Chapter – 1

Review Of Basic Concepts

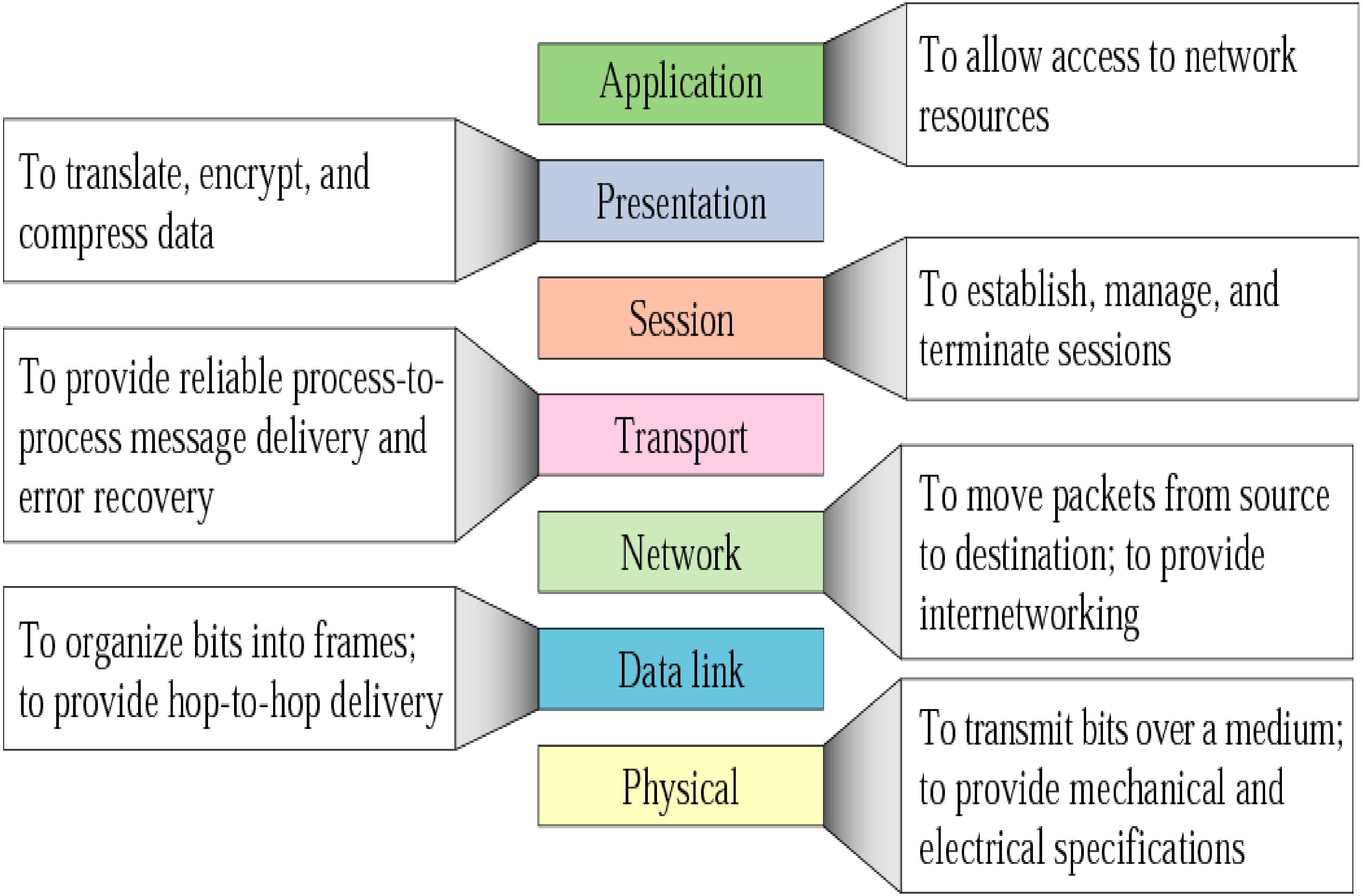
Topics to be covered

- TCP / IP protocol suite
- Underlying technologies : -
  - ➢ Wired LAN (802.3) - Ethernet
  - ➢ Wireless LAN (802.11)
  - ➢ Bluetooth
  - ➢ WAN

ISO-OSI Model of the network

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

Summary of layers



Application: To allow access to network resources

Presentation: To translate, encrypt, and compress data

Session: To establish, manage, and terminate sessions

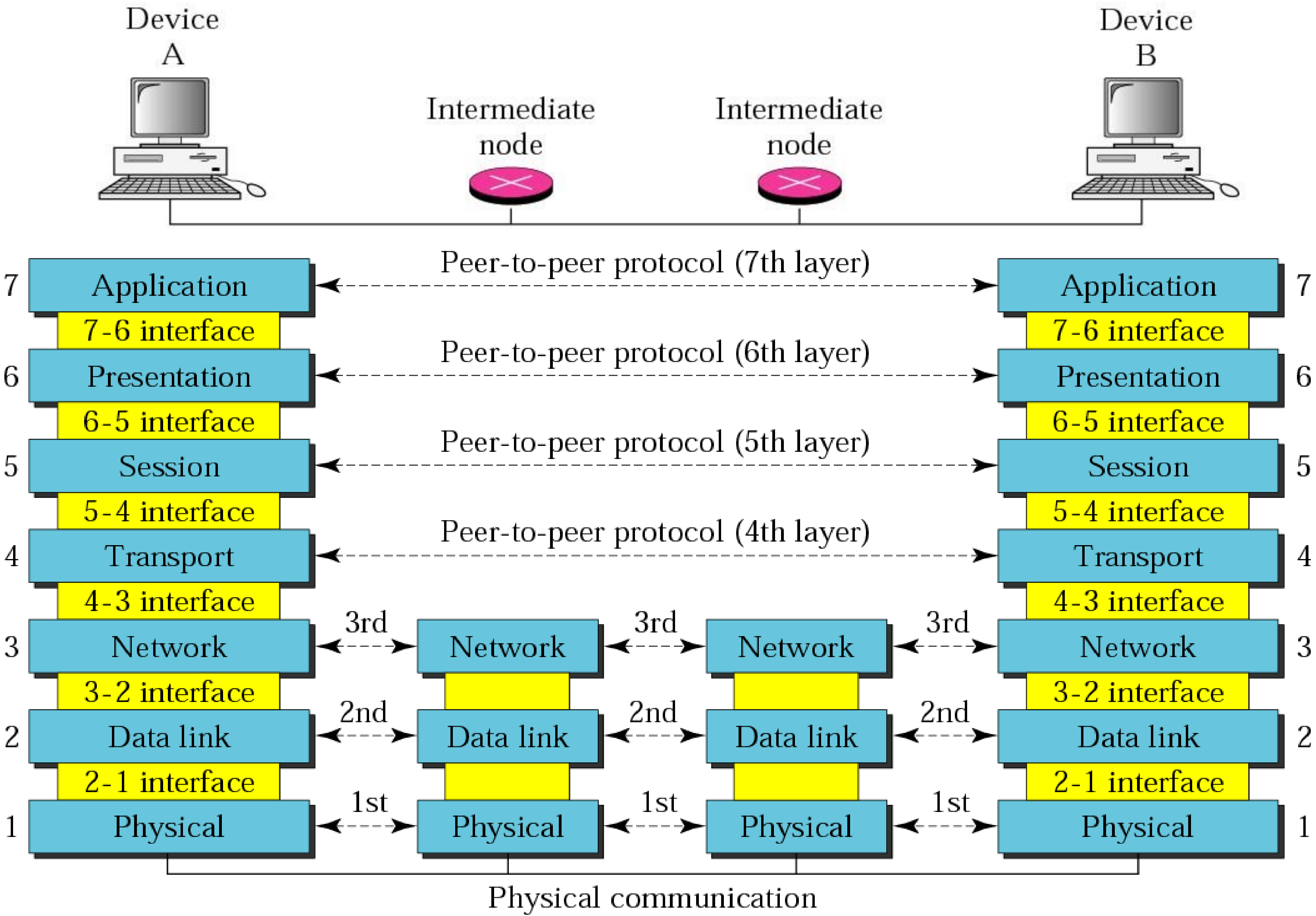
Transport: To provide reliable process-to-process message delivery and error recovery

