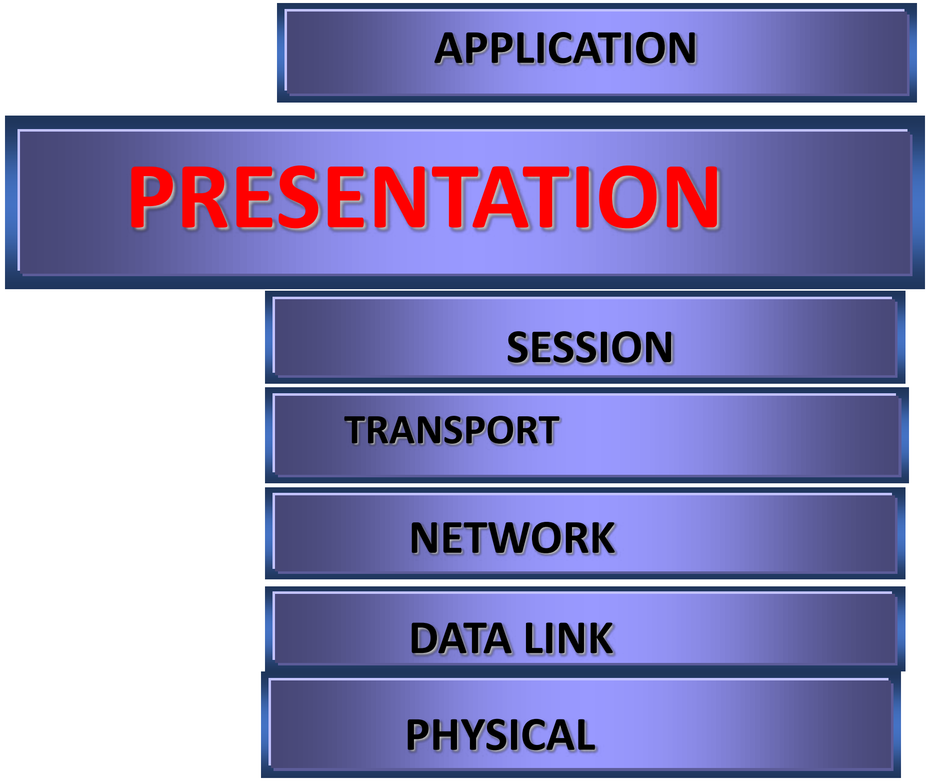
PRESENTATION

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



PRESENTATION

- Translation
- Encryption
- Compression



APPLICATION

PRESENTATION

SESSION

TRANSPORT

NETWORK

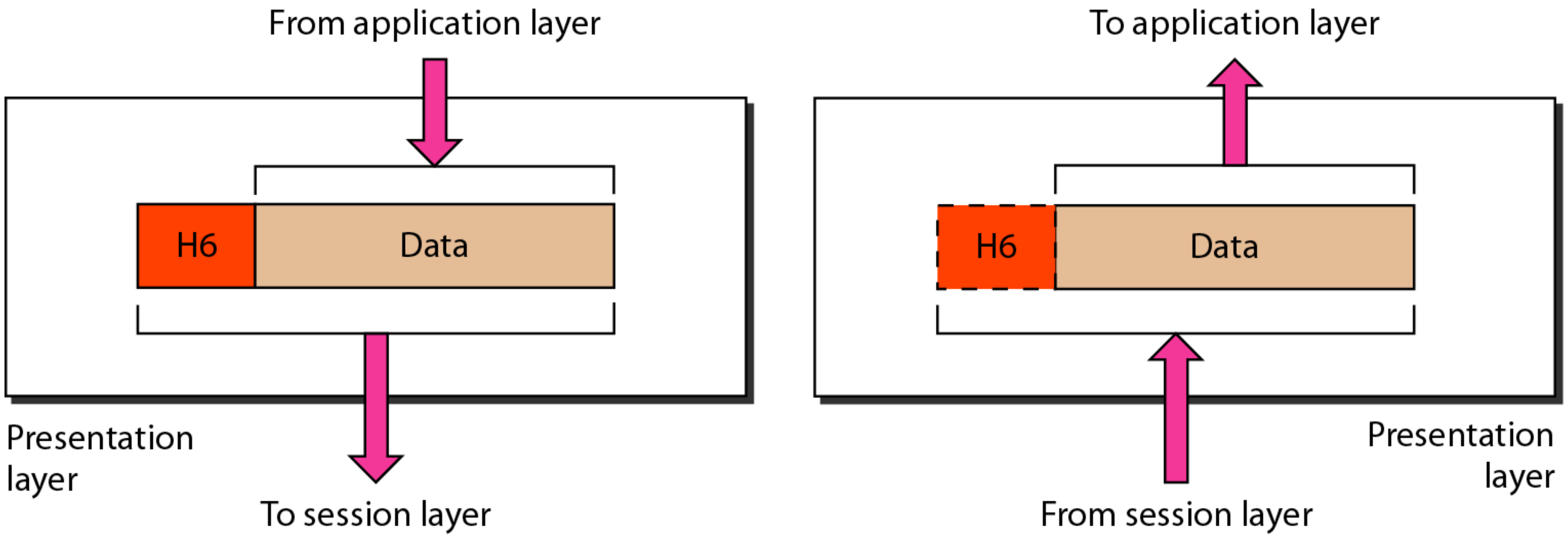
DATA LINK

PHYSICAL

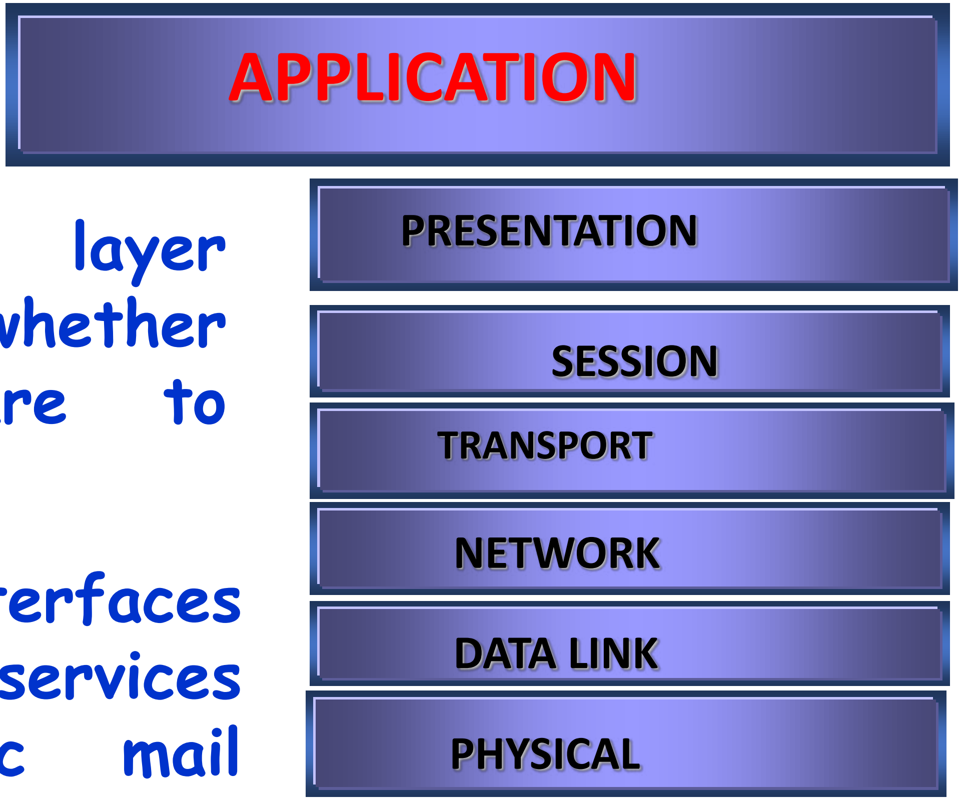
Presentation Layer.

- The presentation layer ensures that the information that the application layer of one system sends out is readable by the application layer of another system.
- The major duties of the presentation layer are:
  - Format conversion:
    - Convert message from one format into another format .i.e. for ASCII to EBCEDIC or vice versa.
  - Compression.
    - Compress the message to take less bandwidth on the transmission media and less time for transmission.
  - Encryption:
    - Convert the message into a form that will not be readable by others.
    - Provides security to the message.
- Protocols of the presentation layer are JPEG, MPEG, ASCII, EBCDIC etc.

Presentation Layer.



APPLICATION



APPLICATION

PRESENTATION

SESSION

TRANSPORT

NETWORK

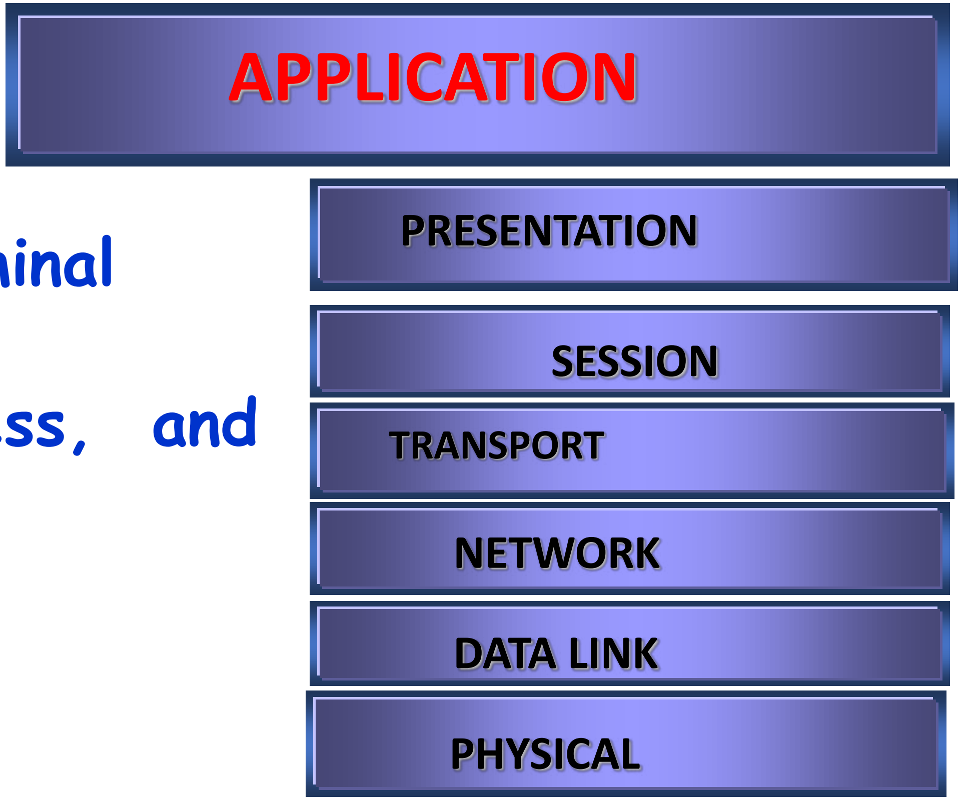
DATA LINK

PHYSICAL

- 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 type of distributed information services.

APPLICATION

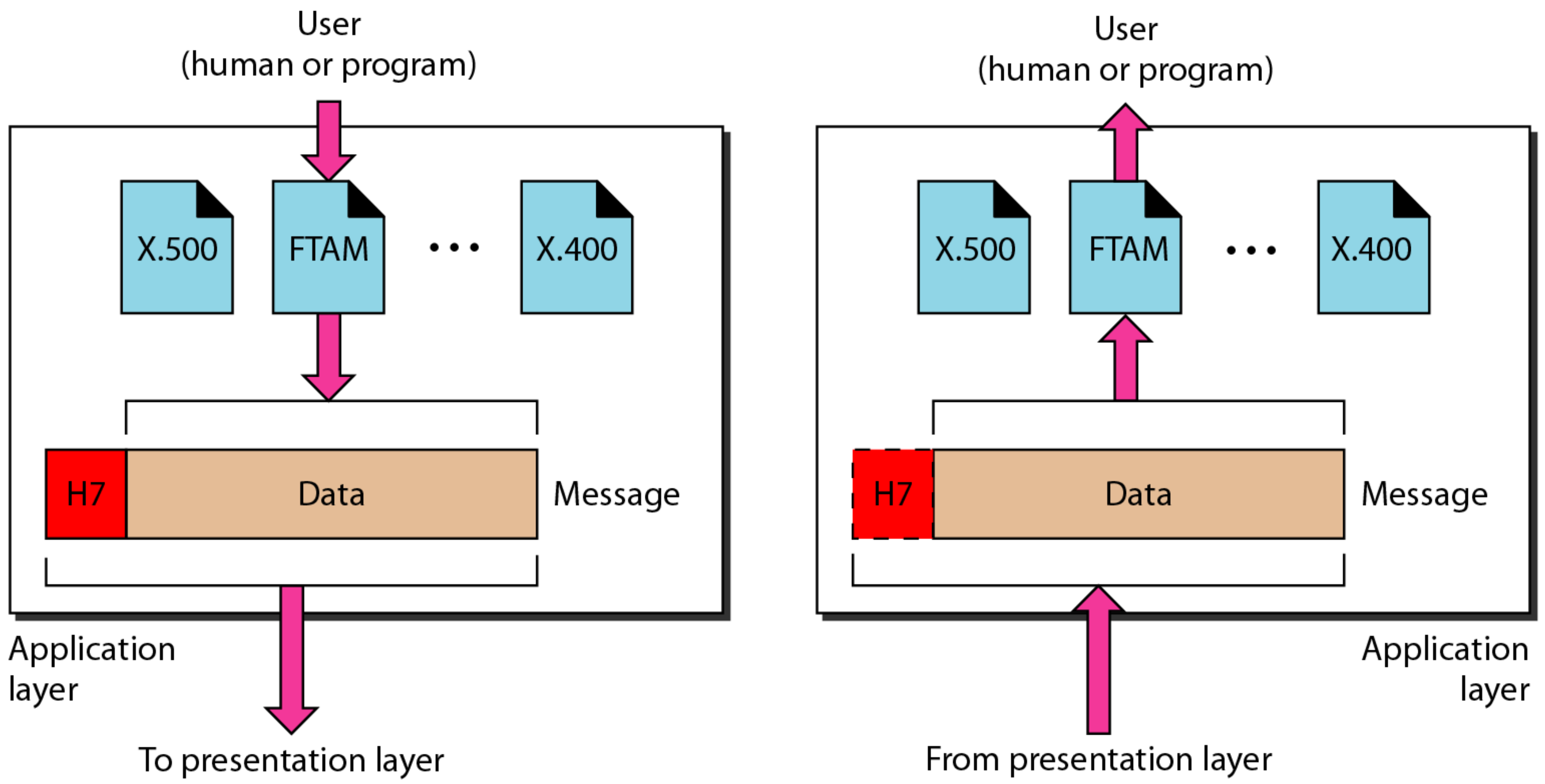


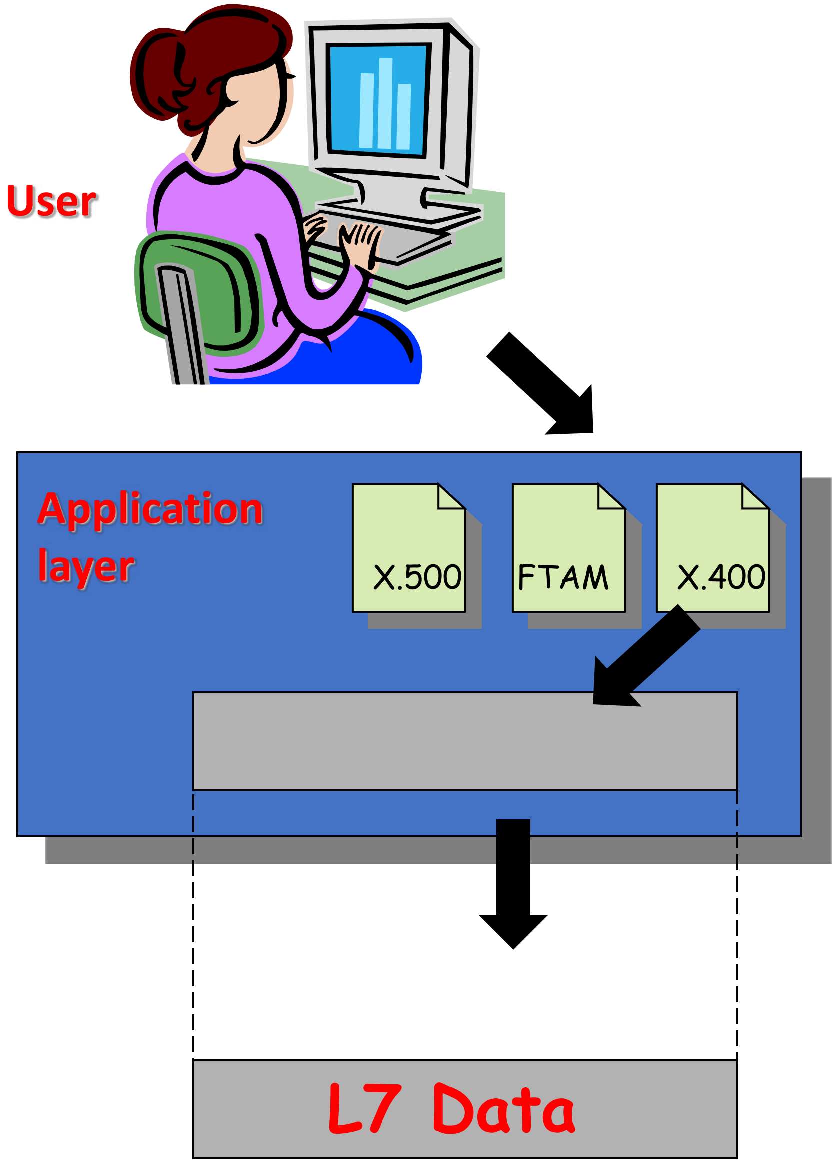
- Network virtual terminal
- File transfer, access, and management (FTAM)
- Mail services
- Directory services

Application Layer.

- The application layer is the OSI layer that is closest to the user.
- It provides network services to the user’s applications (.i.e. spreadsheet etc).
- The major duties are:
  - Mail service:
    - It provides network services for the email application.
  - File transfer and Access:
    - It provides network services for a user to access files on a remote computer, to retrieve files from a remote computer for use in the local computer and to manage or control files in a remote computer locally.
  - World Wide Web:
    - It provides network services to access the World Wide Web.

Application Layer.





User

Application layer

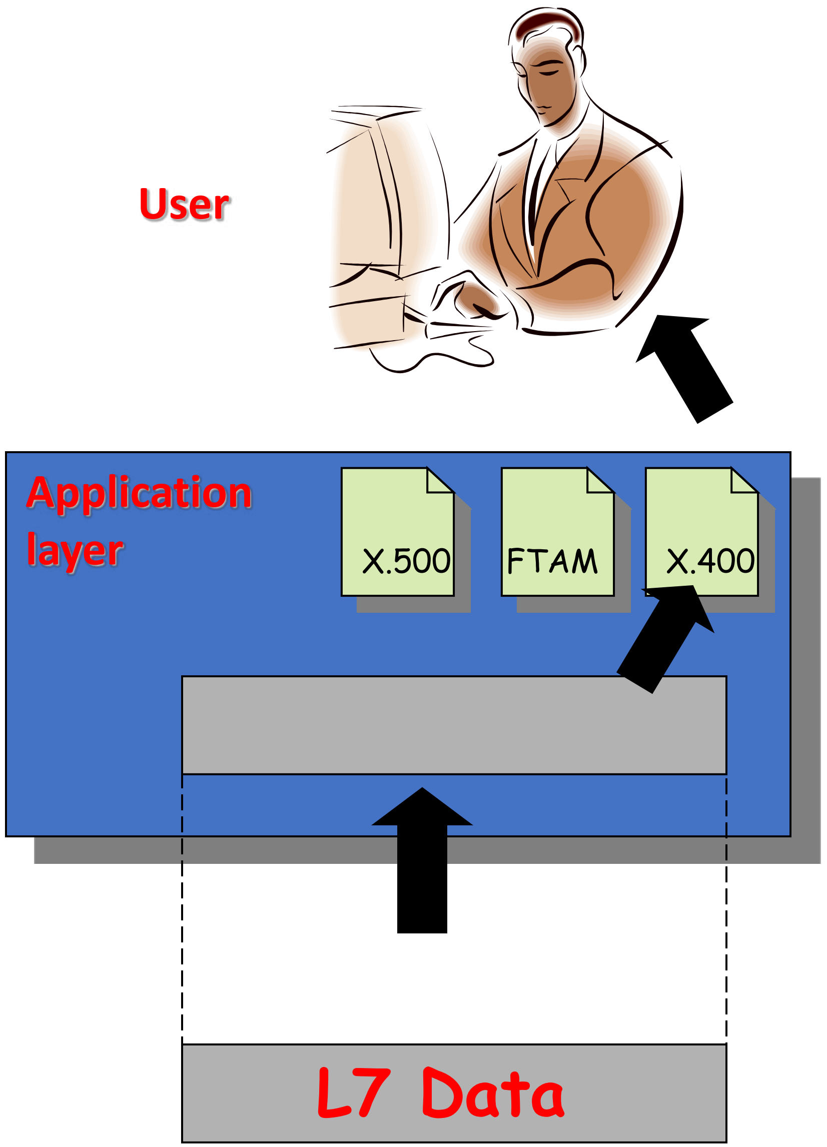
X.500

FTAM

X.400

L7 Data

To presentation layer



User

Application layer

X.500

FTAM

X.400

L7 Data

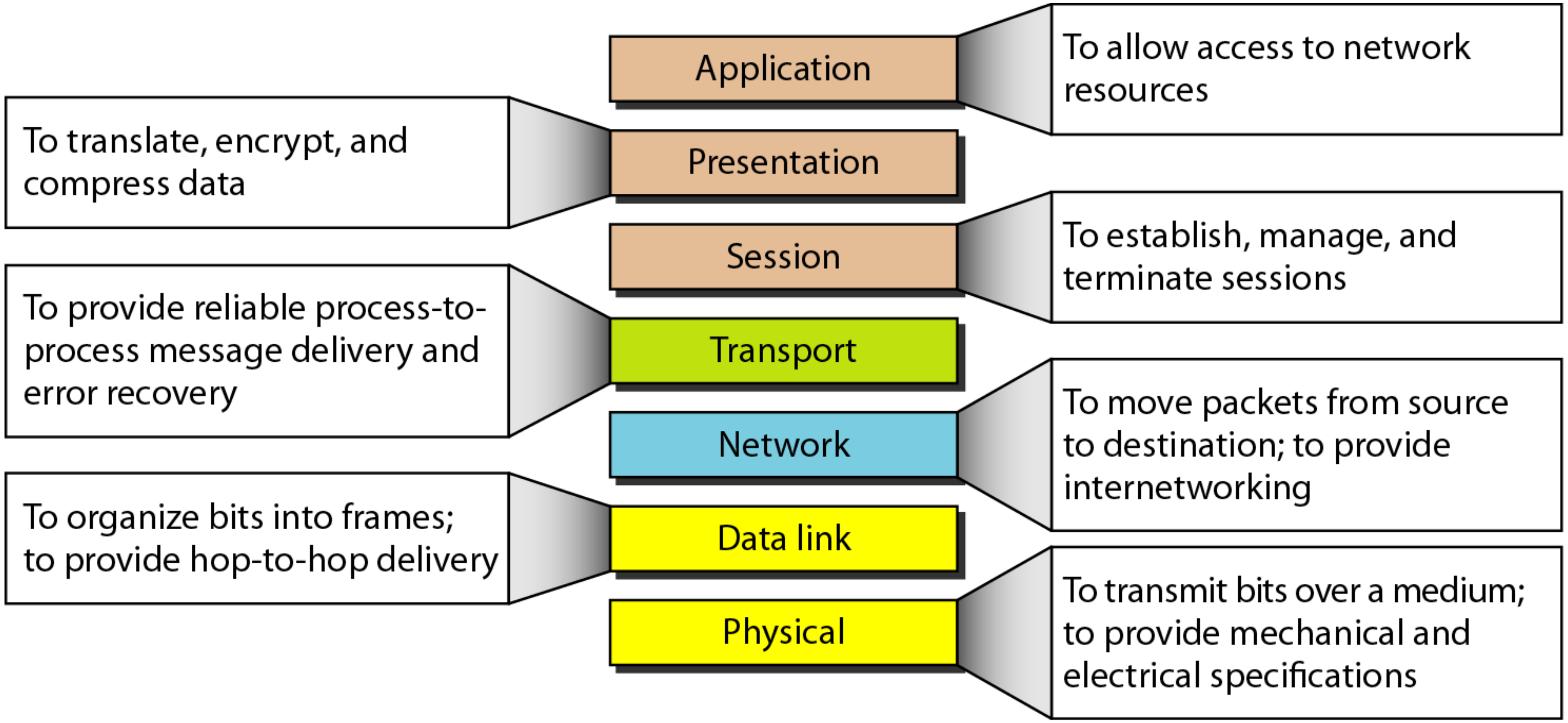
From presentation layer

APPLICATION LAYER

Summary.

