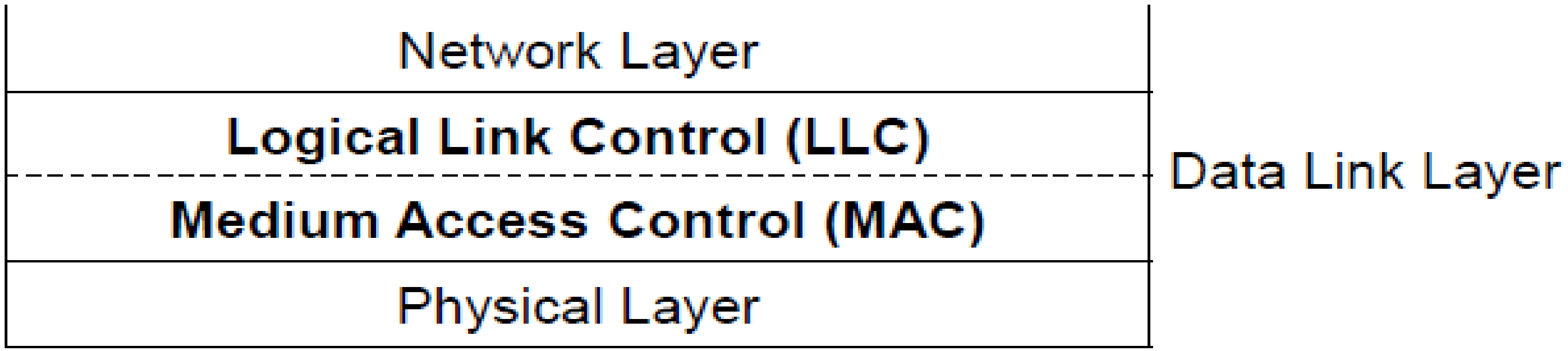
# The Medium Access Control Sublayer and Network Layer

# The Medium Access Control Sublayer

- In broadcast networks, several stations share a ***single communication channel.***
- The major issue in these networks is, **which station should transmit data at a given time.**
- This process of deciding the turn of different stations is known as **Channel Allocation**.
- To coordinate the access to the channel, multiple access protocols are required.
- All these protocols belong to the MAC sublayer.

Reference: http://www.eazynotes.com/



- Data Link layer is divided into two sublayers:
  - Logical Link Control (LLC)
  - Medium Access Control (MAC)
- **LCC** is responsible for **error control** & **flow control**.
- **MAC** is responsible for **multiple access resolutions**.

# The channel allocation problem

- In broadcast networks, single channel is shared by several stations.
- This channel can be allocated to *only one transmitting user at a time*.
- There are two different methods of channel allocations:
  - **Static Channel Allocation**
  - **Dynamic Channel Allocation**

# Static Channel Allocations

- In this method, **a single channel is divided among various users** either on the **basis of frequency** or on the **basis of time**.
- It either uses FDM (Frequency Division Multiplexing) or TDM (Time Division Multiplexing).
- In FDM, fixed frequency is assigned to each user, whereas, in TDM, fixed time slot is assigned to each user.

## ❖FDM

- In FDM, the **total bandwidth** is divided to a **set of frequency bands** that **do not overlap**.
- Each of these bands is a carrier of a different signal that is generated and modulated by one of the sending devices.
- *Example*: **Broadcast radio** and **television channels** are separated in the frequency spectrum using FDM

## ❖TDM

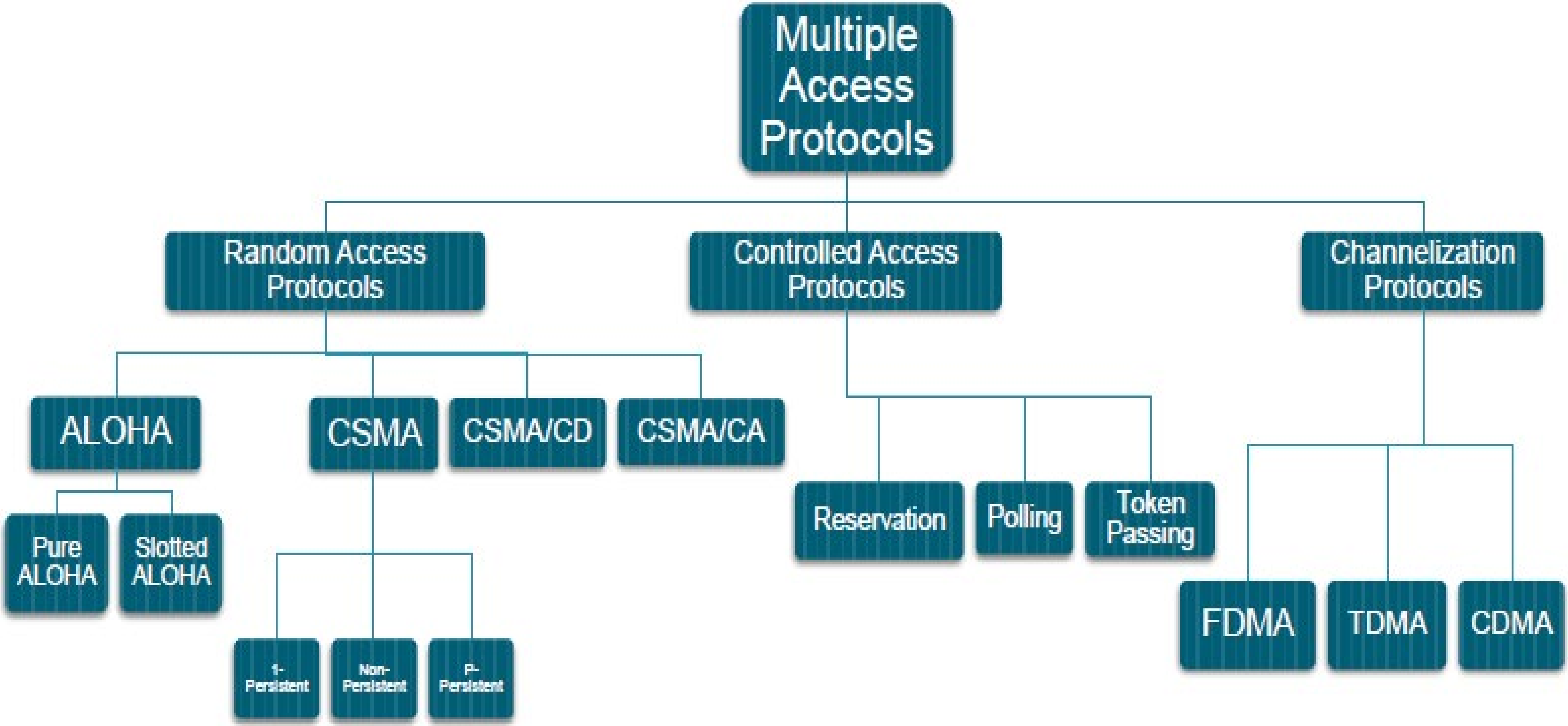
- In TDM, the **total time** available in the channel is divided **between several users**.
- Each user is allotted a particular a time interval called **time slot** or **time slice** during which the data is transmitted by that user.
- *Example:* It is widely used in **telephone** and **cellular networks**.

