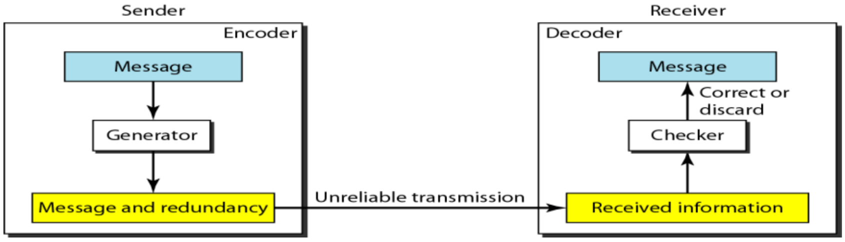
End-Sem:

Unit – 3: 10, 12, 14, 15

Chapter – 10: Error Detection and Correction

- **Intro:** Networks must be able to transfer data from one device to another with acceptable accuracy. For most applications, a system must guarantee that the data received are identical to the data transmitted. Data can become corrupted in passage from one node to the next. Many factors can alter one or more bits of a message. Some applications require a mechanism for detecting and correcting the errors. Some applications can tolerate a small level of error. Ex – random errors in audio or video transmission may be tolerable.
- **Types of error:** whenever bits flow from one point to another, they are subject to unpredictable changes because of interference. Interference can change the shape of the signal.
  - **Single-Bit Error:** only one bit of a given data unit (such as byte, packets or character) is changed from 0 to 1 or from 1 to 0. Least likely type of error in serial data transmission. (diagram)
  - **Burst error:** means that two or more bits in the data unit have changed from 1 to 0 and 0 to 1. Length of burst is measure from first corrupted bit to the last corrupted bit. Some bits in between may not have been corrupted. More likely to occur than single-bit error since the duration of noise is normally longer than the duration of 1 bit, which means when noise affects data, it affects a set of bits. Number of bits affected depends on data rate and duration of noise. (diagram)
- **Redundancy:** Central concept in correcting and detecting errors. To detect errors, we need to send extra (redundant) bits with data. These redundant bits are added by the sender and removed by the receiver. Their presence allows the receiver to detect or correct corrupted bits. This is achieved through various coding schemes like block coding.
- **Detection vs Correction:** Correction of errors is more difficult than detection of errors. In error detection, we only check if an error has occurred, it is a yes or no question. We do not care about the size of error (no. of corrupted bits) or even the number of errors. A single-bit error is the same as a burst error.

  Error correction requires us to know the number of bits that are corrupted, their location in the message. The number of errors and the size of the message is important. We will have to consider 8 possible error location for a single-bit error in 8-bit data unit. If we have 2 errors in the data unit of the same size, then we will have to consider 28 different possibilities. Imagine finding 10 errors in 1000 bits!
- **Coding:** Redundancy is achieved through various coding schemes. Sender adds redundant bits through a process that creates a relationship between the redundant bits and the actual data bits (for ex – ration between redundant bits and actual bits). The receiver checks the relationship between two sets of bits to check or correct the error. Schemes can be block coding or convulsion coding (not in syllabus).

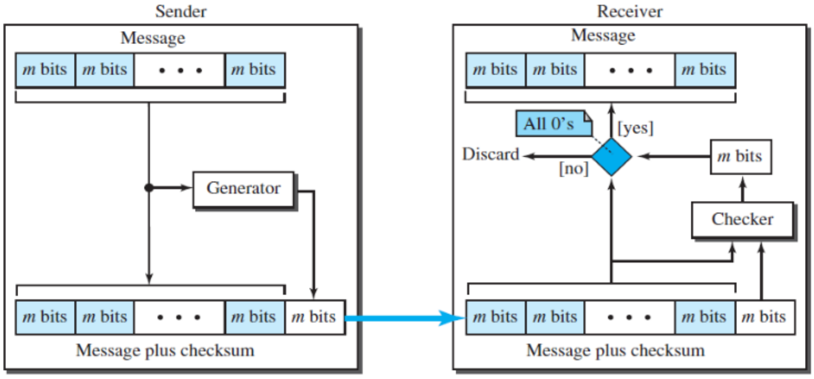


- **Block Coding:** Message is divided into blocks, each of k-bits, called *datawords*. ‘r’ redundant bits are added to each block to make the length of blocks n = k + r. Resulting n-bits blocks are called *codewords*. Number of possible datawords = 2^k, no. of possible codewords = 2^n. Blocking coding process is one to one i.e. same datawords is always encoded as same codeword. Since n > k, we have (2^n – 2^k) codewords which are not used and are called invalid or illegal. Table below shows 2B/3B block coding scheme. Keep in mind, an error detecting code can only detect the types of error it is designed for i.e. some other types of errors may remain undetected.

