Data Link Layer-2
07.10.2019

BLM 3051 Veri İletişimi
(Data Communication)

Tech. Assist. Kübra ADALI
Assoc. Prof. Dr. Veli Hakkoymaz

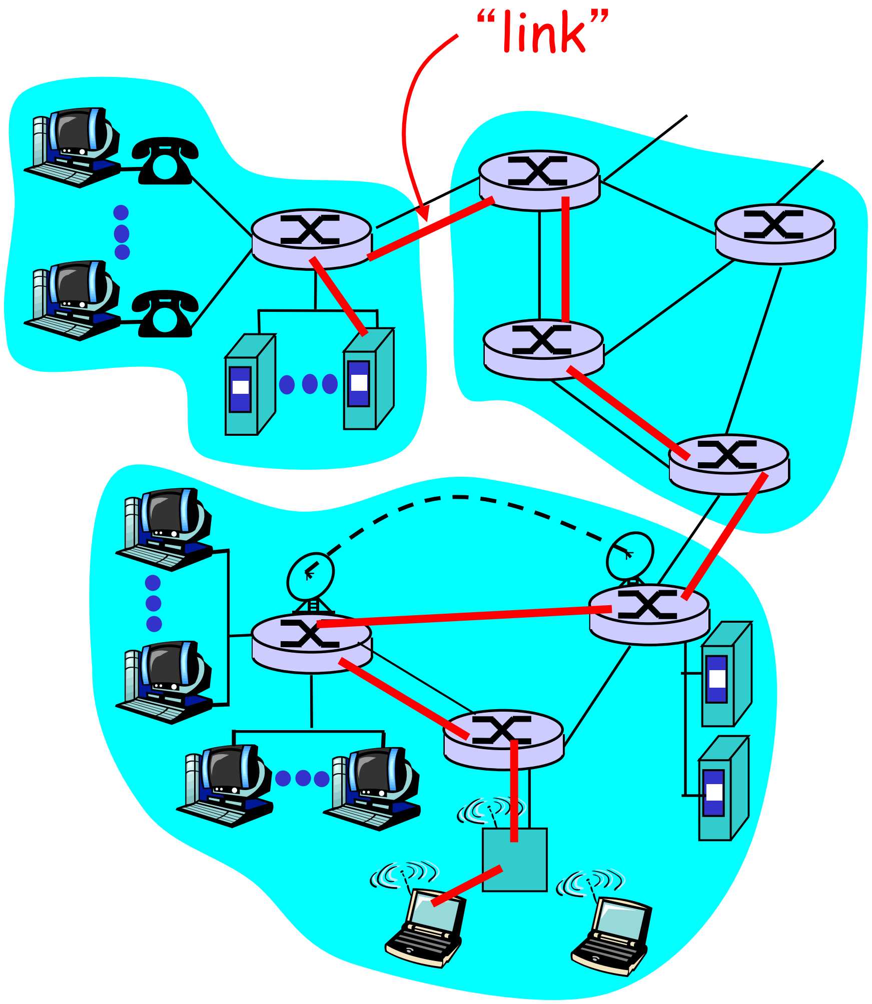
References:

- *Computer Networks*, Andrew Tanenbaum, Pearson, 5th Edition,2010.
- *Computer Networking, A Top-Down Approach Featuring the Internet*, James F.Kurose, Keith W.Ross, Pearson-Addison Wesley, 6th Edition, 2012.

.**BLG 337 Slides** from İTÜ prepared by Assoc. Prof.Dr. Berk CANBERK

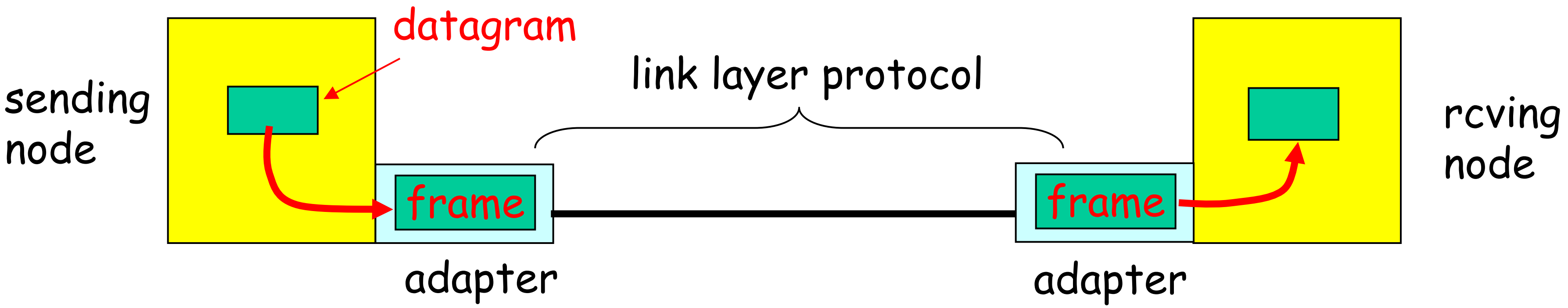
Data Link Layer

- ✓ This layer has the responsibility of the transfer of the "datagrams" from one node to another node.
- ✓ To remind the terminologies:
  - hosts and routers are **nodes**
  - communication channels that connect adjacent nodes along communication path are **links**
    - wired links
    - wireless links
  - layer-2 packet is called **frame**.



Sending- Receiving Side

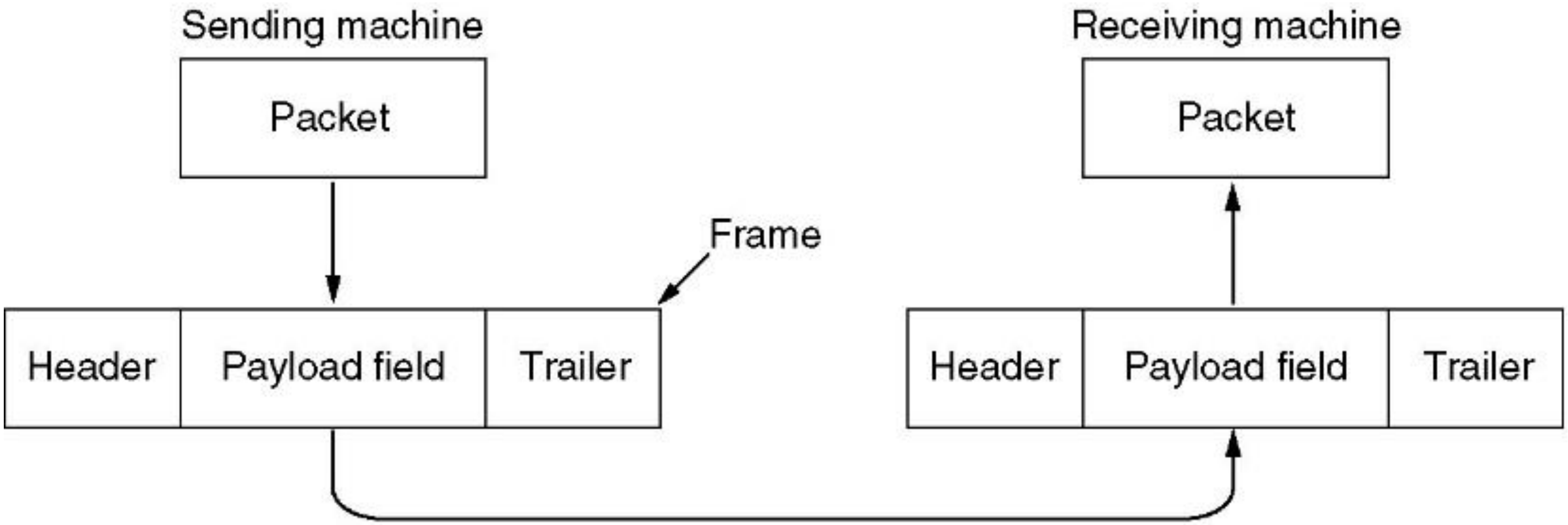
- link layer implemented in “adaptor” ,network interface card(NIC)



- **sending side:**
  - encapsulates datagram in a frame
  - adds error checking bits, flow control, etc.
- **receiving side**
  - looks for errors, flow control, etc
  - extracts datagram, passes to rcving node

- adapter is semi-autonomous link & physical layers

Actions taken to packets in Data Link Layer



Data Link Layer Functions

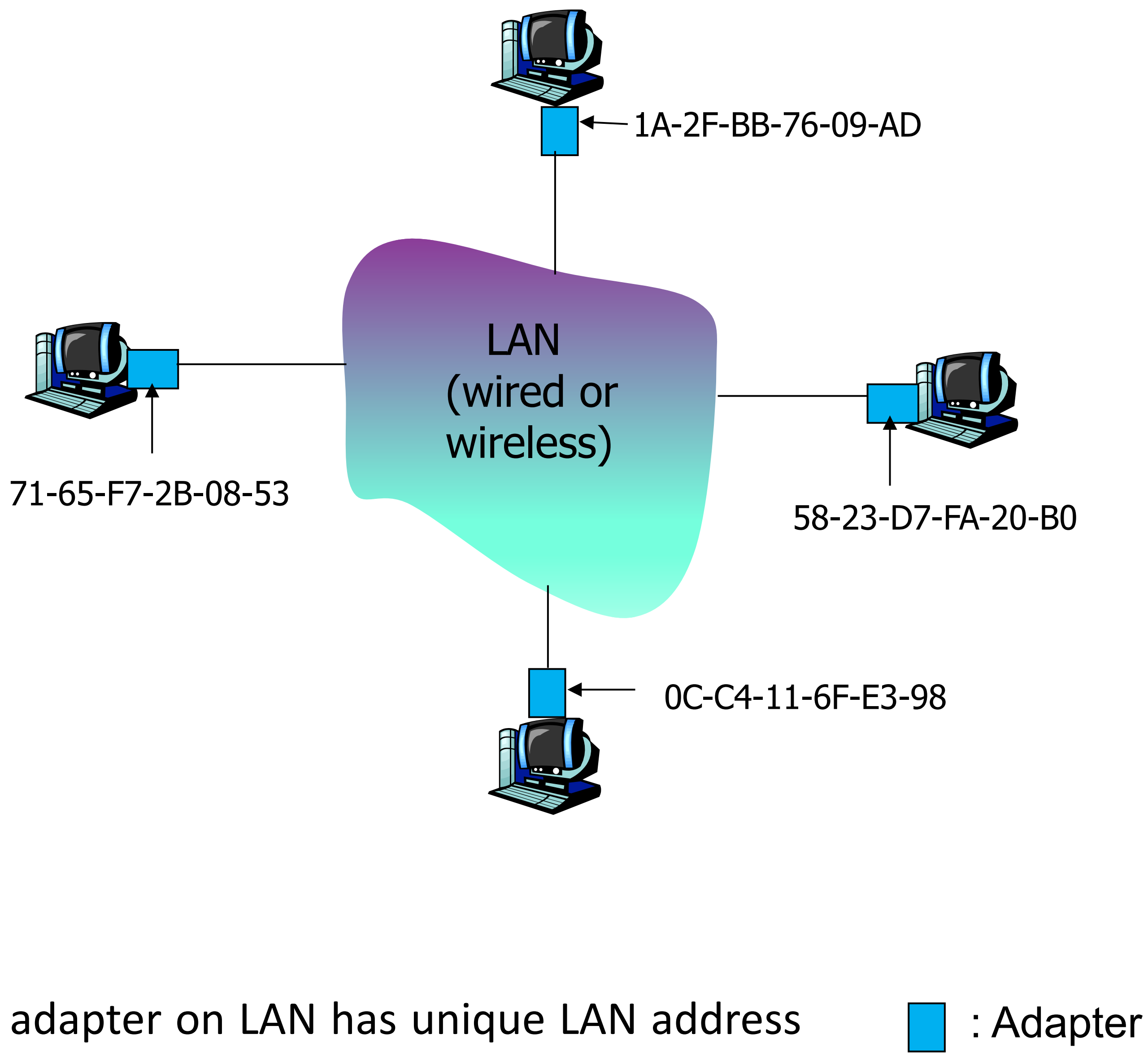
- Data Link layer provides some services to the upper “Network” Layer:
  - Medium Access Control
  - Framing
  - Error Control(Detection & Correction): Dealing with transmission errors
  - Flow Control: Slow receivers not swamped by fast senders