Network: To move packets from source to destination; to provide internetworking

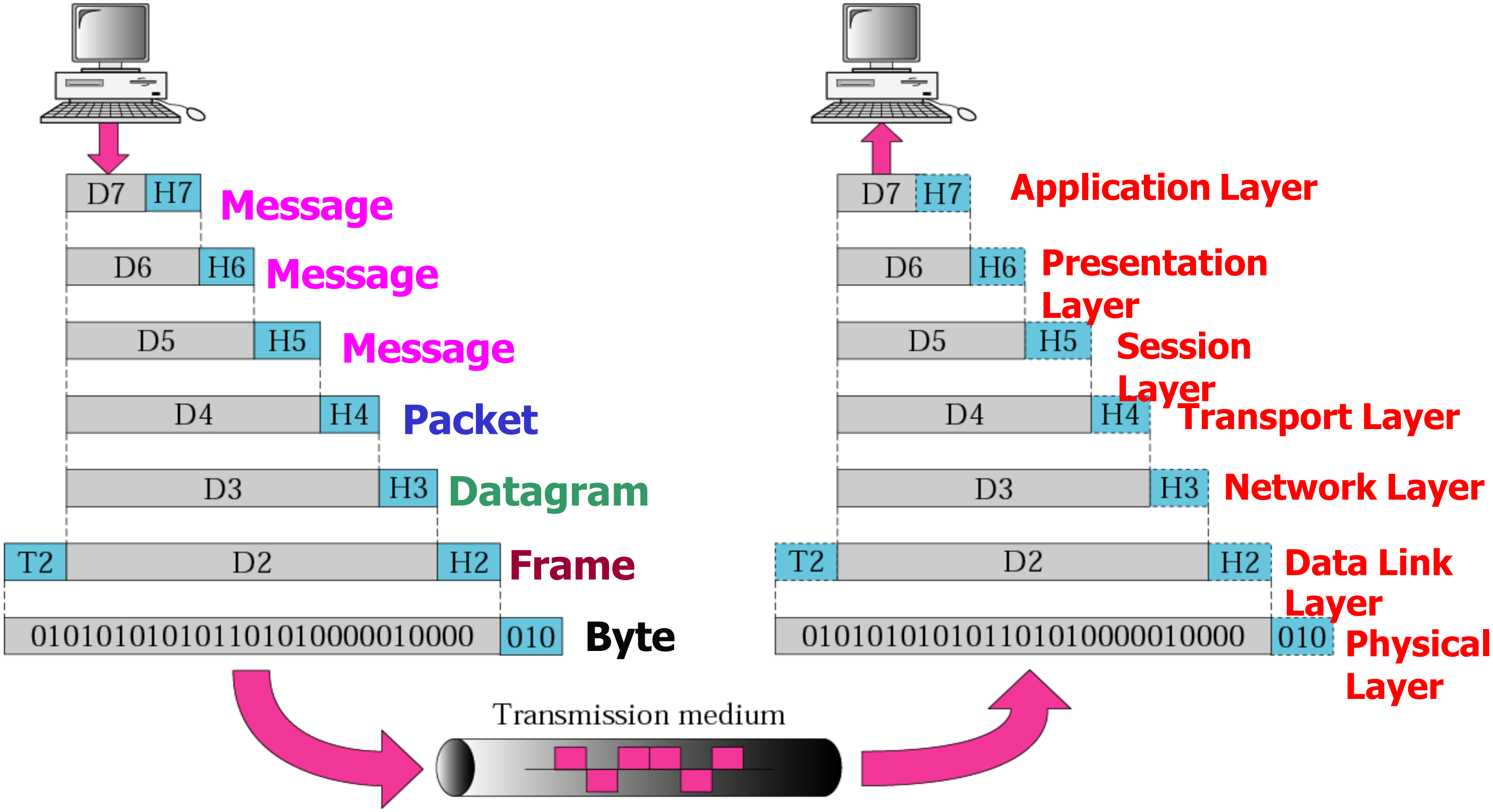
Data link: To organize bits into frames; to provide hop-to-hop delivery

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

OSI Layer


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

Exchange Using the OSI Model



Message

Message

Message

Packet

Datagram

Frame

Byte

Application Layer

Presentation Layer

Session Layer

Transport Layer

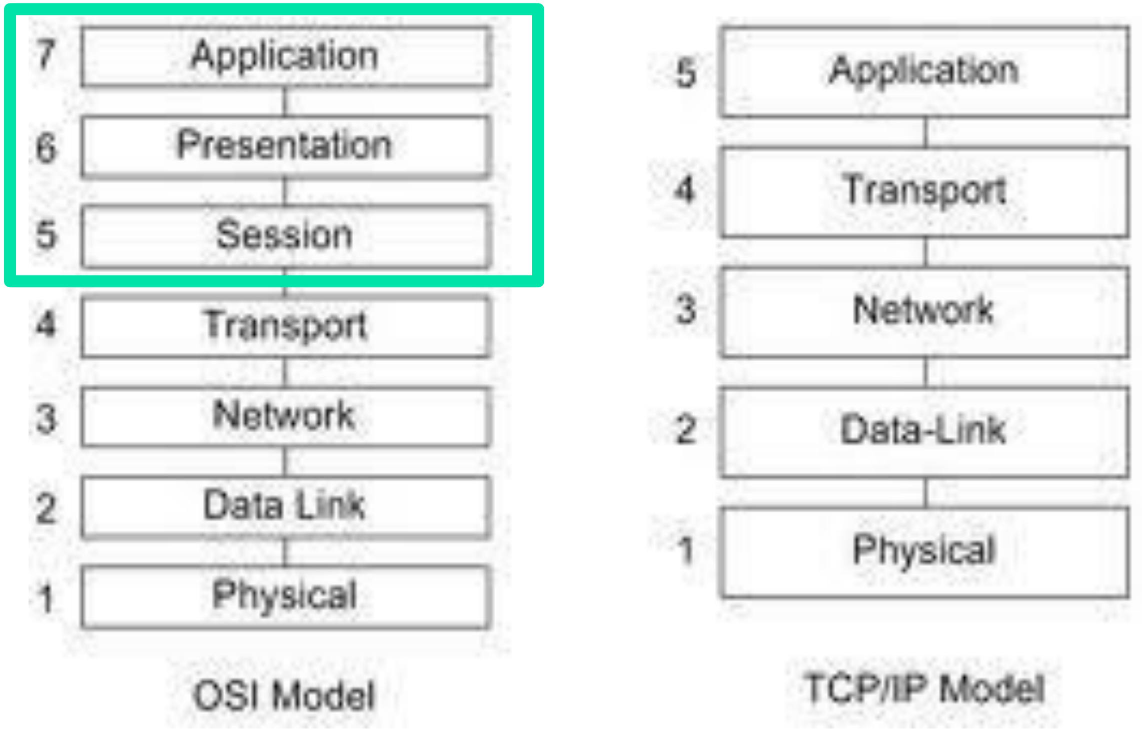
Network Layer

Data Link Layer

Physical Layer

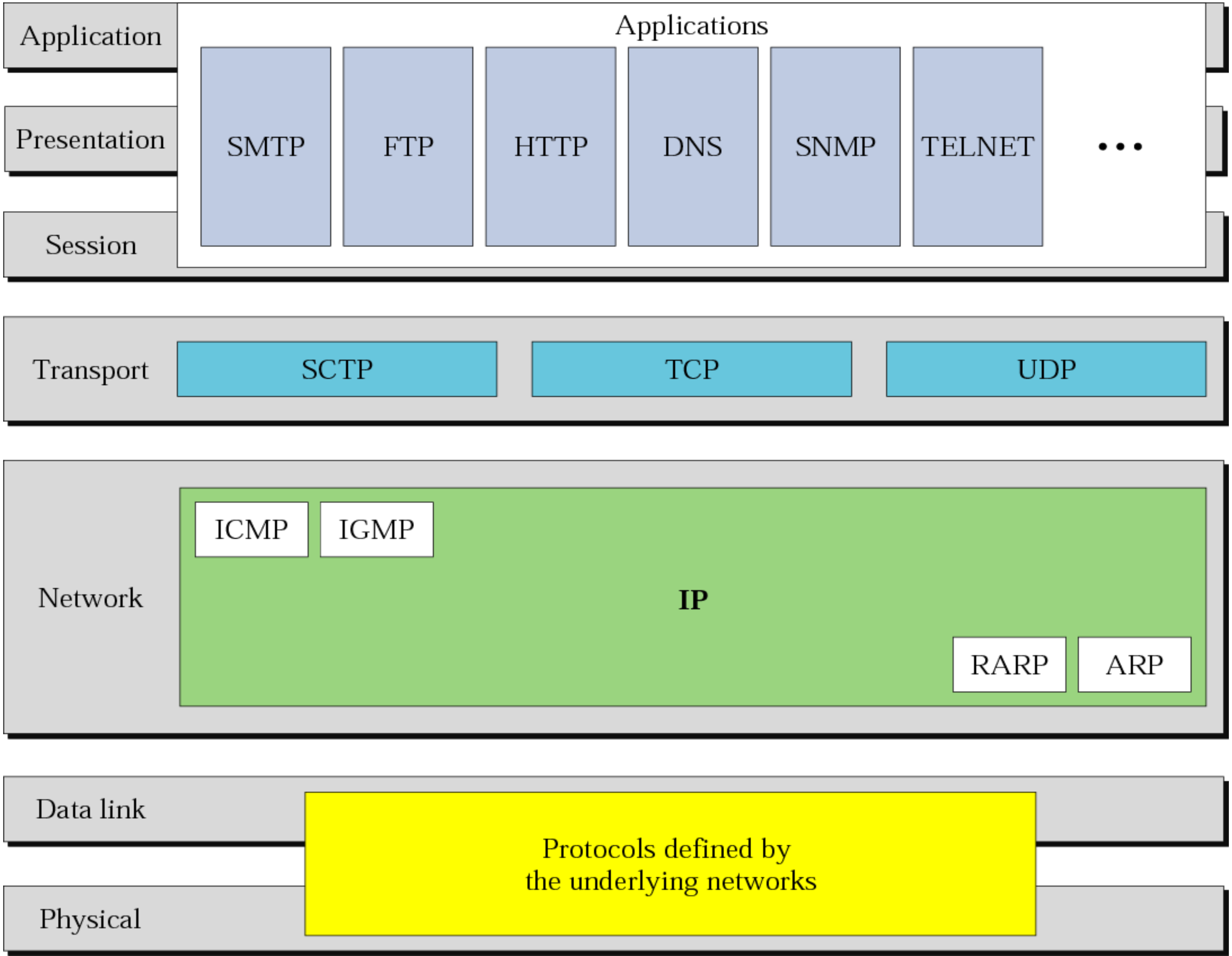
TCP/IP Protocol Suite

- The TCP/IP protocol model is developed prior to OSI model
- The TCP/IP protocol suite is made of five layers:-



- The three topmost layers in the OSI model, however, are represented in TCP/IP by a single layer called the application layer.