# Dynamic Channel Allocation

- In this method, **no user is assigned fixed frequency or fixed time slot**.
- All users are **dynamically assigned frequency or time slot**, *depending upon the requirements of the user.*

# Multiple Access Protocols

- Many protocols have been defined to handle the access to shared link.
- These protocols are organized in three different groups:
  - **Random Access Protocols**
  - **Controlled Access Protocols**
  - **Channelization Protocols**


Multiple Access Protocols
Random Access Protocols
Controlled Access Protocols
Channelization Protocols
ALOHA
CSMA
CSMA/CD
CSMA/CA
Pure ALOHA
Slotted ALOHA
1-Persistent
Non-Persistent
P-Persistent
Reservation
Polling
Token Passing
FDMA
TDMA
CDMA

# Random Access Protocols

- It is also called **Contention Method**.
- In this method, there is **no control station**.
- Any station can send the data.
- The station can make a decision on whether or not to send data. This decision depends on the state of the channel, i.e. channel is busy or idle.
- There is **no scheduled time for a stations to transmit**. They can transmit in random order.

- There is **no rule** *that decides which station should send next*.
- If two stations transmit at the same time, there is collision and the frames are lost.
- The various random access methods are:
  - **ALOHA**
  - **CSMA (Carrier Sense Multiple Access)**
  - **CSMA/CD (Carrier Sense Multiple Access with Collision Detection)**
  - **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)**