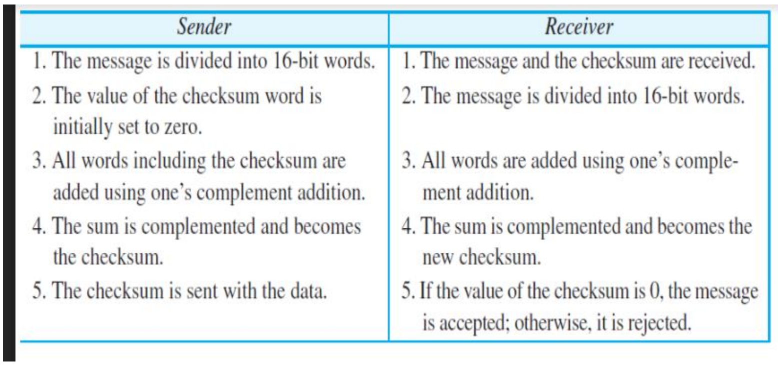
Datawords	*Codewords*
00	000
01	011
10	101
11	110

- **Hamming Distance:** Central concept in coding for error control is the idea of the Hamming distance. Hamming distance between two words x and y is denoted as d(x,y) and it is the number of differences between the corresponding bits. Ex – if sent word is 00000 and received is 00101, then d(00000, 00101) = 2 since two bits are different. Therefore if the Hamming distance between the sent and received codeword is not zero, then the codeword has been corrupted during transmission. This distance can be found by applying the XOR operation on two words and counting the number of 1’s in the result. Ex – d(10101, 11110) = 3 because (10101 XOR 11110) = 01011 (three 1’s)
- **Minimum Hamming distance:** is the smallest hamming distance between all possible pairs in a set of words. This is used while designing a code to correct or detect errors. To guarantee that up to ‘s’ errors will be detected, d_{min}= s + 1.
- **Checksum:** error detection method used in the Internet by several protocols but not at the data link layer. Also based on the concept of redundancy. This can be applied to message of any length. It is mostly used at transport and network layer.

  A message is first divided into m-bits at the source and an extra m-bit is added which is the sum of the original bits with a ‘minus’ sign. At the receiver’s end, sum is taken for all the bits and if the sum is zero, then the message is accepted, otherwise it is discarded. Ex – if we want to send [7, 11, 0, 12, 6] then we add an extra bit ‘-36’ which is the sum of the original message and send [7, 11, 0, 12, 6, -36]. The receiver takes the checksum again up on receiving the message and if the sum is 0, then the message is accepted, otherwise an error has occurred, and one or more bit got corrupted during transmission and the message is discarded. Note: the checksum can be inserted at the middle of the message too, it does not have to be at the end.



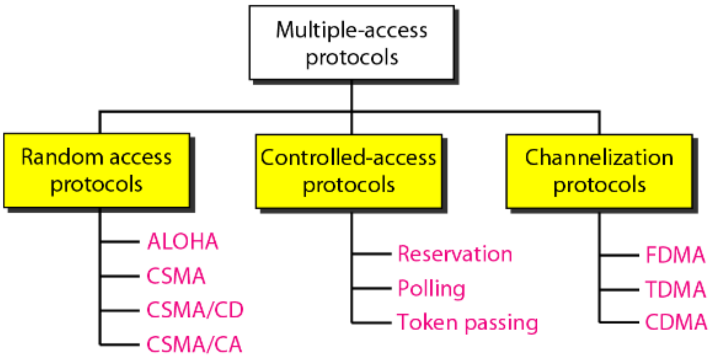
Note that 36 is too big to be written in 4-bits, therefore 1's complement method is used in this case. The table below shows the template for Internet checksum.



Sender	*Receiver*
1. The message is divided into 16-bit words.	1. The message and the checksum are received.
2. The value of the checksum word is initially set to zero.	2. The message is divided into 16-bit words.
3. All words including the checksum are added using one's complement addition.	3. All words are added using one's complement addition.
4. The sum is complemented and becomes the checksum.	4. The sum is complemented and becomes the new checksum.
5. The checksum is sent with the data.	5. If the value of the checksum is 0, the message is accepted; otherwise, it is rejected.

Chapter – 12: <u>Multiple Access</u>

- Data link layer is divided into two functionality-oriented sub layers: Data link control, Multiple-access resolution.
- Taxonomy of MAC (Multiple Access Control):



- **Random Access Protocols:**

In random access or contention methods, no station is superior to other station and none is assigned control over others i.e. no station permits or does not permit other stations to send. A station which has the data to send, uses a procedure described by the protocol to decide whether to send or not. This decision depends on the state of the medium (idle or busy). Therefore, each station can transmit when it desires, given it follows the predefined procedure, including the testing of the state of the medium.

Random Access is called random access because of two features (i) Transmission is random between stations i.e. there is no scheduled transmission time (ii) no rules specify which station should send next i.e. stations compete with another to access the medium. That is why these methods are also called contention methods.

Each station has the right to access the medium however if more than one method tries to send data at the same time, there is access conflict-collision and the frames will either be destroyed or modified.