TCP/IP Protocol Suite



Local Area Networks

- A local area network (LAN) is a data communication system that allows a number of independent devices to communicate directly with each other in a limited geographic area such as a single department, a single building, or a campus.
- Most LANs today are also linked to WANs or the Internet.
- A large organization may need several connected LANs.
- The common LAN technologies which are used are,
    - Wired LANs: Ethernet - IEEE 802.3
    - Wireless LANs: IEEE 802.11

Why standards????

- Standards are published documents that establish specifications and procedures designed to ensure the reliability of the materials, products, methods, and/or services people use every day.

- The primary reason for standards is to ensure that hardware and software produced by different vendors can work together.

- Without networking standards, it would be difficult—if not impossible—to develop networks that easily share information.

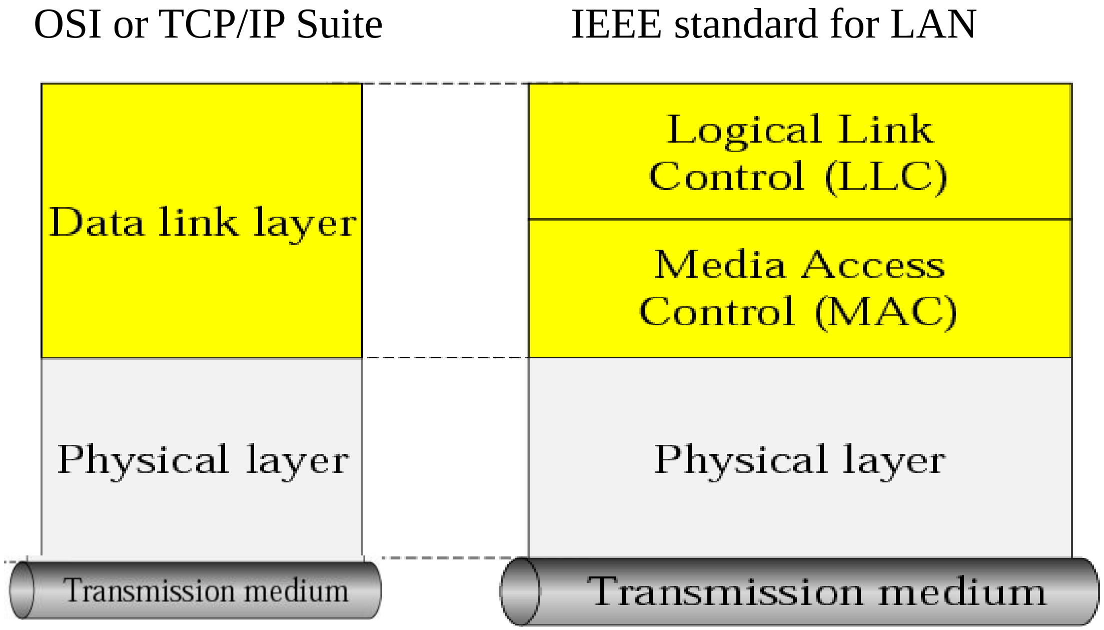
- Standards also mean that customers are not locked into one vendor. They can buy hardware and software from any vendor whose equipment meets the standard.

IEEE 802 standards

- IEEE started a project , Project 802 to set standard *to enable intercommunication among equipments from a variety of manufacturers.*

- *It doesn't replace any part of OSI or TCP/IP model.*

- Instead it is a way of specifying functions of the physical & DLL of major LAN protocols.

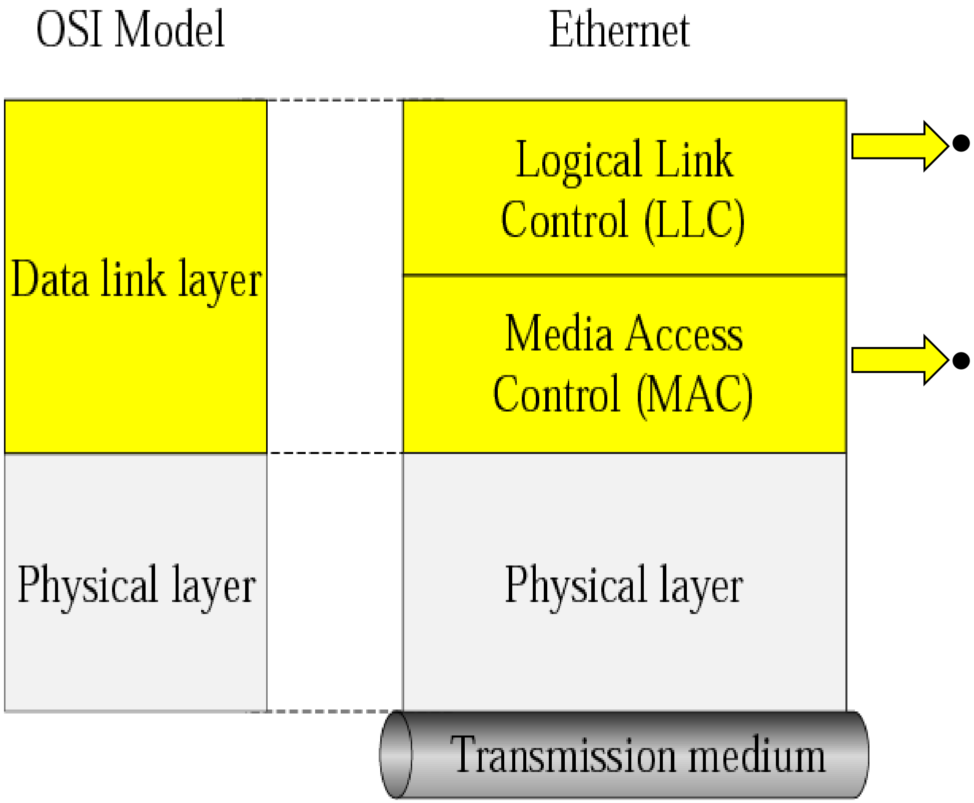


IEEE standards for LANs

Relationship of 802 standard to OSI and TCP/IP model.

Data Link Layer is divided into 2 sub layer

- Logical Link Control (LLC).
- Media Access Control (MAC).

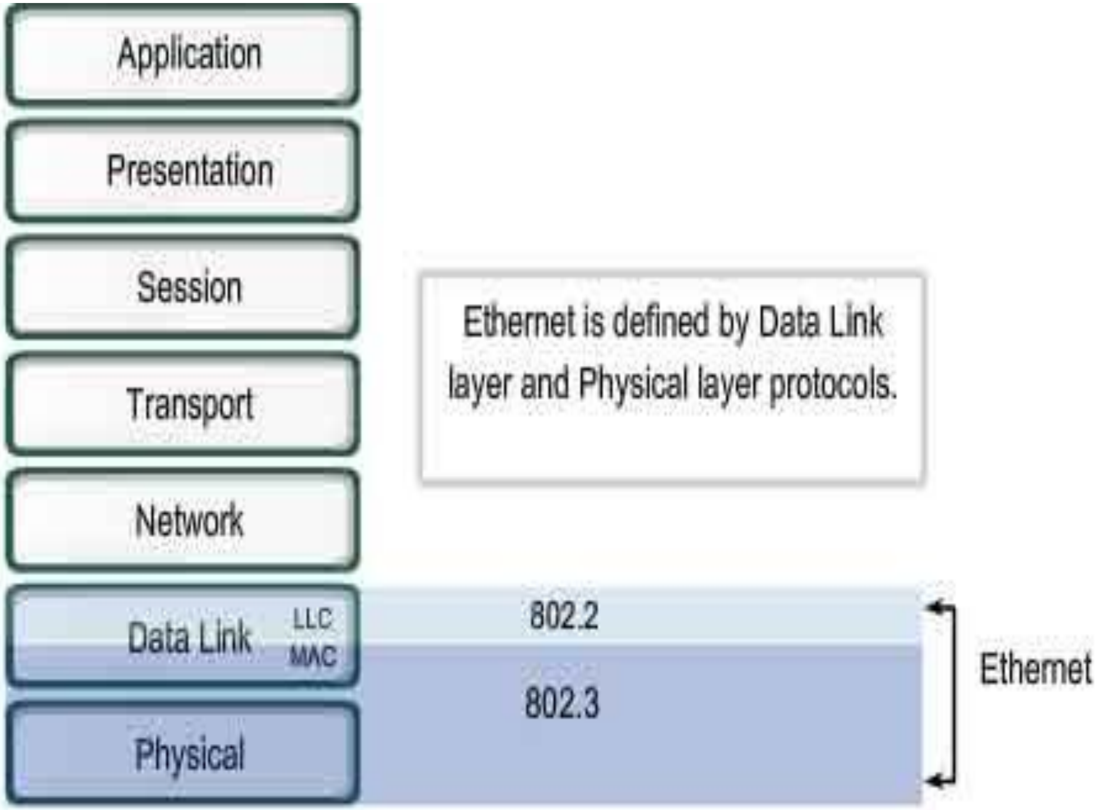


- LLC Layer is responsible for flow & error control at DLL.
- MAC Layer is responsible for
  - use of access methods (prototype).
  - framing the data received from LLC & send it to physical layer.