- There was no standard for networks in the early days and as a result it was difficult for networks to communicate with each other.
- The International Organisation for Standardisation (ISO) recognised this. and researched various network schemes, and in 1984 introduced the Open Systems Interconnection (OSI) reference model.
- The OSI reference model has standards which ensure vendors greater compatibility and interoperability between various types of network technologies.
- The OSI reference model organizes network functions into seven numbered layers.
- Each layer provides a service to the layer above it in the protocol specification and communicates with the same layer's software or hardware on other computers.

Summary of the Layers.



Application

To allow access to network resources

Presentation

To translate, encrypt, and compress data

Session

To establish, manage, and terminate sessions

Transport

To provide reliable process-to-process message delivery and error recovery

Network

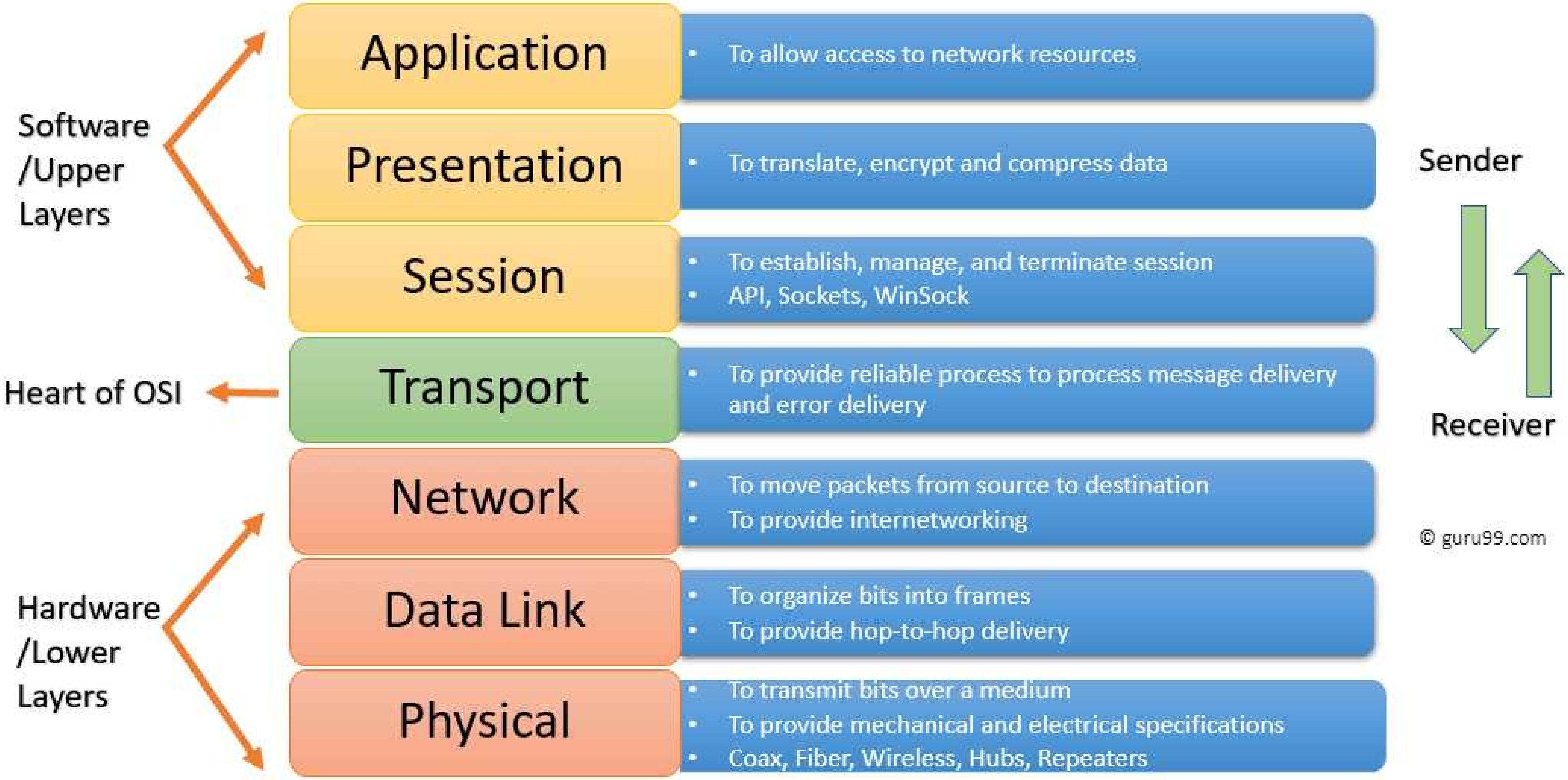
To move packets from source to destination; to provide internetworking

Data link

To organize bits into frames; to provide hop-to-hop delivery

Physical

To transmit bits over a medium; to provide mechanical and electrical specifications

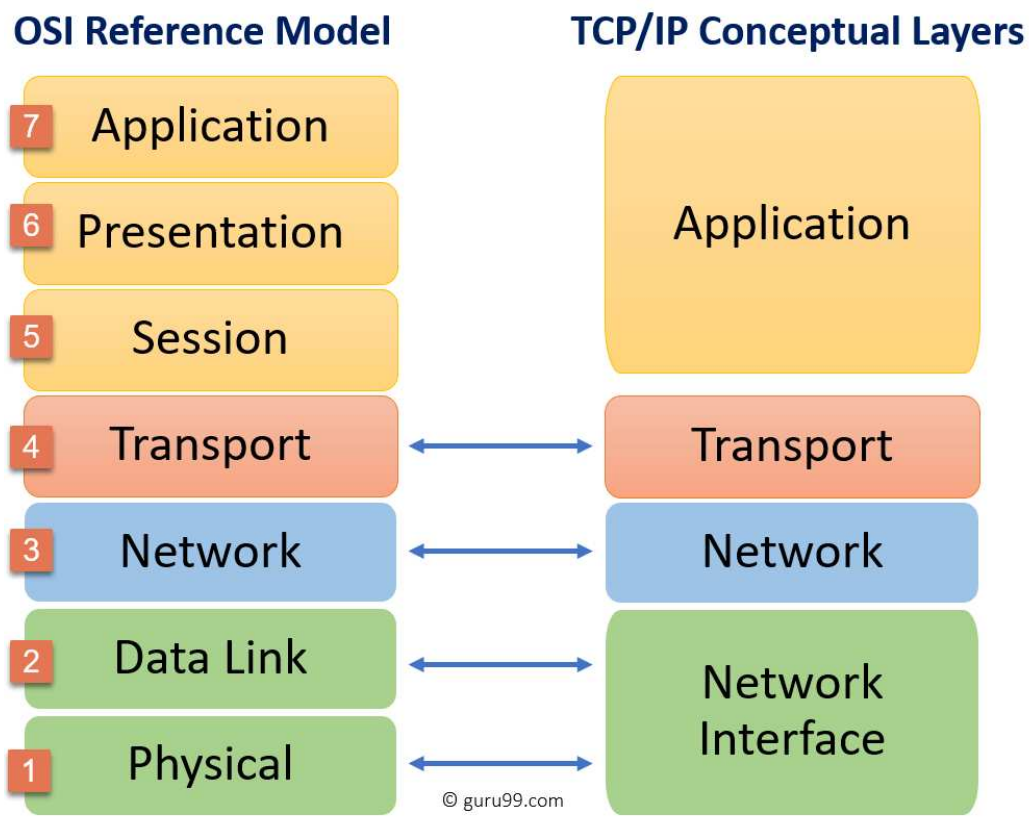


Application	- To allow access to network resources
Presentation	- To translate, encrypt and compress data
Session	- To establish, manage, and terminate session - API, Sockets, WinSock
Transport	- To provide reliable process to process message delivery and error delivery
Network	- To move packets from source to destination - To provide internetworking
Data Link	- To organize bits into frames - To provide hop-to-hop delivery
Physical	- To transmit bits over a medium - To provide mechanical and electrical specifications - Coax, Fiber, Wireless, Hubs, Repeaters

© guru99.com

Protocols supported at various levels

Layer	Name	Protocols
Layer 7	Application	SMTP, HTTP, FTP, POP3, SNMP
Layer 6	Presentation	MPEG, ASCH, SSL, TLS
Layer 5	Session	NetBIOS, SAP
Layer 4	Transport	TCP, UDP
Layer 3	Network	IPV5, IPV6, ICMP, IPSEC, ARP, MPLS.
Layer 2	Data Link	RAPA, PPP, Frame Relay, ATM, Fiber Cable, etc.
Layer 1	Physical	RS232, 100BaseTX, ISDN, 11.

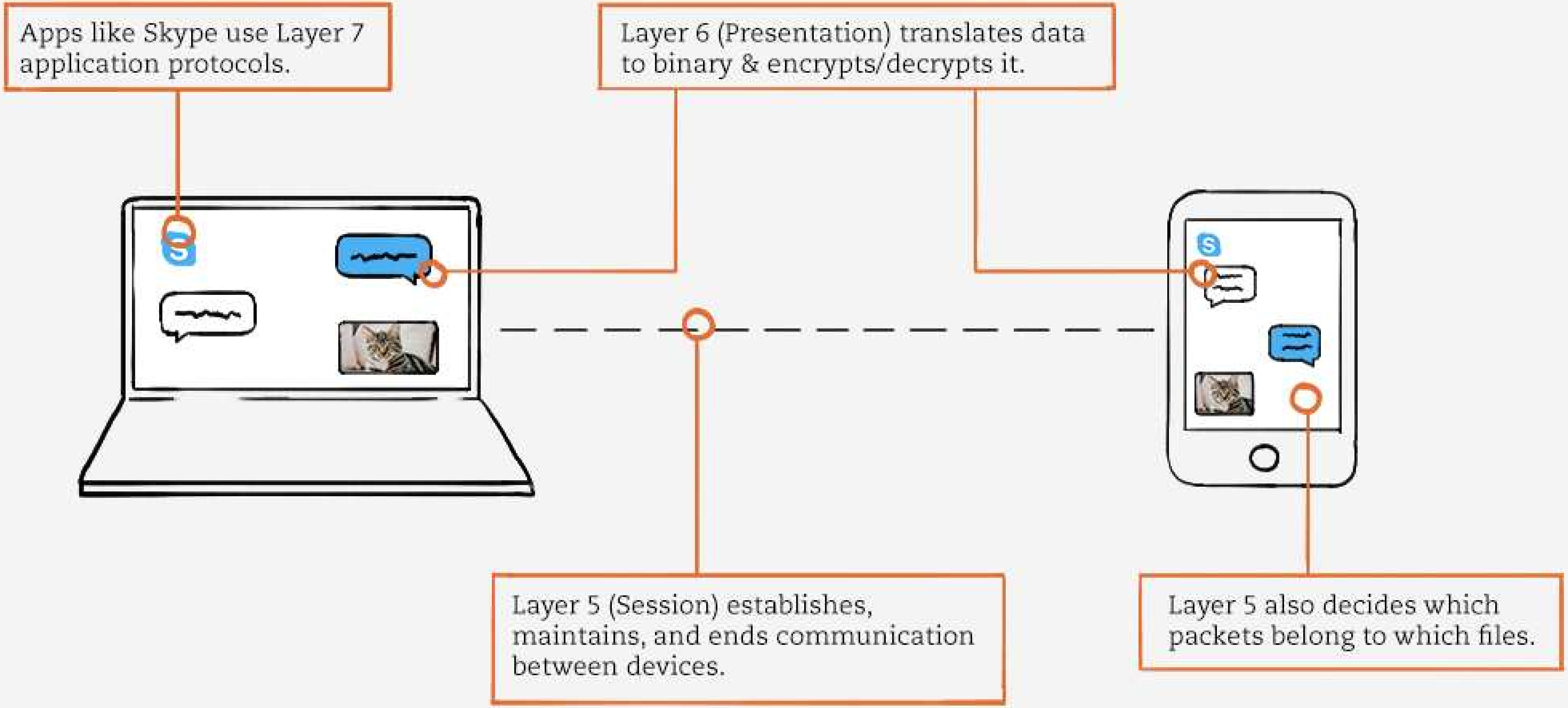


- **Layer 1** (Network Access): Also called the Link or Network Interface layer. This layer combines the OSI model's L1 and L2.
- **Layer 2** (Internet): This layer is similar to the OSI model's L3.
- **Layer 3** (Transport): Also called the Host-to-Host layer. This layer is similar to the OSI model's L4.
- **Layer 4** (Application): Also called the Process layer, this layer combines the OSI model's L5, L6, and L7.

OSI Model	TCP/IP model
OSI model provides a clear distinction between interfaces, services, and protocols.	TCP/IP doesn't offer any clear distinguishing points between services, interfaces, and protocols.
OSI uses the network layer to define routing standards and protocols.	TCP/IP uses only the Internet layer.
OSI model use two separate layers physical and data link to define the functionality of the bottom layers	TCP/IP uses only one layer (link).
OSI model, the transport layer is only connection-oriented.	A layer of the TCP/IP model is both connection-oriented and connectionless.
In OSI model, data link layer and physical are separate layers.	In TCP data link layer and physical layer are combined as a single host-to-network layer.
The minimum size of the OSI header is 5 bytes.	Minimum header size is 20 bytes.

Application, Presentation, and Session Layers

- Let’s suppose you’re using Skype on a laptop. You’re messaging your friend, who’s using Skype on their phone from a different network.
- Skype, as a network-connected application, uses **Layer 7 (Application)** protocols like Telnet. If you send your friend a picture of your cat, Skype would be using the File Transfer Protocol (FTP).
- **Layer 6 (Presentation)** receives application data from Layer 7, translates it into binary, and compresses it. When you send a message, Layer 6 encrypts that data as it leaves your network. Then it decrypts the data when your friend receives it.
- Applications like Skype consist of text files and image files. When you download these files, **Layer 5 (Session)** determines which data packets belong to which files, as well as where these packets go. Layer 5 also establishes, maintains, and ends communication between devices.



Apps like Skype use Layer 7 application protocols.

Layer 6 (Presentation) translates data to binary & encrypts/decrypts it.

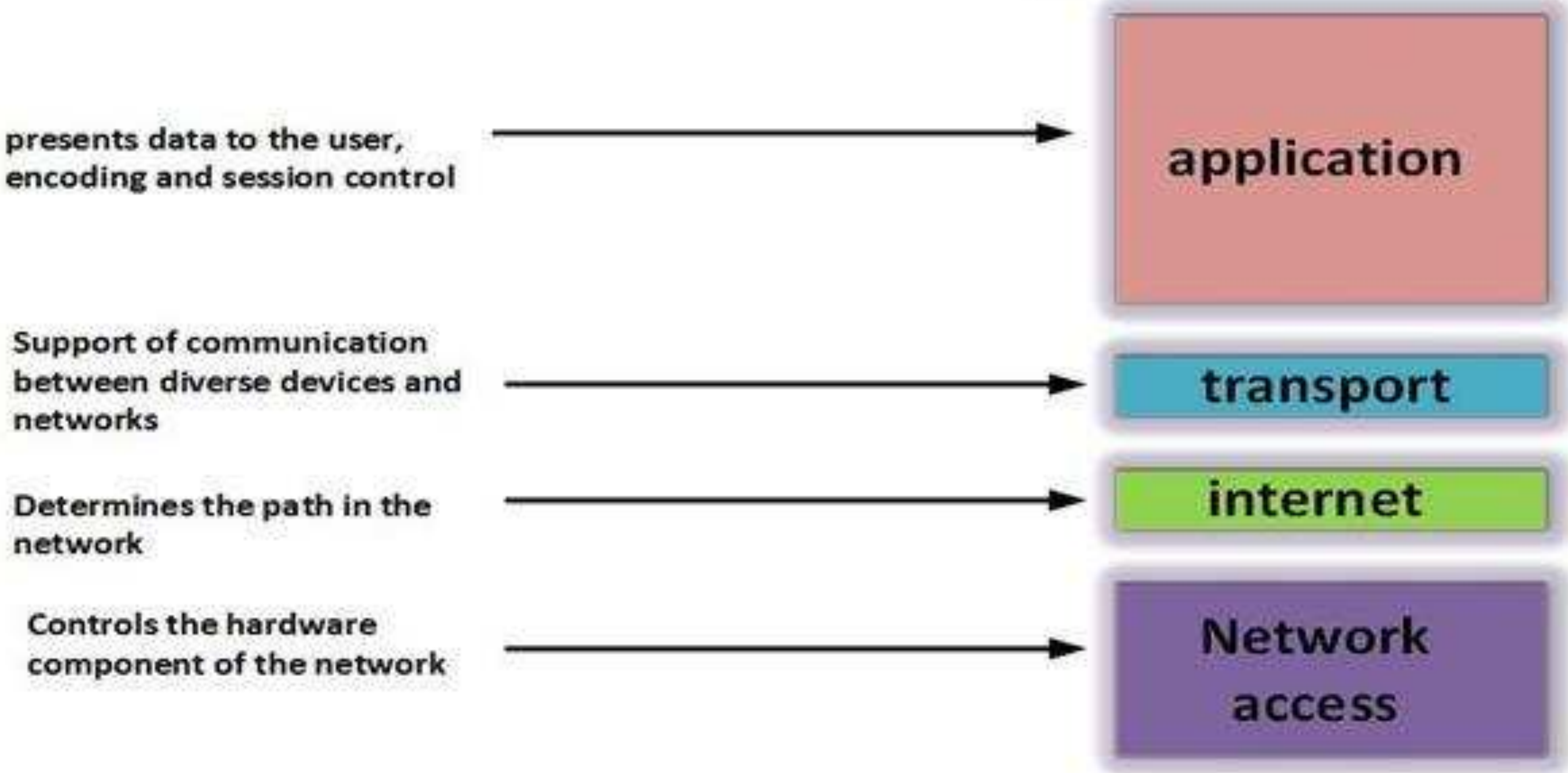
Layer 5 (Session) establishes, maintains, and ends communication between devices.

Layer 5 also decides which packets belong to which files.

TCP/IP Model

- TCP/IP helps you to determine how a specific computer should be connected to the internet and how you can transmit data between them. It helps you to create a virtual network when multiple computer networks are connected together.
- TCP/IP stands for Transmission Control Protocol/ Internet Protocol. It is specifically designed as a model to offer highly reliable and end-to-end byte stream over an unreliable internetwork.