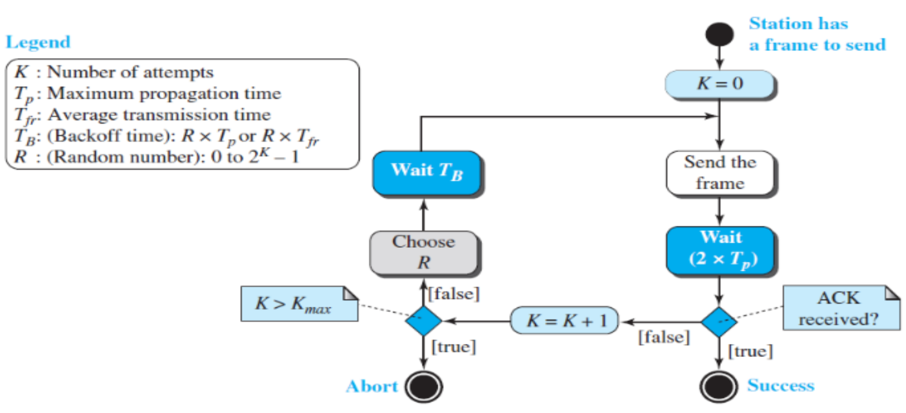
The random-access methods we will study have evolved from a protocol called ALOHA which used a simple procedure called multiple access (MA). This method was improved by addition of a procedure which forced the stations to sense the medium before transmitting. This was called Carrier-Sense-Multiple-Access (CSMA). CSMA later evolved into two parallel methods: CSMA/CD (CSMA with collision detection) and CSMA/CA (CSMA with collision avoidance). CSMA/CD tells the station what to do when a collision is detected, and CSMA/CA tries to avoid the collision.

- **ALOHA:** earliest random-access method, developed at University of Hawaii in early 1970's. Designed for radio (wireless) LAN but can be used for any shared medium. Since the medium is shared between 2 stations, there are possible collisions.
  - **Pure ALOHA:** original ALOHA protocol is called pure ALOHA. Simple but elegant. The idea is that whenever a medium wants to send a frame, it does so and then waits for an acknowledgement. If the ack does not arrive within a time-out period, the sender assumes there was a collision and the frame has been destroyed. It then re-sends the frame.

    If all these stations try to resend their frames after the time-out, the frames will collide again. Pure ALOHA dictates that when the time-out period passes, each station waits a random amount of time before resending its frame. The randomness will help avoid more collisions. We call this time the back-off time *TB.*

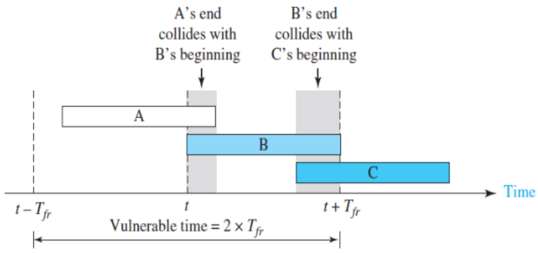
    It also uses the concept of maximum number of re-transmission, K_{max} to prevent congesting the channel with retransmissions. After the maximum number of attempts, a station must give up and try later.

Figure 12.3 *Procedure for pure ALOHA protocol*


Legend
K : Number of attempts
T_p : Maximum propagation time
T_fr : Average transmission time
T_B : (Backoff time): R × T_p or R × T_fr
R : (Random number): 0 to 2^K – 1
Station has a frame to send
K = 0
Send the frame
Wait (2 × T_p)
ACK received?
[true]
Success
[false]
K = K + 1
K > K_max
[true]
Abort
[false]
Choose R
Wait T_B

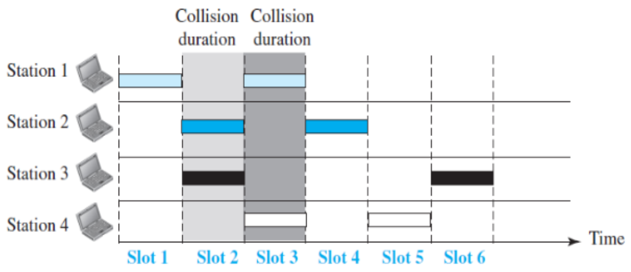
Vulnerable time in Pure ALOHA is (2 * T_{fr}) i.e. the length of time when there is a possibility of collision assuming the stations send fixed-length time frames with times taken to send the frame = T_{fr}.

Figure 12.4 *Vulnerable time for pure ALOHA protocol*


A's end collides with B's beginning
B's end collides with C's beginning
A
B
C
Time
t – T_fr
t
t + T_fr
Vulnerable time = 2 × T_fr

  - **Slotted ALOHA:** As we can see in the above diagram, in pure ALOHA, a station may send soon after another station has started or soon before another station has finished. Slotted ALOHA was invented to improve the efficiency of PURE ALOHA. Here, the time is divided in slots of T_{fr} seconds and the stations are forced to send only one frame at the beginning of each slot. Because a station can send only at the beginning of the synchronized time slot, if a station misses this moment, it must wait until the beginning of the next time slot. The vulnerable time is therefore reduced to T_{fr}. This is shown in the diagram below.