Data Link Control

Data Link Layer Functions

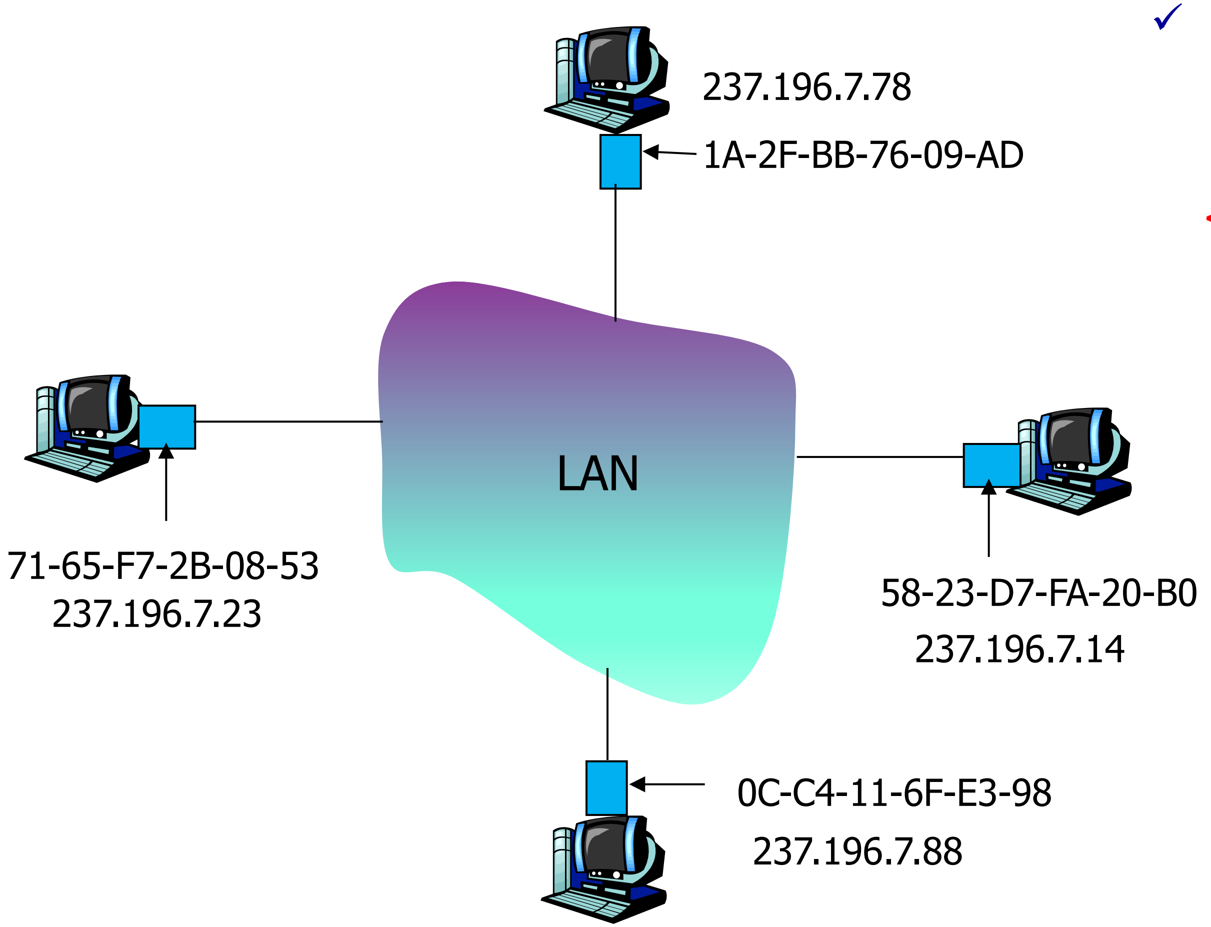
- ✓ **Medium Access Control**
  - Less oftenly used on low bit error link (fiber, some twisted pair)
  - wireless links: high error rates
- ✓ **Framing**
  - encapsulate datagram into frame, adding header, trailer
  - “MAC” addresses used in frame headers to identify source, destination
  - channel access if shared medium
- ✓ **Error Control(Detection & Correction):**
  - **Error Detection**
    - errors caused by signal attenuation, noise.
    - Receiver does this mission (warns sender in order to retransmission or drops frame.)
  - **Error Correction**
    - receiver finds *and corrects* bit error(s) without another retransmission
- ✓ **Flow Control**
  - Adaptation of data rates between adjacent sending and receiving nodes

Address Management in LANs



✓ Each adapter on LAN has unique LAN address

Address Resolution Protocol



- ✓ Each IP node on LAN has **ARP table**
- ✓ **ARP Table:** IP/MAC address mappings for some LAN nodes

< IP address; MAC address; TTL>

  - TTL (Time To Live): the forget time of the related address mapping (typically 20 min)

ARP Scenerios *(Same LAN):*

- ✓ A wants to send datagram to B, and B's MAC address not in A's ARP table.

- ✓ A broadcasts ARP query packet, containing B's IP address:
  - B's (Dest) MAC address = FF-FF-FF-FF-FF-FF

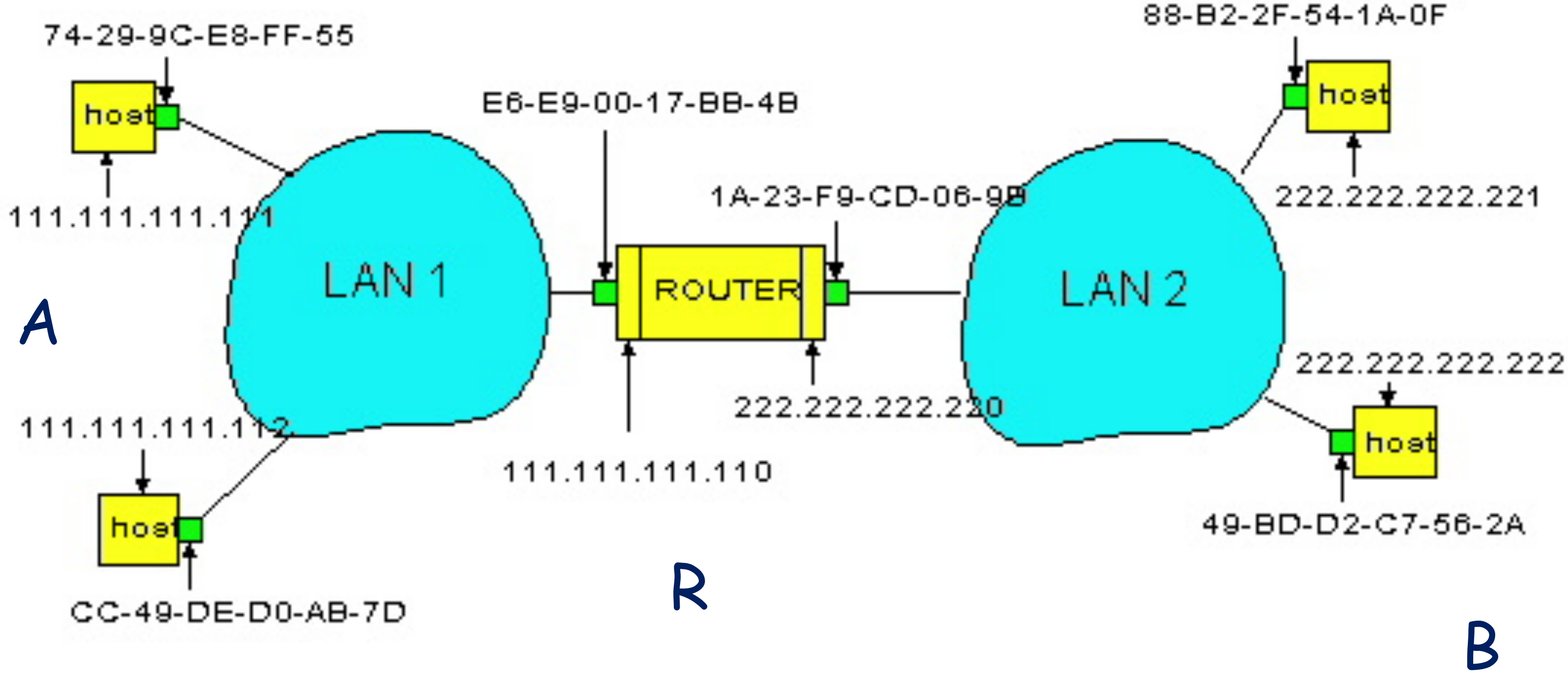
- ✓ All hosts on LAN receive ARP query packet.

- ✓ B receives ARP packet, replies to A with its (B's) MAC address

- ✓ A saves IP-to-MAC address pair in its ARP table until information becomes old.
  - information times out (goes away) unless refreshed

ARP Scenerios *(Different LAN):*

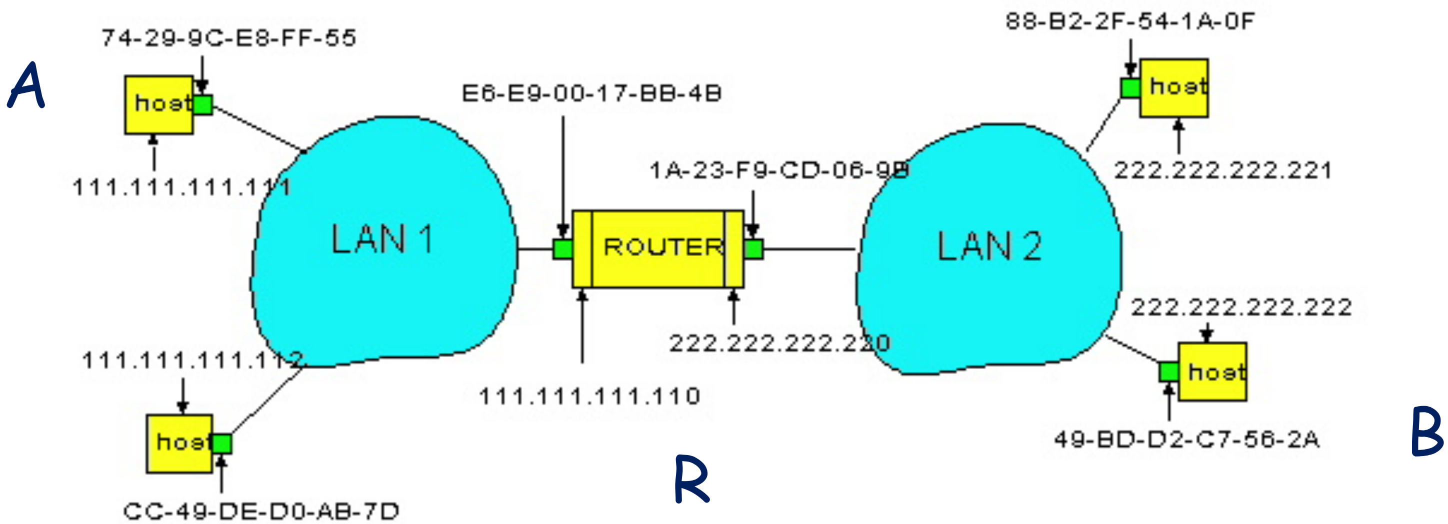
- ✓ A wants to send datagram to B, A knows B's IP address.



- ✓ There are two ARP tables in router, one for LAN1, and one for LAN2.
- ✓ A broadcasts ARP query packet, containing B's IP address, B's IP address does not exist in LAN1, so, A changes to different LAN mode.

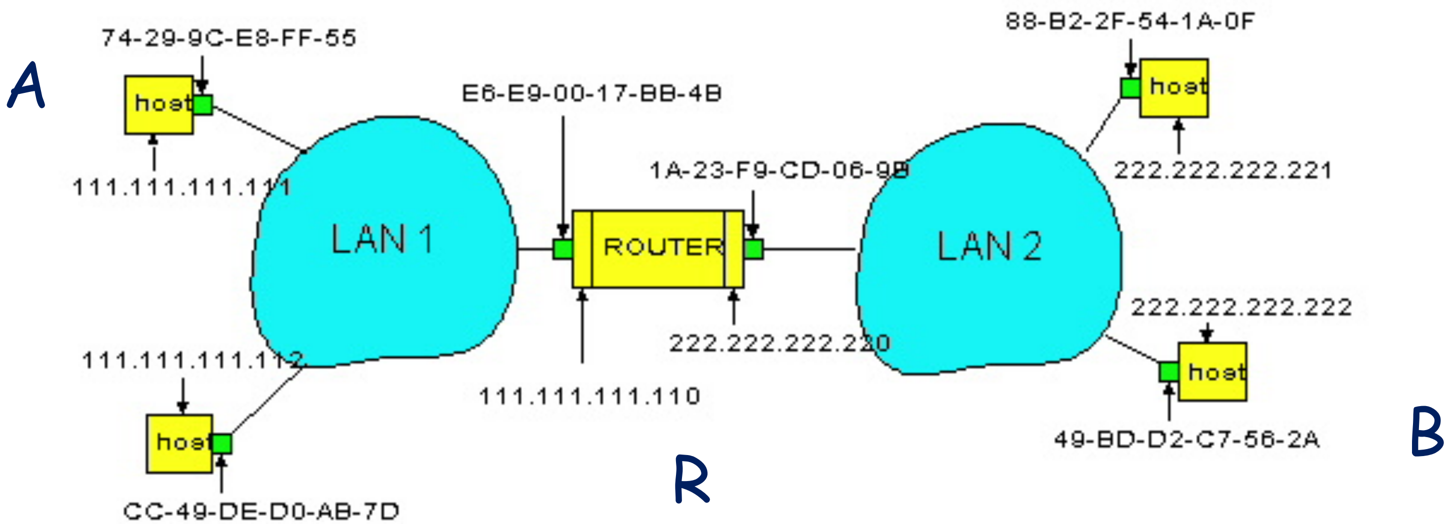
ARP Scenerios *(Different LAN):*

- ✓ A looks for the router in its table, the ip address: 111.111.111.110.
- ✓ If exists, it finds the MAC address of the router: E6-E9-00-17-BB-4B
- ✓ A creates datagram with ip addresses(A and B).
- ✓ A creates frame with source and dest mac addresses.(A and router).
- ✓ A's adapter sends the frame.
- ✓ Router's adapter receives the frame.