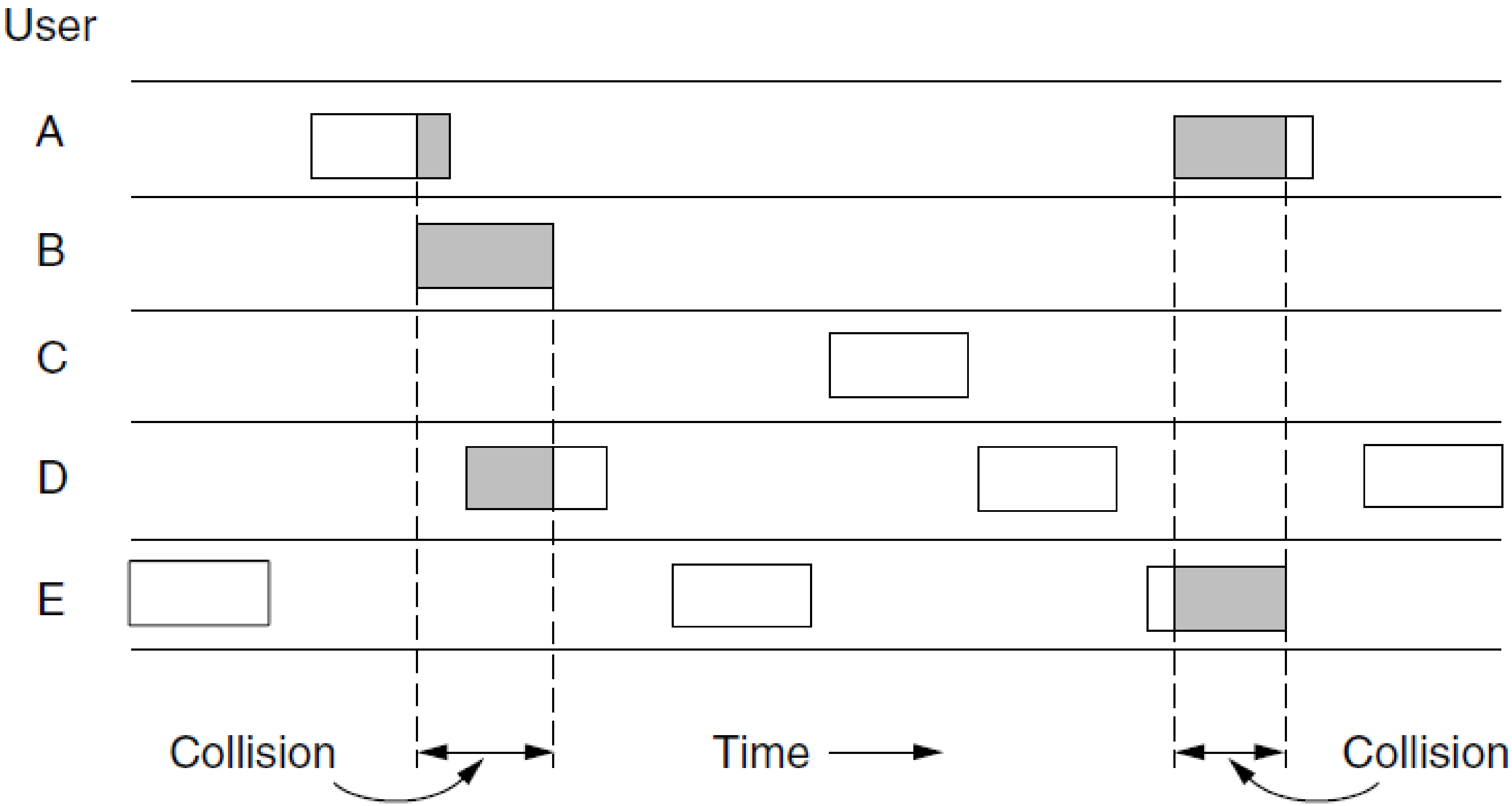
# ALOHA

- ALOHA was developed at **University of Hawaii** in early **1970s** by **Norman Abramson**.
- It was used for **ground based radio broadcasting**.
- In this method, **stations share a common channel**.
- When two stations transmit simultaneously, collision occurs and frames are lost.
- There are two different versions of ALOHA:
  - **Pure ALOHA**
  - **Slotted ALOHA**

# Pure ALOHA

- In pure ALOHA, stations transmit frames whenever they have data to send.
- When two stations transmit simultaneously, there is collision and frames are lost.
- In pure ALOHA, whenever any station transmits a frame, it expects an acknowledgement from the receiver.
- If ***acknowledgement is not received within specified time***, the station assumes that the frame has been lost.

- If the frame is lost, station waits for a random amount of time and **sends it again**.
- This waiting time must be random, otherwise, same frames will collide again and again.
- Whenever two frames try to occupy the channel at the same time, there will be collision and both the frames will be lost.
- If first bit of a new frame overlaps with the last bit of a frame almost finished, both frames will be lost and both will have to be retransmitted.

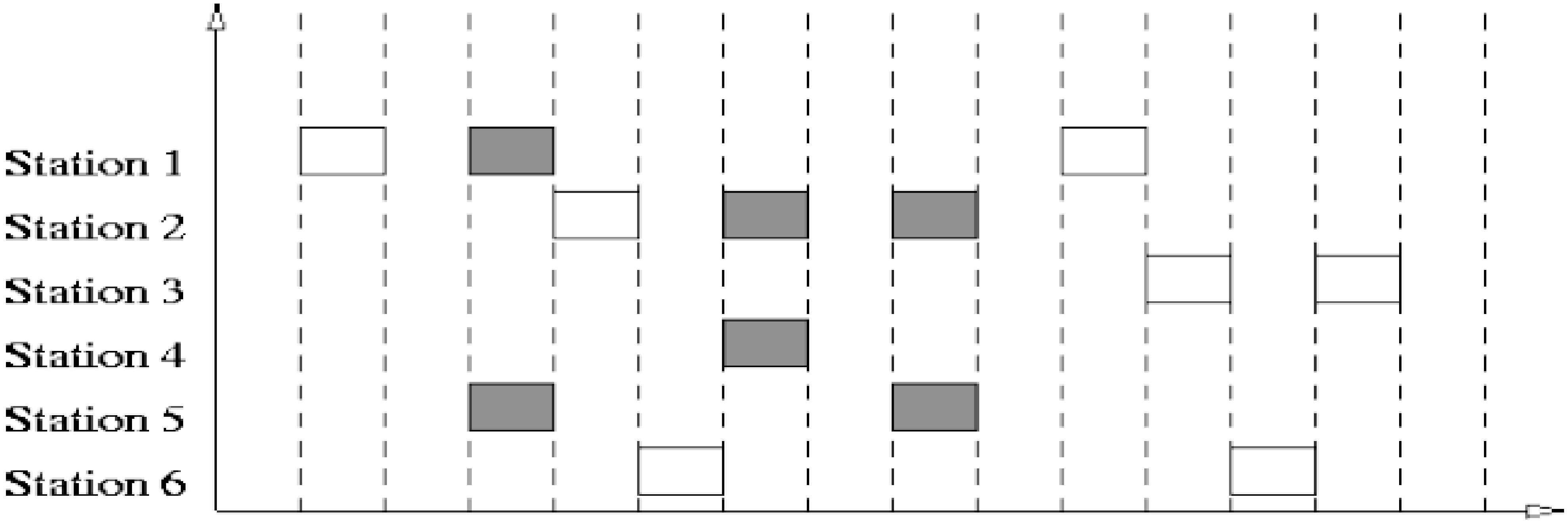


In pure ALOHA, frames are transmitted at completely arbitrary times.

# Slotted ALOHA

- Slotted ALOHA was *invented to improve the efficiency of pure ALOHA*.
- In slotted ALOHA, time of the channel is divided into intervals called **slots**.
- The station can *send a frame* **only at the beginning of the slot** and **only one frame is sent in each slot**.
- If any station is not able to place the frame onto the channel at the beginning of the slot, it has to wait until the next time slot.
- *There is still a* ***possibility of collision*** *if two stations try to send at the* ***beginning of the same time slot****.*