Figure 12.5 *Frames in a slotted ALOHA network*



- **CSMA**: **Carrier Sense Multiple Access**. Can reduce the possibility of collision by sensing the medium before using it but cannot eliminate it. Requires each station to check the medium (if busy/idle) before sending. Based on the concept of 'listen before talking'.

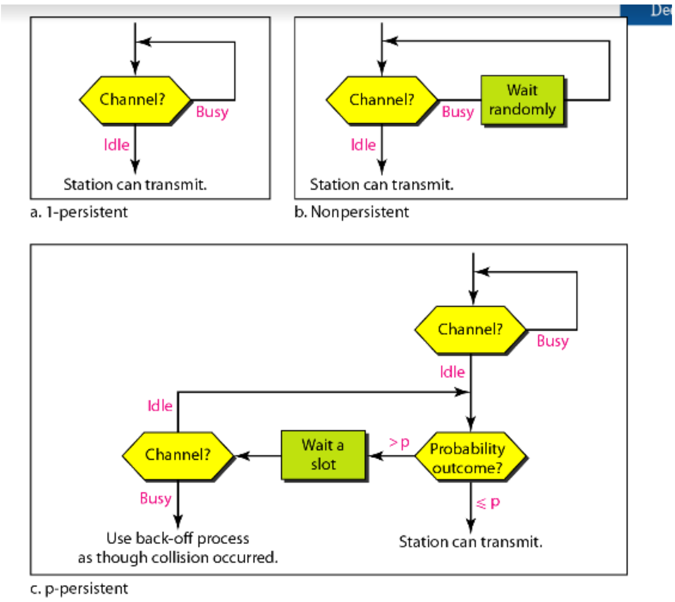
  Possibility of collision still exists because of propagation delay i.e. it still takes time (although very short) for the sent bit to be received by another station. Therefore, a station can find the medium idle because the first bit sent by another station still might be travelling and has not been received. Therefore, the vulnerable time for CSMA is T_p which is the propagation time. This is the time needed for a signal to propagate from one end of a medium to another.

  - **Persistent methods:** What should a station do if the channel is busy? What should a station do if the channel is idle? Three methods have been devised to answer these questions:

    (i) **the I-persistent method** - after the station finds the line idle, it sends frames immediately with probability 1. This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately. Used in Ethernet.

    (ii) **the nonpersistent method –** station senses the medium, if it is idle, it sends immediately. If it is busy, it waits a random amount of time and senses the line again. Reduces the chance of collision because it is unlikely that two or more stations will wait for the same amount of random time. But this method reduces efficiency because medium remains idle even when there are frames to send.

    (iii) **p-persistent method –** used if a channel has time slots with a slot duration equal to or greater than the maximum propagation time. Combines advantages of other two methods. Reduces chance of collision and improves efficiency. Does two things: (i) with probability p, it sends frame (ii) with probability q=1-p, station waits for the beginning of the next time slot and checks the line again. If it is idle – go to step (i), if line is busy, acts as collision has occurred and use the back-off approach.

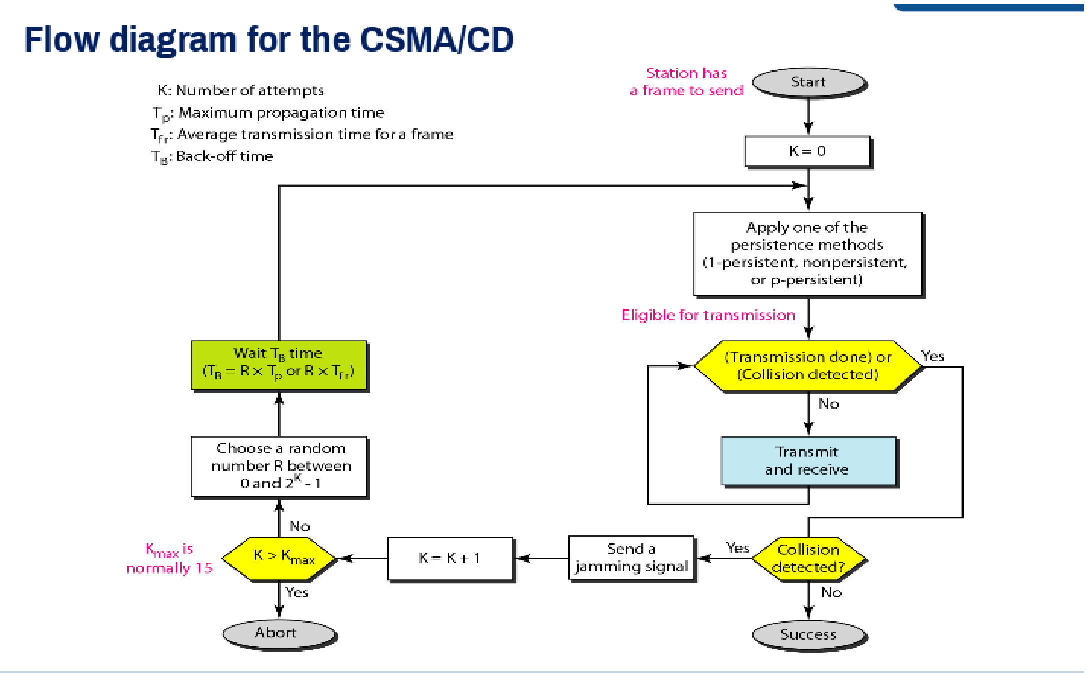


a. 1-persistent

b. Nonpersistent

c. p-persistent

- **CSMA/CD: Carrier sense multiple access with collision detection.**
  In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished. If, however, there is a collision, the frame is sent again.