TCP/IP model

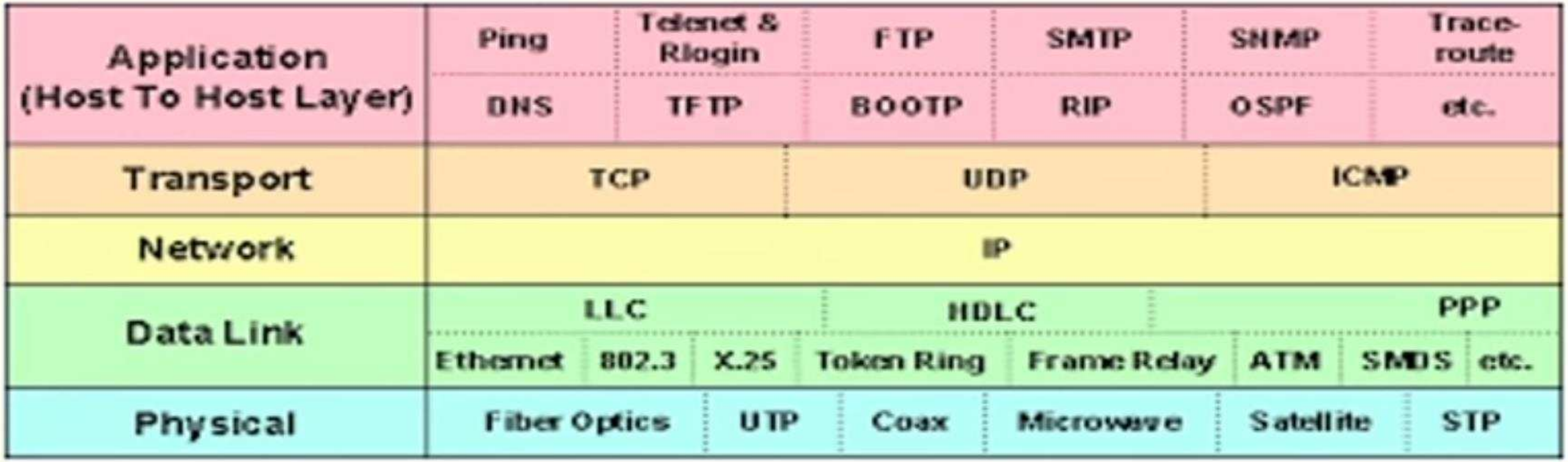


presents data to the user, encoding and session control → application

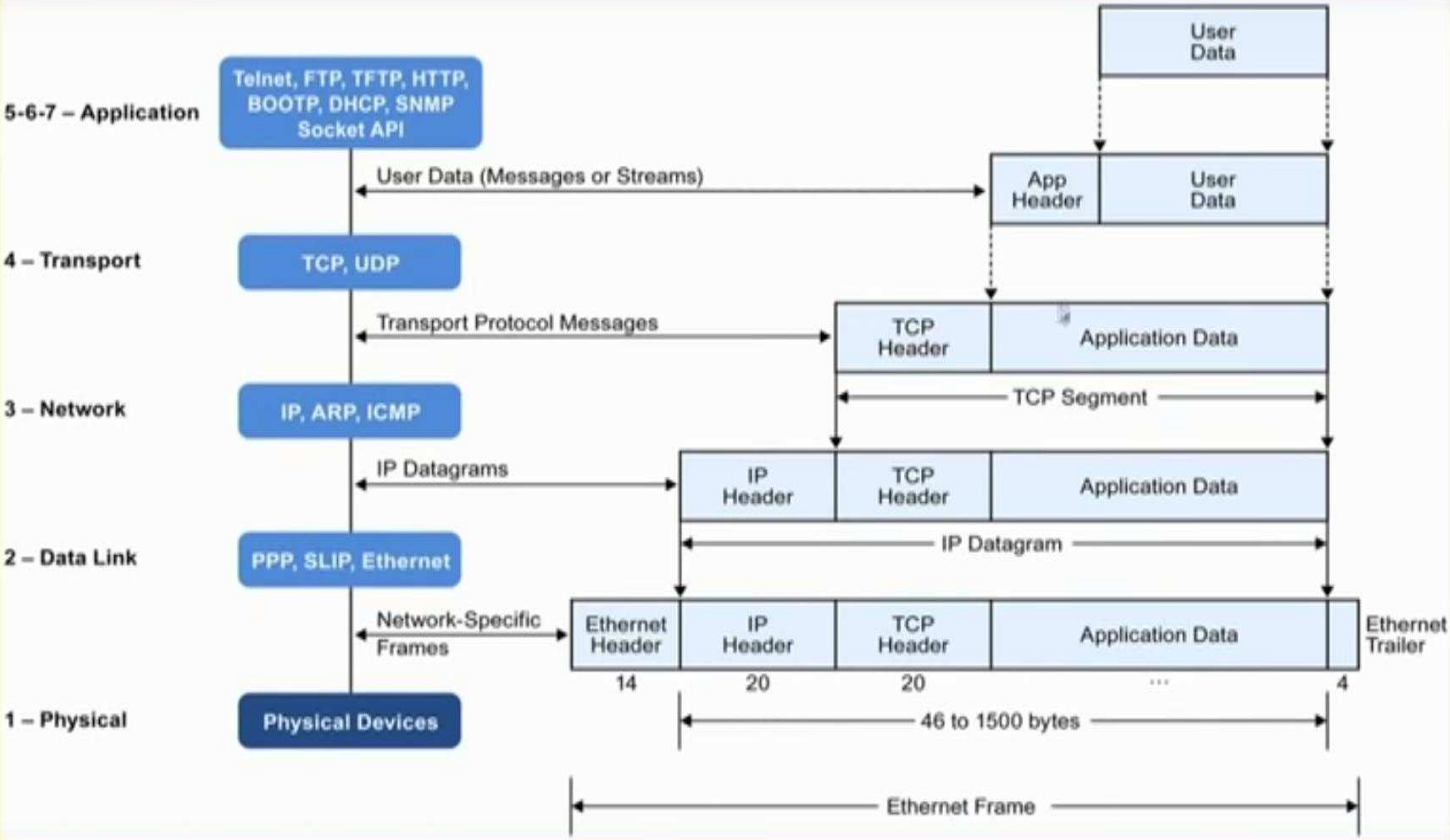
Support of communication between diverse devices and networks → transport

Determines the path in the network → internet

Controls the hardware component of the network → Network access



Application (Host To Host Layer)	Ping	Telenet & Rlogin	FTP	SMTP	SNMP	Trace-route		
	DNS	TFTP	BOOTP	RIP	OSPF	etc.		
Transport	TCP	UDP	ICMP					
Network	IP							
Data Link	LLC	HDLC	PPP					
	Ethernet	802.3	X.25	Token Ring	Frame Relay	ATM	SMDS	etc.
Physical	Fiber Optics	UTP	Coax	Microwave	Satellite	STP		



5-6-7 – Application

Telnet, FTP, TFTP, HTTP, BOOTP, DHCP, SNMP Socket API

4 – Transport

TCP, UDP

3 – Network

IP, ARP, ICMP

2 – Data Link

PPP, SLIP, Ethernet

1 – Physical

Physical Devices

User Data (Messages or Streams)

Transport Protocol Messages

IP Datagrams

Network-Specific Frames

User Data

App Header | User Data

TCP Header | Application Data

TCP Segment

IP Header | TCP Header | Application Data

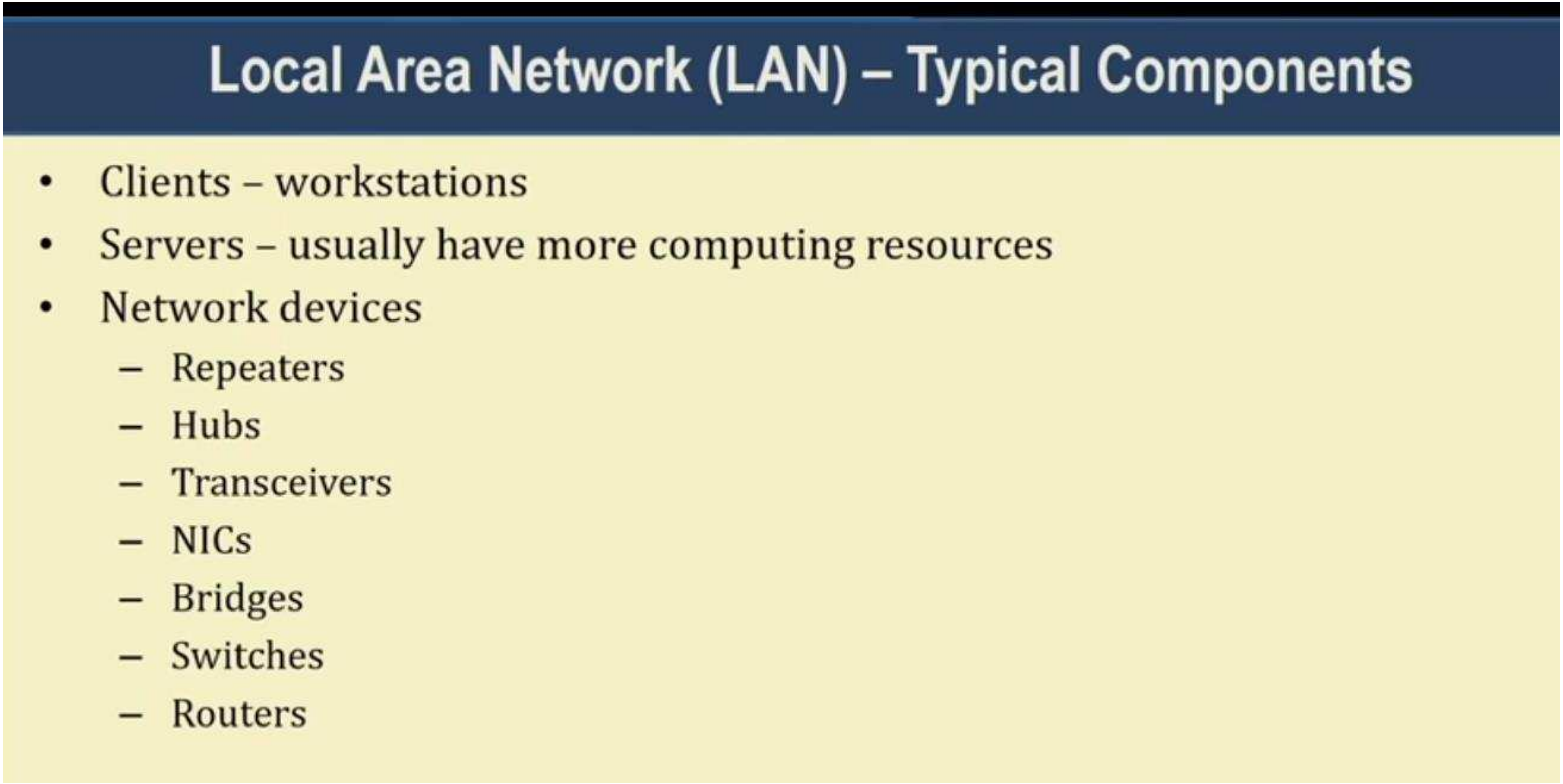
IP Datagram

Ethernet Header | IP Header | TCP Header | Application Data | Ethernet Trailer

14 | 20 | 20 | ... | 4

46 to 1500 bytes

Ethernet Frame



Local Area Network (LAN) – Typical Components

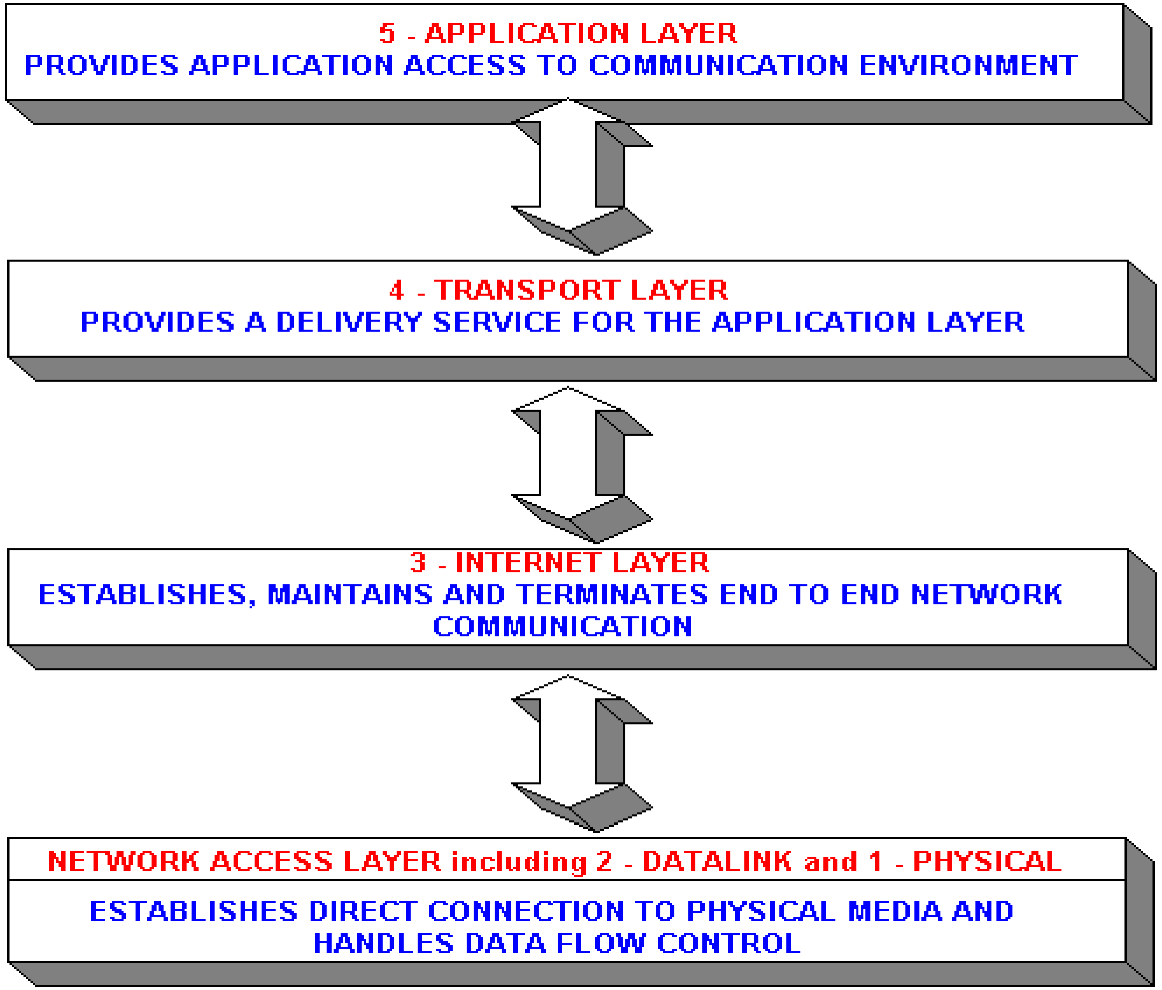
- Clients – workstations
- Servers – usually have more computing resources
- Network devices
  - Repeaters
  - Hubs
  - Transceivers
  - NICs
  - Bridges
  - Switches
  - Routers

OSI Model	**TCP/IP Model**
It is developed by ISO (International Standard Organization)	It is developed by ARPANET (Advanced Research Project Agency Network).
OSI model provides a clear distinction between interfaces, services, and protocols.	TCP/IP doesn't have any clear distinguishing points between services, interfaces, and protocols.
OSI refers to Open Systems Interconnection.	TCP refers to Transmission Control Protocol.
OSI uses the network layer to define routing standards and protocols.	TCP/IP uses only the Internet layer.
OSI follows a vertical approach.	TCP/IP follows a horizontal approach.
OSI layers have seven layers.	TCP/IP has four layers.
In the OSI model, the transport layer is only connection-oriented.	A layer of the TCP/IP model is both connection-oriented and connectionless.
In the OSI model, the data link layer and physical are separate layers.	In TCP, physical and data link are both combined as a single host-to-network layer.
Session and presentation layers are a part of the OSI model.	There is no session and presentation layer in the TCP model.
It is defined after the advent of the Internet.	It is defined before the advent of the internet.
The minimum size of the OSI header is 5 bytes.	The minimum header size is 20 bytes.

TCP/IP

- The TCP/IP model was created in the 1970s by the Defense Advance Research Project Agency (DARPA).
- Like the OSI model, it describes general guidelines for designing and implementing computer protocols.
  It consists of four layers: Network Access, Internet, Transport, and Application.
- The Application, Presentation, and Session layers of the OSI model are merged in only one layer, Application layer, in the TCP/IP model.
- Also, Physical and Data Link layers are called Network Access layer in the TCP/IP model.

TCP/IP Layered Protocol

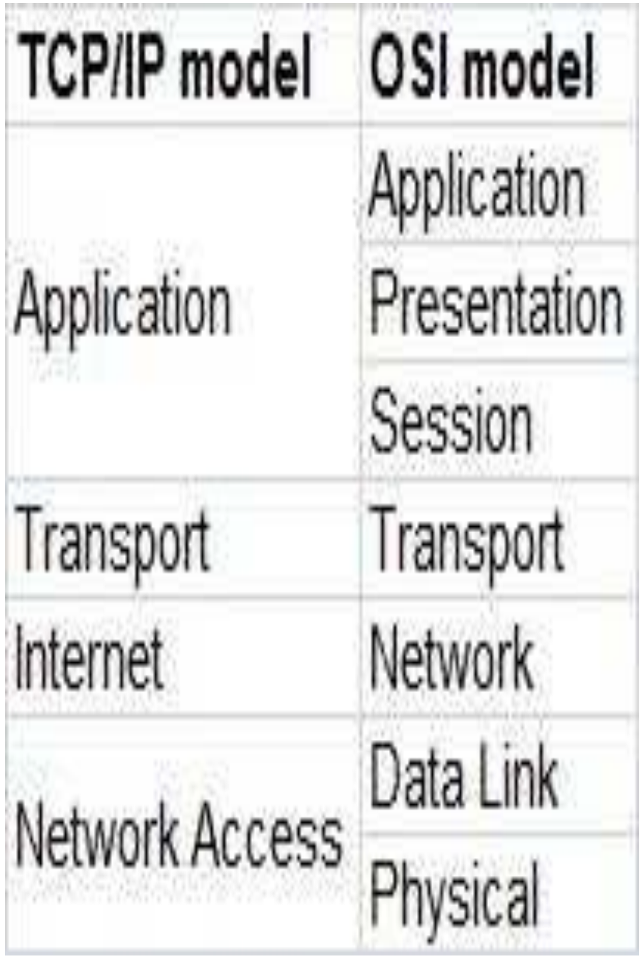


5 - APPLICATION LAYER
PROVIDES APPLICATION ACCESS TO COMMUNICATION ENVIRONMENT

4 - TRANSPORT LAYER
PROVIDES A DELIVERY SERVICE FOR THE APPLICATION LAYER

3 - INTERNET LAYER
ESTABLISHES, MAINTAINS AND TERMINATES END TO END NETWORK COMMUNICATION

NETWORK ACCESS LAYER including 2 - DATALINK and 1 - PHYSICAL
ESTABLISHES DIRECT CONNECTION TO PHYSICAL MEDIA AND HANDLES DATA FLOW CONTROL



TCP/IP model	OSI model
Application	Application
	Presentation
	Session
Transport	Transport
Internet	Network
Network Access	Data Link
	Physical

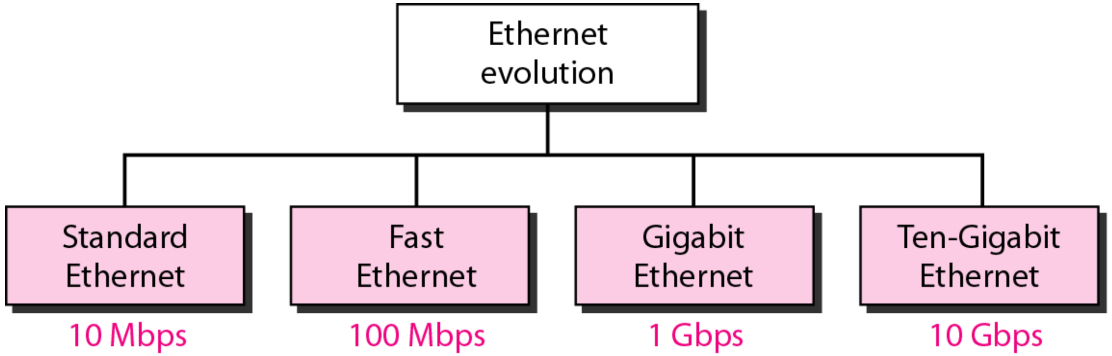
http://programmerhelp404.blogspot.in/2014/01/iso-osi-layer-model-tcpip-model.html

Wired LANs

- Ethernet is the most widely installed LAN technology
- It is link layer protocol in the TCP/IP Stack.
- It describes how networked devices can format data for transmission to other network devices on the same network segment and how to put that data out on the network.
- A **wired** home network uses **Ethernet** cable to connect the computers to the network router.
- It defines two units of transmission
  - Packet
  - Frame

It is a LAN protocol that is used in Bus and Star topologies and implements CSMA/CD as the medium access method

History of Ethernet



- Developed by Bob Metcalfe and others at Xerox PARC in mid-1970s
- Roots in Aloha packet-radio network
- Standardized by Xerox, DEC, and Intel in 1978
- LAN standards define MAC and physical layer connectivity
  - IEEE 802.3 (CSMA/CD - Ethernet) standard – originally 2Mbps
  - IEEE 802.3u standard for 100Mbps Ethernet
  - IEEE 802.3z standard for 1,000Mbps Ethernet

LAN Technology

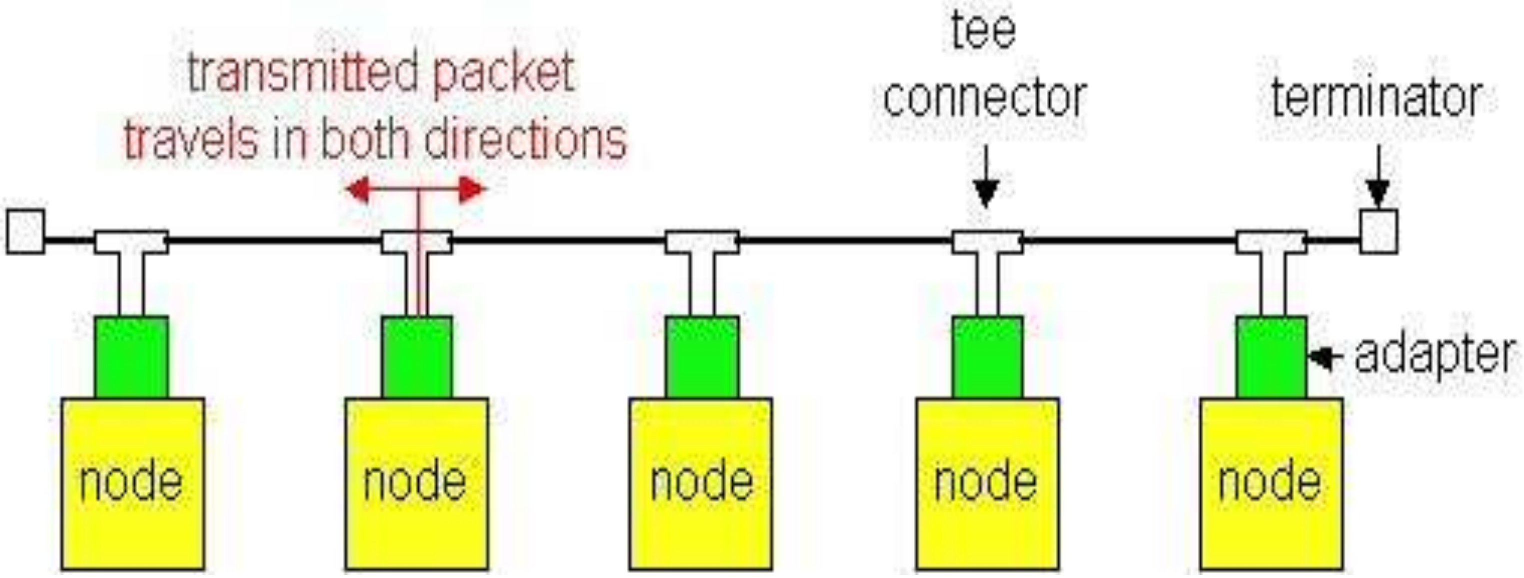
- Ethernet is the most popular physical layer LAN technology in use today.
- A standard Ethernet network can transmit data at a rate up to 10 Megabits per second (10 Mbps).
- Other LAN types include Token Ring, Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet, Fiber Distributed Data Interface (FDDI) etc.
- Ethernet is popular because it strikes a good balance between speed, cost and ease of installation.
- The Institute for Electrical and Electronic Engineers developed an Ethernet standard known as IEEE Standard 802.3.
- This standard defines rules for configuring an Ethernet network and also specifies how the elements in an Ethernet network interact with one another.

Fast Ethernet

- The Fast Ethernet standard (IEEE 802.3u) has been established for Ethernet networks that **need higher transmission speeds.**
- This standard raises the Ethernet speed limit from 10 Mbps to 100 Mbps with only minimal changes to the existing cable structure.
- Fast Ethernet provides faster throughput for video, multimedia, graphics, Internet surfing and stronger error detection and correction.

Ethernet Technologies: 10Base2

- 10: 10Mbps; 2: under 185 (~200) meters cable length
- Thin coaxial cable in a bus topology



- Repeaters used to connect multiple segments
  - Repeater repeats bits it hears on one interface to its other interfaces: physical layer device only!

- Repeaters used to connect multiple segments
  - Repeater repeats bits it hears on one interface to its other interfaces: physical layer device only!

Ethernet Code

In order to understand standard Ethernet code, one must understand what each digit means. Following is a guide:

Guide to Ethernet Coding

For example: 100BASE-TX indicates a Fast Ethernet connection (100 Mbps) that uses a twisted pair cable capable of full-duplex transmissions.