# Slotted ALOHA

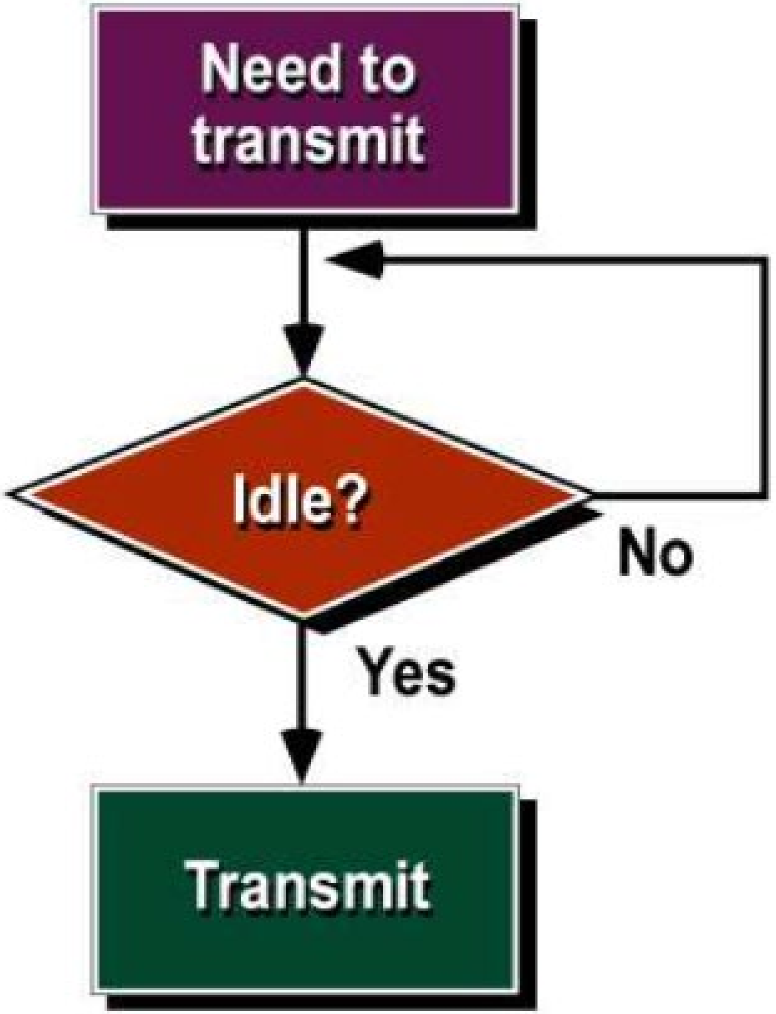


Time (shaded slots indicate collisions)

# Carrier Sense Multiple Access (CSMA)

- CSMA was developed to **overcome the problems of ALOHA** i.e. to minimize the chances of collision.
- CSMA is based on the principle of "**carrier sense**".
- The station sense the carrier or channel before transmitting a frame. It means the station checks ***whether the channel is*** **idle** or **busy**.
- The chances of collision reduces to a great extent if a station checks the channel before trying to use it.

# Carrier Sense Multiple Access (CSMA)



- The *chances of collision still exists* because of **propagation delay.**

- [**Propagation delay** In computer networks, **propagation delay** is the amount of time it takes for the head of the signal to travel from the sender to the receiver.
- **Transmission delay-** In a network based on packet switching, transmission delay is the amount of time required to push all the packet's bits into the wire.]

- The frame transmitted by one station **takes some time to reach the other station**.
- In the meantime, other station may sense the channel to be idle and transmit its frames. This results in the **collision**.
- There are three different types of CSMA protocols:
  - **1-Persistent CSMA**
  - **Non-Persistent CSMA**
  - **P-Persistent CSMA**

# 1-Persistent CSMA

- In this method, station that wants to transmit data, **continuously senses the channel to check whether he channel is idle or busy**.
- If the channel is busy, station **waits until it becomes idle**.
- When the station detects an idle channel, it immediately transmits the frame.
- This method has the highest chance of collision because two or more stations may find channel to be idle at the same time and transmit their frames.

# Non-Persistent CSMA

- A station that has a frame to send, senses the channel.
- If the channel is idle, it sends immediately.
- If the *channel is busy*, **it waits a random amount of time** and **then senses the channel again.**
- It reduces the chance of collision because the stations wait for a random amount of time .
- It is unlikely that two or more stations will wait for the same amount of time and will retransmit at the same time.

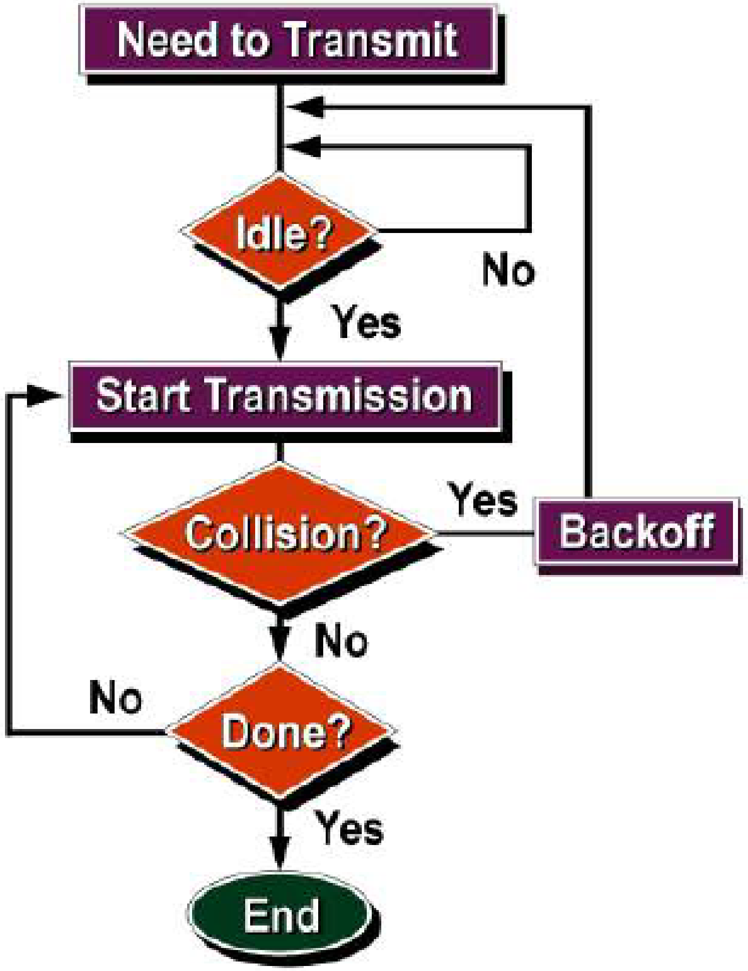
# P-Persistent CSMA

- In this method, **the channel has time slots** such that the time slot duration is equal to or greater than the maximum propagation delay time.
- When a station is ready to send, it senses the channel.
- If the channel is busy, station waits until next slot.
- If the channel is idle, it transmits the frame.
- *It reduces the chance of collision and improves the efficiency of the network.*

# CSMA with Collision Detection (CSMA/CD)

- In this protocol, **the station senses the channel** *before transmitting the frame*. If the channel is busy, the station waits.
- Additional feature in CSMA/CD is that the **stations can detect collisions.**
- The stations **abort** their transmission as soon as they detect collision.
- This feature is not present in CSMA. As in CSMA, the stations continue to transmit even though they find that collision has occurred.