Flow diagram for the CSMA/CD

K: Number of attempts
T_p: Maximum propagation time
T_{fr}: Average transmission time for a frame
T_B: Back-off time
Station has a frame to send
Start
K = 0
Apply one of the persistence methods (1-persistent, nonpersistent, or p-persistent)
Eligible for transmission
(Transmission done) or (Collision detected)
Yes
No
Transmit and receive
Collision detected?
Yes
No
Success
Send a jamming signal
K = K + 1
$K > K_{max}$
K_{max} is normally 15
No
Yes
Abort
Choose a random number R between 0 and $2^K - 1$
Wait T_B time ($T_B = R \times T_p$ or $R \times T_{fr}$)

Observations: First difference is the addition of persistence process i.e. we need to sense the channel before sending the frames by using one of the persistence methods.

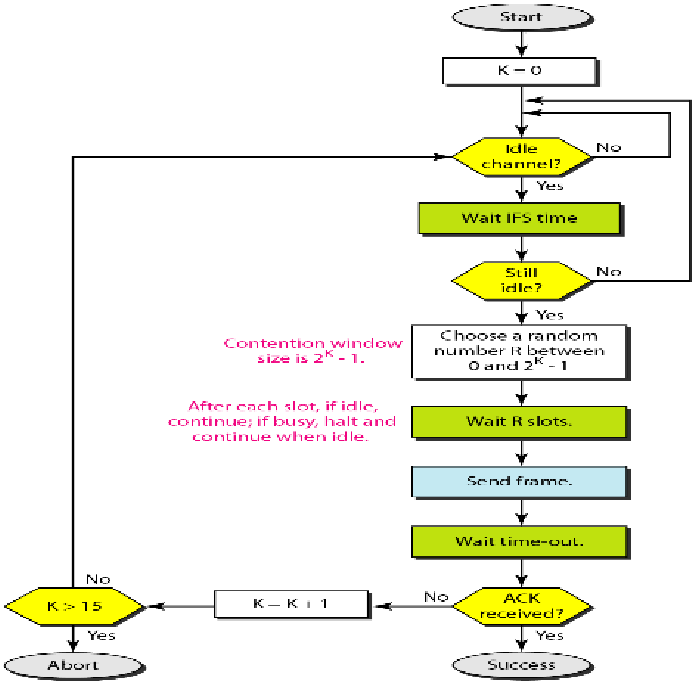
Second difference is frame transmission. In ALOHA, we first transmit the entire frame and then wait for acknowledgement. In CSMA/CD, transmission and collision detection are continuous processes. We do not send the entire frame and wait for a collision. Station transmits and receives continuously and simultaneously.

Third difference is the sending of a short jamming signal to makure all other stations become aware of the collision.

- **CSMA/CA: Carrier sense multiple access with collision avoidance.**
  This was invented for wireless networks. Collisions are avoided through three strategies:
  (i) Interframe space –

(ii) Contention window – is the amount of time divided into slots. A station which is ready to send chooses a random number of slots as its wait time.

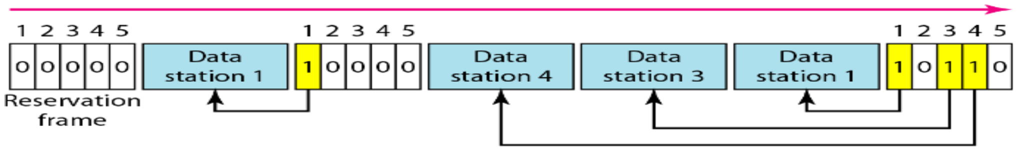
(iii) Acknowledgements


Start
K = 0
Idle channel?
No
Yes
Wait IFS time
Still idle?
No
Yes
Contention window size is $2^K - 1$.
Choose a random number R between 0 and $2^K - 1$
After each slot, if idle, continue; if busy, halt and continue when idle.
Wait R slots.
Send frame.
Wait time-out.
ACK received?
No
Yes
Success
K = K + 1
K > 15
No
Yes
Abort

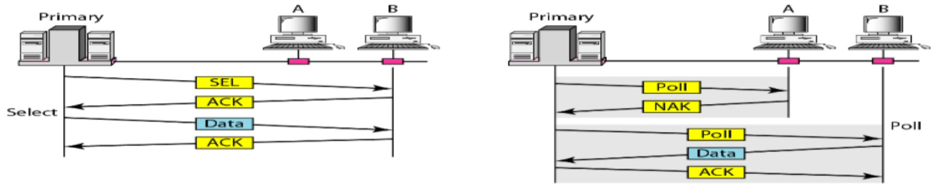
- **Controlled Access Protocols:**

  In controlled-access, station consult each other to find which station has the right to send. A stations cannot send unless it has been authorized by other stations.