10	at the beginning means the network operates at 10Mbps.
BASE	means the type of signaling used is baseband.
2 or 5	at the end indicates the maximum cable length in meters.
T	the end stands for twisted-pair cable.
X	at the end stands for full duplex-capable cable.
FL	at the end stands for fiber optic cable.

There are four major types of media in use today: Thickwire for 10BASE5 networks; thin coax for 10BASE2 networks; unshielded twisted pair (UTP) for 10BASE-T networks; and fiber optic for 10BASE-FL or Fiber-Optic Inter-Repeater Link (FOIRL) networks.

Ethernet Overview

- Most popular packet-switched LAN technology
- Bandwidths: 10Mbps, 100Mbps, 1Gbps
- Max bus length: 2500m
  - 500m segments with 4 repeaters
- Bus and Star topologies are used to connect hosts
  - Hosts attach to network via Ethernet transceiver or hub or switch
    - Detects line state and sends/receives signals
  - Hubs are used to facilitate shared connections
  - All hosts on an Ethernet are competing for access to the medium
    - Switches break this model
- Problem: Distributed algorithm that provides fair access

Collision Problem

- Ethernet is a shared medium, so there are rules for sending packets of data to avoid conflicts and to protect data integrity.
- Nodes determine when the network is available for sending packets.
- It is possible that two or more nodes at different locations will attempt to send data at the same time.
- When this happens, a packet collision occurs.

CSMA/CD

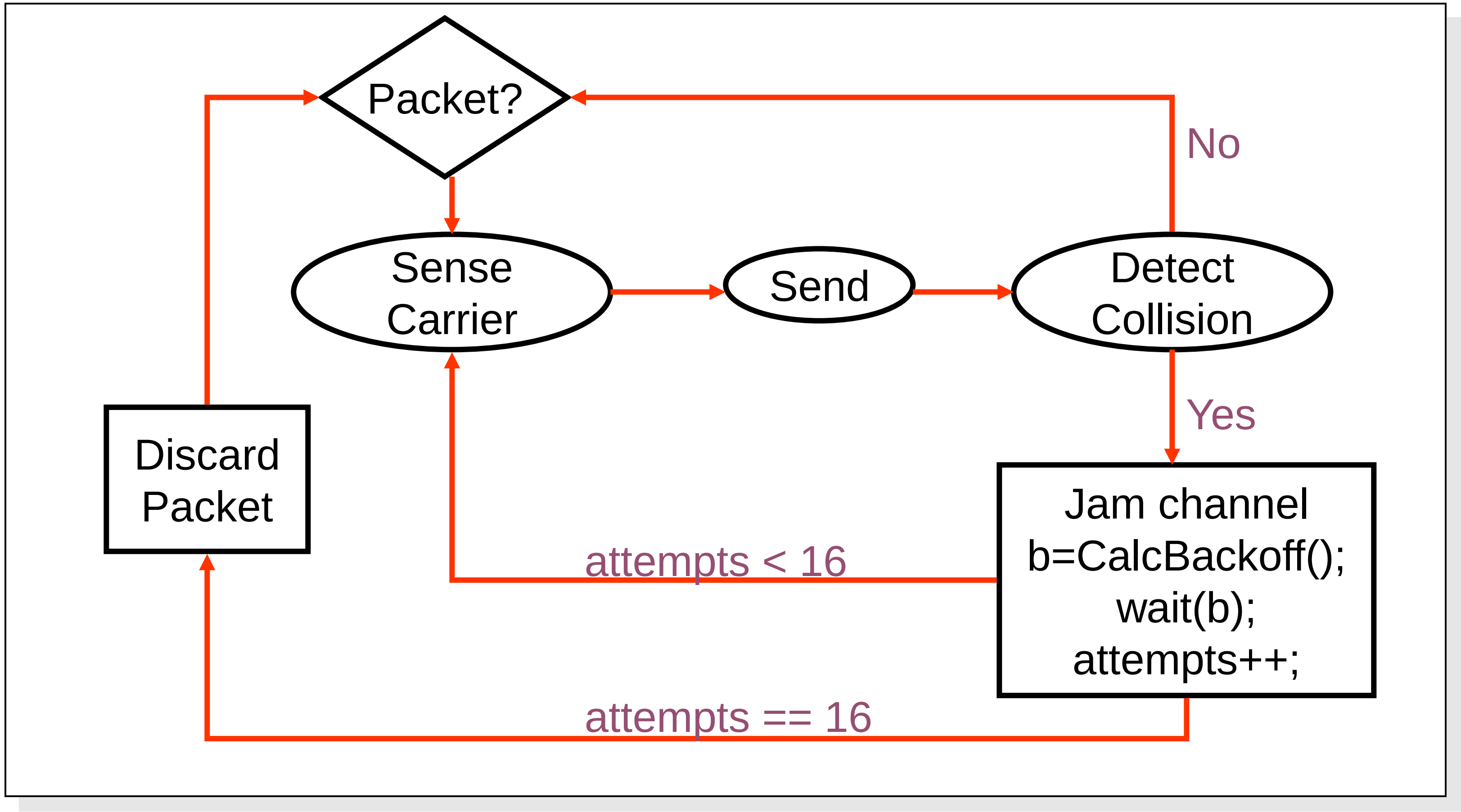
- The CSMA/CD protocol used for Ethernet and a variety of other applications falls into three categories.
- The first is Carrier Sense. Here each station listens on the network for traffic and it can detect when the network is quiet.
- The second is the Multiple Access aspect where the stations are able to determine for themselves whether they should transmit. The final element is the Collision Detect element.
- Even though stations may find the network free, it is still possible that two stations will start to transmit at virtually the same time.
- If this happens then the two sets of data being transmitted will collide.
- If this occurs then the stations can detect this and they will stop transmitting. They then back off a random amount of time before attempting a retransmission.
- The random delay is important as it prevents the two stations starting to transmit together a second time.

Protocol used in Ethernet
State Diagram for CSMA/CD

In order to manage collision Ethernet uses

CSMA/CD: Ethernet’s Media Access Control (MAC) policy

- CS = carrier sense
  - Send only if medium is idle
- MA = multiple access
- CD = collision detection
  - Stop sending immediately if collision is detected

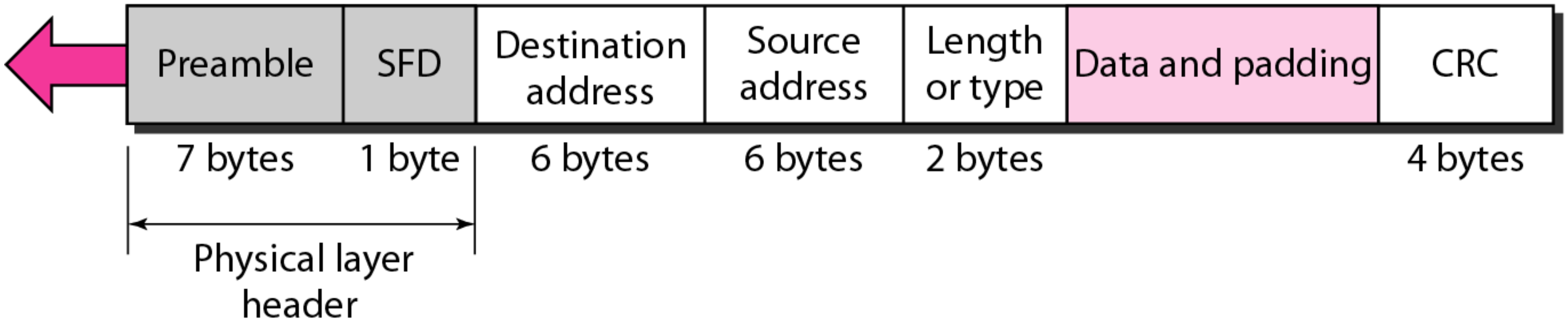


Ethernet Frame Format

- ***Header***
  - *Preamble (PRE)* - This is seven bytes long and it consists of a pattern of alternating ones and zeros. It indicates the receiver that frame is coming and allow the receiver to lock onto the data stream before the actual frame begins.. (10 Mbps Ethernet)
  - *Start Of Frame delimiter (SOF)* - This consists of one byte and contains an alternating pattern of ones and zeros but ending in two ones.

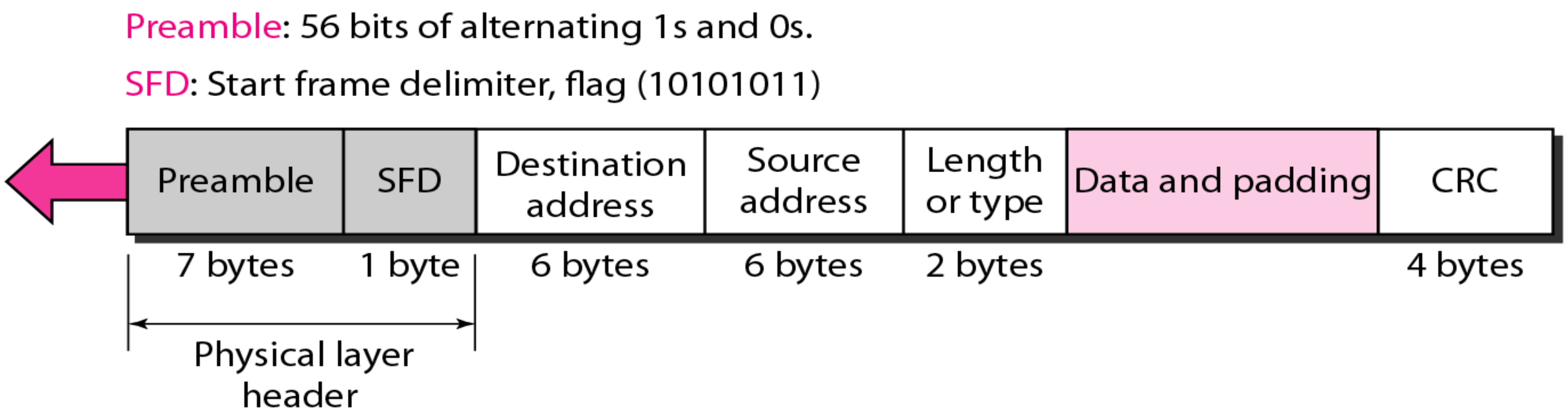
Preamble: 56 bits of alternating 1s and 0s.

SFD: Start frame delimiter, flag (10101011)



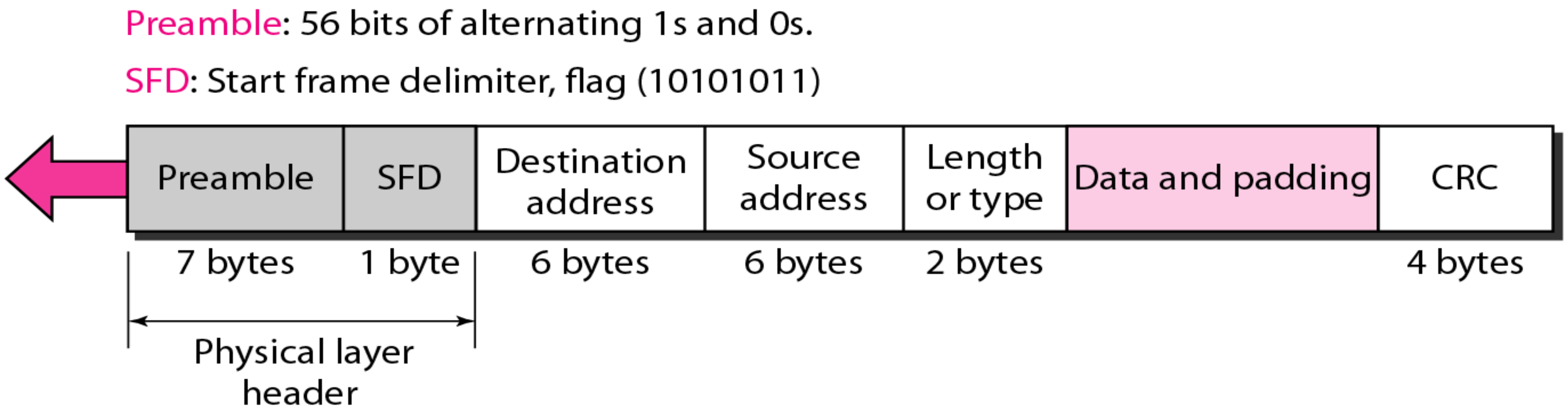
Ethernet Frame Format

- *Destination Address (DA)* - This is 6-Byte field which contains the MAC address of machine for which data is destined.
- *Source Address (SA)* - This is a 6-Byte field which contains the MAC address of source machine.



Ethernet Frame Format

- ***Length / Type*** **-** This field is two bytes in length. It provides MAC information and indicates the number of client data types that are contained in the data field of the frame.

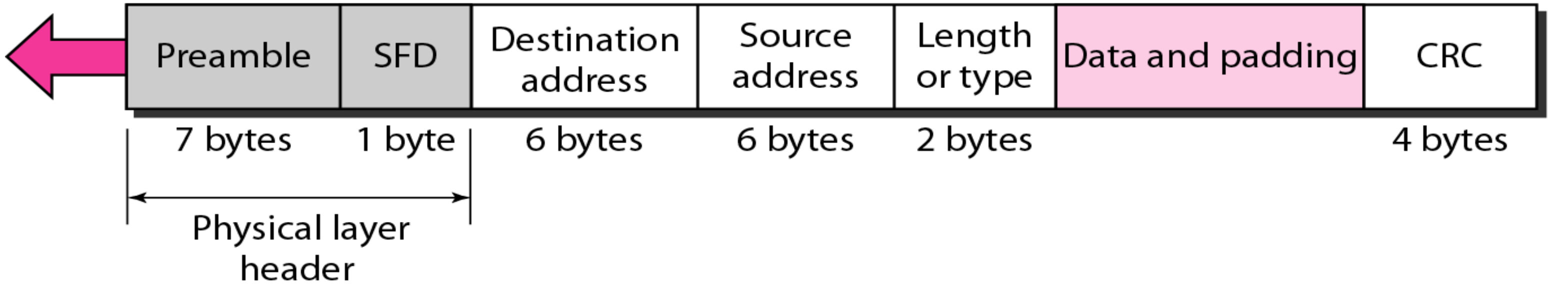


Ethernet Frame Format

- ***Payload***
  - *Data* - This block contains the payload data and it may be up to 1500 bytes long. If the length of the field is less than 46 bytes, then padding data is added to bring its length up to the required minimum of 46 bytes.
- ***Trailer***
  - *Frame Check Sequence (FCS)* - This field is four bytes long. It contains a 32 bit Cyclic Redundancy Check (CRC) which is generated over the DA, SA, Length / Type and Data fields.

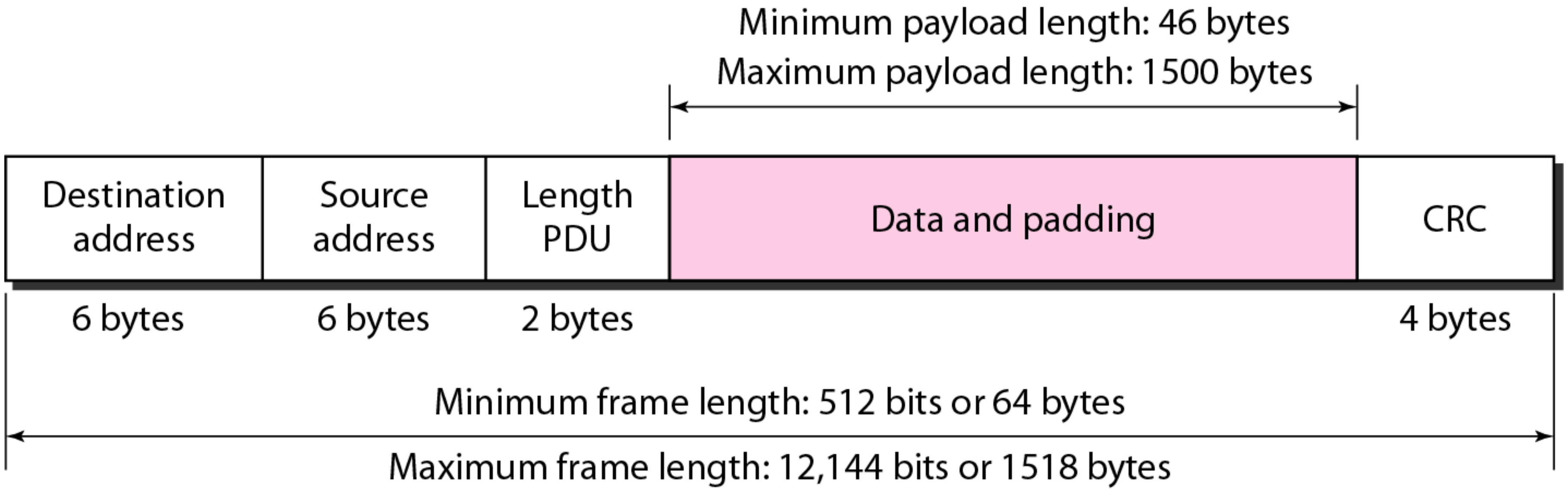
Preamble: 56 bits of alternating 1s and 0s.

SFD: Start frame delimiter, flag (10101011)

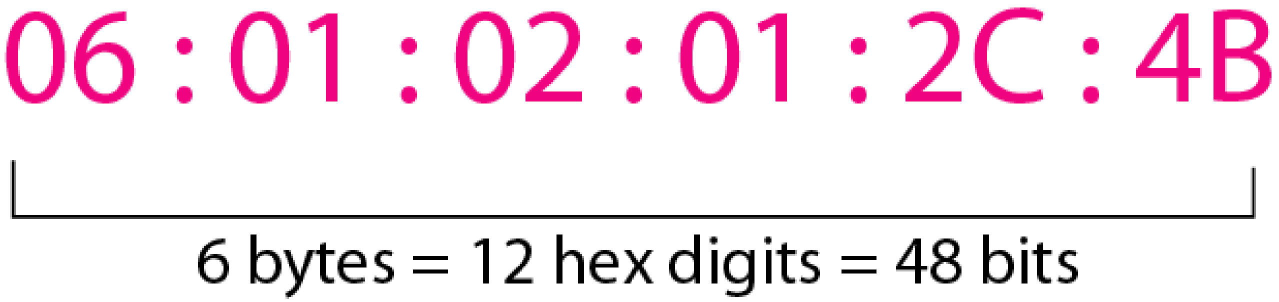


Minimum and maximum lengths

- Size of frame of Ethernet IEEE 802.3 varies 64 bytes to 1518 bytes including data length (46 to 1500 bytes).


Minimum payload length: 46 bytes
Maximum payload length: 1500 bytes
Destination address
Source address
Length PDU
Data and padding
CRC
6 bytes
6 bytes
2 bytes
4 bytes
Minimum frame length: 512 bits or 64 bytes
Maximum frame length: 12,144 bits or 1518 bytes

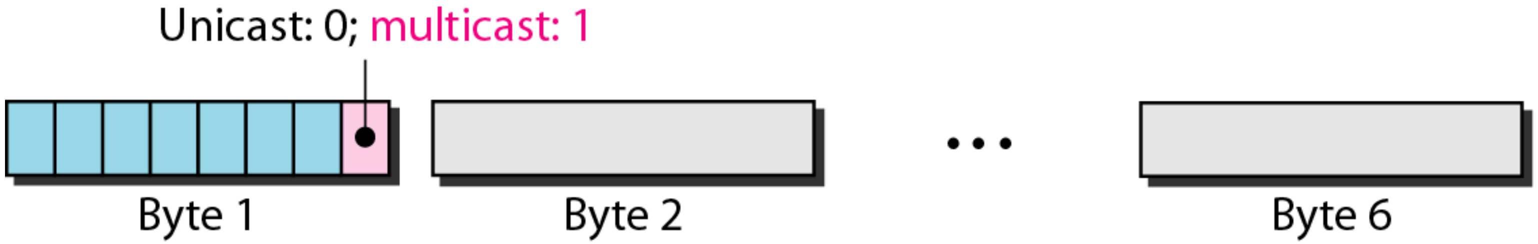
Example of an Ethernet address in hexadecimal notation



06 : 01 : 02 : 01 : 2C : 4B

6 bytes = 12 hex digits = 48 bits

Figure 13.7 Unicast and multicast addresses



Note

The least significant bit of the first byte defines the type of address.
If the bit is 0, the address is unicast;
otherwise, it is multicast.

Example 13.1

Define the type of the following destination addresses:

a. 4A:30:10:21:10:1A   b. 47:20:1B:2E:08:EE

c. FF:FF:FF:FF:FF:FF

Solution

To find the type of the address, we need to look at the second hexadecimal digit from the left. If it is even, the address is unicast. If it is odd, the address is multicast. If all digits are F's, the address is broadcast. Therefore, we have the following:

a. This is a unicast address because A in binary is 1010.

b. This is a multicast address because 7 in binary is 0111.

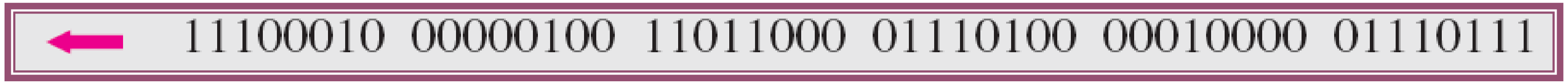
c. This is a broadcast address because all digits are F's.

Example 13.2

Show how the address 47:20:1B:2E:08:EE is sent out on line.