# CSMA with Collision Detection (CSMA/CD)

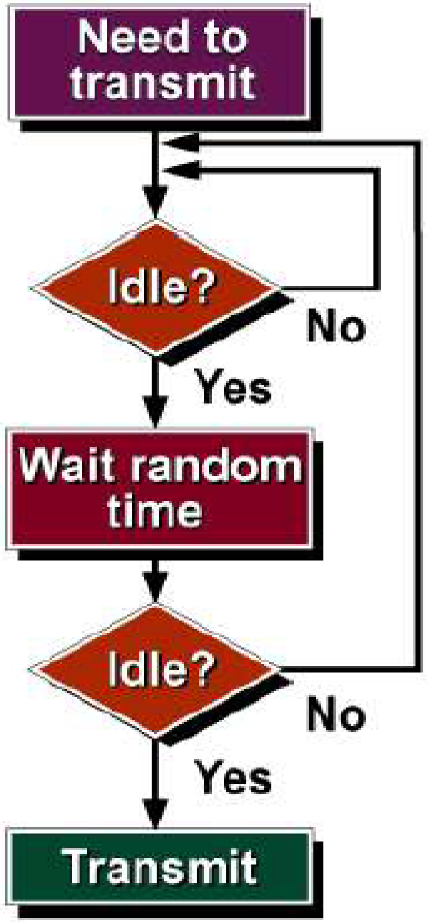


- In CSMA/CD, the station that sends its data on the channel, *continues to sense the channel even after data transmission.*
- If **collision is detected**, the station aborts its transmission and waits for a random amount of time & sends its data again.
- As soon as a collision is detected, the transmitting station release a ***jam*** **signal**.
- Jam signal alerts other stations. Stations are not supposed to transmit immediately after the collision has occurred.

# CSMA with Collision Avoidance (CSMA/CA)

- This protocol is used in **wireless networks** because *they cannot detect the collision.*
- So, *the only solution is* **collision avoidance**.
- It avoids the collision by using three basic techniques:
  - **Interframe Space**
  - **Contention Window**
  - **Acknowledgements**

# CSMA with Collision Avoidance (CSMA/CA)



# Ethernet

- Ethernet is a **set of technologies** and **protocols** that are used primarily in **LANs**.
- It was first standardized in 1980s by **IEEE 802.3** standard.
- IEEE 802.3 defines the physical layer and the medium access control (MAC) sub-layer of the data link layer for wired Ethernet networks.
- Ethernet is classified into two categories:
  - **Classic Ethernet**
  - **Switched Ethernet**

## ❑ Classic Ethernet

- It is the original form of Ethernet that provides ***data rates between 3 to 10 Mbps***.
- The varieties are commonly referred as **10BASE-X**.
  - Here, **10** is the maximum throughput, i.e. **10 Mbps**,
  - **BASE** denoted use of **baseband transmission** *(baseband describe how data is transmitted between two nodes. It transmits a single data at a time)*
  - **X** is the **type of medium used**. Most varieties of classic Ethernet have become obsolete in present communication scenario.

## ❑ Switched Ethernet

- It uses *switches to connect to the stations in the LAN*.
- It *replaces the repeaters* used in classic Ethernet and *allows full bandwidth utilization.*

# *IEEE 802.3 Popular Versions*

There are a number of versions of IEEE 802.3 protocol. The most popular ones are –

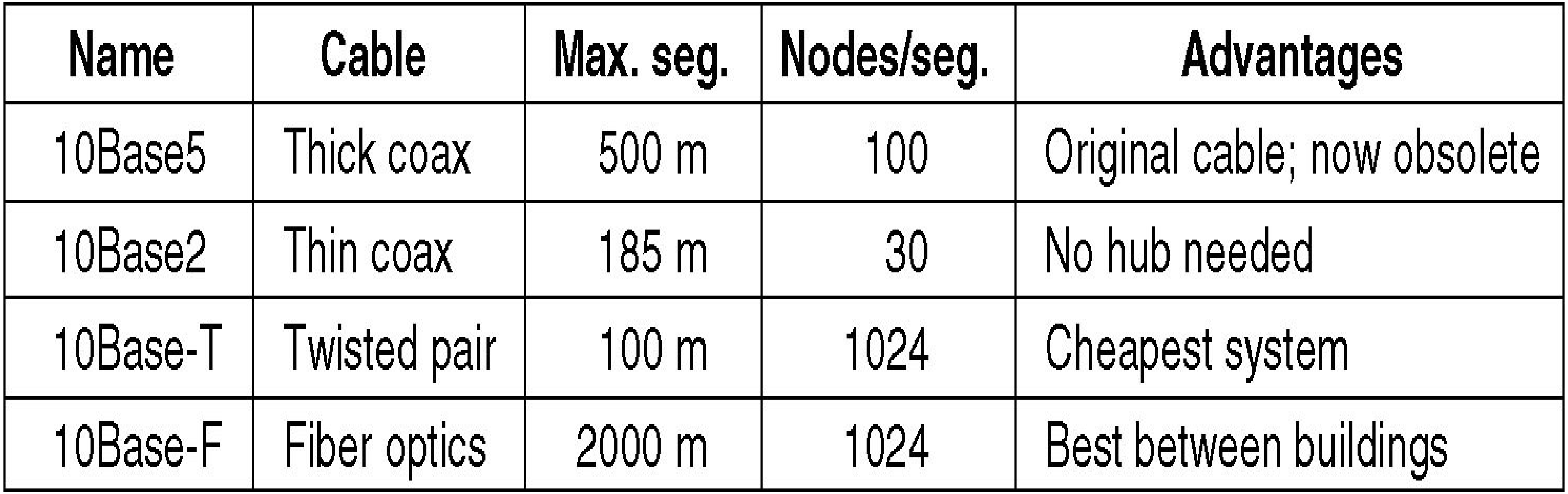
- **IEEE 802.3**:
  - This was the original standard given for **10BASE-5**.
  - It used a **thick single coaxial cable** into which a connection can be tapped by drilling into the cable to the core.
  - Here, **10 is the maximum throughput**, i.e. **10 Mbps**, **BASE** denoted use of **baseband transmission**, and **5** refers to the maximum **segment length** of **500m**.