Wired LAN -IEEE 802.3

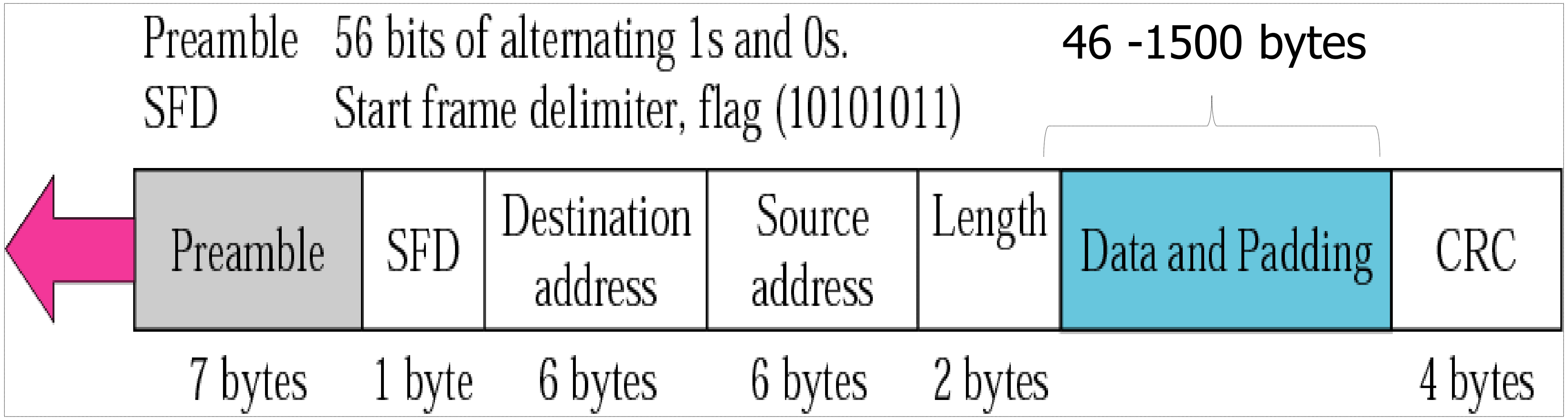
Ethernet

- Packet sent in Ethernet LAN is called *Frame*.
- Ethernet frame contains seven fields.
- It does not have any mechanism for acknowledging received frames, making it unreliable.



Wired LAN IEEE 802.3

Ethernet MAC Frame - Ethernet frame min length of 64 bytes & Max. is 1518 bytes.



- Preamble : - alerts receiving system about the coming frame & enables it to synchronize it's input.
- SFD :- signals beginning of the frame.
- Destination Address:- physical address of receiver
- Source Address:- physical address of sender
- Length :- number of bytes in the frame.
- Data & padding
- CRC :- contains error detection information.

Wired LAN IEEE 802.3

Ethernet MAC Frame length

- Ethernet has imposed restriction on min. & max. length of a frame. It is required for the correct operation of underlying protocol.
- Ethernet frame min length of 64 bytes & Max. is 1518 bytes. (without counting preamble and SFD)
- 18 bytes are of header and trailer (6 + 6 + 2 + 4), So min. length of the data from upper layer is 46 bytes (64-18).
- If upper layer packet is less than 46 bytes, padding is added to make up the difference.
- On the same line, max length of frame is 1518 without counting preamble and SFD. If we subtract 18 bytes of header and trailer, max length of payload is 1500.

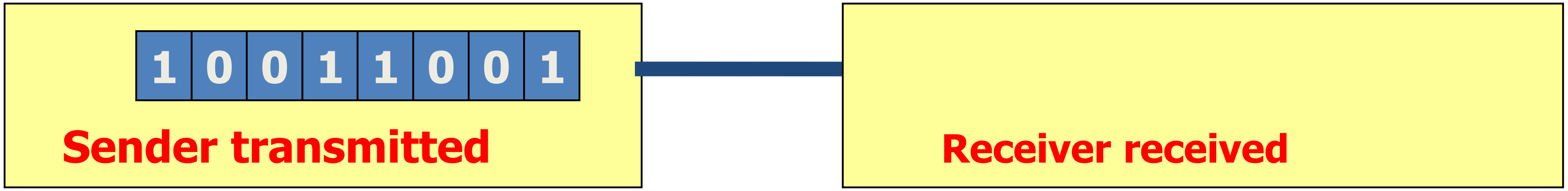
Ethernet Addressing

- Each station on Ethernet network has it's own NIC (Network Interface Card) which provides 6 byte physical address.

- Address is 6bytes(48bits) written in hexadecimal notation with a colon to separate the bytes.

  For e.g 07:01:02:01:2C:4B

- Addresses are sent byte to byte, left to right



- Three type of addresses are used
  - Unicast : LSB of first byte is 0
  - Multicast : LSB of first byte is 1
  - Broadcast : has 48 1's

Wired LAN – Ethernet (IEEE 802.3)

Standard Ethernet (Traditional Ethernet)

Here stations are connected using physical bus or star topology, but logical topology is bus. i.e. channel (medium) is shared between the stations & at a time only one station can use it.

All in between stations receive a frame sent by a station (broadcasting).

The real destination keeps the frame while the rest drop it.

Now if two stations are using the channel at the same time, their frames will collide with each other.

How can we be sure that two stations are not using the medium at the same time?

Wired LAN – Ethernet (IEEE 802.3)

Standard Ethernet (Traditional Ethernet)

Access method (protocol) used for Ethernet is CSMA/CD. ***(Carrier Sense Multiple Access with Collision Detection).***

To increase the performance & decrease the chance of collision CSMA method was developed.

Chance of collision can be reduced if a station senses the medium before trying to use it.

CSMA basic principle - ***“sense before transmit” or “listen before talk”***

CSMA/CD reduces the possibility of the collision but can not eliminate it.

Possibility of collisions still exists because of propagation delay.

CSMA/CD

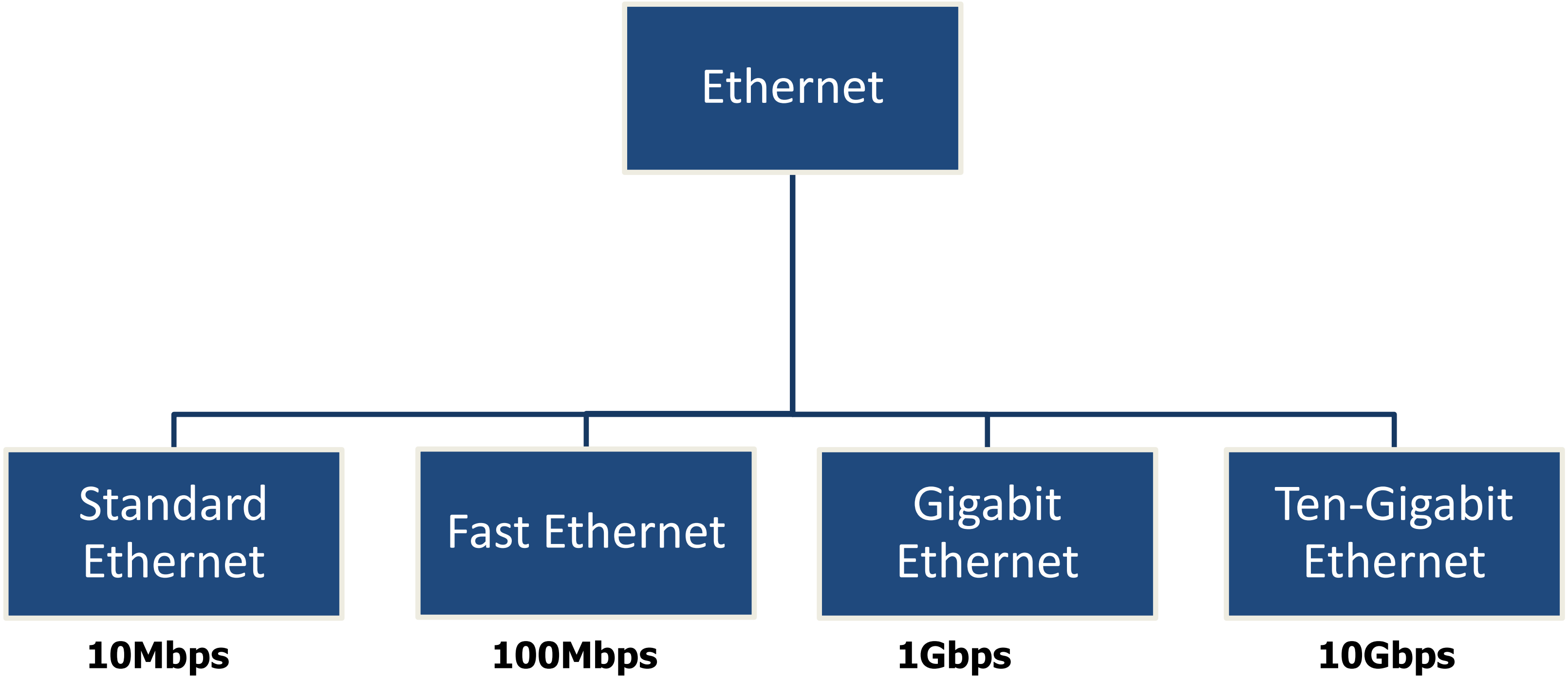
Principles those CSMA/CD should follow..