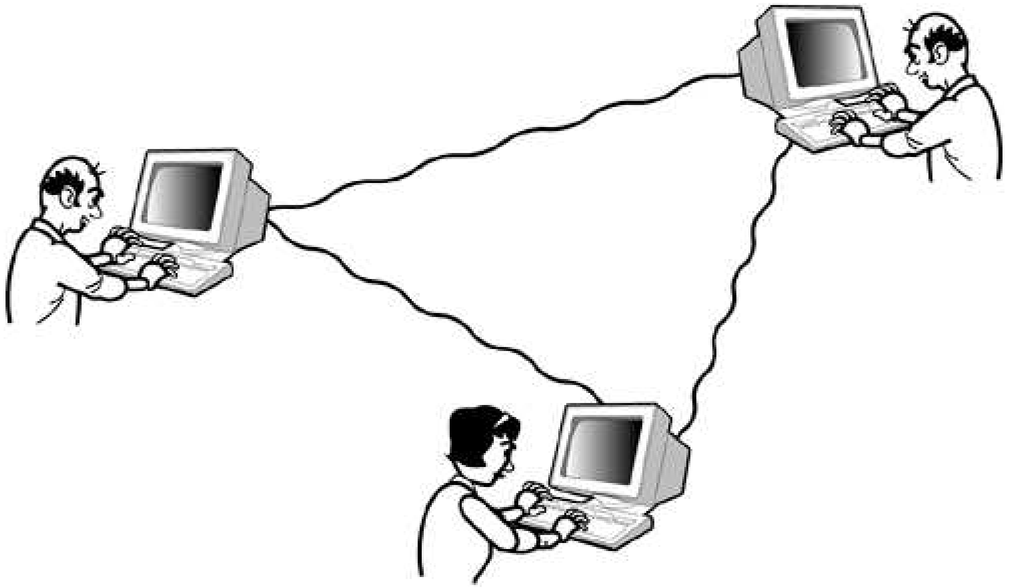
Solution

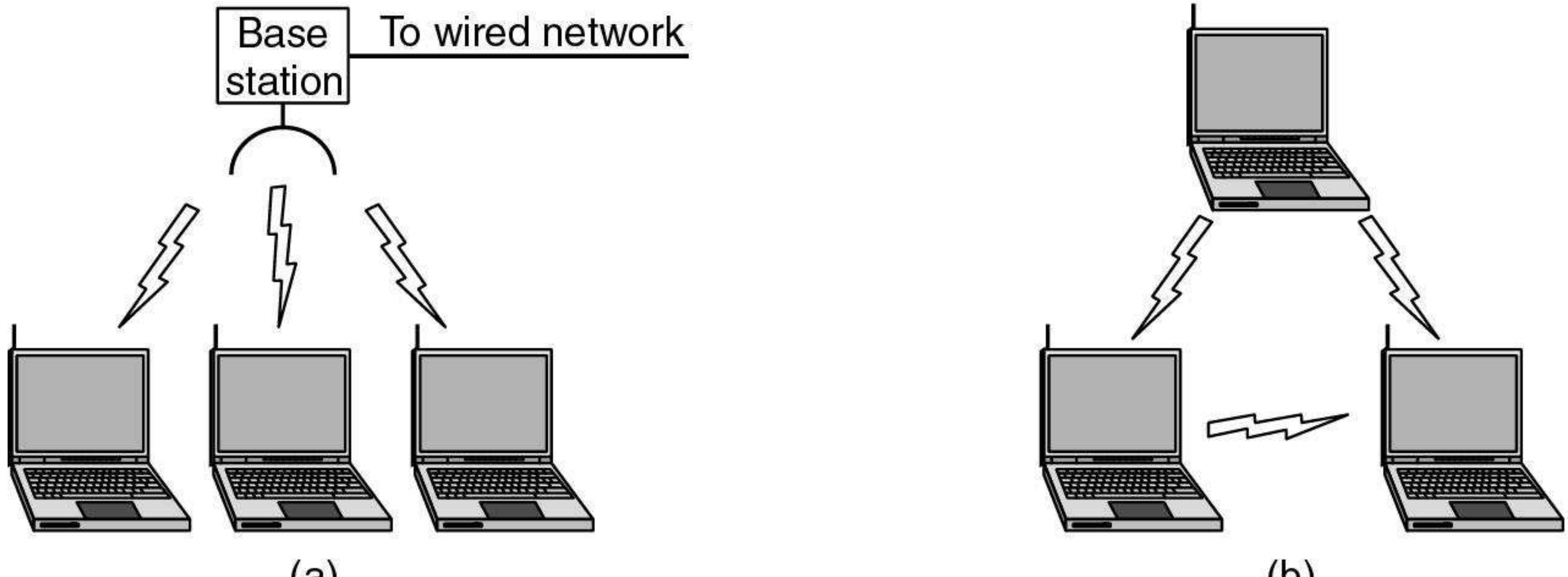
The address is sent left-to-right, byte by byte; for each byte, it is sent right-to-left, bit by bit, as shown below:



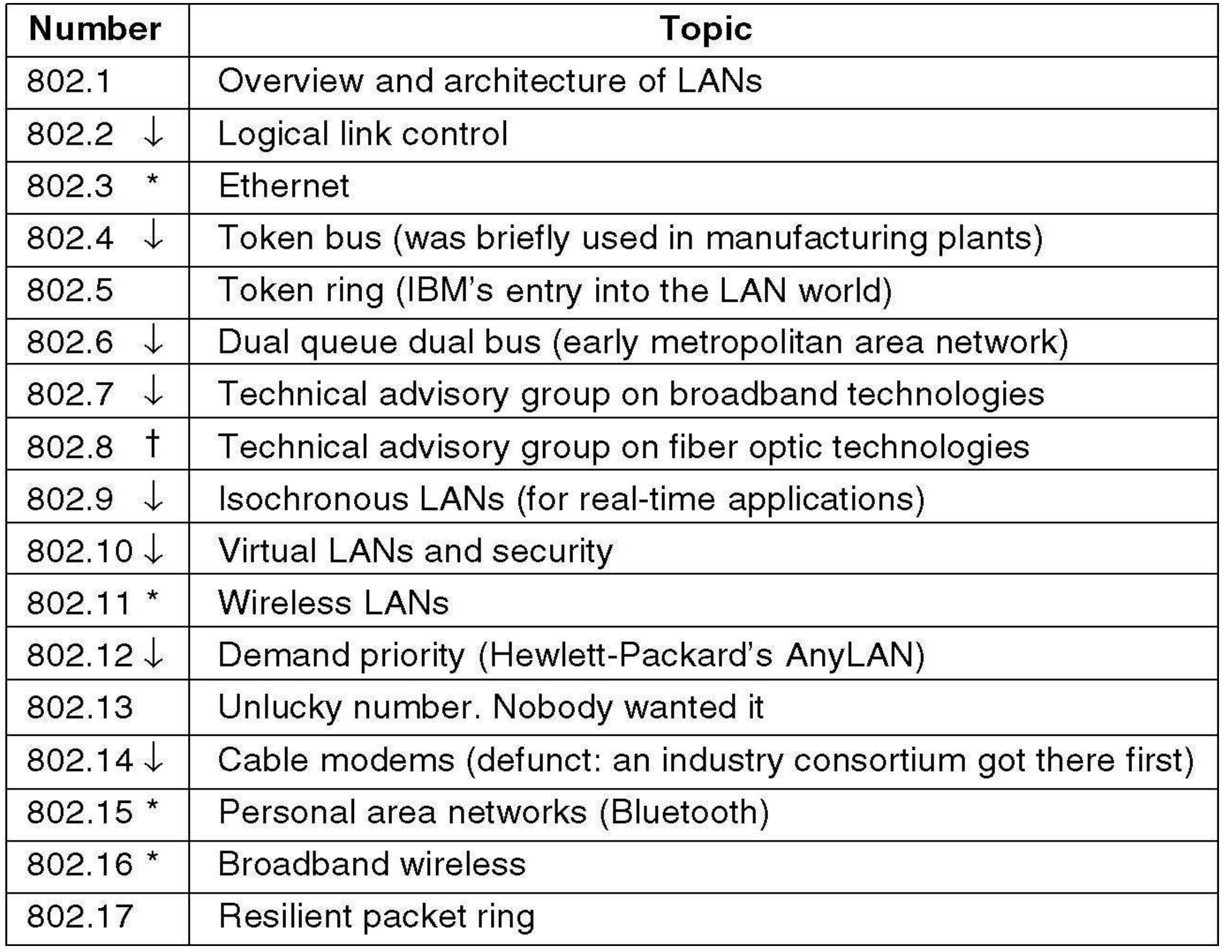
← 11100010 00000100 11011000 01110100 00010000 01110111

Wireless LANs





IEEE 802 Standards Working Groups



Number	Topic
802.1	Overview and architecture of LANs
802.2 ↓	Logical link control
802.3 *	Ethernet
802.4 ↓	Token bus (was briefly used in manufacturing plants)
802.5	Token ring (IBM's entry into the LAN world)
802.6 ↓	Dual queue dual bus (early metropolitan area network)
802.7 ↓	Technical advisory group on broadband technologies
802.8 †	Technical advisory group on fiber optic technologies
802.9 ↓	Isochronous LANs (for real-time applications)
802.10 ↓	Virtual LANs and security
802.11 *	Wireless LANs
802.12 ↓	Demand priority (Hewlett-Packard's AnyLAN)
802.13	Unlucky number. Nobody wanted it
802.14 ↓	Cable modems (defunct: an industry consortium got there first)
802.15 *	Personal area networks (Bluetooth)
802.16 *	Broadband wireless
802.17	Resilient packet ring

Wireless LANs

- Popular WLAN technologies all follow one of the three main Wi-Fi communication standards.
- The benefits of wireless networking depend on the standard employed:
- 802.11b was the first standard to be widely used in WLANs.
- The 802.11a standard is faster but more expensive than 802.11b; 802.11a is more commonly found in business networks.
- The newest standard, 802.11g, attempts to combine the best of both 802.11a and 802.11b, though it too is more a more expensive home networking option.

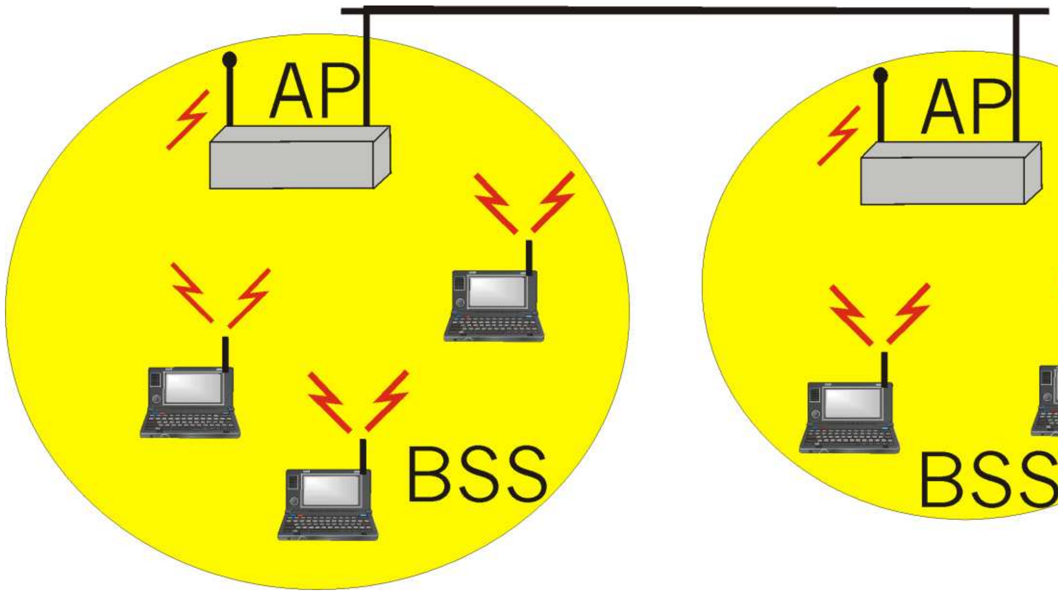
Wireless LANs

- Wireless LANs suffer a few more reliability problems than wired LANs.
- High Cost than wired LANs.
- WLANs support 54 Mbps, that is approximately one-half the bandwidth of Fast Ethernet.
- Wireless LANs are less secure than wired LANs, because wireless communication signals travel through the air and can easily be intercepted.

Wired Vs Wireless LANs

	Wired	**Wireless**
Installation	moderate difficulty	easier, but beware interference
Cost	less	more
Reliability	high	reasonably high
Performance	very good	good
Security	reasonably good	reasonably good
Mobility	limited	outstanding

Wireless LAN Architecture



- Src: https://www.youtube.com/watch?v=5hJx5WabV_g

Access-Point (AP)

Device that provide access to a distribution system for associated stations.

- Most often infra-structure products that connect to wired backbones
- Stations select an Access-Point and “associate with it

Access-Points :

- Support roaming
- Provide time synchronization functions (beaconing)
- Provide Power Management support

Traffic typically flows through Access-Point

- direct Station-to-Station communication takes place

Basic Service Set (BSS)

- A set of stations controlled by a single **“Coordination Function”** (=the logical function that determines when a station can transmit or receive)
- A BSS can have an **Access-Point (both in standalone networks and in building-wide configurations)**, or can run **without and Access-Point (in standalone networks only)**

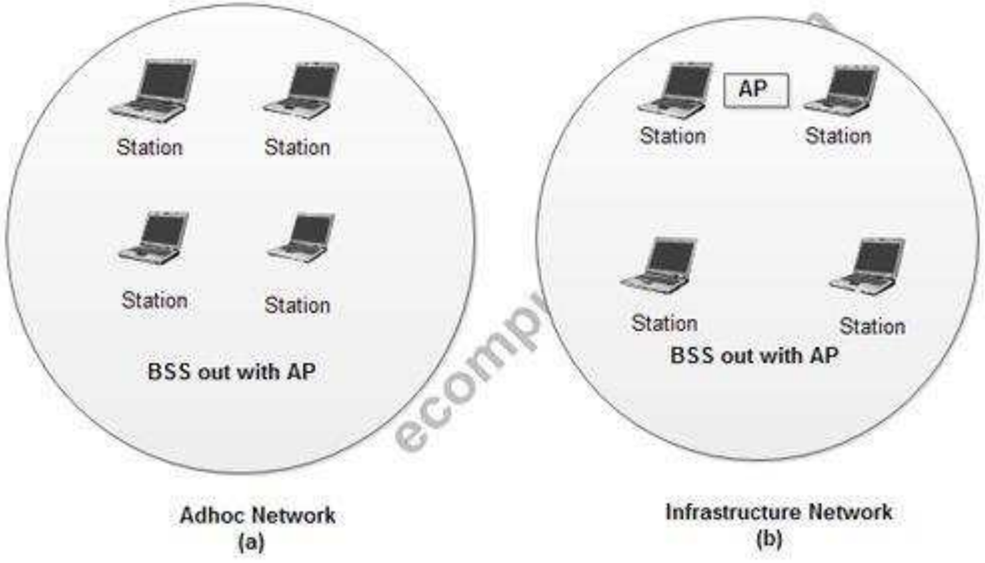
Basic Service Set

- The basic services set contain stationary or mobile wireless stations and a central base station called access point (AP).
- The use of access point is optional.
- If the access point is not present, it is known as stand-alone network.

  Such a BSS cannot send data to other BSSs.

This type of architecture is known as ad hoc architecture.

- The BSS in which an access point is present is known as an infrastructure network.



Basic Service Sets

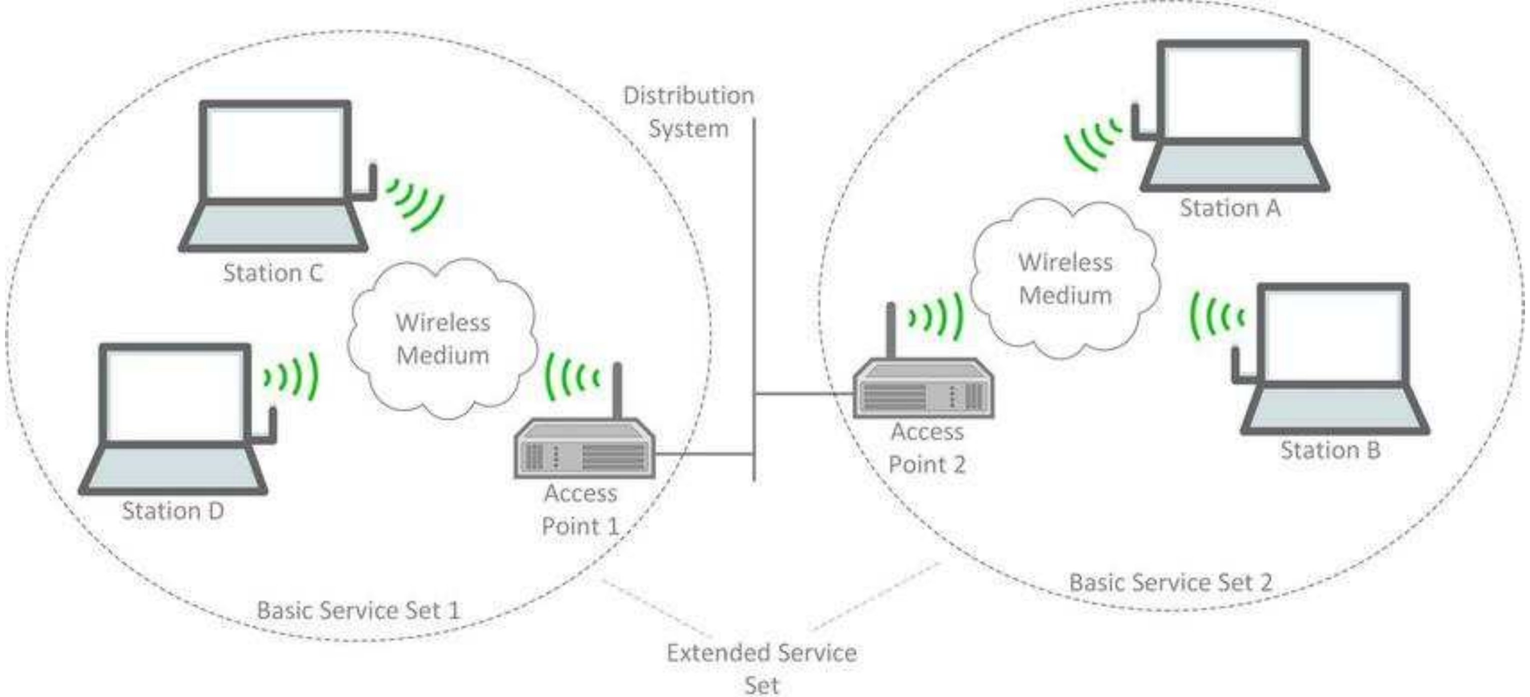
Independent Basic Service Set (IBSS)

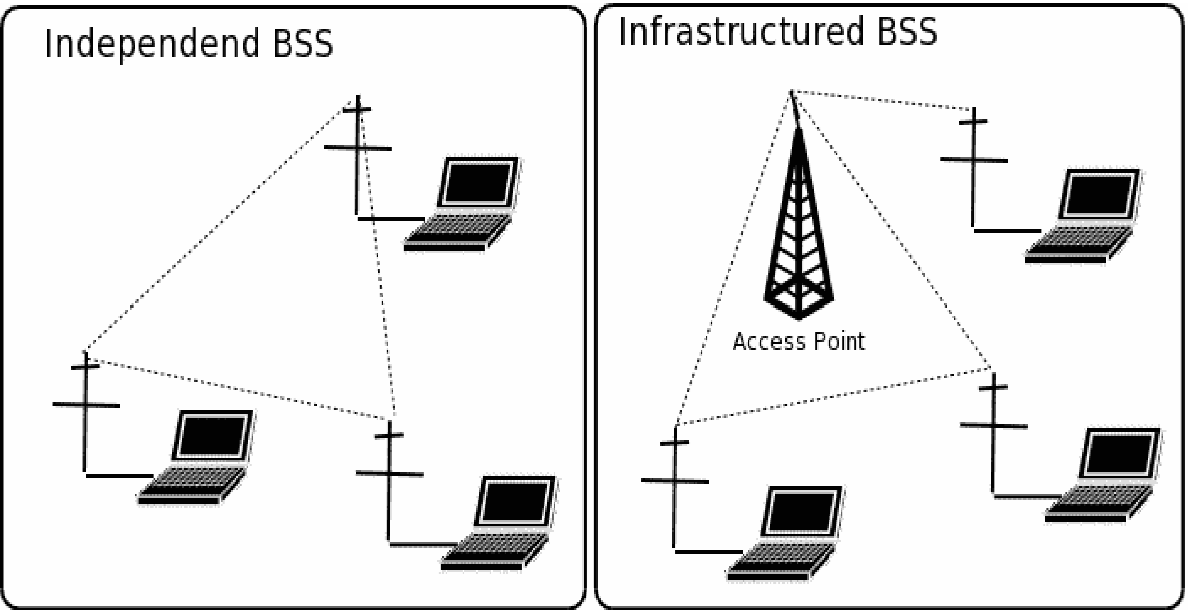
- A Basic Service Set (BSS) which forms a self-contained network in which no access to a Distribution System is available

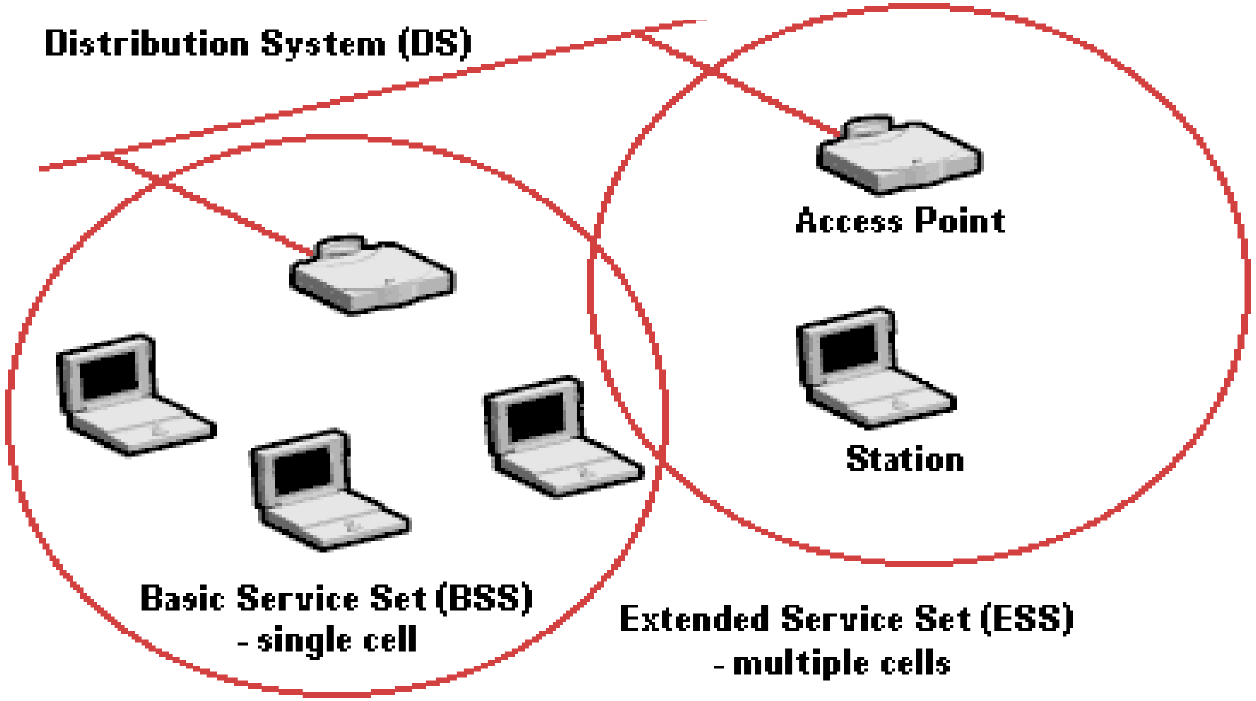
- A BSS without an Access-Point

- One of the stations in the IBSS can be configured to “initiate” the network and assume the Coordination Function

- Diameter of the cell determined by coverage distance between two wireless stations


Distribution System
Station C
Wireless Medium
Station D
Access Point 1
Basic Service Set 1
Station A
Wireless Medium
Access Point 2
Station B
Basic Service Set 2
Extended Service Set

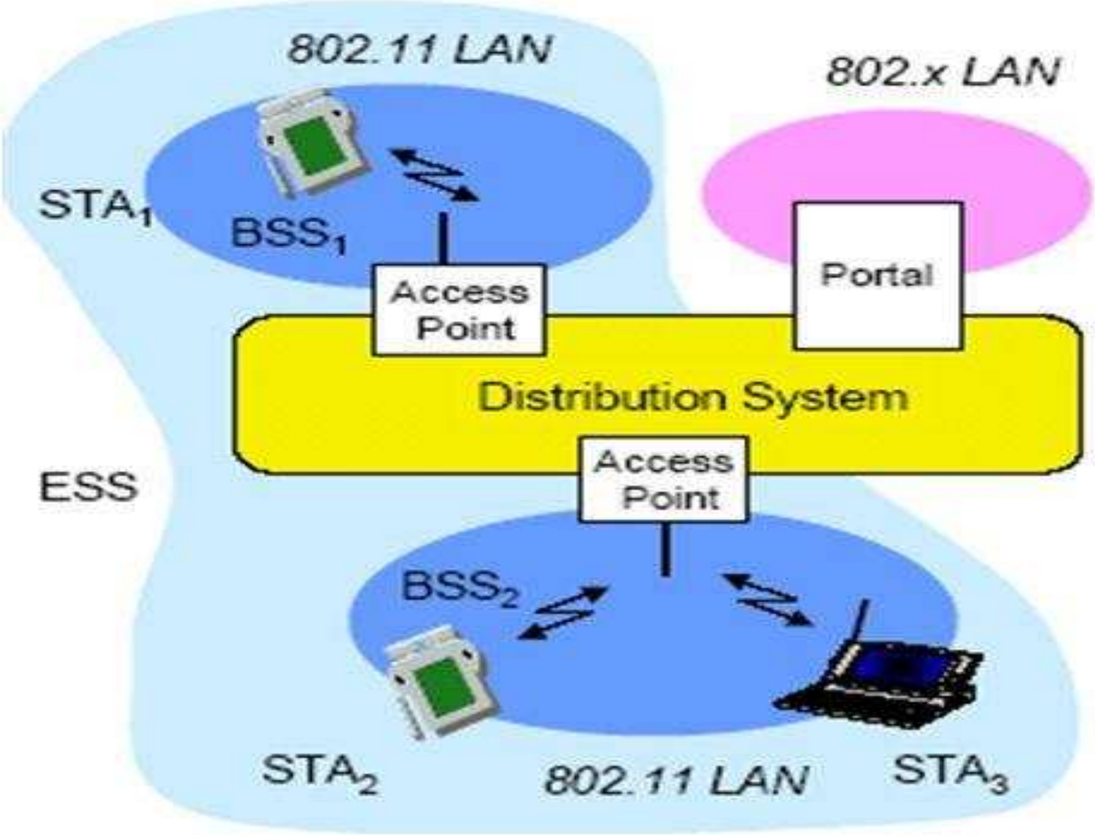

Independend BSS
Infrastructured BSS
Access Point


Distribution System (DS)
Access Point
Station
Basic Service Set (BSS)
- single cell
Extended Service Set (ESS)
- multiple cells

Wireless LAN -Architecture

- ✓ IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data link layers.