- **IEEE 802.3a**:
  - This gave the standard for thin coax (**10BASE-2**), which is a thinner variety where the segments of coaxial cables are connected by BNC connectors.
  - The **2** refers to the maximum segment length of about **200m** (185m to be precise).

- **IEEE 802.3i**:
  - This gave the standard for twisted pair (**10BASE-T**) that uses unshielded twisted pair (UTP) copper wires as physical layer medium.
  - The further variations were given by **IEEE 802.3u for 100BASE-TX**, **100BASE-T4** and **100BASE-FX**.

- **IEEE 802.3j**:
  - This gave the standard for Ethernet over Fiber (**10BASE-F**).
  - It uses fiber optic cables as medium of transmission.

# *Ethernet Cabling*



| Name | Cable | Max. seg. | Nodes/seg. | Advantages |
|---|---|---|---|---|
| 10Base5 | Thick coax | 500 m | 100 | Original cable; now obsolete |
| 10Base2 | Thin coax | 185 m | 30 | No hub needed |
| 10Base-T | Twisted pair | 100 m | 1024 | Cheapest system |
| 10Base-F | Fiber optics | 2000 m | 1024 | Best between buildings |

The most common kinds of Ethernet cabling.

# Wireless LANs

- Wireless LANs (WLANs) are wireless computer networks that use high-frequency radio waves instead of cables for connecting the devices within a limited area forming LAN (Local Area Network).
- Users connected by wireless LANs can move around within this limited area such as home, school, campus, office building, railway platform, etc.
- Most WLANs are based upon the standard **IEEE 802.11** standard or WiFi.

# Types of WLAN Protocols

IEEE 802.11 or WiFi has a number of variations, the main among which are –

❖ **802.11a Protocol:**

- This protocol supports very high transmission speeds of 54Mbps.
- It has a high frequency of 5GHz range, due to which signals have difficulty in penetrating walls and other obstructions.

❖ **802.11b Protocol:**

- This protocol operates within the frequency range of 2.4GHz and supports 11Mbps speed.
- It facilitates path sharing and is less vulnerable to obstructions.
- It uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) with Ethernet protocol.

## ❖ 802.11g Protocol:

- This protocol combines the features of **802.11a** and **802.11b** protocols.
- It supports both the frequency ranges 5GHz (as in 802.11a standard) and 2.4GHz (as in 802.11b standard).
- 802.11g provides high speeds, varying signal range, and resilience to obstruction. However, it is more expensive for implementation.

## ❖ 802.11n Protocol:

- Popularly known as Wireless N, this is an upgraded version of 802.11g.
- It provides very high bandwidth up to 600Mbps and provides signal coverage.
- It uses **Multiple Input/Multiple Output (MIMO),** having multiple antennas at both the transmitter end and receiver ends.
- In case of signal obstructions, alternative routes are used. However, the implementation is highly expensive.

# Bluetooth

- It is a Wireless Personal Area Network (WPAN) technology and is used for exchanging data over smaller distances.
- This technology was invented by **Ericson** in **1994**.
- It operates in the unlicensed, industrial, scientific and medical (ISM) band at 2.4 GHz to 2.485 GHz.
- Bluetooth is also known as **IEEE 802.15** standard
- Maximum devices that can be connected at the same time are **7.**
- Bluetooth ranges up to 10 meters.
- It provides data rates up to 1 Mbps or 3 Mbps depending upon the version.