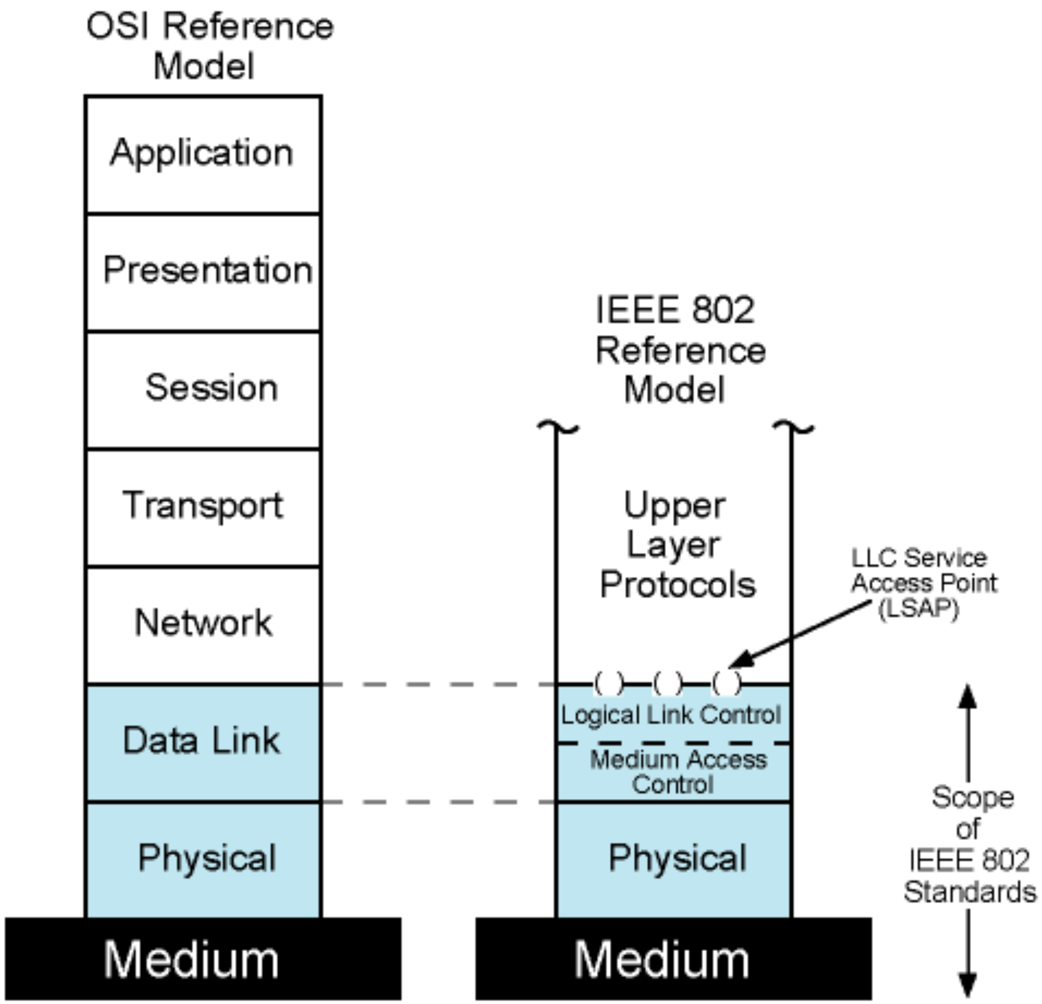


ARP Scenerios *(Different LAN):*

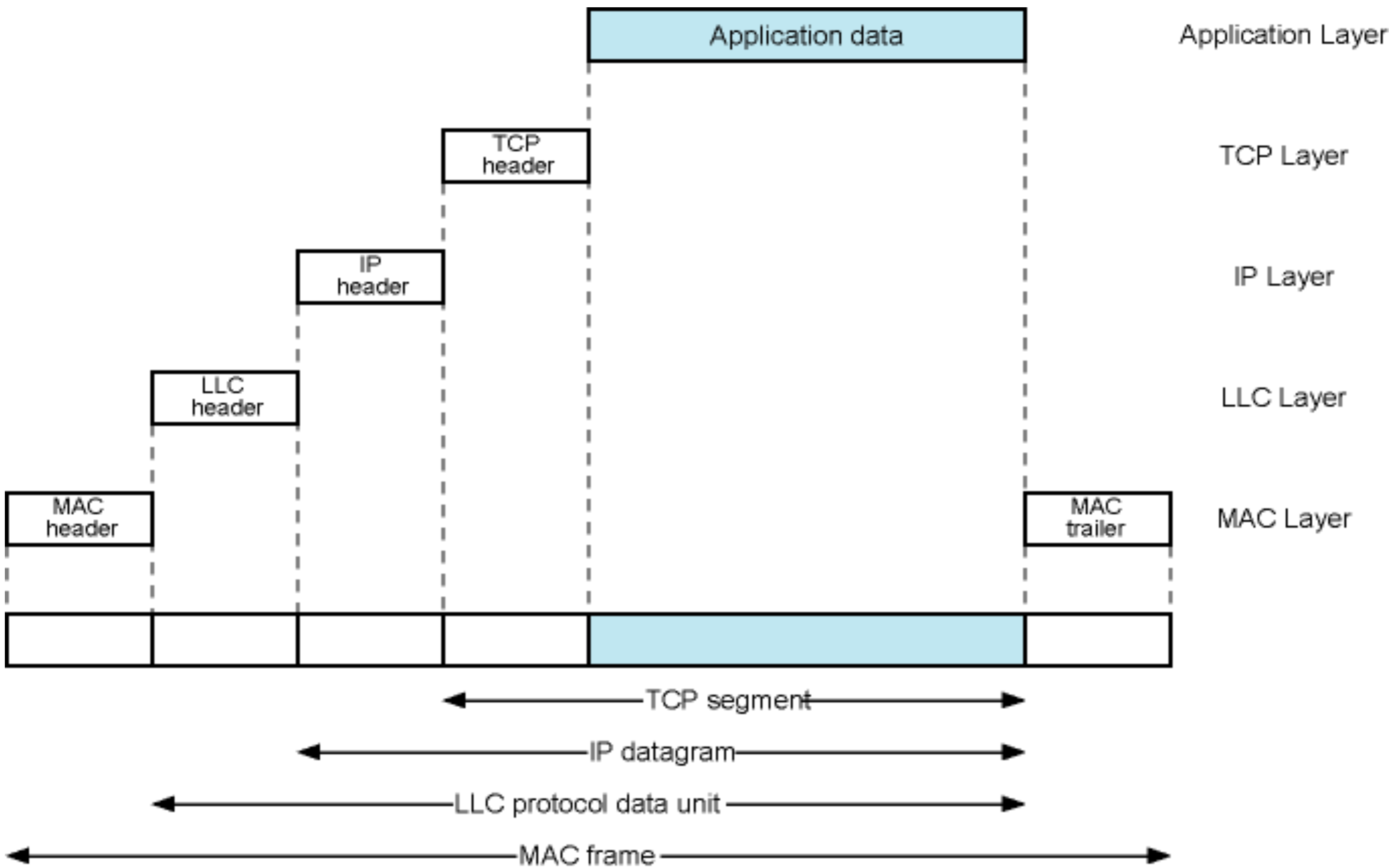
- ✓ Router's adapter receives the frame.
- ✓ Router removes the mac addresses from frame and gets the IP address from the datagram.
- ✓ By using the IP address of B and ARP, router finds B's Mac address.
- ✓ Router creates the frame by using MAC addresses A and B and datagram and sends to B.



IEEE 802 Protocol Layer Organization & OSI Reference Model

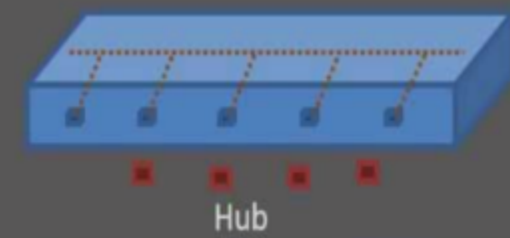


Protocols and Packet Organization

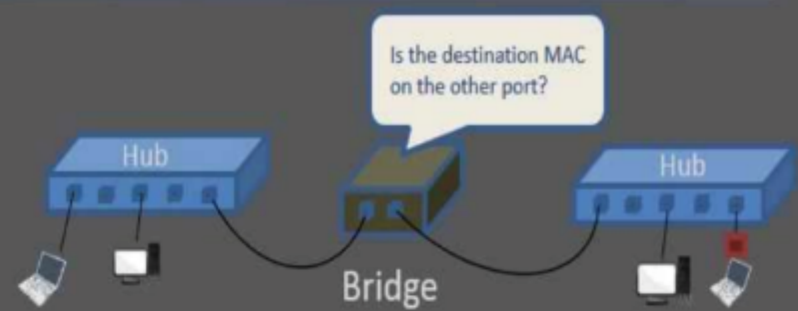


Connection Points: Hubs, Bridge,Switch

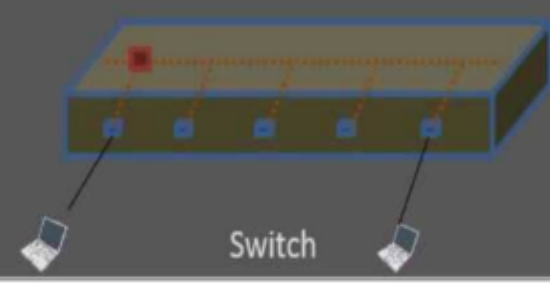
- Hub is really a *repeater*
- A message sent by one host is sent to all other hosts.
- One of the simplest ways to create a network.



- Bridge is a more intelligent form of Hub
- Packets are processed based on MAC address (Hardware Address) inside the incoming packet.



- Switch = Bridge with more than 2 Ports
- More scalable and practical
  - Bridge is not very useful for end-computing devices
  - Hubs cannot handle large data traffic



Connection Points: Hubs, Bridge,Switch

Hub

Switch

Bridge

One Channel, Multiple Users…

- Allocate a single broadcast channel among multiple users : "Channel Allocation"
  - Static Channel Allocation
    - TDM, FDM
  - Dynamic Channel Allocation
    - Multiple Access Protocols: ALOHA, CSMA etc.

Dynamic Channel Allocation: “**Assumptions**”

- ✓ Station Model:
  - N independent stations (computers, phones, PDAs etc.) each pf which sends frames with a mean rate of l frames/sec.
- ✓ Single Channel:
  - A single channel is used for all communication.
- ✓ Collision Assumption:
  - If two frames are given to the channel at the same time, they crash in time and the resulting signal is garbled → **COLLISION**.
  - All stations can detect collision and collided frame must be resent.
- ✓ Continuous Time:
  - Frame transmission can start at any time, no clock intervals are used.

Dynamic Channel Allocation: "**Assumptions**"

- Slotted Time:
  - Frame transmission should start at the beginning of each time slot, the clock intervals are called slots.
- Carrier Sense:
  - Stations can know if the channel is busy or not.
  - If busy, no station will send any until it goes idle.
- No Carries Sense:
  - Stations don't have the ability to detect the channel is busy or not.
  - They determine if the transmission was successful or not.