Basic Service Set (BSS)
Access Point (AP)
Distribution System (DS)
Extended Service Set (ESS)
Portal



Extended Service Set

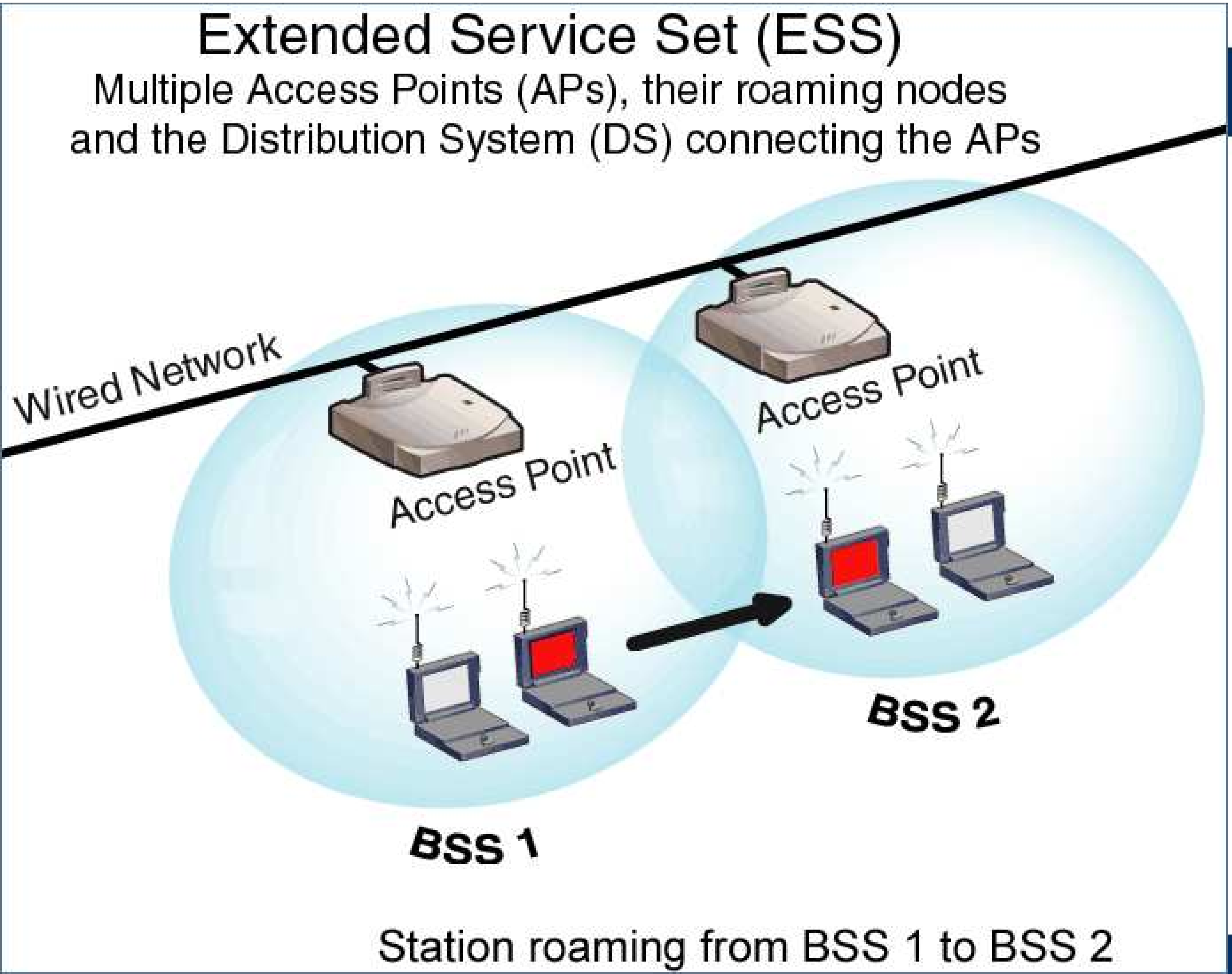
- An extended service set is created by joining two or more basic service sets (BSS) having access points (APs).
- These extended networks are created by joining the access points of basic services sets through a wired LAN known as distribution system.
- There are two types of stations in ESS:

(i) **Mobile stations**: These are normal stations inside a BSS.

(ii) **Stationary stations**: These are AP stations that are part of a wired LAN.

- Communication between two stations in two different BSS usually occurs via two APs.
- A mobile station can belong to more than one BSS at the same time.

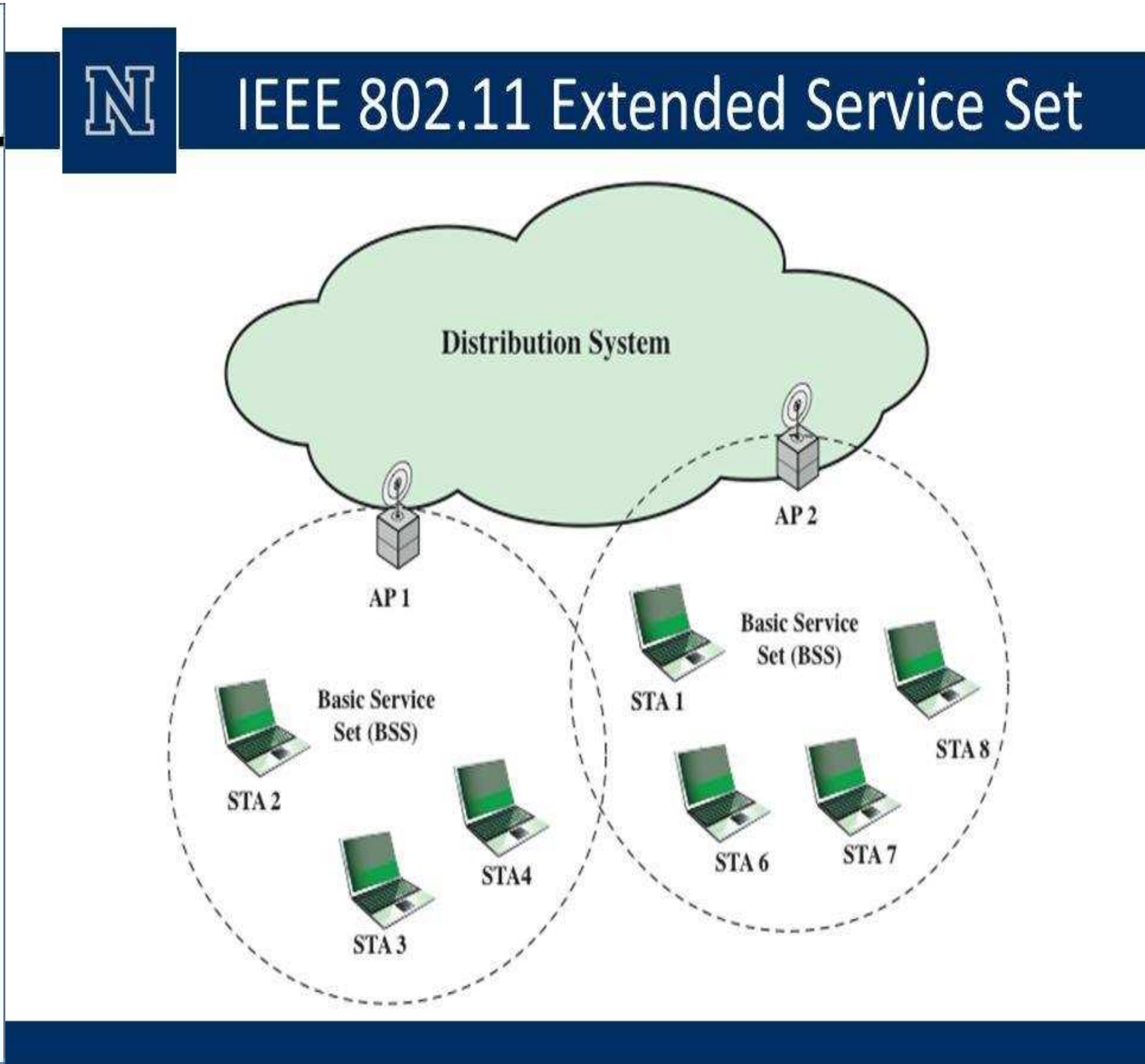
Extended Service Set



Extended Service Set (ESS)

Multiple Access Points (APs), their roaming nodes and the Distribution System (DS) connecting the APs

Station roaming from BSS 1 to BSS 2



IEEE 802.11 Extended Service Set

802.11 Station Types

- IEEE 802.11 defines three types of stations on the basis of their mobility in wireless LAN. These are:

1. No-transition Mobility

2. BSS-transition Mobility

3. ESS-transition Mobility

1.**No-transition Mobility**: These types of stations are either stationary *i.e.* immovable or move only inside a BSS.

2. **BSS-transition mobility**: These types of stations can move from one BSS to another but the movement is limited inside an ESS.

3. **ESS-transition mobility**: These types of stations can move from one ESS to another. The communication mayor may not be continuous when a station moves from one ESS to another ESS.

Distribution System (DS)

- A system to interconnect a set of Basic Service Sets

– Integrated; A single Access-Point in a standalone network

– Wired; Using cable to interconnect the Access-Points

– Wireless; Using wireless to interconnect the Access-Points

Wireless Media

- Physical layers used in wireless networks
  - have neither absolute nor readily observable boundaries outside which stations are unable to receive frames
  - are unprotected from outside signals
  - communicate over a medium significantly less reliable than the cable of a wired network
  - have dynamic topologies
  - lack full connectivity and therefore the assumption normally made that every station can hear every other station in a LAN is invalid (i.e., STAs may be "hidden" from each other)
  - have time varying and asymmetric propagation properties

Limitations of the Wireless environment

- Limitations of the Wireless Network
  - limited communication bandwidth
  - frequent disconnections
  - heterogeneity of fragmented networks

- Limitations Imposed by Mobility
  - route breakages
  - lack of mobility awareness by system/applications

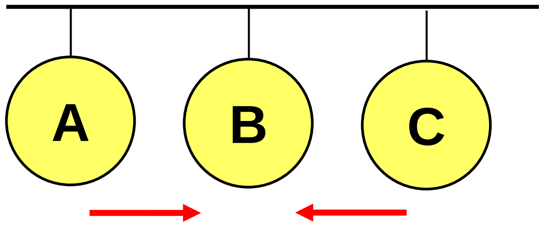
- Limitations of the Mobile Device
  - short battery lifetime
  - limited capacities

Wireless v/s Wired networks

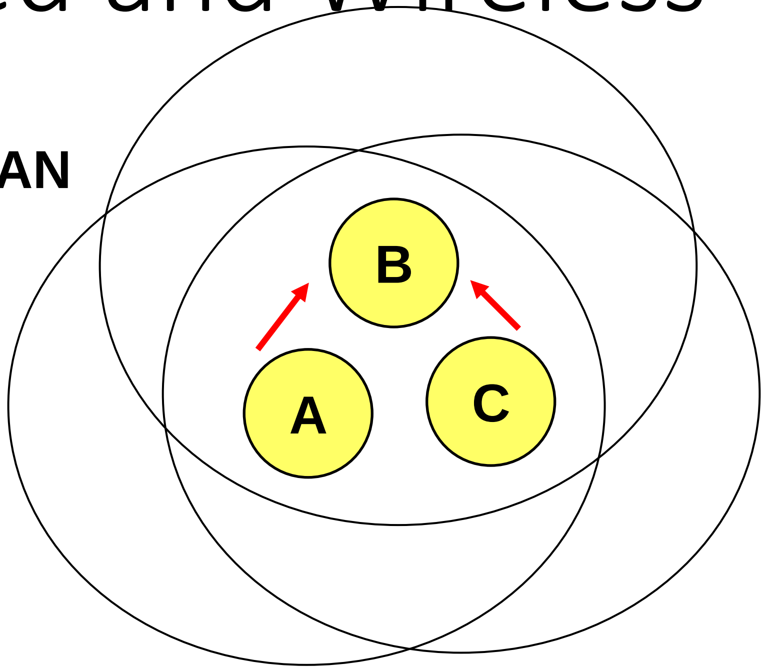
- Regulations of frequencies
  - Limited availability, coordination is required
  - useful frequencies are almost all occupied
- Bandwidth and delays
  - Low transmission rates
    - few Kbps to some Mbps.
  - Higher delays
    - several hundred milliseconds
  - Higher loss rates
    - susceptible to interference, e.g., engines, lightning
- Always shared medium
  - Lower security, simpler active attacking
  - radio interface accessible for everyone
  - Fake base stations can attract calls from mobile phones
  - secure access mechanisms important

Difference Between Wired and Wireless

Ethernet LAN



Wireless LAN



- If both A and C sense the channel to be idle at the same time, they send at the same time.
- Collision can be detected at sender in Ethernet.
- Half-duplex radios in wireless cannot detect collision at sender.

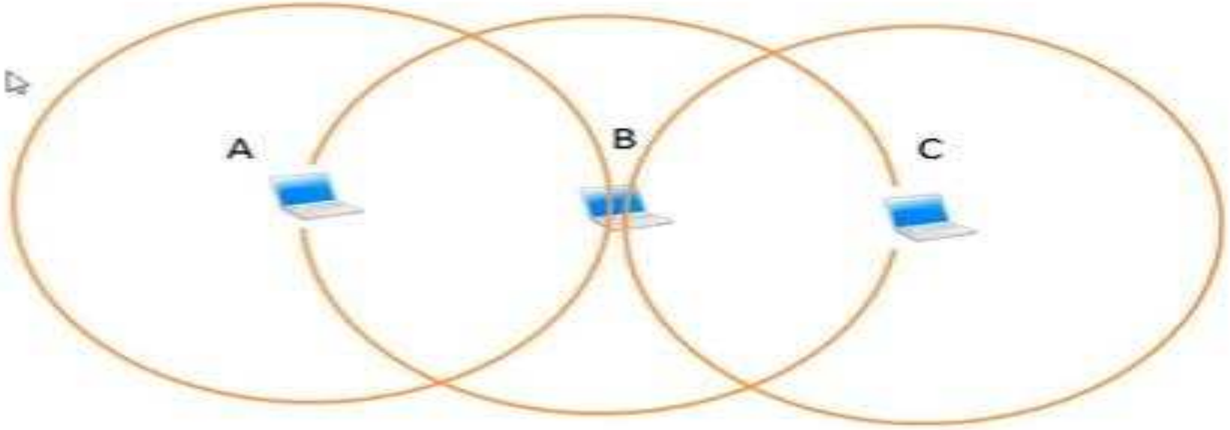
Issues in WLANs

- There are three problems in a wireless LAN, which are not found in wired LANs.
- These problems are as follows:

- Hidden terminal problem
- Exposed terminal problem

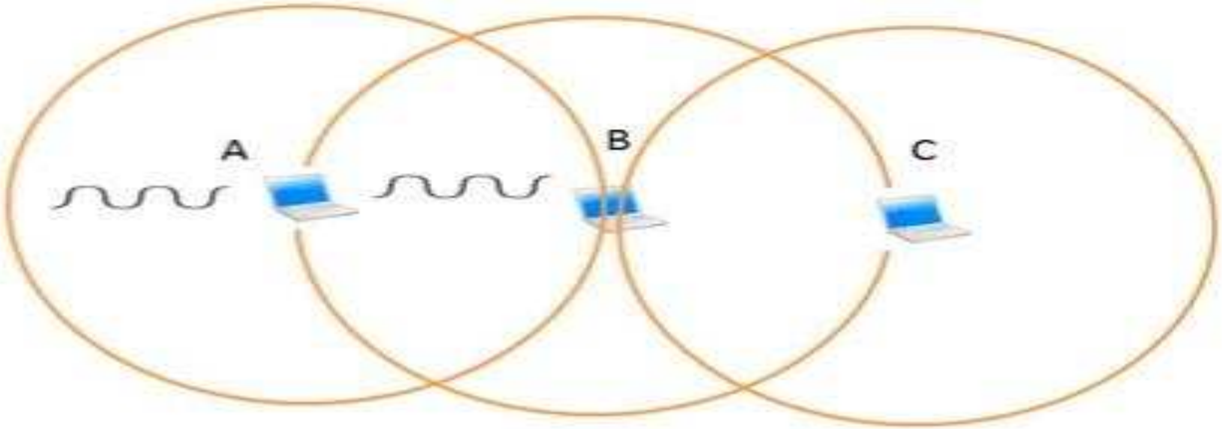
CSMA/CA-Hidden Terminal Problem

A wants to send data to B.
A will Sense channel, it finds channel free and start sending data.



CSMA/CA-Hidden Terminal Problem

A wants to send data to B.
A will Sense channel, it finds channel free and start sending data.

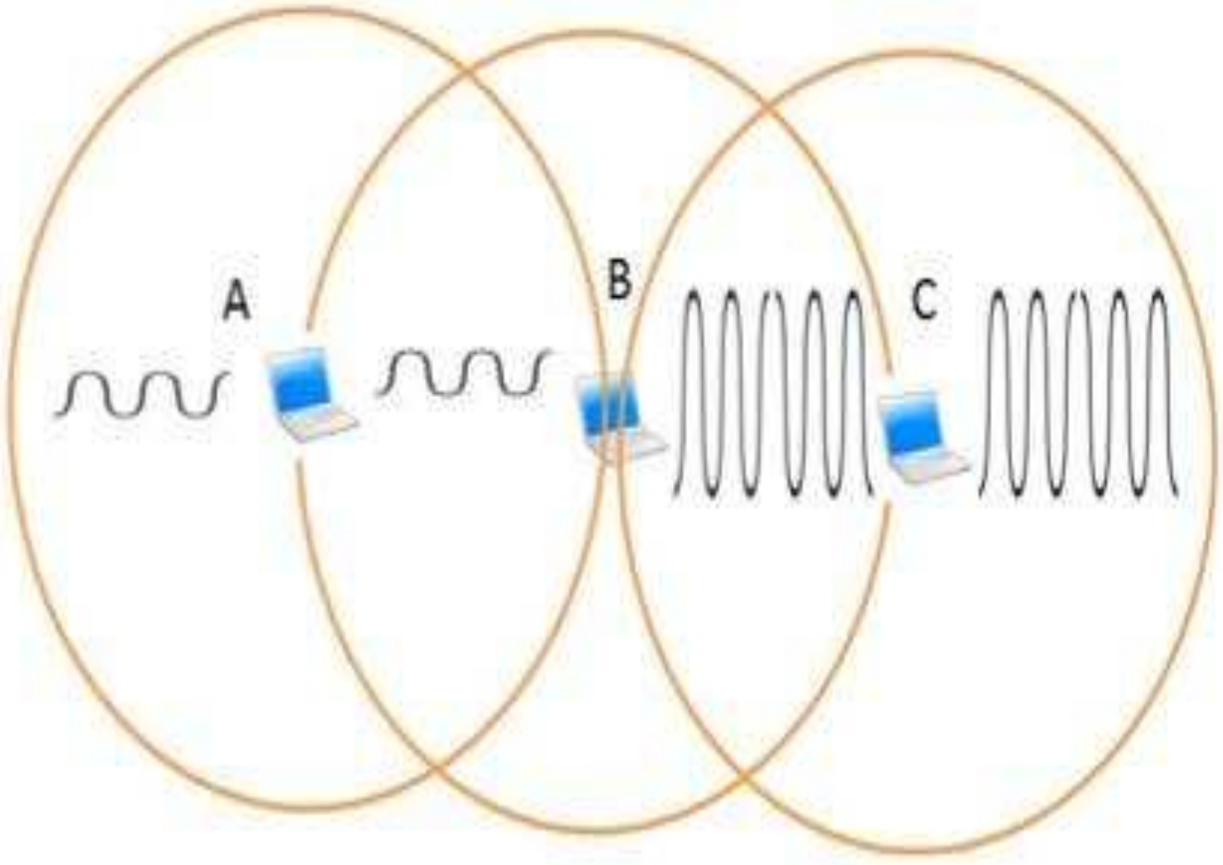


CSMA/CA-Hidden Terminal Problem

A wants to send data to B.
A will Sense channel, it finds channel free and start sending data.