- **Reservation -** time is divided into intervals and stations need to make a reservation before sending the data. In each time interval, a reservation frame precedes the data frames sent in that interval. If there are N stations in the system, there are exactly N reservation mini-slots in the reservation frame where each mini-slot belongs to one station. When a station needs to send a data frame, it makes a reservation at its mini slot. Station that was made a reservation can send the data after the reservation frame.



- **Polling -** works with topologies where there is one primary device. All the data exchanges must be sent through the primary device even if the destination is secondary device. Therefore, the primary device controls the link and the secondary device follows its instructions. The primary device is always the initiator of a session and decides which station can use the channel. Drawback is if the primary device fails, the whole system goes down. Polling uses ‘Poll’ and ‘Select’ functions to avoid collision.



'Select' is used if a primary device has something to send. The thing is, even if primary is ready to send, secondary might not be ready to receive. Therefore, primary must inform the secondary device and wait for an acknowledgement of its ready status. Before sending the data, primary creates a 'SEL' frame, one field of which has the address of the secondary device the information is being sent to.

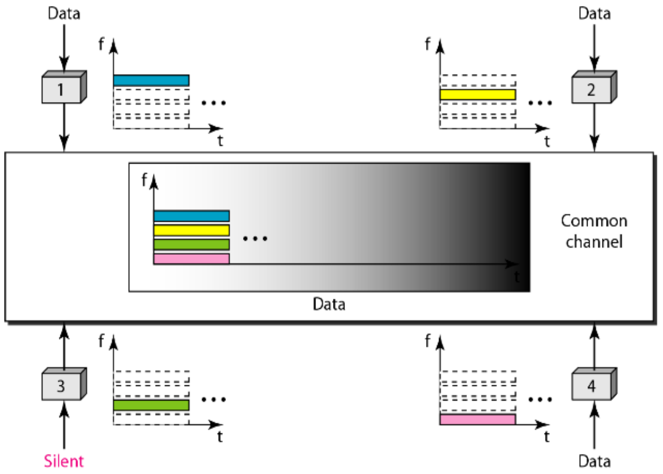
'Polling' is used by primary device to ask the secondary device is they have something to send.

- **Token Passing –** in this method, stations are organised in a network are organized in a logical ring. Hence, there is a predecessor and successor for each station.
  A special packed, called a 'token' circulates through the ring. Whichever station has the token, can access the channel, and send its data. Once the station is done, it passes the token to its successor in the ring.

➢ **Channelization protocol:**
Multiple-access method where available bandwidth of a link is shared in time, frequency, or through code, between different stations.

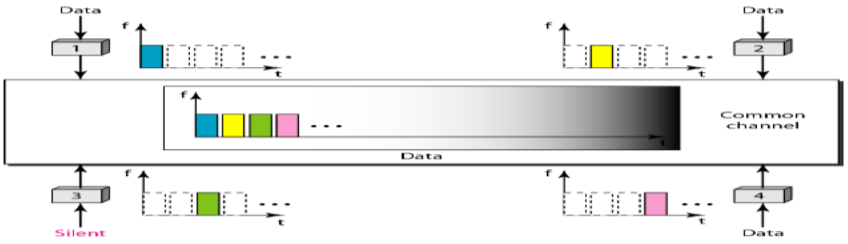
- **FDMA (Frequency-division multiple access):** Available bandwidth is divided into frequency bands. Each station is allocated a band to send its data. These bands are separated by guard bands to avoid collisions. In other words, each band is reserved for a specific station, and it belongs to the station all the time.

Frequency-division multiple access (FDMA)



- **TDMA (Time division Multiple Access):** stations share the bandwidth of the channel in time. Each station gets assigned a time slot and it only transmits the data in its time slot. Problem arises related to synchronisation between different stations. Stations need to know the beginning of its slots and the location of its slots. This can be difficult due to propagation delays if the stations are spread over a large area. To deal with this, we can insert guard times.