1. To send the frame, station should first listen to the channel, if no data on channel, start sending. (Carrier Sense)

2. Every station has equal right to the channel. (Multiple Access)

3. If two stations are sending data simultaneously and if collision occurs, then all stations senses the collision and actual data sending station sends the jam signal to destroy the data. (Collision Detect)

Ethernet Evolution



Wireless LANs – IEEE 802.11

- Called as Wireless Ethernet.
- IEEE 802.11 covers the physical & Data link layer.

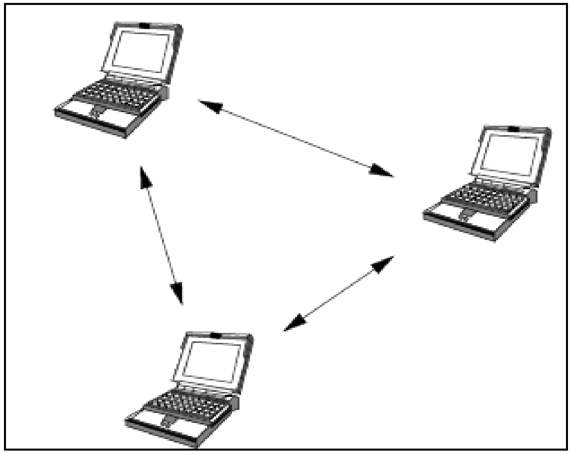
- The standard defines two kinds of services :-

1. Basic Service Set (BSS)
2. Extended Service Set (ESS)

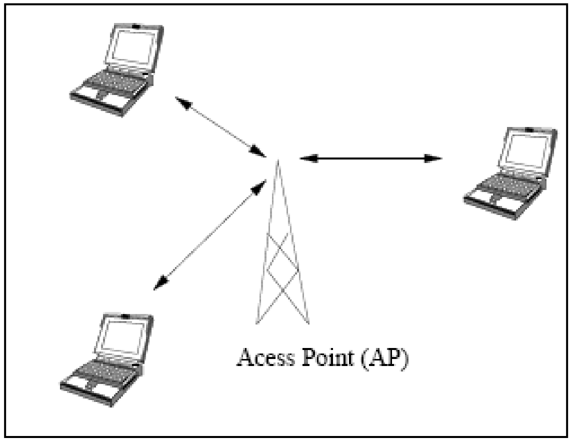
Wireless LANs – IEEE 802.11 - Basic Service Set (BSS)

Basic Service Set (BSS) - Made up of stationary or mobile wireless stations & an optional central base station called as Access Point (AP).

- BSS Without AP (Independent BSS)
  - Standalone network
  - Can’t send data to other BSSs.
  - Called as an ad hoc network
  - Station can locate one another
  - & agree to be a part of BSS

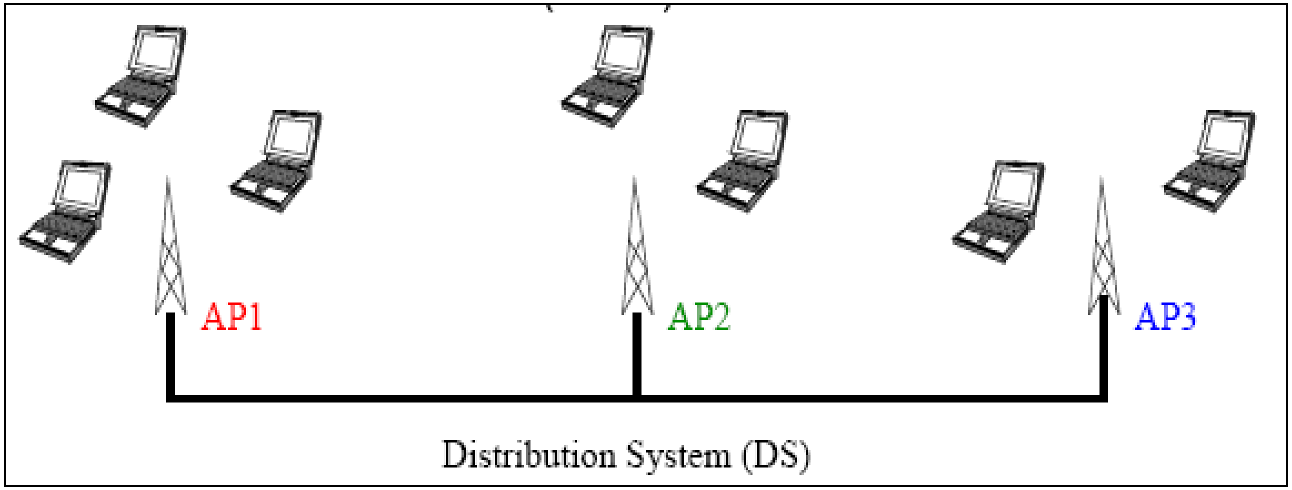


- BSS With AP
  - Can send data to other BSSs.
  - Called as an infrastructure network
  - Station can locate one another via AP



Wireless LANs – IEEE 802.11- **Extended Service Set (ESS)**

- Made up by connecting 2 or 3 BSS.
- BSS are connected through distribution system which is wired LAN.



- Distribution system connects the APs in the BSSs.
- ESS uses two types of stations :-
  - Mobile (Normal stations inside BSS.)
  - Stationary (AP stations)
- Distribution system can be any IEEE LAN such as an Ethernet.

Wireless LANs – IEEE 802.11

- Station category : -
  - No transition :

    mobility is stationary or moving only inside a BSS.

  - BSS transition

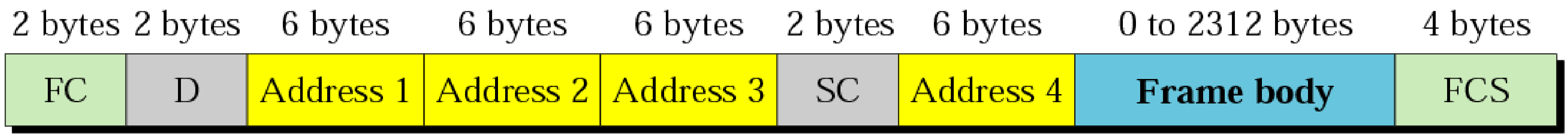
    station can move from one BSS to another.

  - ESS transition

    station can move from one ESS to another.

Wireless LANs – IEEE 802.11

Frame Format

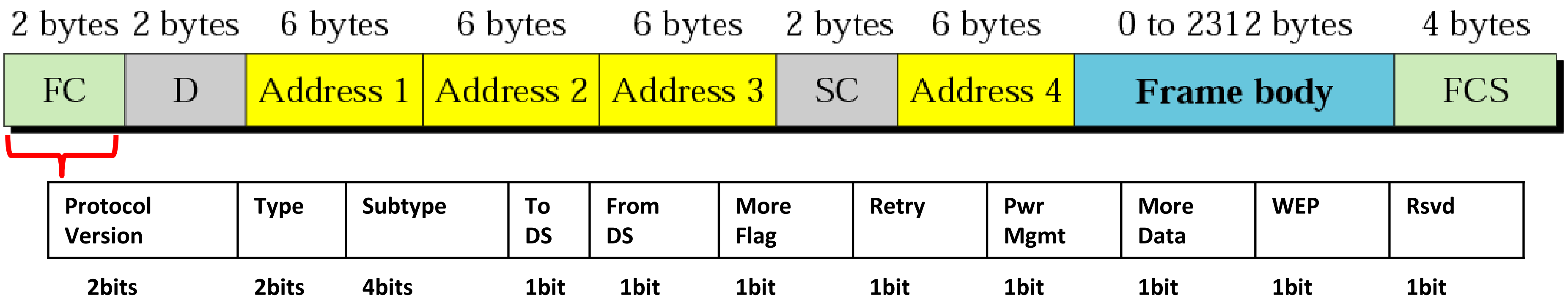


2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	0 to 2312 bytes	4 bytes
FC	D	Address 1	Address 2	Address 3	SC	Address 4	**Frame body**	FCS

- Frame Control (FC) :- defines type & control information.
- D :- defines duration of transmission.
- SC (Sequence Control) :- defines sequence number of the frame.
- Frame body :- contains information based on the type & subtype field.
- FCS :-error detection sequence.