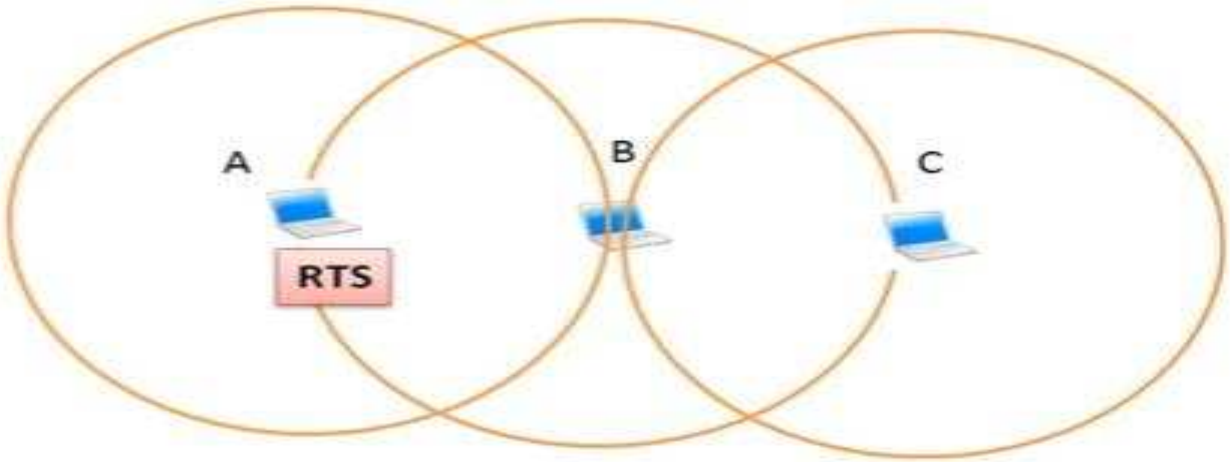
C also wants to send data to B.
C will sense channel and finds channel free and start sending.

Both signal reach Node B and collide.
Collision not detected.



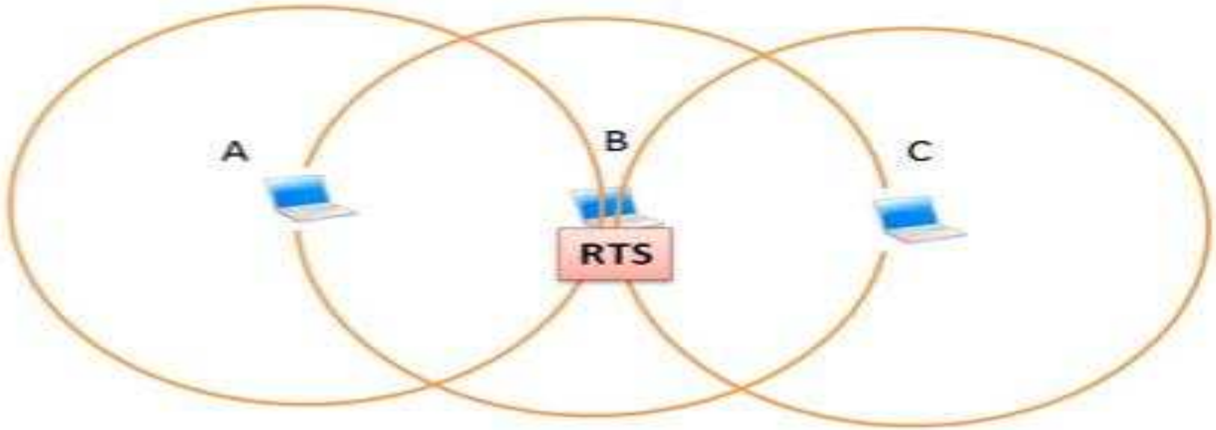
CSMA/CA-Hidden Terminal Problem

A wants to send data to B.
A will send RTS to B.



CSMA/CA-Hidden Terminal Problem

A wants to send data to B.
A will send RTS to B.

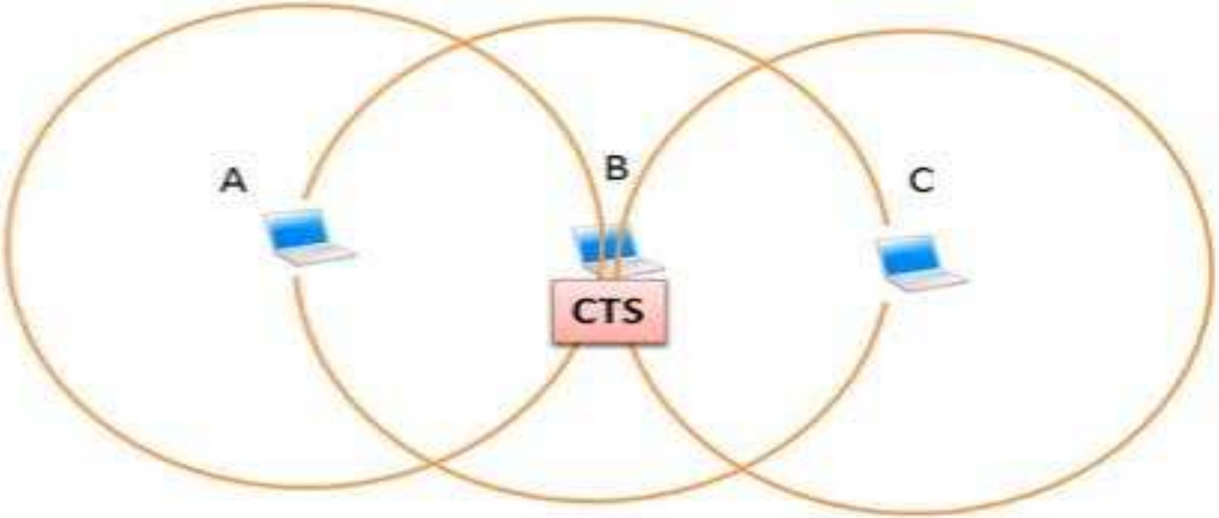


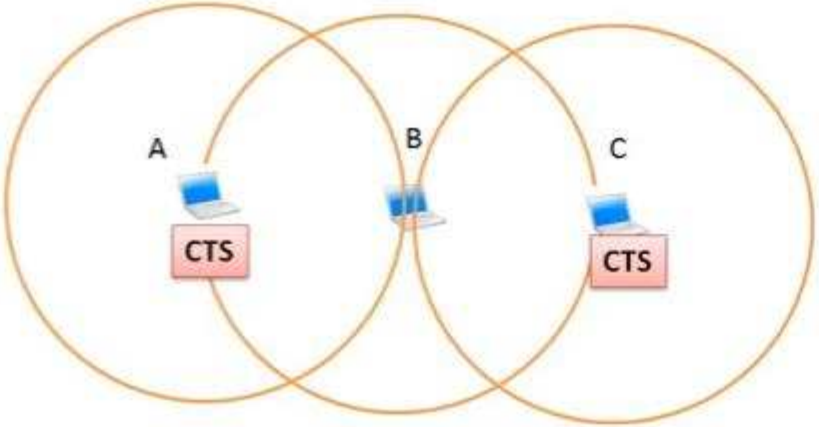
CSMA/CA-Hidden Terminal Problem

A wants to send data to B.
A will send RTS to B.

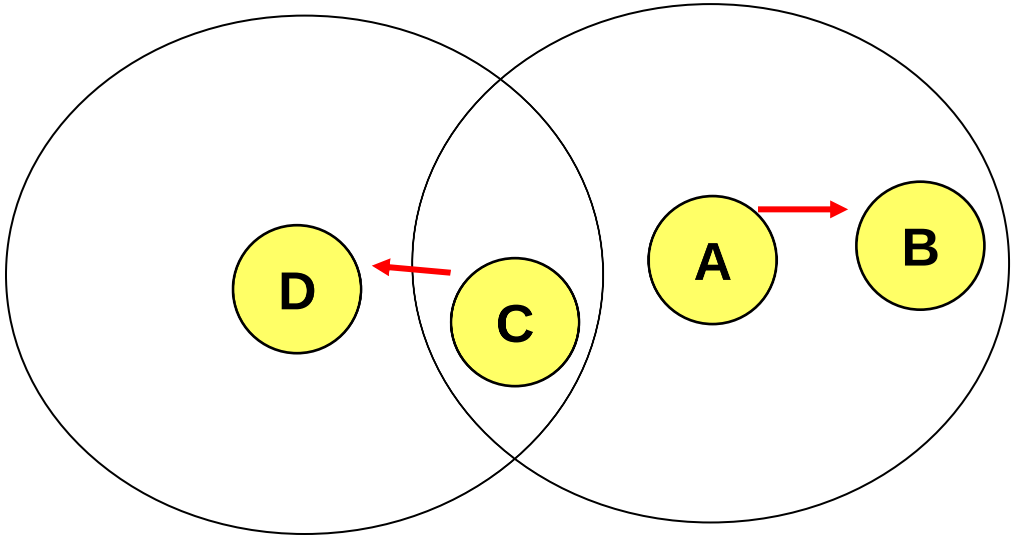
B will received RTS and Reply to A that you can transmit data by sending CTS.
CTS packet also include duration of this communication.

CTS packet reach A and C both.
C check CTS packet and learn that B going to start communication with A for Duration mentioned in packet.





Exposed Terminal Problem



- A starts sending to B.
- C senses carrier, finds medium in use and has to wait for A->B to end.
- D is outside the range of A, therefore waiting is not necessary.
- A and C are “exposed” terminals

Difference

1.CSMA CD takes effect after a collision while CSMA CA takes effect before a collision.
2.CSMA CA reduces the possibility of a collision while CSMA CD only minimizes the recovery time.
3.CSMA CD is typically used in wired networks while CSMA CA is used in wireless networks.

Medium Access Control protocol

- It is a one of sublayers of Data Link layer in OSI model.
- The MAC is a set of rules to determine how to access the medium and data link components. The MAC rides on every transmission of user data into the air. It provides the core framing operations and the interaction with a wired network backbone.
- MAC purpose:
  - Coordinates and shares use of bandwidth
  - Timing synchronization
  - User datagram transfer function
  - MAC layer management functions

MAC mechanism in 802.11

- Distributed Foundation Wireless MAC(DFWMAC)
- 802.11 uses DCF(Distributed Coordination Function) based on CSMA/CA mechanism (Carrier Sense Multiple Access with Collision Avoidance)
- It is considered to be ‘fair’ for all users because treats them equally.
- Two mechanisms:

  - Basic access

  - RTS/CTS

MAC Modes

- The 802.11 MAC protocol designed with two modes of communication

- **Distributed Coordination Function (DCF)** based on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

  – all stations are equal

  – "listen before talk"

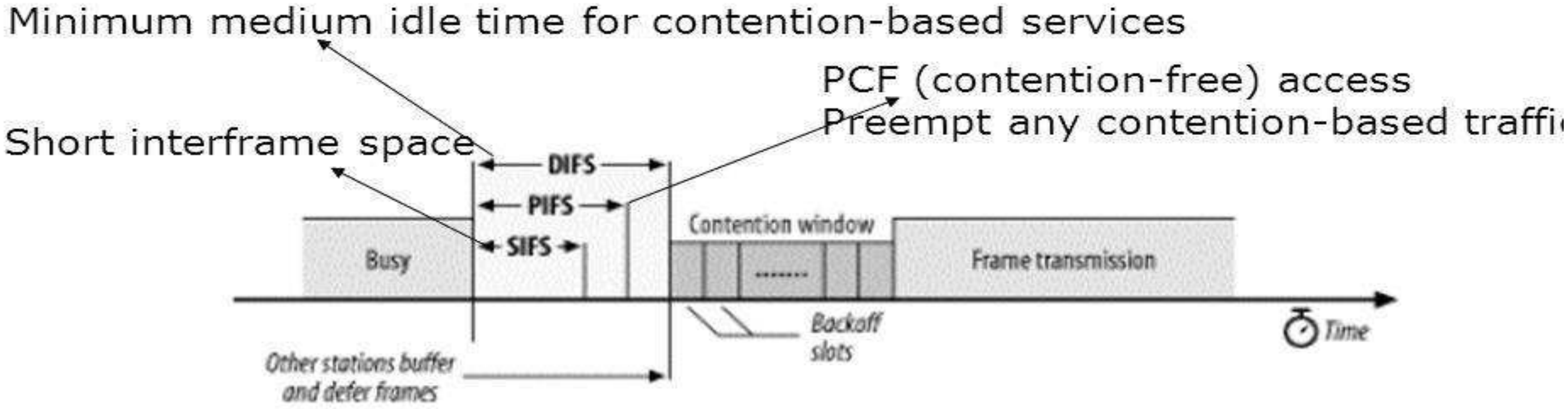
  - station waits for quiet period on network

  - begins to transmit data - detects possible collisions

- **Point Coordination Function (PCF)** – It is implemented to provide real time services.
- When PCF is in operation the AP controls medium access and avoids simultaneous transmissions by the nodes.

Inter-frame Spacing

- Create different **priority levels** for different types of traffic
- The higher the priority the smaller the wait time after the medium becomes idle



Minimum medium idle time for contention-based services

PCF (contention-free) access
Preempt any contention-based traffi

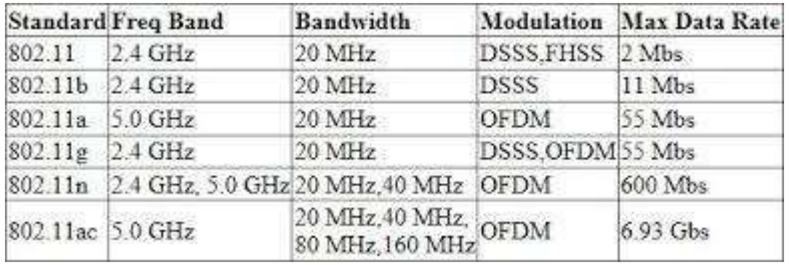
Short interframe space

- Inter frame Spacing
  - Time Interval between the transmission of two successive frame by any station.

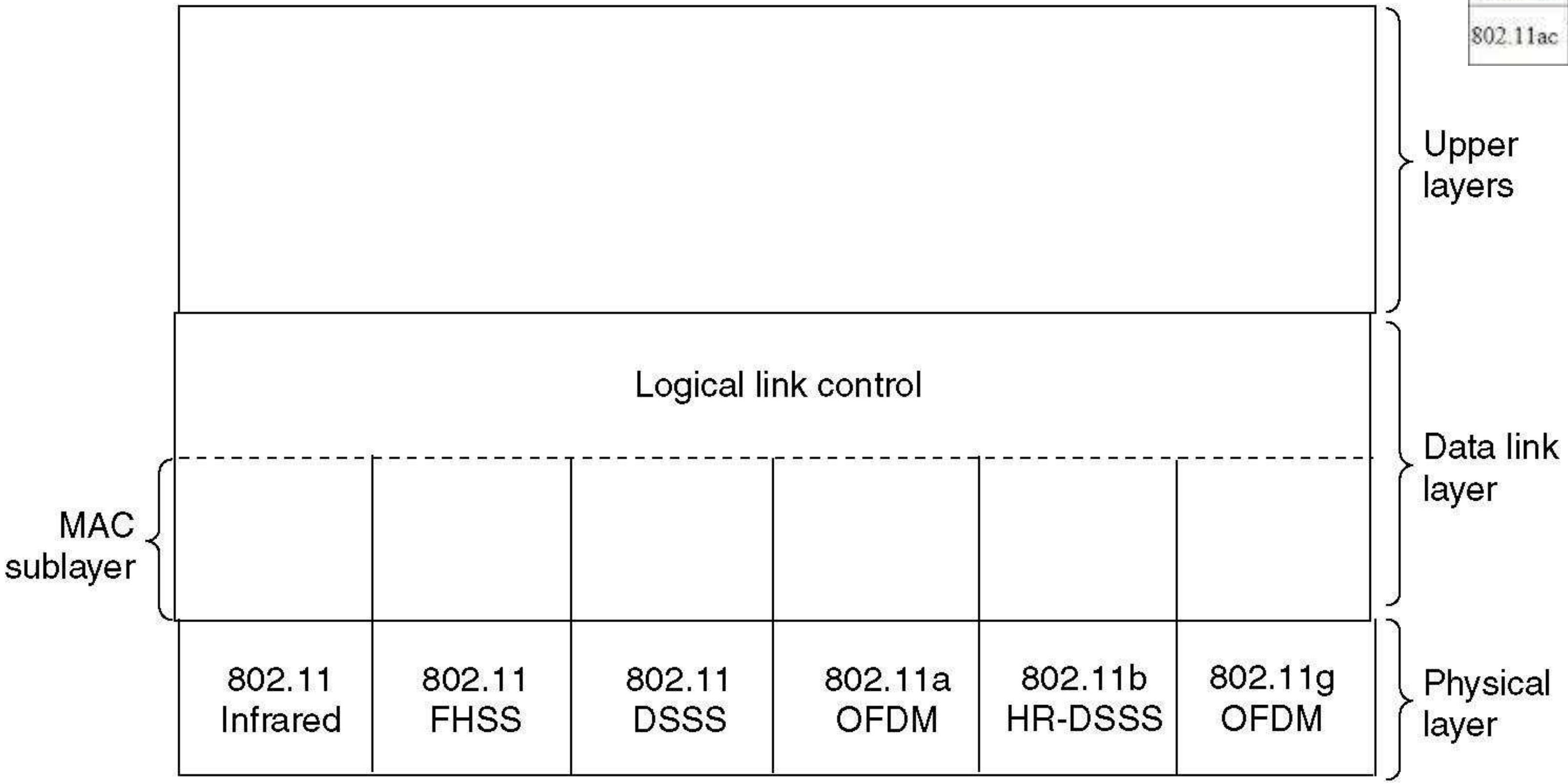
A **contention-based protocol** (CBP) is a communications **protocol** for operating wireless telecommunication equipment that allows many users to use the same radio channel without pre-coordination. The "listen before talk" operating procedure in IEEE 802.11 is the most well known **contention-based protocol**

802.11-based Wireless LANs
Architecture and Physical Layer

The 802.11 Protocol Stack



Standard	Freq Band	Bandwidth	Modulation	Max Data Rate
802.11	2.4 GHz	20 MHz	DSSS,FHSS	2 Mbs
802.11b	2.4 GHz	20 MHz	DSSS	11 Mbs
802.11a	5.0 GHz	20 MHz	OFDM	55 Mbs
802.11g	2.4 GHz	20 MHz	DSSS,OFDM	55 Mbs
802.11n	2.4 GHz, 5.0 GHz	20 MHz,40 MHz	OFDM	600 Mbs
802.11ac	5.0 GHz	20 MHz,40 MHz, 80 MHz,160 MHz	OFDM	6.93 Gbs



Spread-Spectrum techniques

- Methods by which a signal (e.g. an electrical, electromagnetic, or acoustic signal) generated with a particular bandwidth is deliberately spread in the frequency domain, resulting in a signal with a wider bandwidth.
- These techniques are used for a variety of reasons, including the establishment of secure communications, increasing resistance to natural interference, noise and jamming, to prevent detection, and to limit power flux density (e.g. in satellite downlinks).
- Spread spectrum is designed to be used in wireless applications (LANs and WANs). In wireless applications, all stations use air (or a vacuum) as the medium for communication. Stations must be able to share this medium without interception by an eavesdropper and without being subject to jamming from a malicious intruder.

Wireless Physical Layer

- Physical layer conforms to OSI (five options)
  - 1997: **802.11** infrared, FHSS, DHSS
  - 1999: **802.11a** OFDM and **802.11b** HR-DSSS
  - 2001: **802.11g** OFDM
- **802.11 Infrared**
  - Two capacities 1 Mbps or 2 Mbps.
  - Cannot penetrate walls.
- **802.11 FHSS (Frequence Hopping Spread Spectrum)**
  - 79 channels, each 1 Mhz wide at low end of 2.4 GHz ISM band.
  - Same pseudo-random number generator used by all stations.
  - Dwell time: min. time on channel before hopping (400msec).

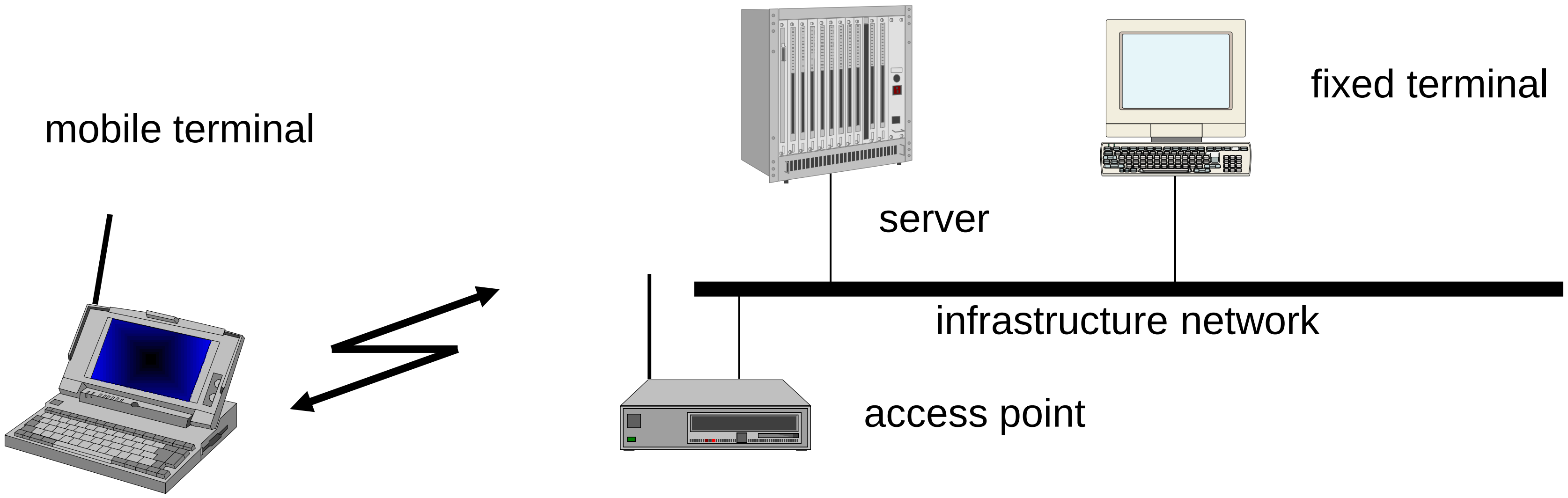
Wireless Physical Layer

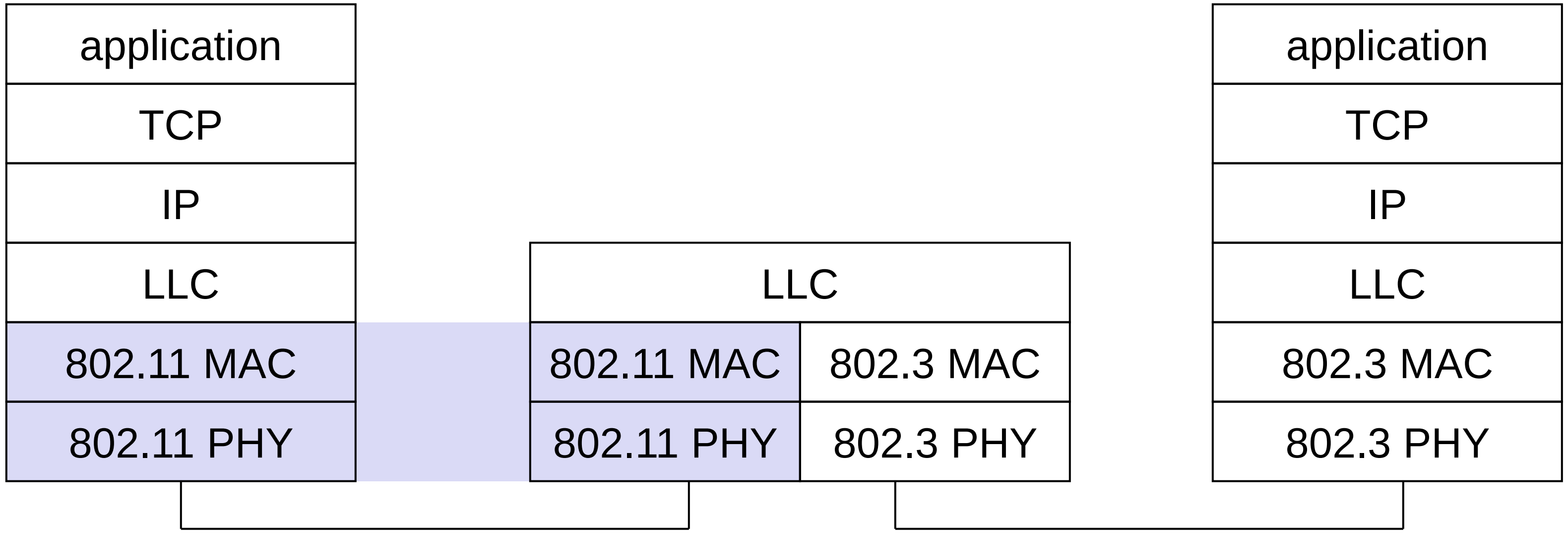
- **802.11 DSSS (Direct Sequence Spread Spectrum)**
  - Spreads signal over entire spectrum using pseudo-random sequence (similar to CDMA see Tanenbaum sec. 2.6.2).
  - Each bit transmitted as 11 chips (Barker seq.)
  - 1 or 2 Mbps.
- **802.11a OFDM (Orthogonal Frequency Divisional Multiplexing)**
  - Compatible with European HiperLan2.
  - 54Mbps in wider 5.5 GHz band ➔ transmission range is limited.
  - Encoding is complex
  - E.g., at 54Mbps 216 data bits encoded into into 288-bit symbols.
  - More difficulty penetrating walls.