Classification of MAC Protocols

We have three channel partitioning MAC protocols:

- ✓ channel partitioning
  - ○ divide channel into smaller parts such as (time slots, frequency, code)
  - ○ allocate piece to node for personal use
- ✓ random access
  - ○ channel not divided
  - ○ allow collisions and "recover" from collisions
- ✓ taking turns
  - ○ Each node takes turn
  - ○ Nodes with more to send can take longer turns

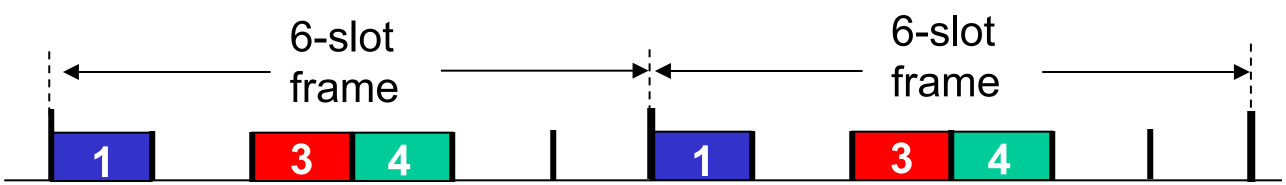
Channel Partitioning MAC Protocols

We have three channel partitioning MAC protocols:

- ✓ TDMA:Time Division Multiple Access
- ✓ FDMA: Frequency Division Multiple Access
- ✓ CDMA: Code Division Multiple Access

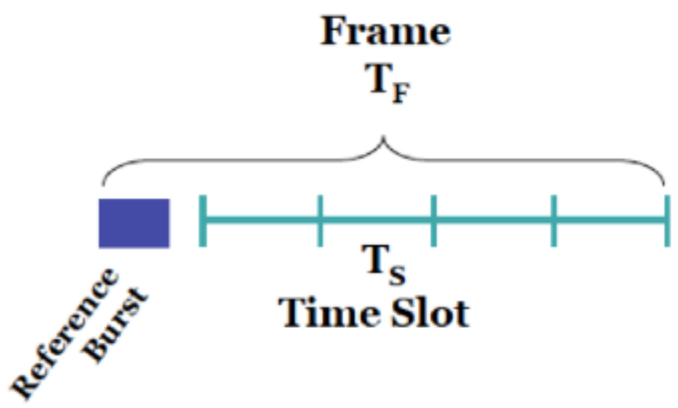
TDMA : Time Division Multiple Access

- ✓ Users access to channel in time slots
- ✓ Each user have the right to use fixed length slot (length = packet trans time) in each round.
- ✓ Each user has to use fixed slot, different users have to transmit their packet in different time slots.
- ✓ While transmitting, the current user occupies the whole frequency bandwidth.
- ✓ unused slots go idle
  - ○ example: 6-station LAN, 1,3,4 have pkt, slots 2,5,6 idle

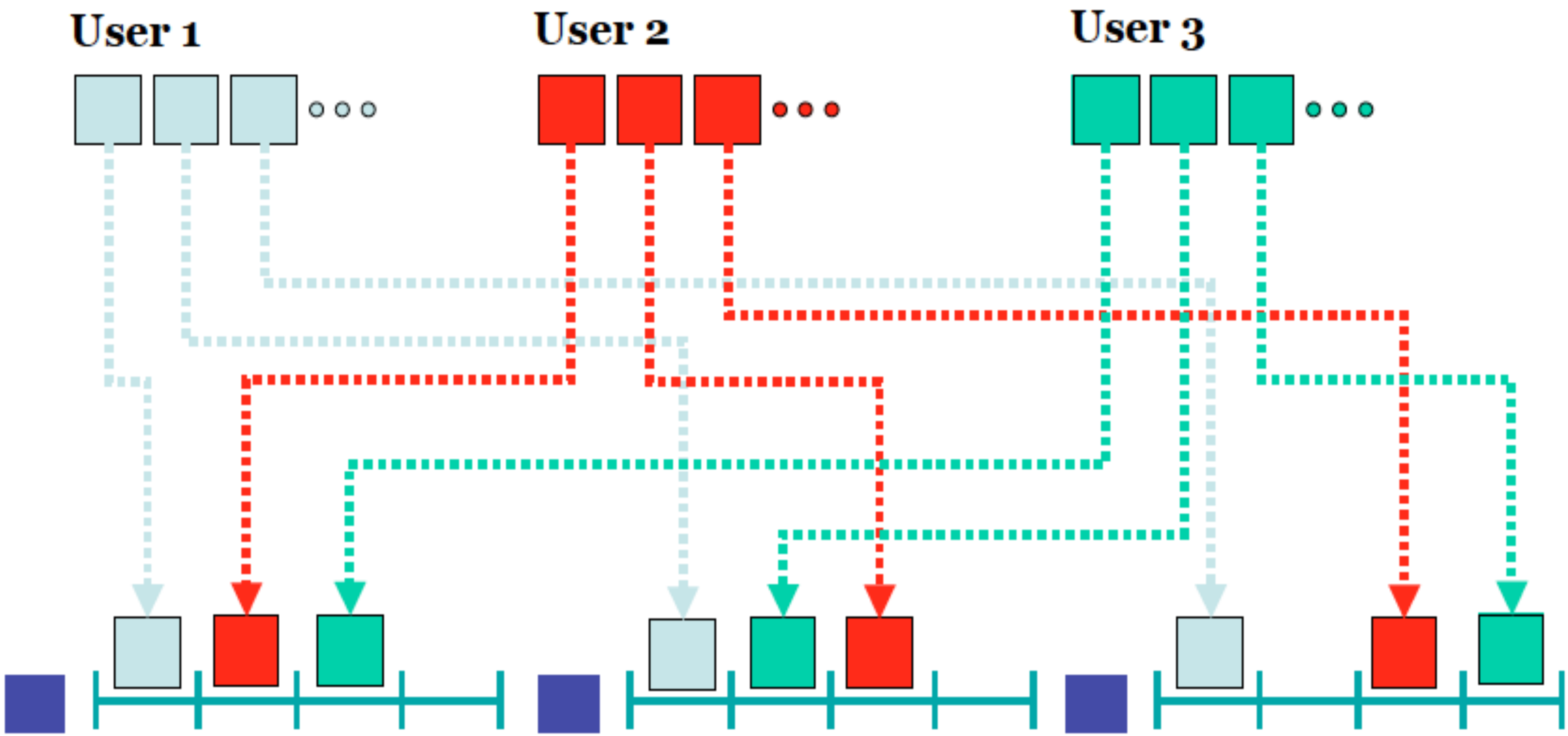


TDMA : Time Division Multiple Access

- ✓ TDMA uses centralized control node for transmitting the reference burst in order to define a frame and its amount.
- ✓ This frame is divided into time slots, and each user is assigned to a time slot.



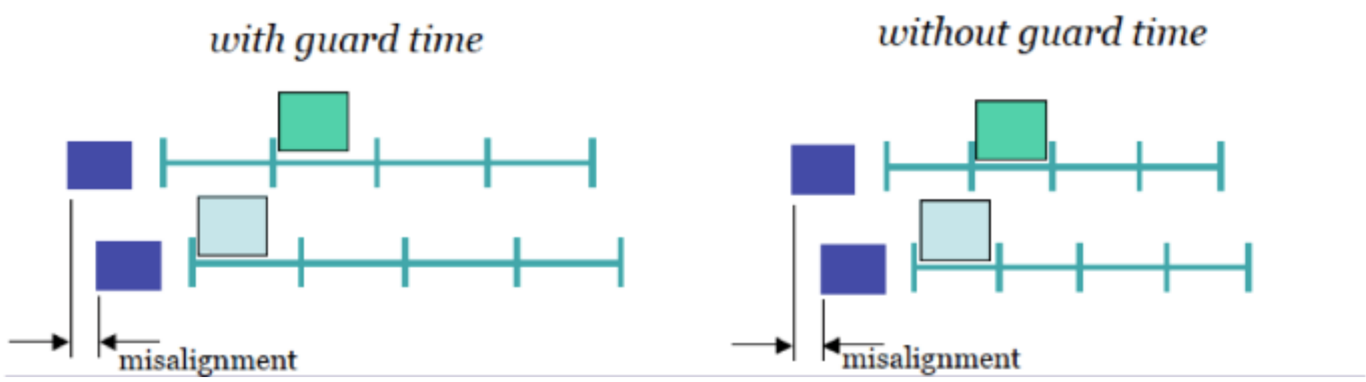
TDMA : Time Division Multiple Access



TDMA : Time Division Multiple Access

✓ Guard Time

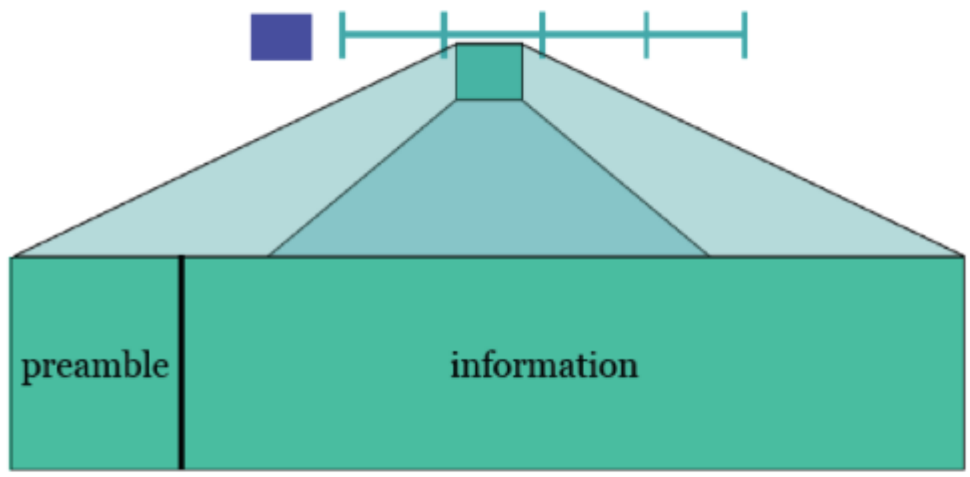
- In some cases, there occurs some delays between users, and these delays causes the users receive the reference burst with a different phase.
- For this reason, the user transmits its packet with a different phase in its time slot.
- To avoid this problem, tdma uses guard time.
- By the guard time, each time slot is longer than needed actual traffic burst, so the system avoids the overlap in the traffic bursts



TDMA : Time Division Multiple Access

✓ Preamble

- Each traffic burst is transmitted independently with a personal phase relative to the reference burst.
- For this reason, there is a need for a seperator called “preamble”
- The preamble gives the information of timing and carrier sense to the receiver side for the synchronization.