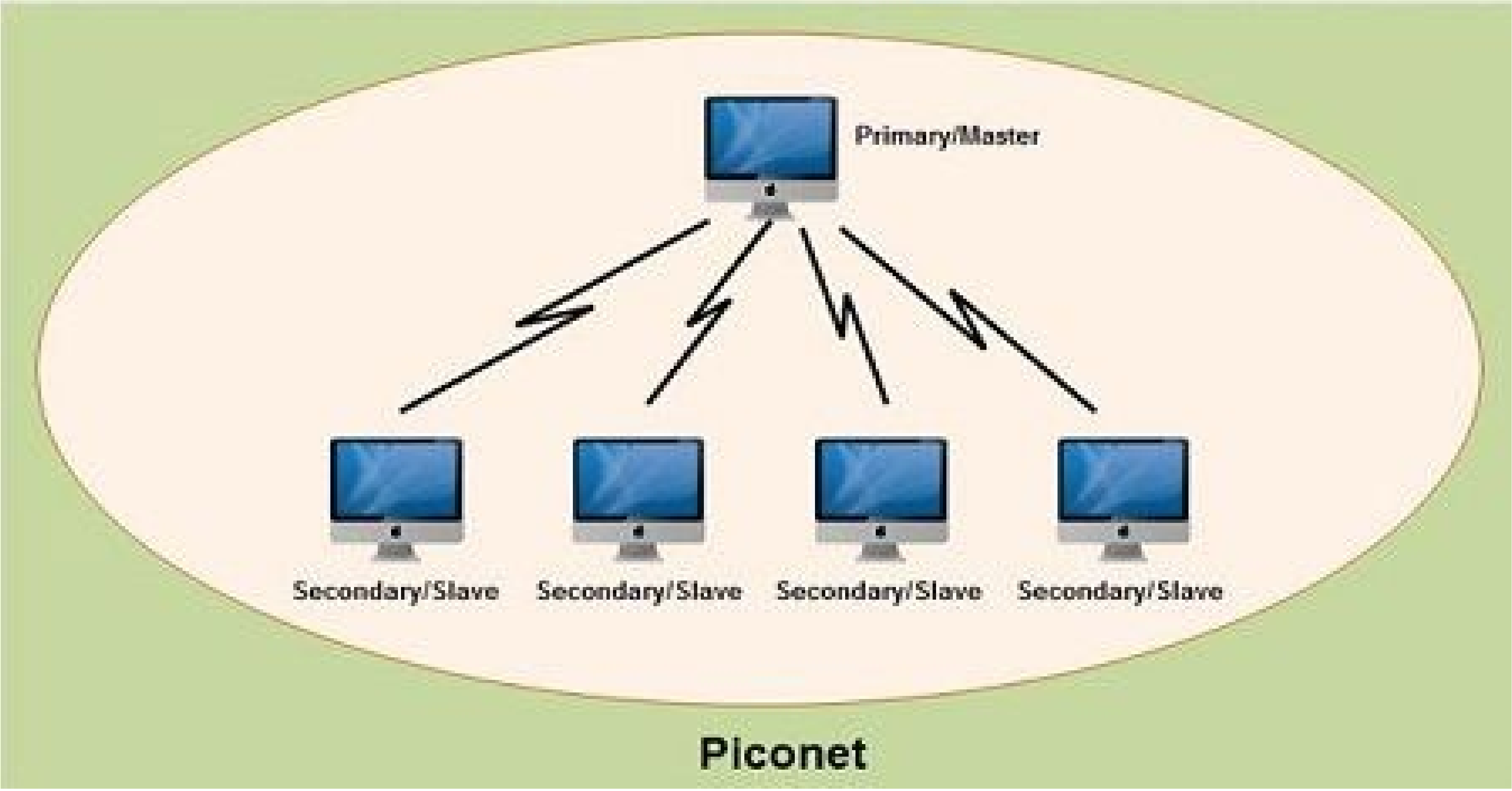
# Bluetooth Architecture

Bluetooth architecture defines two types of networks:

1. Piconet
2. Scatternet

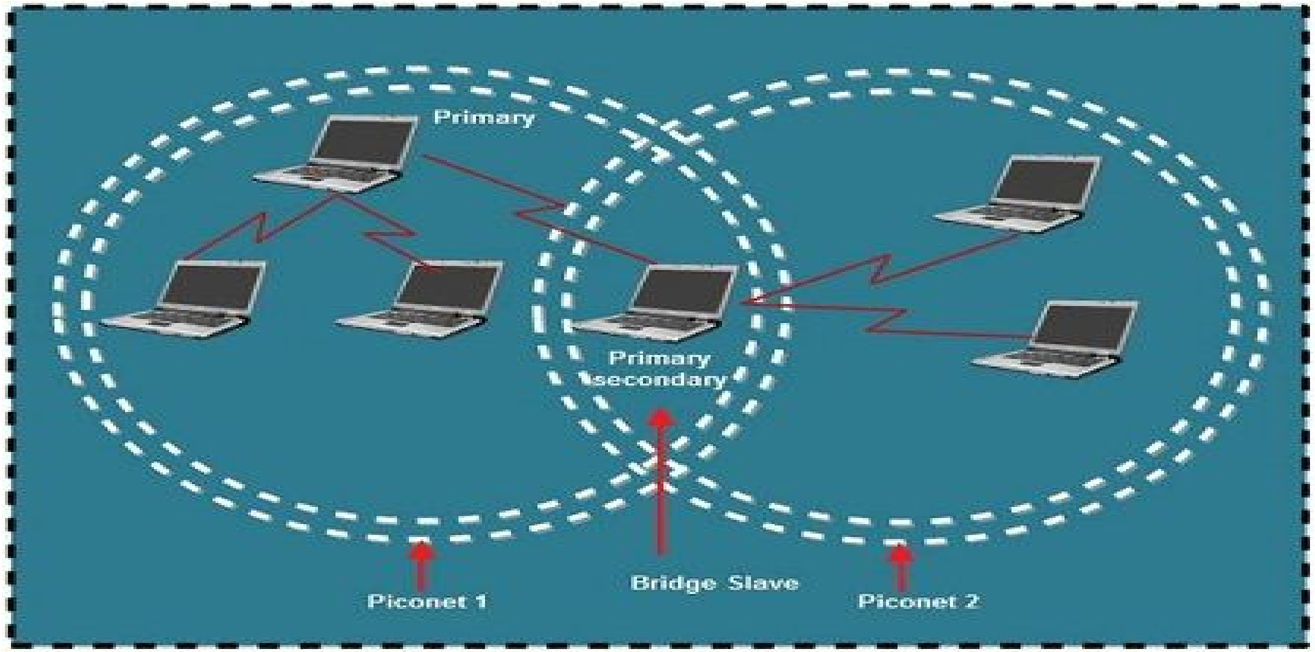
## ❖ Piconet

- Piconet is a Bluetooth network that consists of **one primary** (**master**) node and **seven active secondary** (**slave**) nodes.
- A **master node** is a node from which **data is being sent** and **slave node** is which the **data is received**.
- The communication between the primary and the secondary can be **one-to-one** or **one-to-many**.


Primary/Master
Secondary/Slave
Secondary/Slave
Secondary/Slave
Secondary/Slave
Piconet

## Scatternet

- Scatternet is formed by **combining various piconets.**
- A **slave in one piconet** can **act as a master** or **primary** in **other piconet**.
- Such a station or node can receive messages from the master in the first piconet and deliver the message to its slaves in other piconet where it is acting as master. This node is also called **bridge slave**.
- Thus a station can be a member of two piconets.
- A station cannot be a master in two piconets.



# RFID

- RFID stands for **Radio Frequency Identification**.
- As mentioned RFID devices use radio frequency waves to communicate.
- The common method used to **identify person/object** is to use serial number for each tags.
- RFID tag usually will have smaller micro-chip along with the antenna. RFID tags communicate with the reader with the help of antenna.
- The reader converts reflected or transmitted information from tags to useful digital information which can be further processed by software running in the computer.
- RFID works on different frequency bands, mainly in **UHF frequency** range.