TDMA



Chapter – 14: Wireless LANS

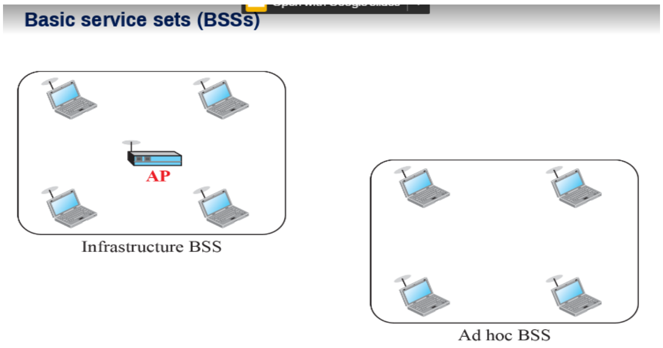
Introduction:

- Wireless communication is one of the fastest-growing technologies. The demand for connecting devices without the use of cables is increasing everywhere. Wireless LANs can be found on college campuses, in office buildings, and in many public areas.
- **Comparison of Wired and wireless:**
  - **Medium:** The first difference we can see between a wired and a wireless LAN is the medium. In a wired LAN, we use wires to connect hosts. In a wireless LAN, the medium is air, the signal is generally broadcast.
  - **Hosts:** In a wired LAN, a host is always connected to its network at a point with a fixed link-layer address related to its network interface card (NIC). In a wireless LAN, a host is not physically connected to the network. it can move freely and can use the services provided by the network.
  - **Isolated LANS:** A wired isolated LAN is a set of hosts connected via a link-layer switch. A wireless isolated LAN, called an ad hoc network in wireless LAN terminology, is a set of hosts that communicate freely with each other.
  - **Characteristics:** There are several characteristics of wireless LANS that do not apply to wired LANS or are negligible.
    1. i) **Attenuation** - The strength of electromagnetic signals decreases rapidly because the signal disperses in all directions; only a small portion of it reaches the receiver.
    2. ii) **Interference** - Another issue is that a receiver may receive signals not only from the intended sender, but also from other senders if they are using the same frequency band.
    3. **iii)** **Multipath Propagation -** A receiver may receive more than one signal from the same sender because electromagnetic waves can be reflected from obstacles such as walls, the ground, or objects. The result is that the receiver receives some signals at different phases (because they travel different paths). This makes the signal less recognizable.
    4. **iv)** **Error –** If SNR (Signal to Noise Ratio) is high, means signal is stronger than noise, we maybe able to convert signal to actual data. If SNR is low; signal is corrupted by noise and data cannot be recovered.

       CSMA/CD algorithm doesn’t work in wireless LANS because of three reasons: wireless hosts do not have the power to send and receive at the same time, hidden station problem prevents collision detection, distance between stations can be great.

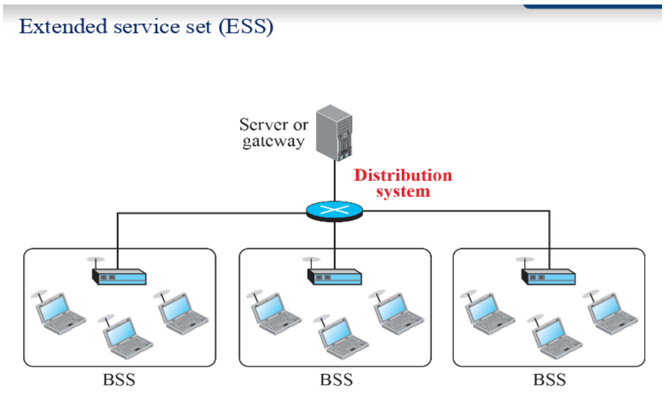
IEEE 802.11:

- IEEE defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data link layers.
- **Architecture:** this standard defines two kinds of services (i) Basic Service Set (BSS) (ii) Extended Service Set (ESS)
  - **BSS**: Basic service set is defined as the building block of a wireless LAN. It’s made of stationary or mobile wireless stations and an optional central base, known as Access Point (AP). A BSS without an AP is called an *Ad hoc* network (stations can locate each other without AP and form a network). A BSS with an AP is called an infrastructure network.



- **ESS:** made up of two or more BSSs with APs. BSS's are connected through a distribution system, usually a wired LAN. This distribution system connects the AP's in the BSS's. The distribution system is not restricted by IEEE 802.11 i.e. it can be any IEEE LAN such as Ethernet. ESS uses two types of stations; mobile and stationary. Mobile stations are normal stations inside BSS, stationary are AP stations which are part of wired LAN.

  When BSSs are connected, the stations within reach of one another can communicate without the use of an AP. However, communication between two stations in two different BSSs usually occurs via two APs.

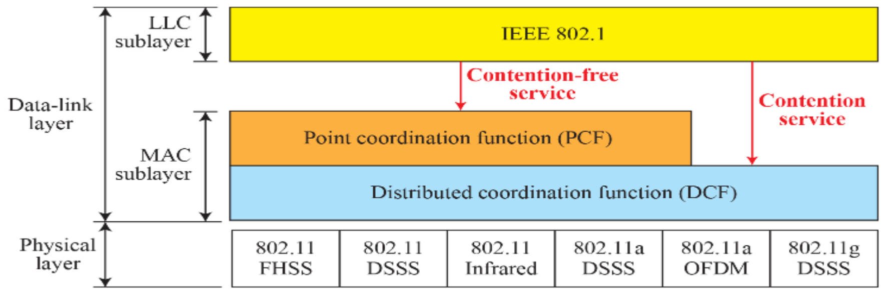


- **MAC Sublayer:** IEEE 802.11 defines two MAC sublayers: the distributed coordination function (DCF) and point coordination function (PCF). Figure below shows the relationship between the two MAC sublayers, the LLC sublayer, and the physical layer.
  - **DCF:** uses CSMA/CA as the access method.
  - **PCF:** Point Coordination Function (PCF) is an optional access method that can be implemented in an infrastructure network (not in an ad hoc network). Implemented on top of DCF and is used mostly for time-sensitive transmission. PCF has a centralized, contention free polling access method.