Wireless LANs – IEEE 802.11

Frame Format : Frame Control (FC)



2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	0 to 2312 bytes	4 bytes
FC	D	Address 1	Address 2	Address 3	SC	Address 4	**Frame body**	FCS

Protocol Version	Type	Subtype	To DS	From DS	More Flag	Retry	Pwr Mgmt	More Data	WEP	Rsvd
2bits	2bits	4bits	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit

Field	**Explanation**
Version	Current version is 0
Type	Frame Type information: management, control, data
Subtype	Subtypes of types
To DS	
From DS	
More flag	Set to 1, means more fragmentation
Retry	Set to 1, means retransmitted frame
Pwr mgmt	Set to 1, means station is in power management mode
More data	Set to 1, means station has more data to send
WEP	Wired Equivalent privacy (encryption implemented)
RSVD	Reserved

Wireless LANs – IEEE 802.11

Frame Format : Frame Control (FC)

2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	0 to 2312 bytes	4 bytes
FC	D	Address 1	Address 2	Address 3	SC	Address 4	**Frame body**	FCS

Protocol Version	**Type**	**Subtype**	**To DS**	**From DS**	**More Flag**	**Retry**	**Pwr Mgmt**	**More Data**	**WEP**	**Rsvd**
2bits	**2bits**	**4bits**	**1bit**	**1bit**	**1bit**	**1bit**	**1bit**	**1bit**	**1bit**	**1bit**

Field	**Explanation**
Version	Current version is 0
Type	Frame Type information: management, control, data
Subtype	Subtypes of types
To DS	
From DS	
More flag	Set to 1, means more fragmentation
Retry	Set to 1, means retransmitted frame
Pwr mgmt	Set to 1, means station is in power management mode
More data	Set to 1, means station has more data to send
WEP	Wired Equivalent privacy (encryption implemented)
RSVD	Reserved

- Management frame(00) : Used for initial communication between station & AP
- Control frame(01) : used for accessing the channel & acknowledging frame.

Subtypes	Meaning
1011	RTS
1100	CTS
1101	ACK

- Data frame (10)

Mrs. A. S. Nimgaonkar

Wireless LANs – IEEE 802.11

Frame Format : Frame Control (FC)

2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	0 to 2312 bytes	4 bytes
FC	D	Address 1	Address 2	Address 3	SC	Address 4	**Frame body**	FCS

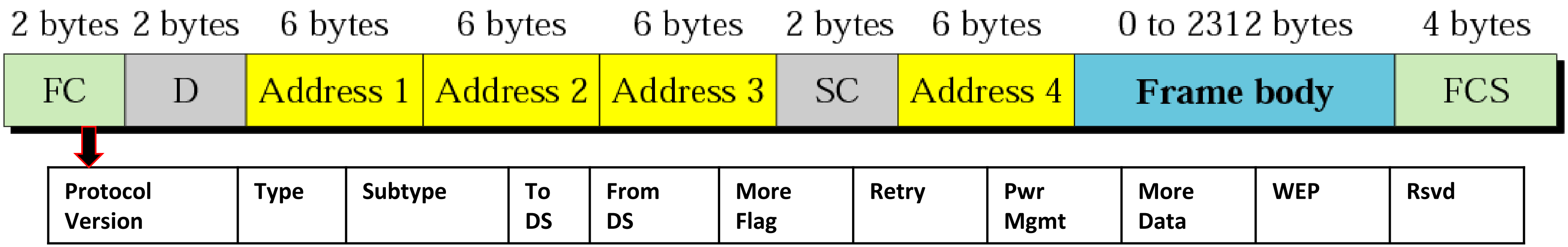
Protocol Version	**Type**	**Subtype**	**To DS**	**From DS**	**More Flag**	**Retry**	**Pwr Mgmt**	**More Data**	**WEP**	**Rsvd**
2bits	**2bits**	**4bits**	**1bit**	**1bit**	**1bit**	**1bit**	**1bit**	**1bit**	**1bit**	**1bit**

Field	**Explanation**
Version	Current version is 0
Type	Frame Type information: management, control, data
Subtype	Subtypes of types
To DS	
From DS	
More flag	Set to 1, means more fragmentation
Retry	Set to 1, means retransmitted frame
Pwr mgmt	Set to 1, means station is in power management mode
More data	Set to 1, means station has more data to send
WEP	Wired Equivalent privacy (encryption implemented)
RSVD	Reserved

To DS	From DS	Add1	Add2	Add3	Add4
0	0	Dest	Src	BSS ID	N/A
0	1	Dest	Sending AP	Src	N/A
1	0	Rec. AP	Src	Desti	N/A
1	1	Receiving AP	Sending AP	Desti	Src

Wireless LANs – IEEE 802.11

Frame Format : Addressing scheme



2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	0 to 2312 bytes	4 bytes
FC	D	Address 1	Address 2	Address 3	SC	Address 4	**Frame body**	FCS

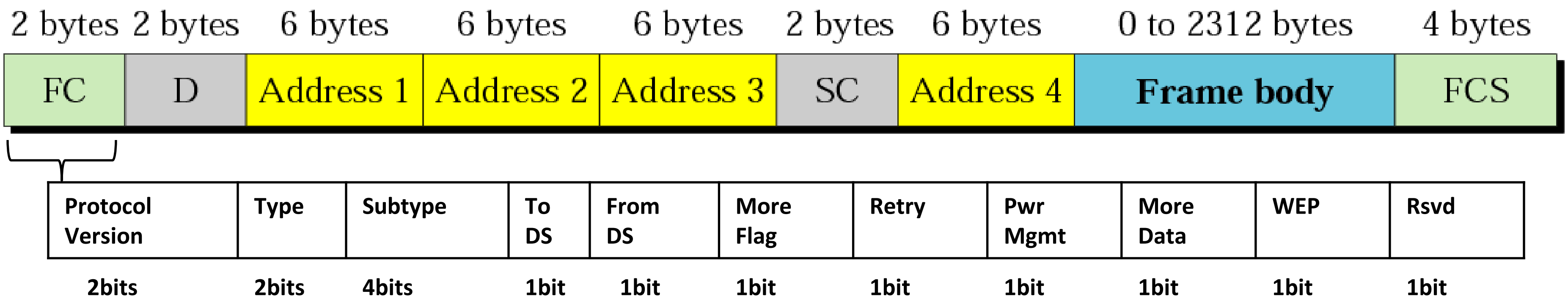
Protocol Version	Type	Subtype	To DS	From DS	More Flag	Retry	Pwr Mgmt	More Data	WEP	Rsvd

- Address1 – Address of next device.
- Address2 – Address of previous device.
- Address3 – Address of final destination station
- Address4 – Address of original source.

To DS	From DS	Add1	Add2	Add3	Add4
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	Sending AP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	Sending AP	Destination	Source

Wireless LANs – IEEE 802.11

Frame Format : Frame Control (FC)



2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	0 to 2312 bytes	4 bytes
FC	D	Address 1	Address 2	Address 3	SC	Address 4	**Frame body**	FCS

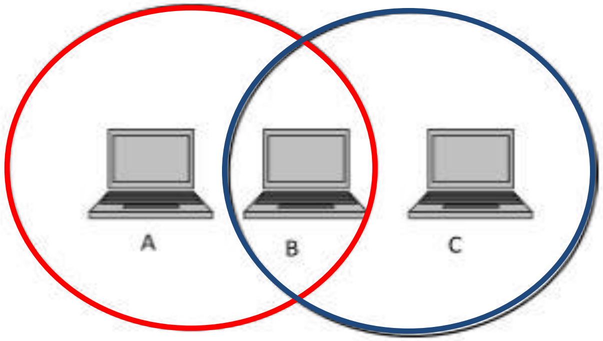
Protocol Version	Type	Subtype	To DS	From DS	More Flag	Retry	Pwr Mgmt	More Data	WEP	Rsvd
2bits	2bits	4bits	1bit	1bit	1bit	1bit	1bit	1bit	1bit	1bit

Field	**Explanation**
Version	Current version is 0
Type	Type information: management(00), control(01), data(10)
Subtype	Subtypes of types
To DS	
From DS	
More flag	Set to 1, means more fragmentation
Retry	Set to 1, means retransmitted frame
Pwr mgmt	Set to 1, means station is in power management mode
More data	Set to 1, means station has more data to send
WEP	Wired Equivalent privacy (encryption implemented)
RSVD	Reserved

Problems with Wireless LANs

- **Hidden station problem**
- **Exposed station problem**

Wireless LANs – IEEE 802.11 …Hidden Station Problem



- The transmission range of A reaches B but not C. Similarly, the range of **C reaches B** but not A. Also the range of B reaches both A and C.