TDMA : Time Division Multiple Access

- **TDD-TDMA & FDD-TDMA**
  - Time division multiple access types

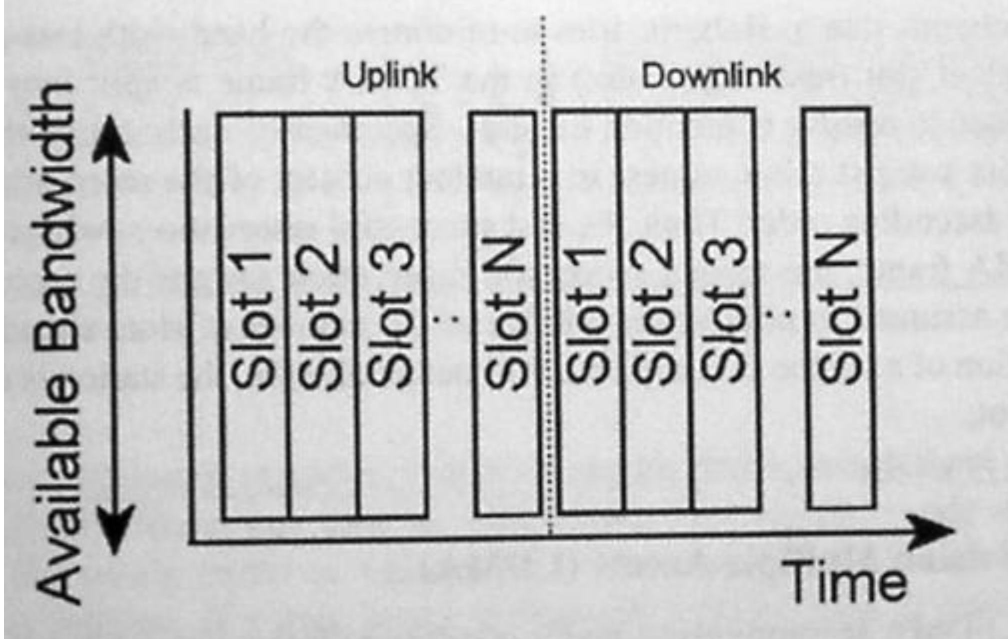


Figure 2.32 Illustration of TDD-TDMA

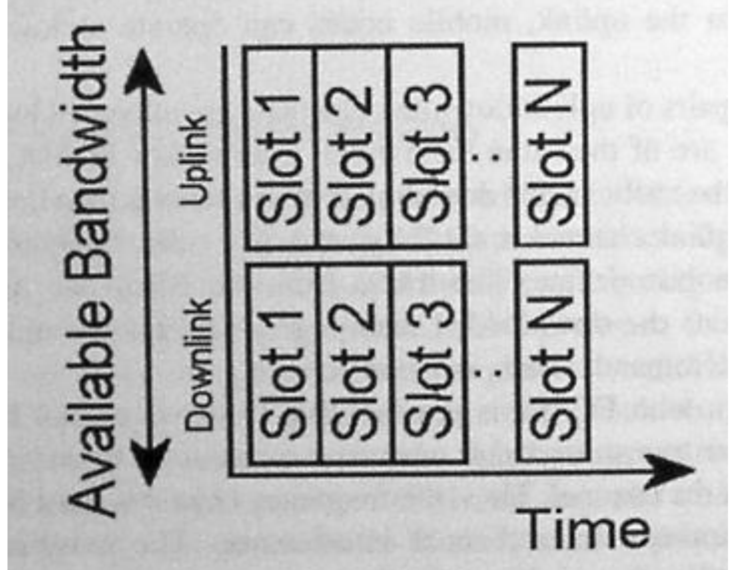
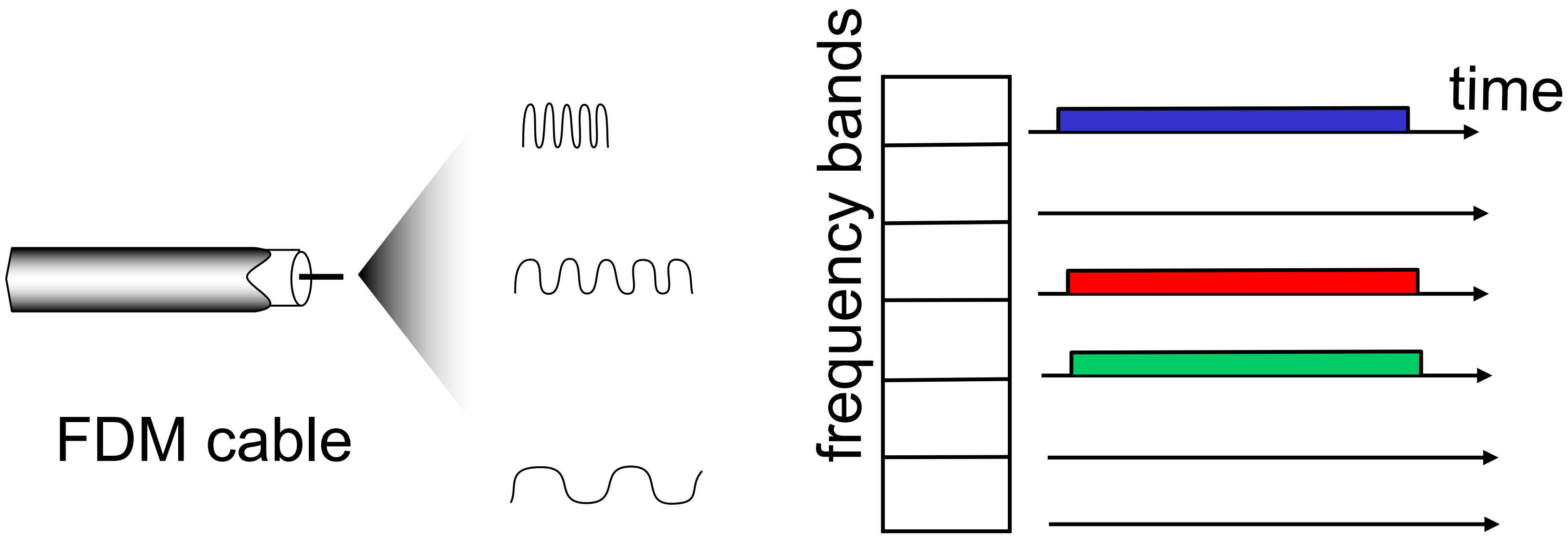


Figure 2.31 Illustration of FDD-TDMA

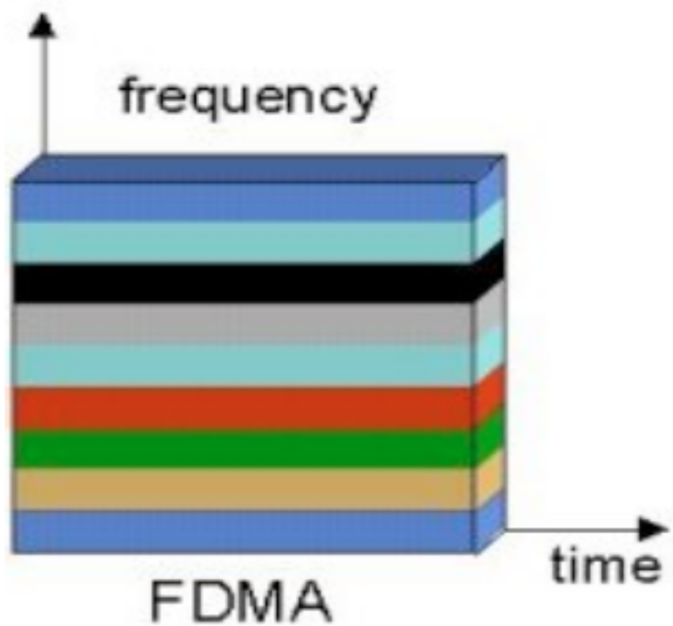
FDMA : Frequency Division Multiple Access

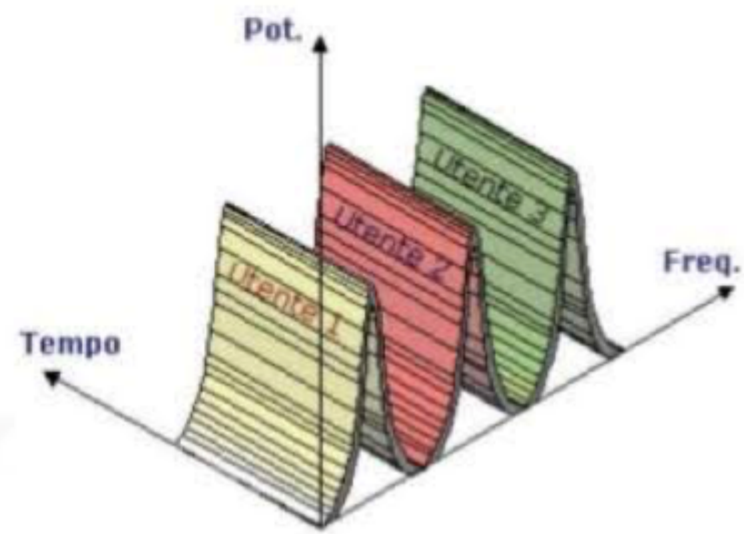
- ✓ Channel spectrum divided into frequency bands
- ✓ Each station is assigned each of the fixed frequency band
- ✓ unused frequency slots in frequency bands go idle
  - example: 6-station LAN, 1,3,4 have pkt, frequency bands 2,5,6 idle



FDMA : Frequency Division Multiple Access

- ✓ Users are differentiated belonging to the frequency bands.
- ✓ Each transmitter uses the band with no limitations in time, however, they use only their limited frequency band.





FDMA : Frequency Division Multiple Access

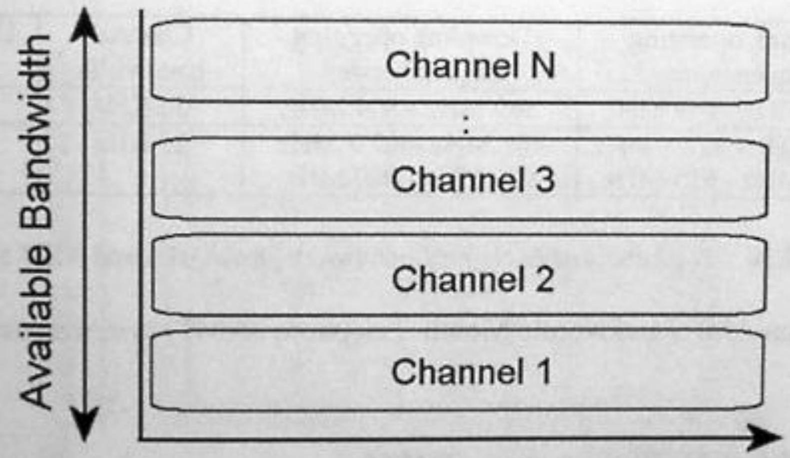


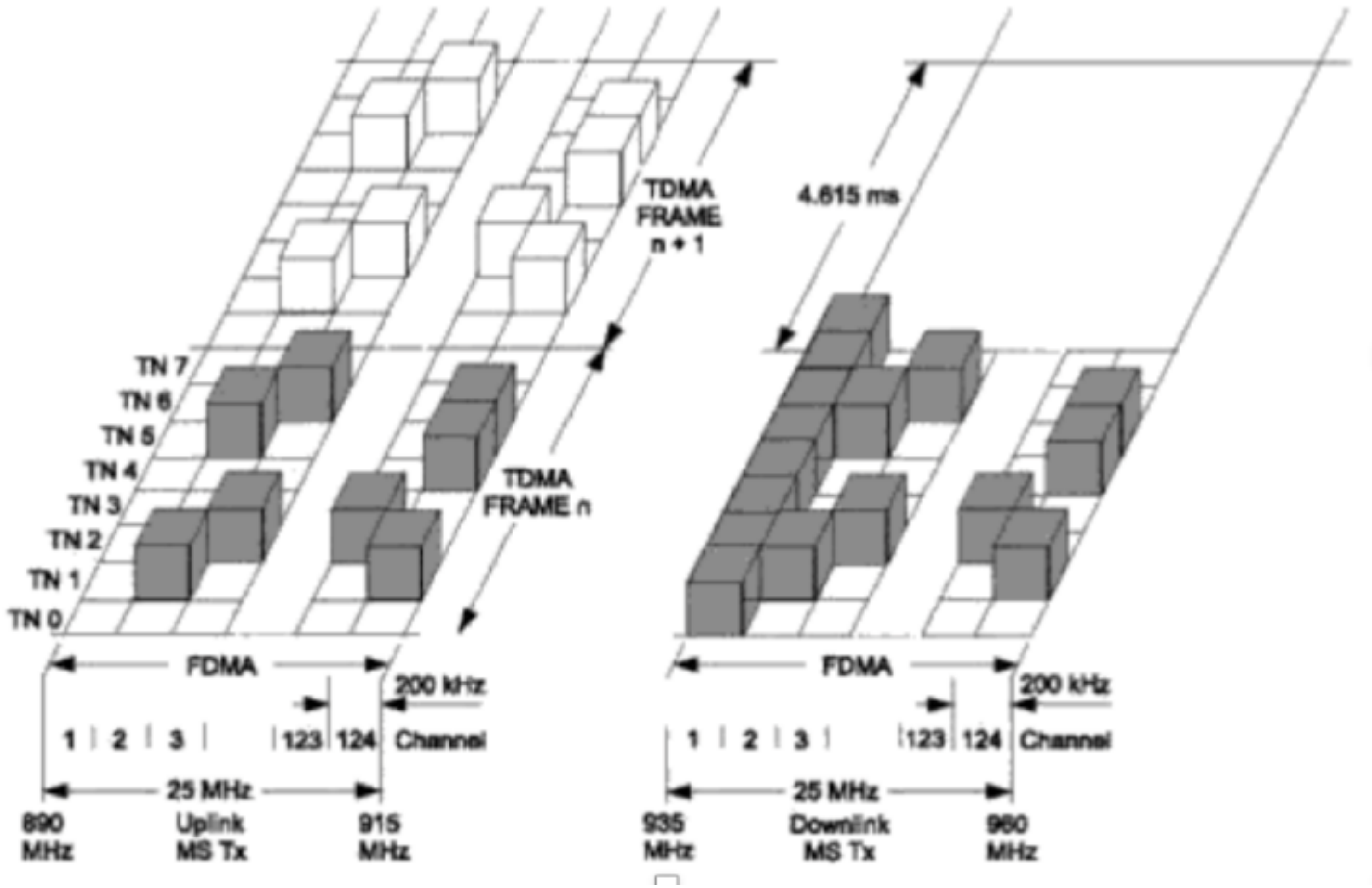
Figure 2.29 Illustration of FDMA

System	Uplink operating frequency range	Downlink operating frequency range	Channel bandwidth	Usable channel bandwidth
AMPS	824 MHz - 849 MHz	869 MHz - 894 MHz	30 KHz	24 KHz
NMT	453 MHz - 457.5 MHz 890 MHz - 915 MHz	463 MHz -467.7 MHz 935 MHz - 960 MHz	25 KHz	9.4 KHz