**RFID Tag**- There are two types of tags

## ❑ Passive Tags:

- It **reflect the radio waves** transmitted by RFID reader and hence reader will come to know about location of the tags.
- Passive tag usually will have coverage of about 3-5 meters.
- Passive tags do not have internal power source/battery.
- Lower storage capacities (few bits to 1 KB)
- Usually Write-Once-Read-Many / Read-Only tags.
- Cost around 25 cents to few dollars

## ❑ Active Tags:

- It **send radio waves** to the RFID reader and hence will inform about its location.
- It will have coverage of about 100 meters.
- Active tag has power source
- Higher storage capacities (512 KB)
- Typically can be rewritten by RF Interrogators.
- Cost around 50 to 250 dollars.

# Datalink Layer Switching

- **Connectionless vs Connection Oriented**

- Circuit Switching
- Message Switching
- Packet Switching

# Network Layer

# Network Layer

- The Network Layer is the **third layer** of the OSI model.
- It handles the service requests from the transport layer and further forwards the service request to the data link layer.
- The network layer **translates the logical addresses into physical addresses.**
- It determines the route from the source to the destination and also **manages** the traffic problems such as **switching**, **routing** and **controls the congestion of data packets.**
- The main role of the network layer is to move the packets from sending host to the receiving host.

The main functions performed by the network layer are:

- **Addressing** – Maintains both the source and destination addresses at the frame header. The network layer performs addressing to find out the specific devices on the network.
- **Packetizing** – The network layer works on the conversion of packets those received from its upper layer. This feature is accomplished by Internet Protocol (IP).
- **Routing** – Being considered as the major functionality, **the network layer chooses the best path for data transmission from a source point to the destination.**
- **Internetworking** – Internetworking works to deliver a logical connection across multiple devices.

# Network Layer Design Issues

A number of design issues exist for the layer to layer approach of computer networks. Some of the main design issues are as follows:

- **Reliability**: Network channels and components may be unreliable, resulting in loss of bits while data transfer. So, an important design issue is to make sure that the information transferred is not distorted.

- **Scalability:** Networks are continuously evolving. The sizes are continually increasing leading to congestion. Also, when new technologies are applied to the added components, it may lead to incompatibility issues. Hence, the design should be done so that the networks are scalable and can accommodate such additions and alterations.

- **Addressing:** At a particular time, innumerable messages are being transferred between large numbers of computers. So, a naming or addressing system should exist so that **each layer can identify the sender and receivers of each message.**

- **Error Control:** Unreliable channels introduce a number of errors in the data streams that are communicated. So, the layers need to agree upon **common error detection** and **error correction methods** so as to protect data packets while they are transferred.

- **Flow Control:** If the rate at which data is produced by the sender is higher than the rate at which data is received by the receiver, there are chances of overflowing the receiver. So, a proper flow control mechanism needs to be implemented.

- **Resource Allocation:** Computer networks provide services in the form of network resources to the end users. The main design issue is to allocate and deallocate resources to processes. The allocation/deallocation should occur so that minimal interference among the hosts occurs and there is optimal usage of the resources.

- **Routing:** There may be multiple paths from the source to the destination. ***Routing involves choosing an optimal path among all possible paths,*** in terms of cost and time. There are several routing algorithms that are used in network systems.

- **Security:** A major factor of data communication is to defend it against threats like eavesdropping and surreptitious alteration of messages. So, there should be adequate mechanisms **to prevent unauthorized access to data through authentication and cryptography.**

# Routing Algorithms

- In order to transfer the packets from source to the destination, the network layer must determine the **best route through which packets can be transmitted.**
- The **routing protocol** is a routing algorithm that provides the best path from the source to the destination. The best path is the path that has the "**least-cost path**" from source to the destination.
- **Routing** is the process of forwarding the packets from source to the destination but the best route to send the packets is determined by the routing algorithm.

# *Classification of a Routing algorithm*

- The Routing algorithm is divided into two categories:
  - Adaptive Routing algorithm
  - Non-adaptive Routing algorithm

## ❑ Adaptive Algorithms:

- These are the algorithms which change their routing decisions whenever network topology or traffic load changes.
- The changes in routing decisions are reflected in the topology as well as traffic of the network. Also known as **dynamic routing**, these make use of dynamic information such as *current topology*, *load, delay*, etc. to select routes.

Further these are classified as follows:

- **Isolated:**
  - In this method each, **node makes its routing decisions using the information it has** without seeking information from other nodes.
  - The sending nodes doesn’t have information about status of particular link.
  - **Disadvantage** is that packet may be sent through a congested network which may result in delay.
  - Examples: Hot potato routing, backward learning.
- **Centralized:**
  - In this method, a centralized node has entire information about the network and **makes all the routing decisions.**
  - **Advantage** of this is only one node is required to keep the information of entire network
  - **Disadvantage** is that if central node goes down the entire network is done.
- **Distributed:**
  - In this method, the node receives information from its neighbors and **then takes the decision about routing the packets.**
  - **Disadvantage** is that the packet may be delayed if there is change in between interval in which it receives information and sends packet.

## ❑ Non-Adaptive Algorithms:

- These are the algorithms which do not change their routing decisions once they have been selected. This is also known as **static routing** as route to be taken is computed in advance and downloaded to routers when router is booted.

Further these are classified as follows:

### ➢Flooding:

- This adapts the technique in which every incoming packet is sent on every outgoing line except from which it arrived.
- **One problem** with this is that packets may go in **loop** and as a result of which a node may receive **duplicate packets**. These problems can be overcome with the help of sequence numbers, hop count and spanning tree.

### ➢Random Walk:

- In this method, packets are sent host by host or node by node to one of its neighbors randomly.
- This is highly **robust** method which is usually implemented by sending packets onto the link which is least queued.