- Now, the node A starts to send something to B and C doesn't receive this transmission.

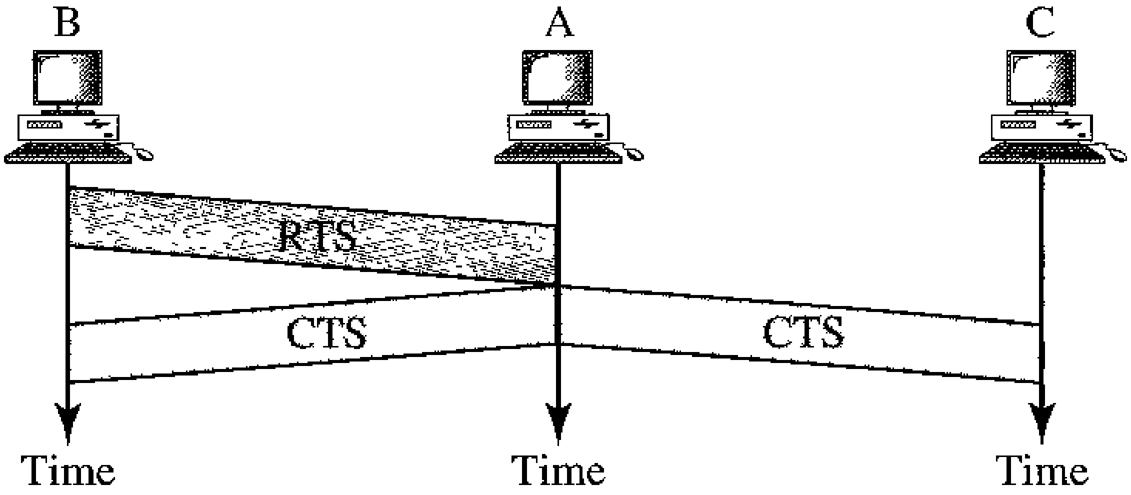
- Now C also wants to send data to B and senses the carrier. As it senses it to be free, it also starts sending to B.

- *Hidden terminal problem occurs when two nodes that are outside each other's range performs simultaneous transmission to a node that is within the range of each of them resulting in a collision*.

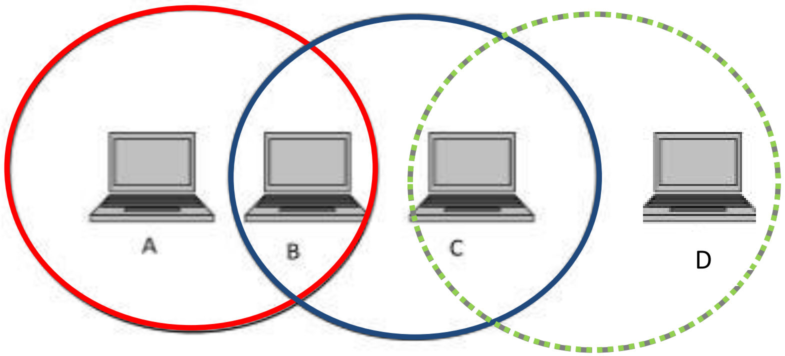
- That means the data from both parties A and C will be lost during the collision.

Wireless LANs – IEEE 802.11

- One of the solution is Handshaking (CSMS/CD).....
- RTS/CTS handshake mechanism was introduced to wireless MAC layers to eliminate the hidden terminal problem.
- However, this mechanism introduces a new problem termed the exposed terminal problem.
- We assume here an RTS/CTS exchange so that the issue of hidden terminal is addressed.



Wireless LANs – IEEE 802.11 .. Exposed station problem



- Here imagine a situation wherein the B node is currently sending some data to node A. Now the other node C which is right now free wants to send data to some node D which is outside the range of A and B.

- Now before starting transmission it senses the carrier and realizes that the carrier is busy (due to interference of B's signal). Hence, the C node postpones the transmission to D until it detects the medium to be idle. However such a wait was un-necessary as A was outside the interference range of C.

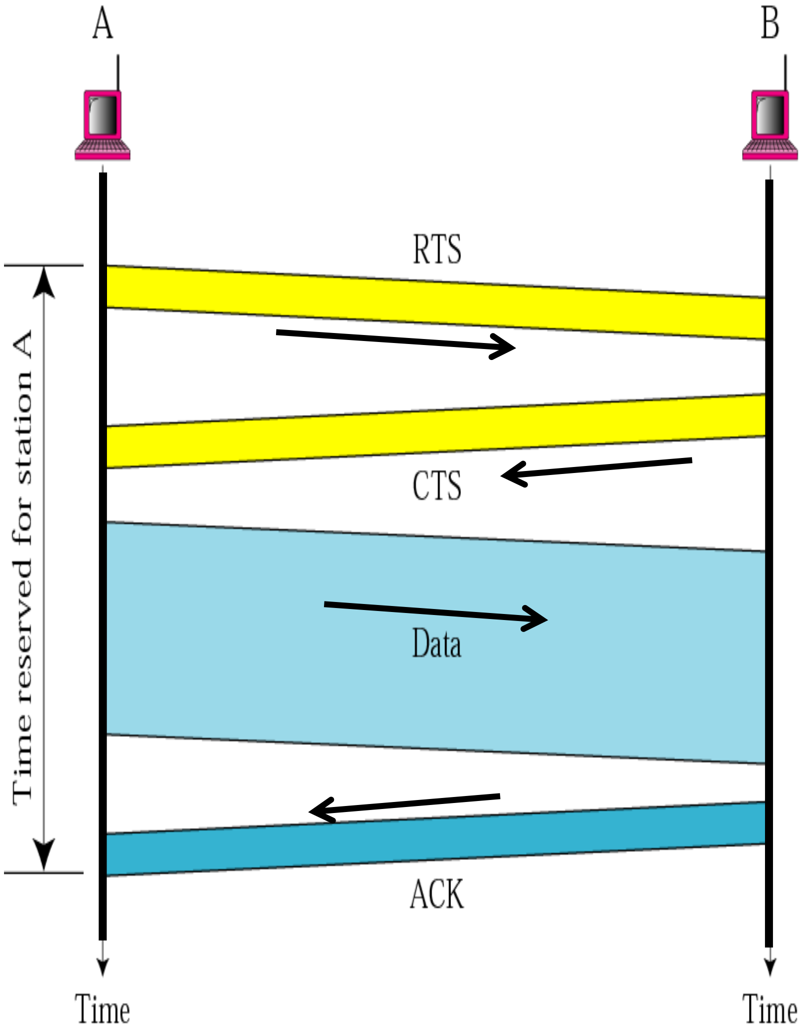
- *Exposed terminal problem occurs when the node is within the range of a node that is transmitting and it cannot be transmitted to any node.*

- Exposed node means denied channel access unnecessarily which ultimately results in under-utilization of bandwidth resources. It also results in wastage

Wireless LANs – IEEE 802.11

CSMA/CA

1. Before sending a frame, the source station senses the medium.
2. After the station is found to be idle, station waits for a period of time called the distributed interframe space (DIFS).
3. Then station sends control frame request to send (RTS).
4. After receiving RTS & waiting a period of a time called short interframe space (SIFS) ,destination station sends control frame called clear to send (CTS) to source to notify that it is ready to receive data.
5. Source station sends data after waiting an amount of time equal to SIFS.
6. Destination station sends an acknowledgment after waiting an amount of time equals to SIFS.