Figure 2.30 Total and usable channel bandwidths for AMPS and NMT systems

FDMA : Frequency Division Multiple Access

- ✓ TDMA + FDMA in GSM900 Standard

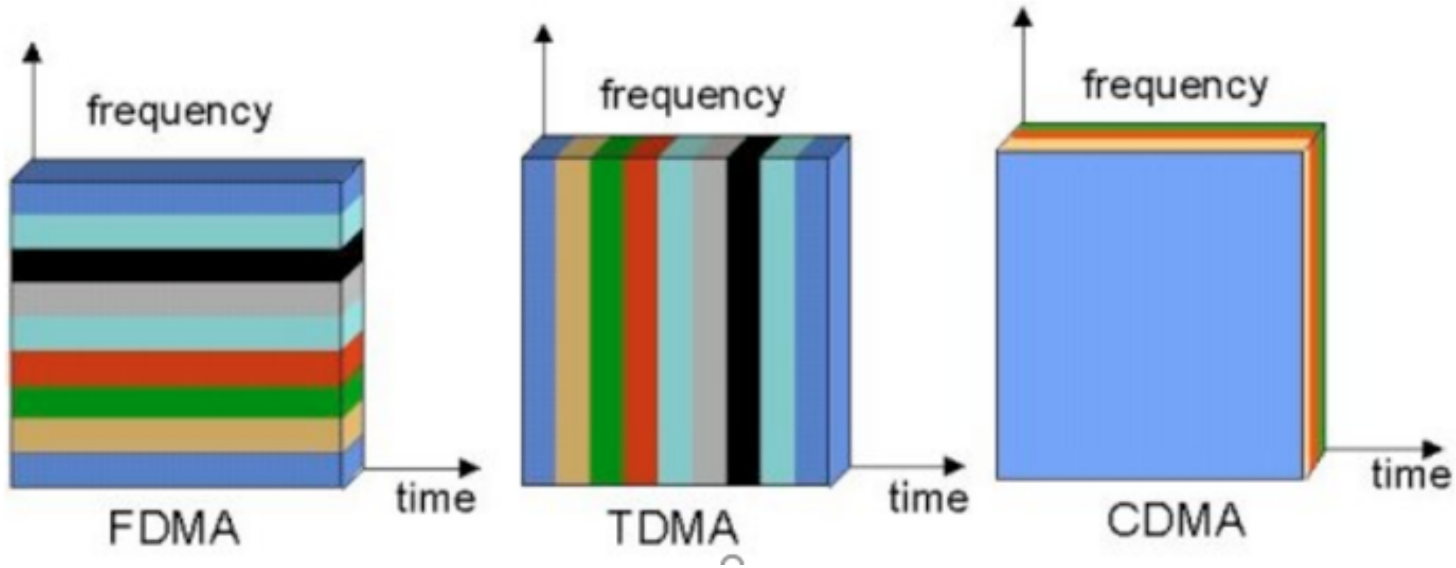


CDMA : Code Division Multiple Access

- ✓ each station has a “station code”

- ✓ each bit is encoded by station code

CDMA : Code Division Multiple Access



CDMA : Details

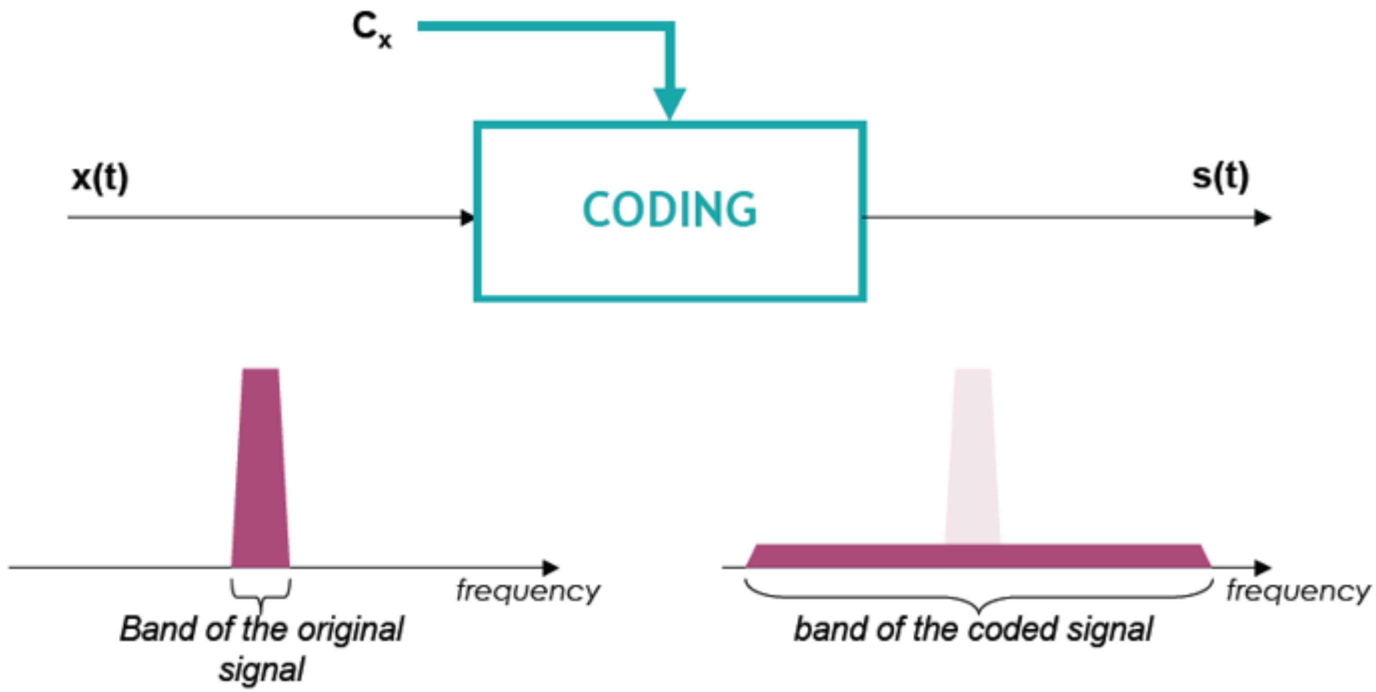
- Each station is given a unique code sequence that is employed by the station to encode its signal or data.

- After the station encodes the signal and sends the signal to the receiver, the receiver can decode the signal and obtains the original signal(because it knows the assigned unique code of the sender.)

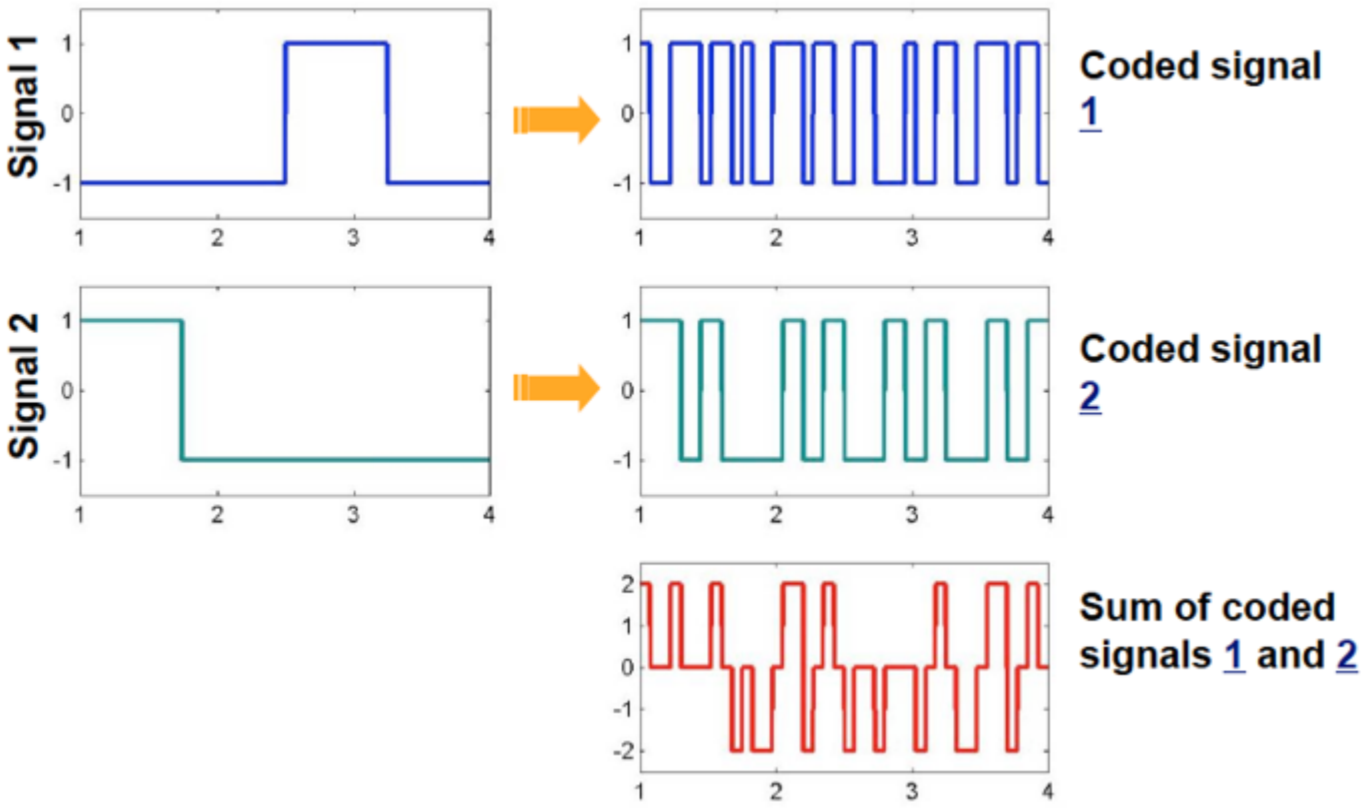
- The action of the encoding enlarges the spectrum of the data signal because the encoded data signal needs more bandwidth than the original signal.

- If two sources sends signals to the same receiver at the same time, the receiver will be able to distinguish the sender of the signal and the original signal because the receiver knows the unique codes of the senders.

CDMA : The Change in Spectrum



CDMA : The Representation of Signals



CDMA : Encoding & Decoding Example

$$\begin{bmatrix} H_n & H_n \\ H_n & -H_n \end{bmatrix}$$

2 codes

1 1

1 -1

4 codes

1 1 1 1

1 1 -1 -1

1 -1 1 -1

1 -1 -1 1

Coding:

M1 10 -> 1 1 1 1 -1-1-1-1

M2 01 -> -1-1 1 1 1 1-1-1

M3 11 -> 1-1 1-1 1-1 1-1

M4 00 -> -1 1 1-1-1 1 1-1

Combined signal:

0 0 4 0 0 0 0 -4

Decoding:

M1 (1,1,1,1)*(0,0,4,0)=4>0 => 1

(1,1,1,1)*(0,0,0,-4)=-4<0 => 0

M2 (1,1,-1,-1)*(0,0,4,0)=-4<0 => 0

(1,1,-1,-1)*(0,0,0,-4)=4>0 => 1

M3 (1,-1,1,-1)*(0,0,4,0)=4>0 => 1

(1,-1,1,-1)*(0,0,0,-4)=4>0 => 1

M4 (1,-1,-1,1)*(0,0,4,0)=-4<0 => 0

(1,-1,-1,1)*(0,0,0,-4)=-4<0 =>0

Random Access MAC Protocols

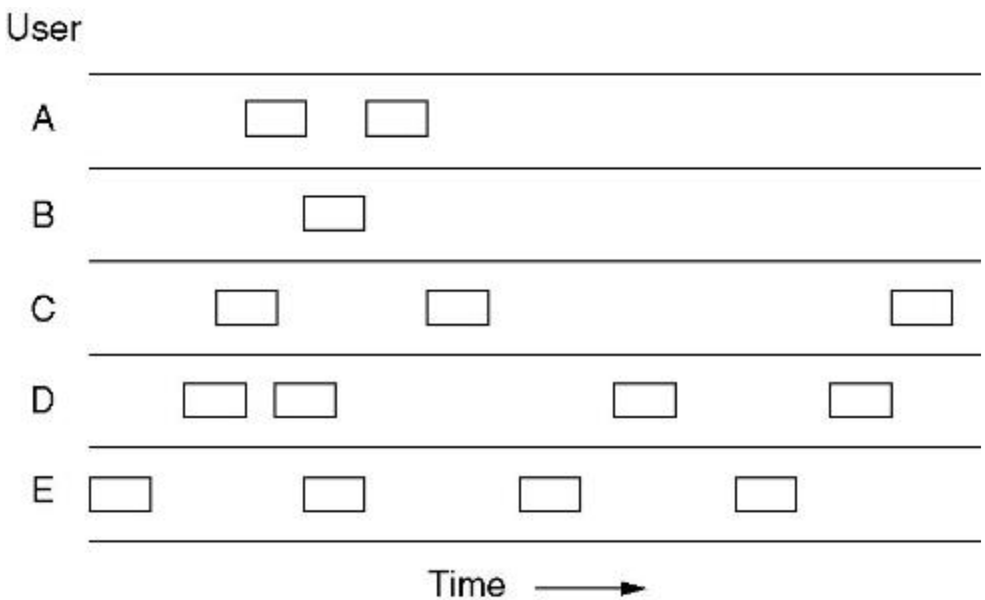
- ✓ Nodes transmit their packet as they have something to send!!!
- ✓ They don't have any priori ,coordination, order for sending.
- ✓ Collusion: Two or more transmitted packets from different nodes at the same time.
- ✓ Random Access Mac protocols are interested in ***detection*** and ***recovering*** from collusions
- ✓ Common types of MAC protocols:
  - slotted ALOHA
  - ALOHA
  - CSMA, CSMA/CD, CSMA/CA

RAMP: ALOHA

- ✓ The simplest type of random Access protocols.
- ✓ They commonly used in packet radio network.
- ✓ The first well-known wireless network as well as network system.
- ✓ Developed by Norman Abramson in Hawaii and it allowed multiple uncoordinated users access to a shared channel (ground based radio broadcasting)
- ✓ Contention-based channel access (random access), multiple users share a common channel in a way that they contend for the channel and lead to conflicts.
- ✓ There are two types of ALOHA:
  - Pure ALOHA: No control mechanism!!!
  - Slotted ALOHA: further divide time axis to slots.

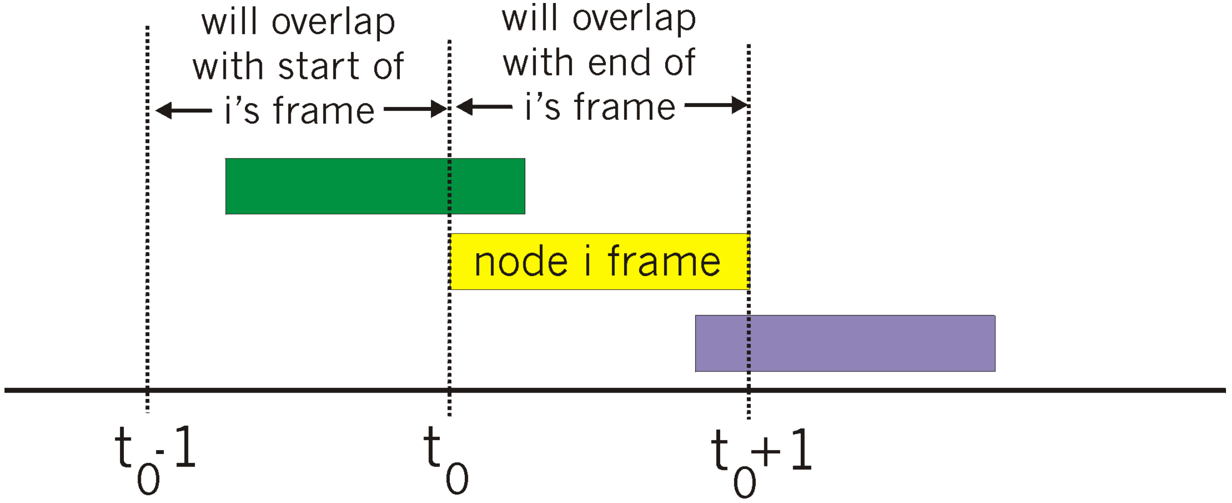
RAMP: Pure (unslotted)ALOHA

- Each station sends packets to the channel whenever it wants.
- The transmission of each frame is done in random times.
- The collusions (probably will occur) will be detected.
- If a collusion occurs, the sender waits a random amount of time and sends the packet again.



RAMP: Pure (unslotted)ALOHA

- ✓ The simplest method of sending packets.
- ✓ There is no synchronization among the stations.
- ✓ The highest probabilty of collusion caused by this method.
- ✓ The frame that is send at t0 collides with other packets sent at t0+1.



RAMP: Pure (unslotted)ALOHA

- **The formulation of efficiency:**

P(success by given node) = P(node transmits) ·
P(no other node transmits in $[t_0-1, t_0]$ ·
P(no other node transmits in $[t_0, t_0+1]$

$$= p \cdot (1-p)^{N-1} \cdot (1-p)^{N-1}$$

$$= p \cdot (1-p)^{2(N-1)}$$

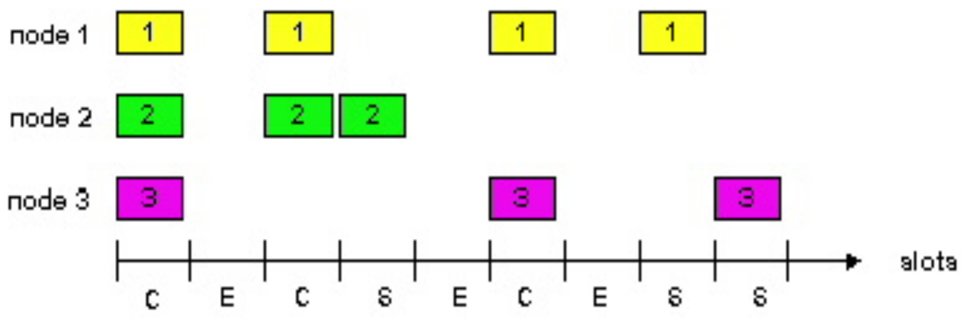
… choosing optimum p and then letting n

$$= 1/(2e) = .18$$

RAMP: Slotted ALOHA

- **Assumptions:**
  - The size of all frames are the same.
  - The timeline is divided into same-size slots.
  - Nodes can be started to be transmitted only at the beginning of the slots.
  - If a collusion (at least two nodes transmit packets at the same time) occurs, all the nodes detect this collusion.
- **Rules:(***When a node have a frame to send***)**
  - If Collusion doesn't occur: node can send the next frame in continueing slot.
  - If collusion occurs: node transmits the frame in continueing slots with prob p until success.

RAMP: Slotted ALOHA

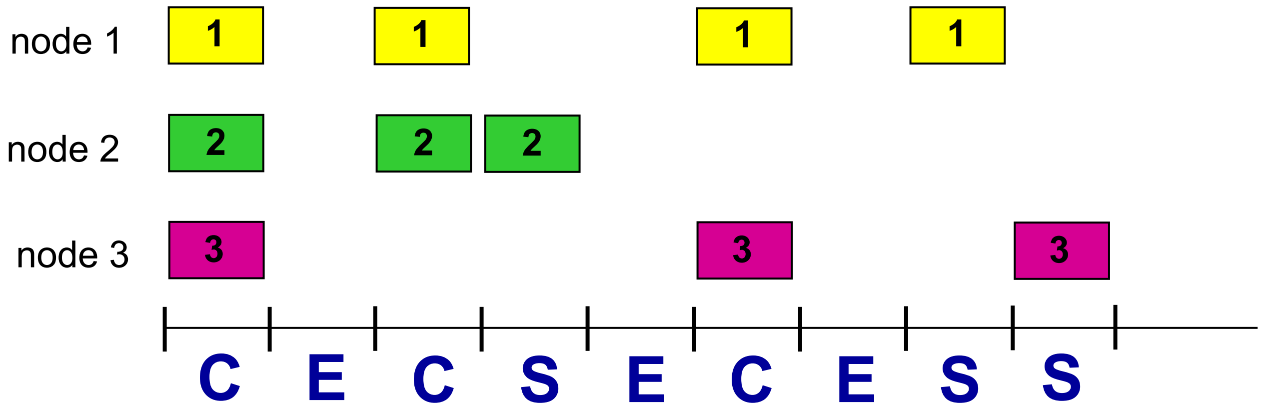


Success (S),
Collision (C),
Empty (E) slots

- ✓ **Important Tips**
  - The aim of the method is to duplicate the transmission capacity of the channel.
  - The timeline is divided to equal intervals which is enough for sending one frame.
  - The timeline should be divided into equal slots on which all the stations agree.
  - Each transmission could only start at the beginning point of a slot.
  - If collusion occurs, sender retransmits the packet in the future slots with probability p.

RAMP: Slotted ALOHA

- **Advantages**
  - One node can continuously transmit at full rate of channel.
  - No Centralization problem: only nodes needs to be synchronized.
  - Simple.
- **Disadvantages**
  - idle slots.
  - Wasting slots because of collusions.
  - Clock synchronization
  - Nodes may detect collusion before transmission ended.



RAMP: Slotted ALOHA Efficiency

- ✓ **Efficiency**
  - The fraction of successful slots to the total number of slots.(many nodes, with their frames to send.

- ✓ **Formulation**
  - N: number of nodes, the frames of which are sent with probability p.
  - Prob that a node becomes successful in a time slot = $p(1-p)^{N-1}$
  - Prob that any node becomes successful in a time slot = $Np(1-p)^{N-1}$
  - ***The maximum value of Efficiency refers to :***
    - p* that maximizes $Np(1-p)^{N-1}$
  - *For a big number of nodes, take limit of* $Np^*(1-p^*)^{N-1}$ as N goes to infinity, gives:

    max efficiency = 1/e = .37

!!!!!!At Best Condition: A channel can be used transmissions successfully with %37.

RAMP: Problems of ALOHA

- **Pure ALOHA**
  - Sends packets as soon as the node has a ready message.
  - Nodes sends their packets if a collusion occurs when they send.
  - **Can not know if the channel is busy or not.**
- **Slotted ALOHA**
  - Time is divided into equal time slots.
  - Avoids collusion partly.
  - Nodes can send at the beginning of the time slots.
  - Increase delay and require synchronization.
  - **Can not know if the channel is busy or not.**

RAMP: Carrier Sense Multiple Access (CSMA) Protocols

✓ General Information

- Stations can listen for a carrier (i.e. transmission)(it is technically possible in LANs) , whether there is a transmission or not.

- Because there is the chance to be aware of collusions in advance, this method group has better throughput rate(% of successfully transmitted frames).

- Protocols that computers can listen for a carrier (signal on the medium) and act accordingly can be divided into three main groups:

  - 1-persistent CSMA
  - nonpersistent CSMA
  - p-persistent CSMA

RAMP: Carrier Sense Multiple Access (CSMA) Protocols

- ✓ **Main working principle:**
  - Listen before transmit:

    if channel sensed idle:
    - Transmit entire frame.
  - if channel sensed busy:
    - Delay transmission.
  - Human analogy: don't interrupt others.
  - Collusions can still occur : (*sometimes one node may not hear each other's transmission*)
  - Collusion: the passed time for transmission is wasted. The features that determine the probability of collusion:
    - ❑Distance
    - ❑Propagation

RAMP: 1-persistent CSMA

- ✓ **Main working principle:**
  1. When a node wants to send a packet, it first listens a channel to see if it is busy,
  2. If channel is busy,
     - The node waits until it becomes idle.
  3. When the station detects an idle channel (),
     - It transmits a frame.(**with probability of 1 → called 1-persistent**)
  4. While transmtting, station listens to channel to see.
  5. If collusion occurs:
     - Station waits a random amount of time and tries to transmit again.(starts all over again).