Wireless Physical Layer

- **802.11g *OFDM*(*Orthogonal Frequency Division Multiplexing*)**
  - Supports 54 Mbps.
  - Uses 2.4 GHz frequency for greater range.

802.11- in the TCP/IP stack





application			application
TCP			TCP
IP			IP
LLC	LLC		LLC
802.11 MAC	802.11 MAC	802.3 MAC	802.3 MAC
802.11 PHY	802.11 PHY	802.3 PHY	802.3 PHY

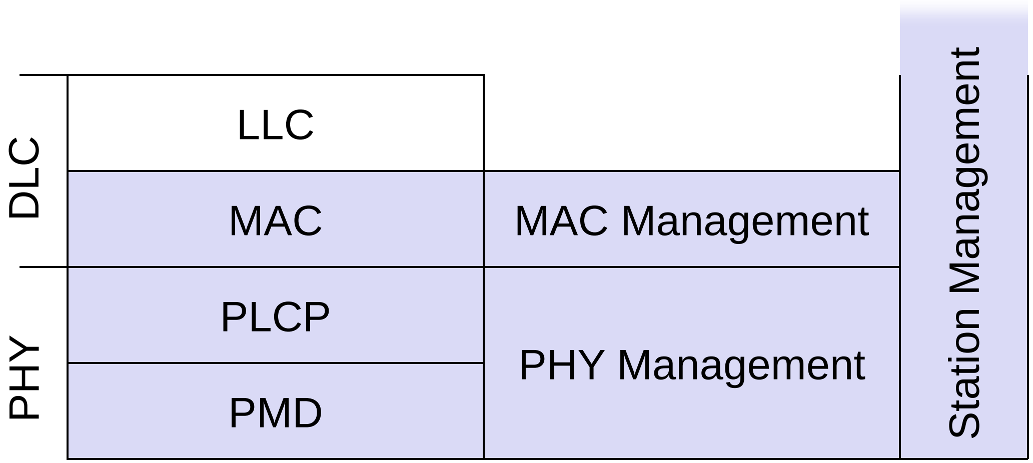
802.11 - Layers and functions

- MAC
    - access mechanisms, fragmentation, encryption
- MAC Management
    - synchronization, roaming, power management

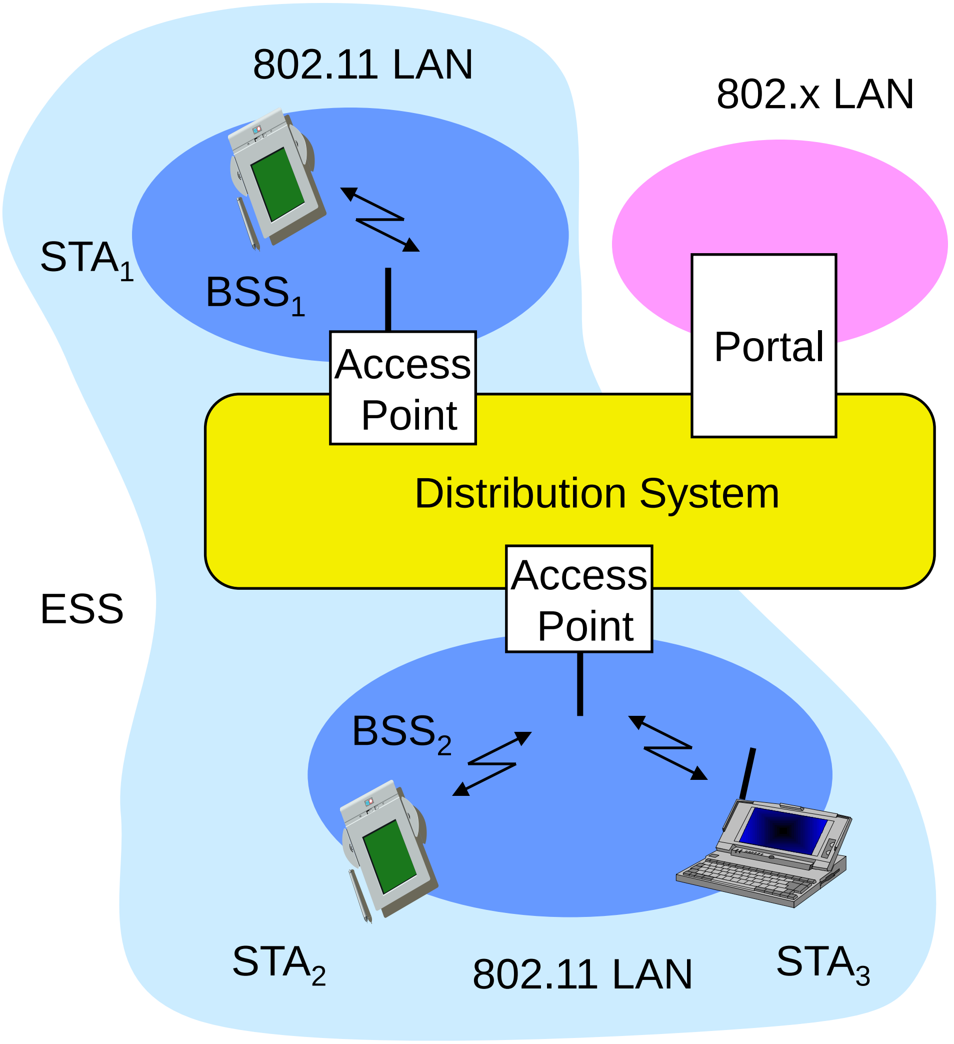
- PLCP Physical Layer Convergence Protocol
    - clear channel assessment signal (carrier sense)
- PMD Physical Medium Dependent
    - modulation, coding
- PHY Management
    - channel selection

Station Management

- coordination of all management functions



802.11 - infrastructure network



- Station (STA)
  - terminal with access mechanisms to the wireless medium and radio contact to the access point
- Basic Service Set (BSS)
  - group of stations using the same radio frequency
- Access Point
  - station integrated into the wireless LAN and the distribution system
- Portal
  - bridge to other (wired) networks
- Distribution System
  - interconnection network to form one logical network (EES: Extended Service Set) based on several BSS

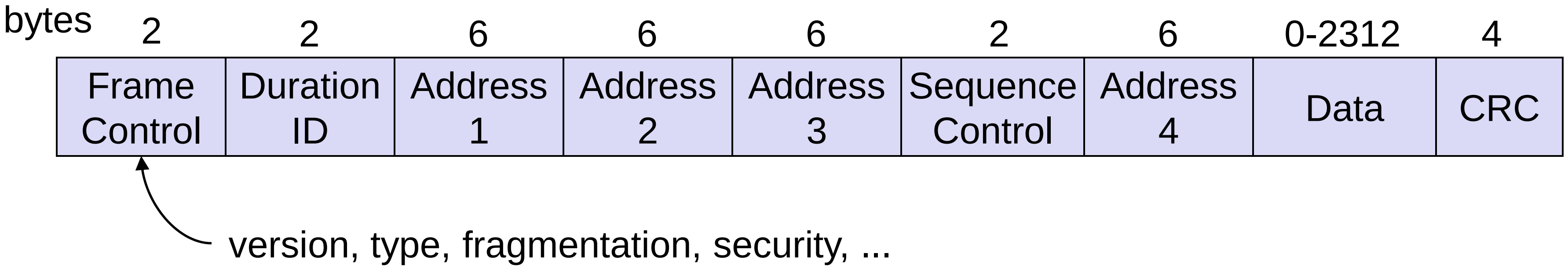
Source: Schiller

Distribution System (DS) concepts

- The Distribution system interconnects multiple BSSs
- 802.11 standard logically separates the wireless medium from the distribution system – it does not preclude, nor demand, that the multiple media be same or different
- An Access Point (AP) is a STA that provides access to the DS by providing DS services in addition to acting as a STA.
- Data moves between BSS and the DS via an AP
- The DS and BSSs allow 802.11 to create a wireless network of arbitrary size and complexity called the Extended Service Set network (ESS)

802.11 - Frame format

- Types
  - control frames, management frames, data frames
- Sequence numbers
  - important against duplicated frames due to lost ACKs
- Addresses
  - receiver, transmitter (physical), BSS identifier, sender (logical)
- Miscellaneous
  - sending time, checksum, frame control, data



bytes	2	2	6	6	6	2	6	0-2312	4
	Frame Control	Duration ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Data	CRC

version, type, fragmentation, security, ...

Types of Frames

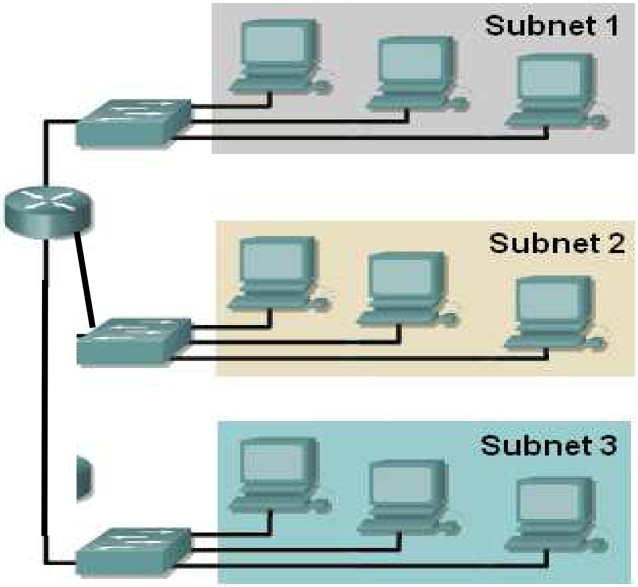
- Control Frames
  - RTS/CTS/ACK
- Management Frames
  - Beacons
  - Request/Response
  - Association Request/Response
  - Dissociation/Reassociation
  - Authentication/Deauthentication
- Data Frames

Virtual LANs

VLANs allow network administrators to partition their networks to match the functional and security requirements of their systems without having to run new cables or make major changes in their current network infrastructure.

IEEE 802.1Q is the standard defining VLANs.

Virtual LANs



3 Collision domains
3 Broadcast domains

If we want to move computers from group1 to group3, then rewiring (physical replacement) has to be done

What is the alternative solution??

VLAN: Virtual (logical) Local Area Network : Local Area Network configured by **software** not by physical wiring

Figure 26-2 **A switch using VLAN software**

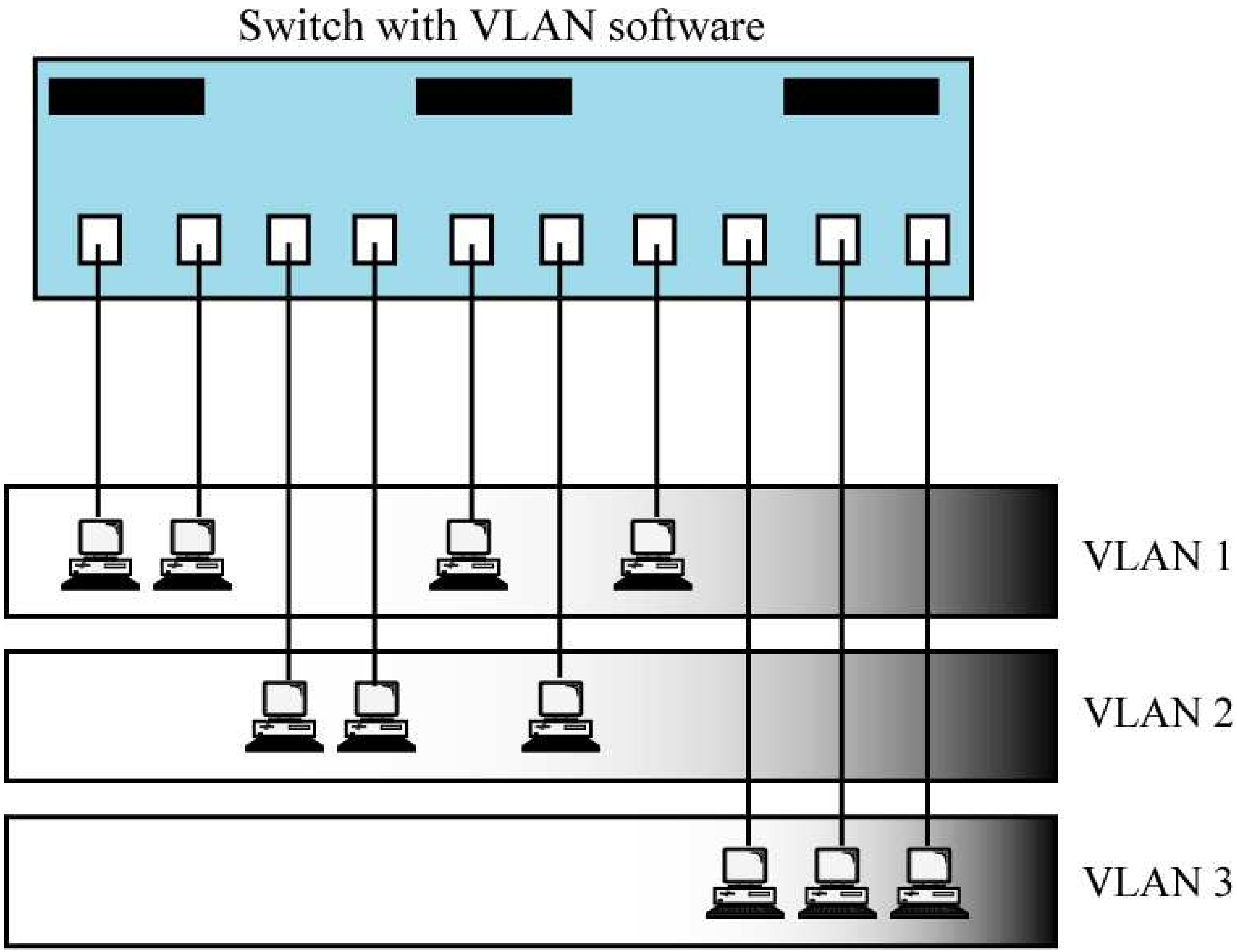


Figure 26-3

Two switches in a backbone using VLAN software

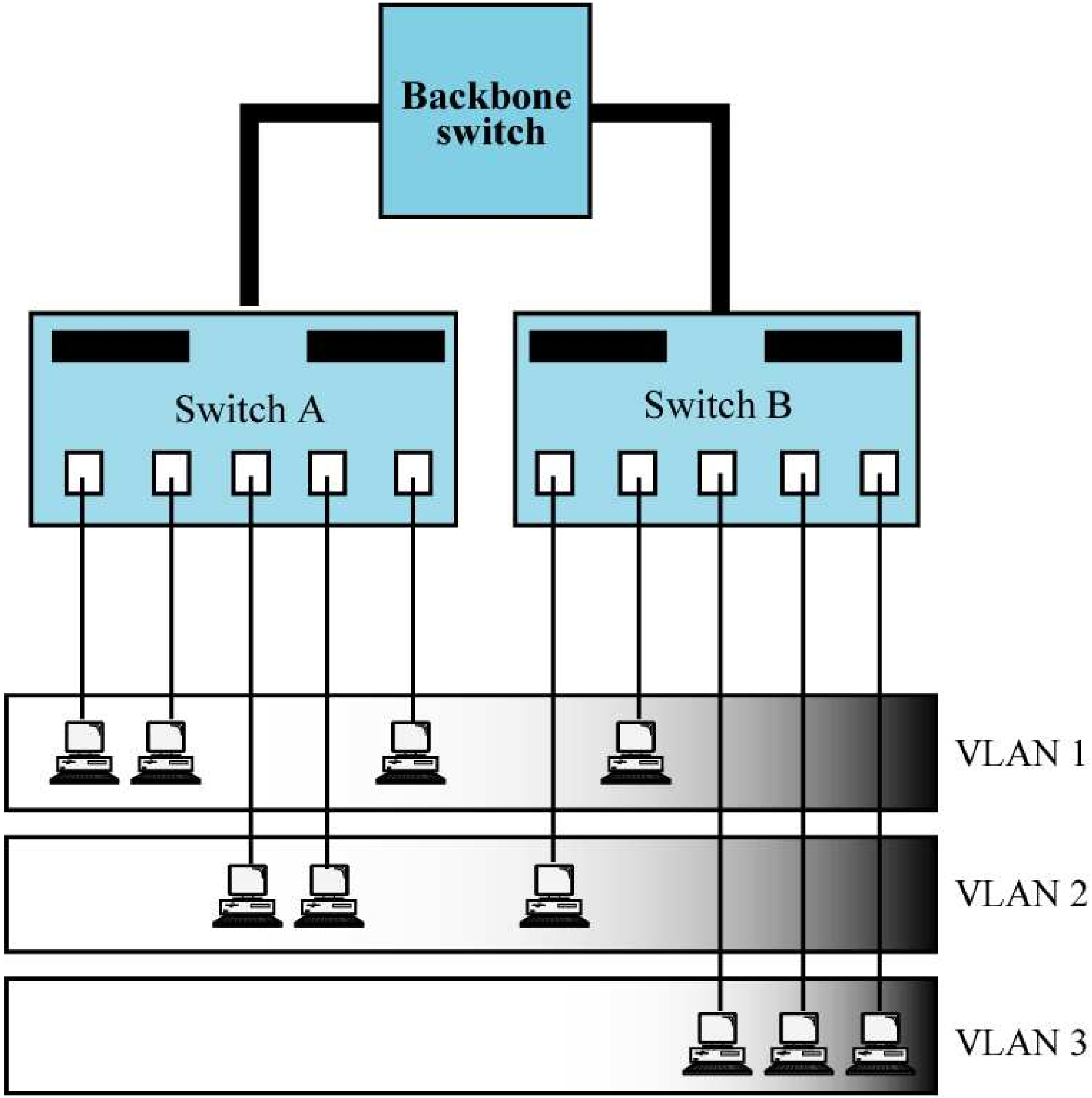
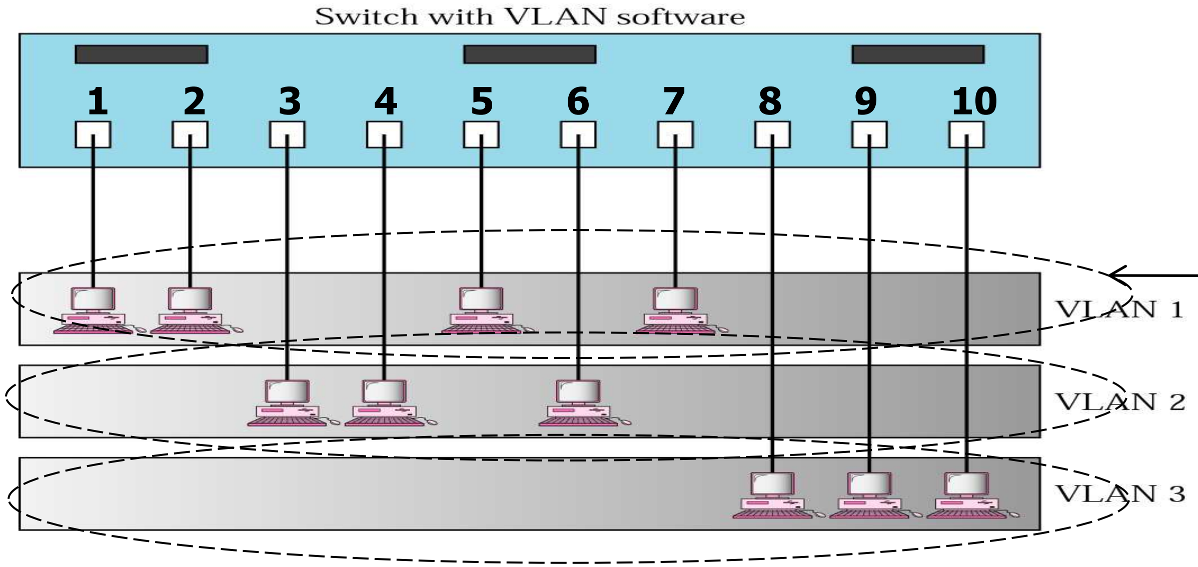


Figure 16.15 A switch using VLAN software



VLAN1: Ports 1,2,5,7

VLAN2: Ports 3,4,6

VLAN3: Ports 8,9,10

Separate broadcast domain ➔ separate network

- Using the Virtual LAN technology will allow **grouping** computers **logically** instead of **physically**.

- VLAN divides the physical LAN into several **Logical LANs** called VLANs

- Switch maintains a look up table to know to which LAN a machine belongs to.

Note:

VLANs create broadcast domains.

Advantages Of VLAN

- **Reduce cost and installation time**:
  - Instead of **physically moving** a station to another segment or another switch, it can be moved by software.
- **Increase security**:
  - A group of users needing a high security can be put into a VLAN so that NO users outside the VLAN can communicate with them.
  - Stations belong to the same group can send **broadcast messages** that will NOT be received by users in others VLAN groups
- **Creating Virtual Workgroups**
  - Stations located at physically different locations can be added easily to the same broadcast domain so that they can send broadcast messages to one another.
    - EXAMPLE: people from different departments working on the same project