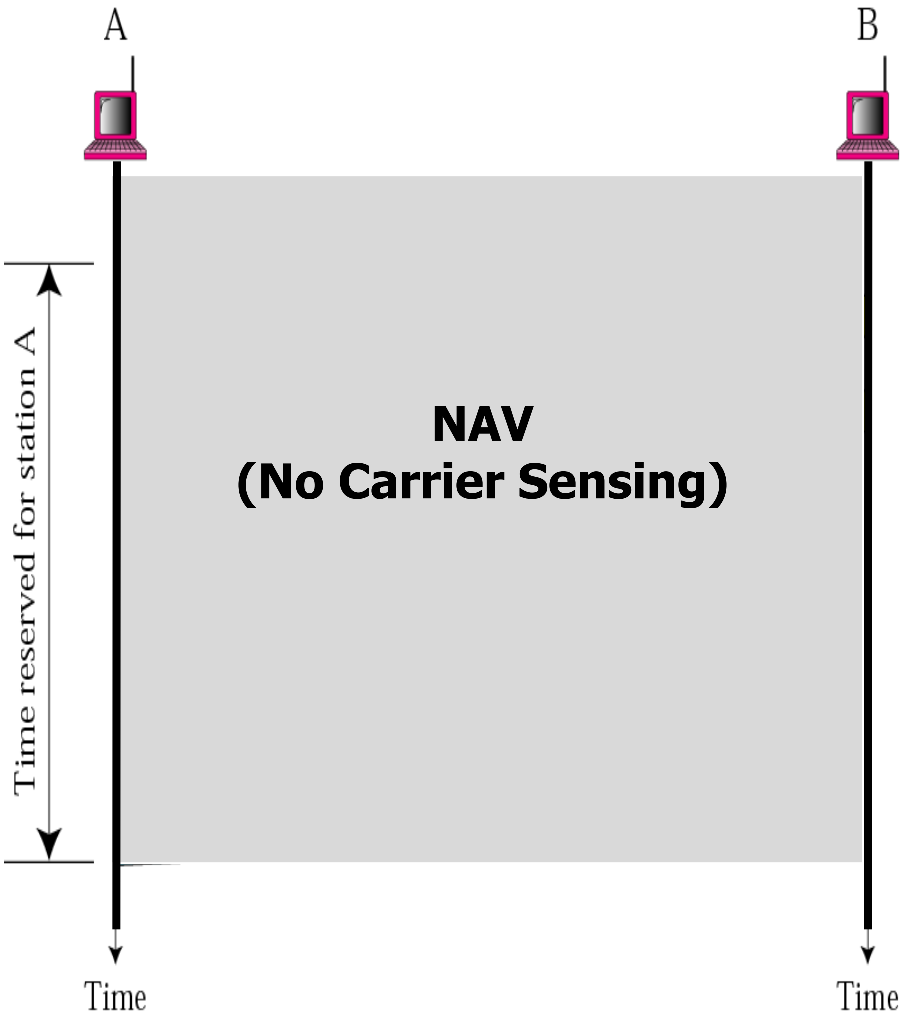
Wireless LANs – IEEE 802.11

CSMA/CA- NAV (Network Allocation Vector)

- RTS includes the duration of time that it needs to occupy the channel.

- The stations which are affected by this transmission create a timer called NAV.

- NAV shows how much time must pass before these stations are allowed to check the channel for idleness.



Wireless LANs

Bluetooth- IEEE 802.15

Wireless LANs – **Bluetooth- IEEE802.15**

- It is used to connect different devices(gadgets) of different functions such as telephone, notebooks , computers, cameras , printers etc.

- It is a an ad hoc network. i.e. network is formed spontaneously.

- Bluetooth LAN can't be large. If there are many gadgets that try to connect , there will be a chaos.

- Bluetooth technology is the implementation of a protocol *IEEE 802.15* standard. This standard defines a *Wireless Personal Area Network* (*W-PAN*) operable in an area the size of a room or a hall.

Wireless LANs – **Bluetooth- IEEE802.15**

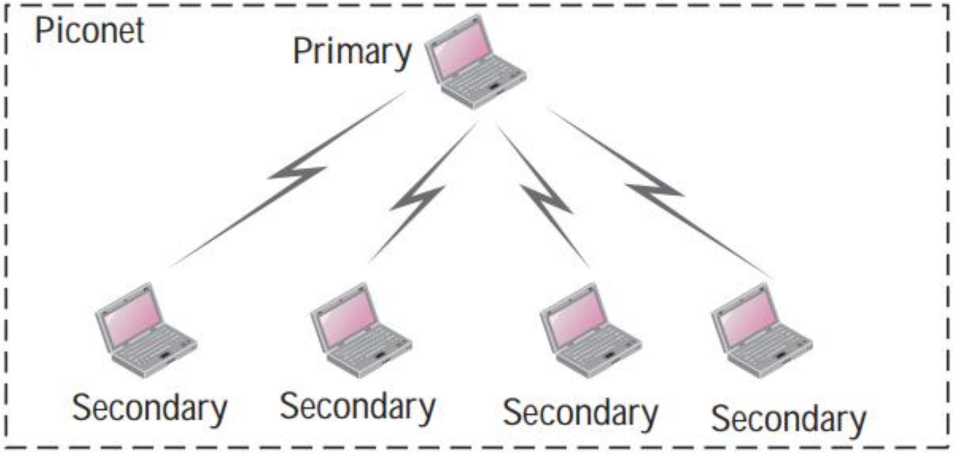
Architecture

- Piconet- Each piconet has *one Primary* and up to 7 simultaneous *secondaries*
  - *Primary* : device that initiates a data exchange.
  - *Secondary* : device that responds to the master
- Scatternet
  - Linking of multiple piconets through the *Primary* or *Secondary* devices.
  - Bluetooth devices have point-to-multipoint capability to engage in Scatternet communication.

Wireless LANs – **Bluetooth- IEEE802.15**

Architecture - Piconet

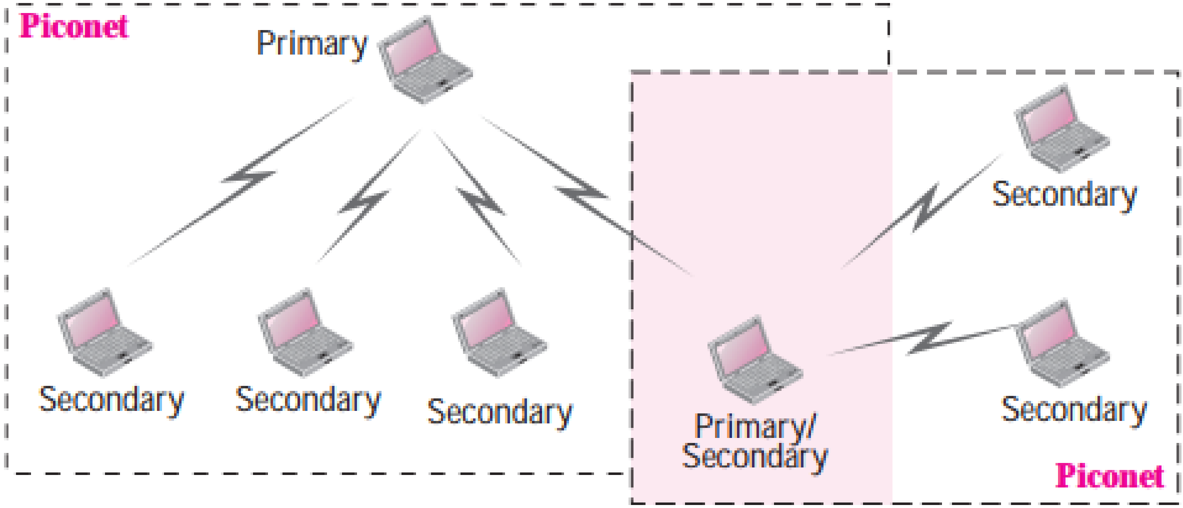
- A piconet can have up to eight stations, one of which is called the primary; the rest are called secondaries.
- All the secondary stations synchronize their clocks and hopping sequence with the primary.
- Note that a piconet can have only one primary station.
- The communication between the primary and the secondary can be one-to-one or one-to-many.
- Although a piconet can have a maximum of seven secondaries, an additional eight secondaries can be in the parked state.



Wireless LANs – **Bluetooth- IEEE802.15**

Architecture - Scatternet

- Piconets can be combined to form what is called a scatternet.
- A secondary station in one piconet can be the primary in another piconet.
- This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet



Point-to-Point WANs

A point-to-point WAN connects two remote devices using a line available from a public network such as a telephone network.

1. Traditional modem.(56k Modems) - traditional modems to upload data to the Internet and download data from the Internet

2. DSL (Digital subscriber line) technology -Developed by telephone companies to provide higher speed to access the internet. Different DSL technologies
   - ADSL – Asymmetric DSL
   - SDSL – Symmetric DSL
   - HDSL – High Speed DSL
   - VDSL - Very High Speed DSL

3. Cable modem
4. T-lines
5. SONET

Switched WANs

The backbone networks in the Internet can be switched WANs

A switched WAN is a wide area network that covers a large area (a state or a country) and provides access at several points to the users.

- Inside the network, there is a mesh of point-to-point networks that connects switches.
- The switches, multiple port connectors, allow the connection of several inputs and outputs.
- Switched WAN technology differs in many ways…..
  - Instead of star topology, switched are used to create multiple paths.
  - LAN is connectionless whereas Switched WAN is connection oriented.

Switched WANs

The backbone networks in the Internet can be switched WANs

- Before a sender can send a packet, a connection must be established between the sender and the receiver.

- After the connection is established, it is assigned an identifier (sometimes called a label) used during the transmission.

- The connection is formally terminated when the transmission is over.

- Switched WAN technologies are……
  - X.25
  - Frame Relay
  - ATM

Summary…..

- The technology of dominant wired LANs, Ethernet, including traditional, fast, gigabit, and ten-gigabit Ethernet. CSMA/CA protocol is used.

- The technology of wireless WANs,
  - IEEE 802.11 LANs –
  - Hidden station problem…solution is handshaking (CSMA/CD)
  - Expose station problem.
  - Bluetooth

- The technology of point-to-point WANs including,
  - 56K modems
  - DSL
  - Cable modem
  - T-lines
  - SONET

- The technology of switched WANs including,
  - X.25
  - Frame Relay
  - ATM