RAMP: 1-persistent CSMA

- ✓ **Pseudocode of 1-persistent CSMA :**

```
while (frame exists) do
begin
    listen to channel (idle);
    if idle then
      repeat
          xmit (frame);
          check (collision);
          if collision then wait (random);
      until (not collision);
end
```

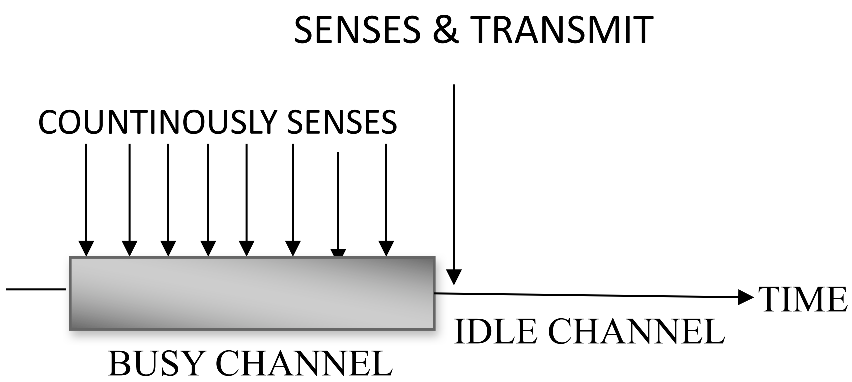
RAMP: 1-persistent CSMA

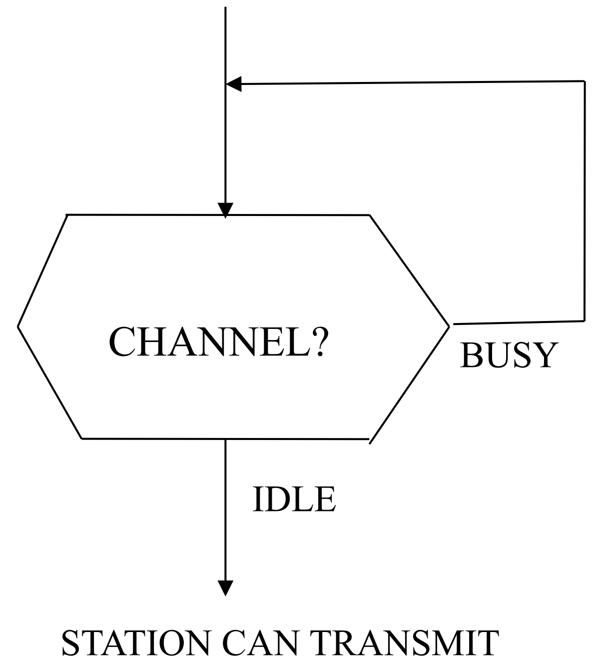
- **Collusion Side:**
  - The term “propagation delay” can be defined as the amount of time that passes during the propagation of signals.
  - When a station begins sending, sends signal that explains the channel is busy.
  - However, if one of the nodes listens the channel before the warning signal propagates every node,the node thinks that the channel is avaliable.
  - So, the node sends the packet to the channel…
  - For this reason, there can be a collusion because of the propagation delay.
  - Even if we accept that the propagation is zero, two stations that are ready for transmission, listen to the channel and send packets at the same time, can cause collusion!!!
  - **This method is better than ALOHA because the stations listen to the channel and wait until the channel is idle.**

RAMP: **Main Points of 1-persistent CSMA**

- The amount of the propagation delay directly affects the number of collusions, if the propagation delay increases, the number of collusions gets bigger.

- Even if we accept that the propagation is zero, two stations that are ready for transmission, listen to the channel and send packets at the same time, can cause collusion!!!





RAMP: Non-persistent CSMA

- **Main working principle:**
  1. When a node wants to send a packet, it firstly listens a channel to see if it is busy,
  2. If channel is busy,
     - The node wait a random time before listening again ***(except of waiting until it becomes idle).***
  3. When the station detects an idle channel (),
     - It transmits its frame.

RAMP: Non-persistent CSMA

- **Pseudocode of Non-persistent CSMA :**

```
while (frame exists) do
begin
        collision=true;
        repeat
            listen to channel (idle);
            if idle then begin
                        collision=false;
                        xmit (frame);
                        check (collision);
            end;
            wait (random);
        until (not collision);
end
```

RAMP: Main Points of Non-persistent CSMA

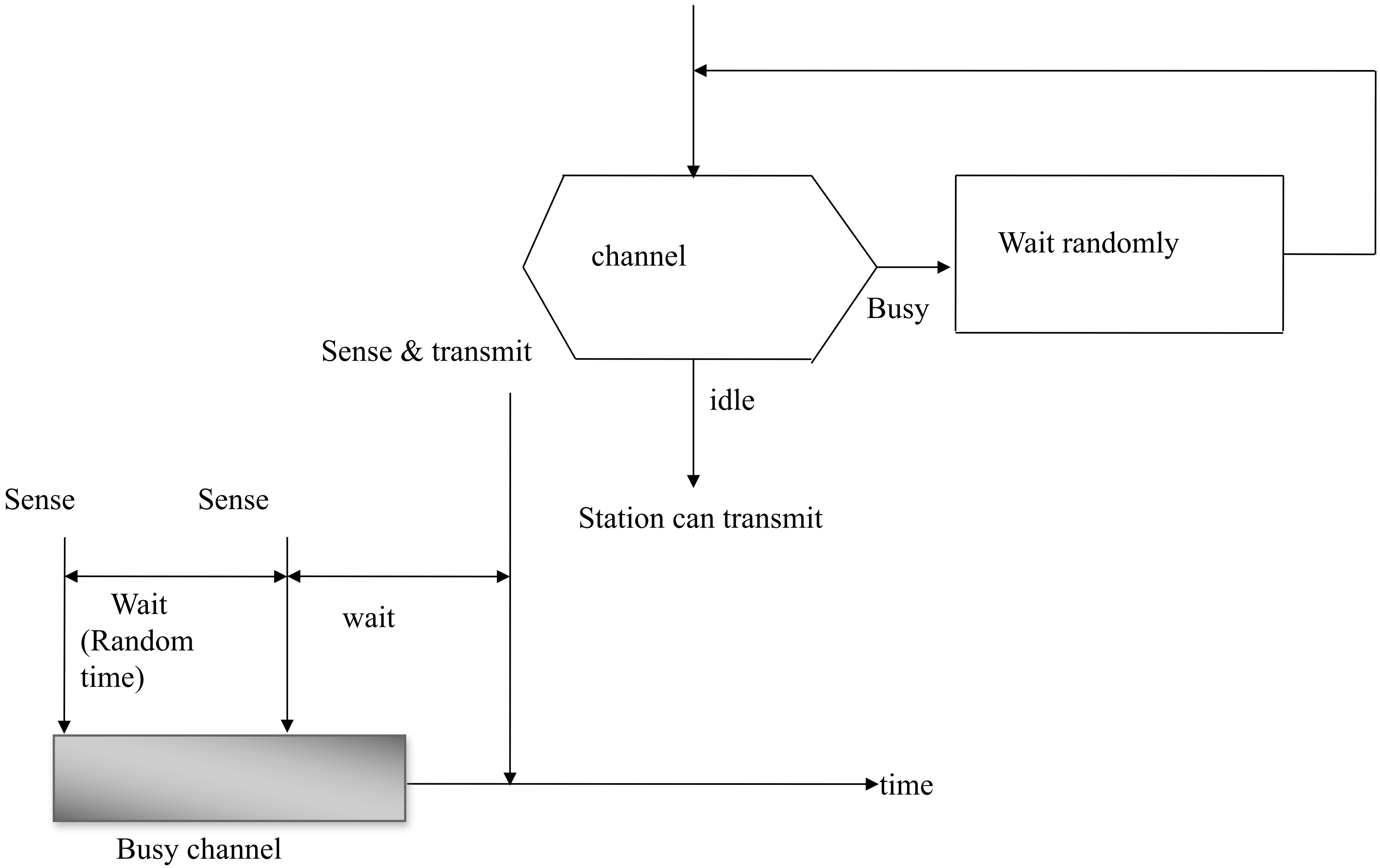
Pros:

- ✓ It reduces the chances of collision because the stations wait a random amount of time.
- ✓ It is unlikely that two or more stations will wait for same amount of time and will retransmit at the same time.

Cons

- ✓ It reduces the efficiency of network because the channel remains idle when there may be station with frames to send.
- ✓ This is due to the fact that the stations wait a random amount of time after the collision.

RAMP: Main Points of Non-persistent CSMA



RAMP: P-persistent CSMA

- ✓ **Main working principle:**

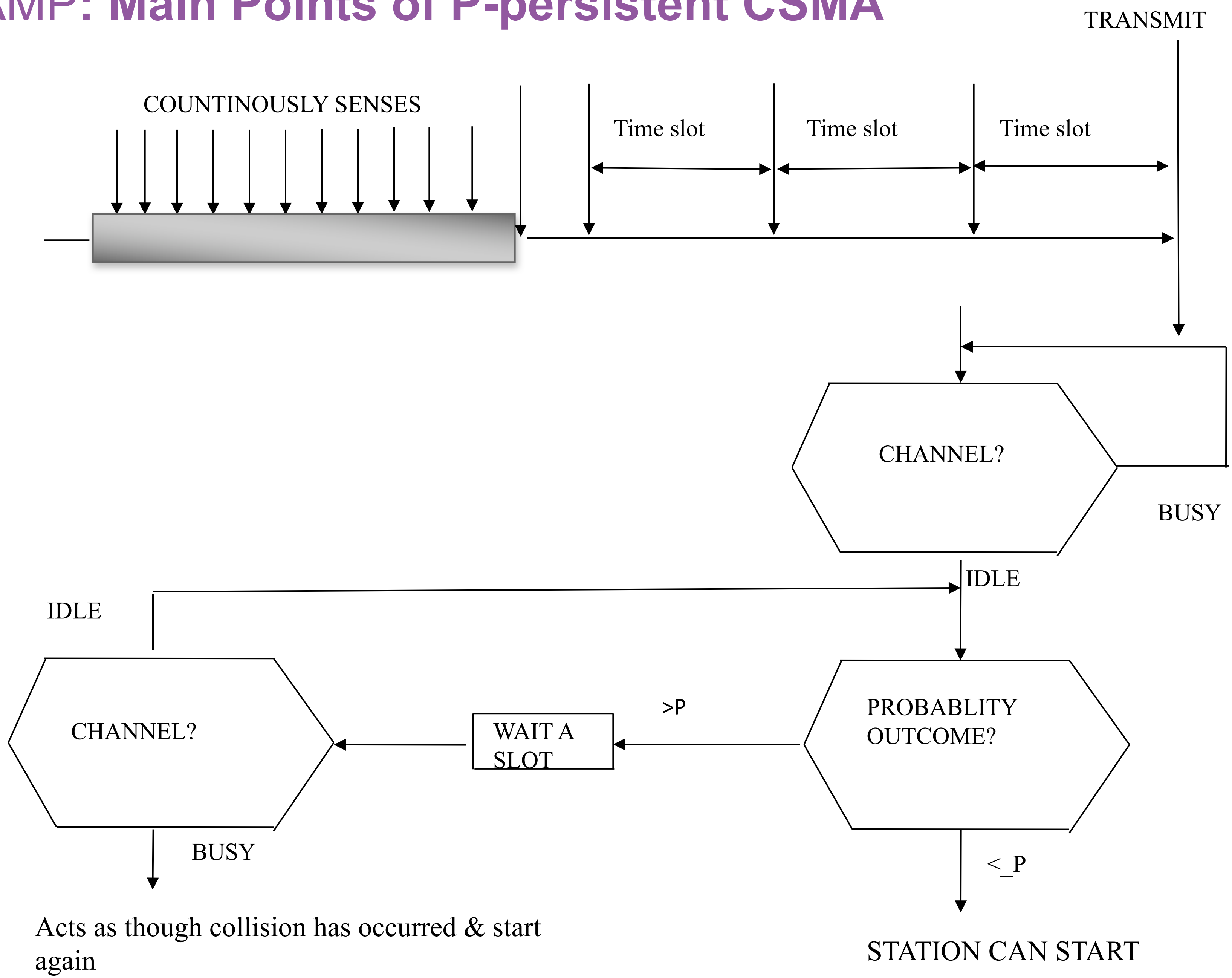
1. This protocol is used for channels that are divided into time slots.
2. When a node wants to send a packet, it firstly listens a channel to see if it is busy,
3. When the channel is idle,
   - the station sends its packet with probability p or waits a further slot with probability q=1 - p.
4. If the channel still idle during this slot
   - then again it either transmits or defers with probabilities p or q.
5. This is repeated until either the frame is transmitted or another station has begun transmitting,
   - If the channel is busy (another station transmitting), station acts as if collision → waits a random time and starts again.
6. If the channel is initially busy
   - it waits until the next slot and applies above algorithm.

RAMP: P-persistent CSMA

- **Pseudocode of P-persistent CSMA :**

```
while (frame exists) do
begin
      collision=true;
      repeat
         listen to channel (idle);
         if idle then
                  if (rand <p) then begin
                           collision=false;
                           xmit (frame);
                           check (collision);
                           if collision then wait (random)
                  end;
         until (not collision);
end
```

RAMP: Main Points of P-persistent CSMA



RAMP: Persistent and Non-persistent

- Comparison of the channel utilization versus load for various random access protocols.
- CSMA has better channel utilization (and longer delays than ALOHA)