    The AP performs polling for stations capable of being polled. They are polled one after the other and send the data to the AP.

    Another interframe space, PIFS has been defined which gives priority to PCF over DCF. PIFS (PCF IFS) is shorter than DIFS meaning if a station wants to use only DCF and AP wants to use PCF, AP has priority.

MAC layers in IEEE 802.11 standard



FHSS - frequency hopping spread spectrum
DSSS - direct sequence spread spectrum
OFDM - orthogonal frequency division multiplexing

- **Contention Free Service:** A contended service is a service which offers the users of the network a minimum statistically guaranteed contention ratio, while typically offering peaks of usage of up to the maximum bandwidth supplied to the user.

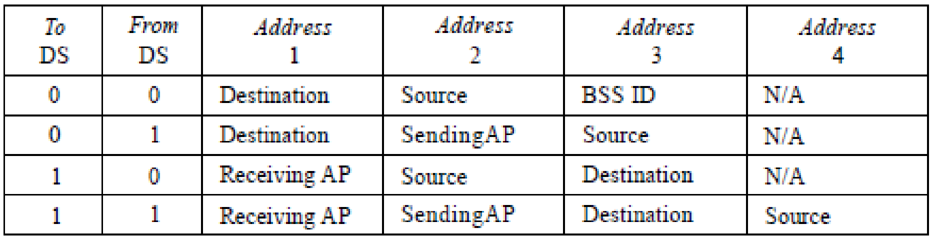
  In order to support applications that require near real-time service, the 802.11 standard includes a second coordination function to provide a different way of accessing the wireless medium.

  Due to the priority of PCF over DCF, stations that only use DCF may not gain access to the medium. To prevent this, a repetition interval has been designed to cover both contention-free PCF and contention-based DCF traffic. The repetition interval, which is repeated continuously, starts with a special control frame, called a beacon frame.

  When the stations hear the beacon frame, they start their NAV(Network Allocation Vector) for the duration of the contention-free period of the repetition interval. When the stations hear the beacon frame, they start their NAV for the duration of the contention-free period of the repetition interval. At the end of the contention-free period, the PC sends a CF end (contention-free end) frame to allow the contention-based stations to use the medium.
- **Fragmentation:** The wireless environment is very noisy; a corrupt frame has to be retransmitted. The protocol, therefore, recommends fragmentation-the division of a large frame into smaller ones. It is more efficient to resend a small frame than a large one.
- **Frame types:** A wireless LAN defined by IEEE 802.11 has three categories of frames: management frames, control frames, and data frames.
  - **Management frames:** are used for the initial communication between stations and access points (AP).
  - **Control frames:** are used for accessing the channel and acknowledging frames.
  - **Data Frames:** are used for carrying data and control information.
  - Acknowledgment is needed in this protocol because the station does not have any means to check for the successful arrival of its data at the destination. On the other hand, the lack of collision in CSMA/CD is a kind of indication to the source that data have arrived. (Collision During Handshaking)
- **Addressing mechanism:**

  The IEEE 802.11 addressing mechanism specifies four cases, defined by the value of the two flags in the FC field, To DS and From DS. Each flag can be either 0 or I, resulting in four different situations.

Table 14.3 *Addresses*



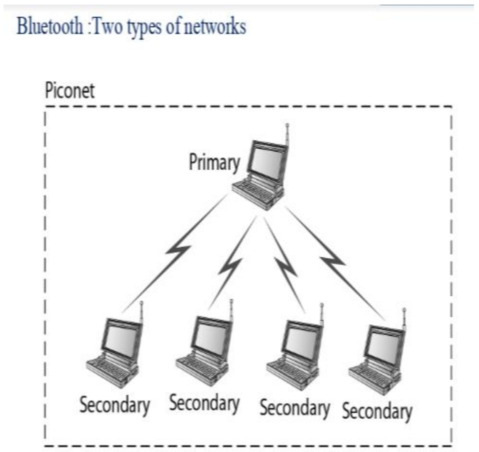
To DS	*From* DS	*Address* 1	*Address* 2	*Address* 3	*Address* 4
0	0	Destination	Source	BSS ID	N/A
0	1	Destination	SendingAP	Source	N/A
1	0	Receiving AP	Source	Destination	N/A
1	1	Receiving AP	SendingAP	Destination	Source

- Address 1 is always the address of the next device that the frame will visit.
- Address 2 is the address of the previous device the frame has left
- Address 3 is the address of the final destination if it is not defined by address 1 or original source station if it not defined by address 2
- Address 4 is the original source when the distribution system is also wired.

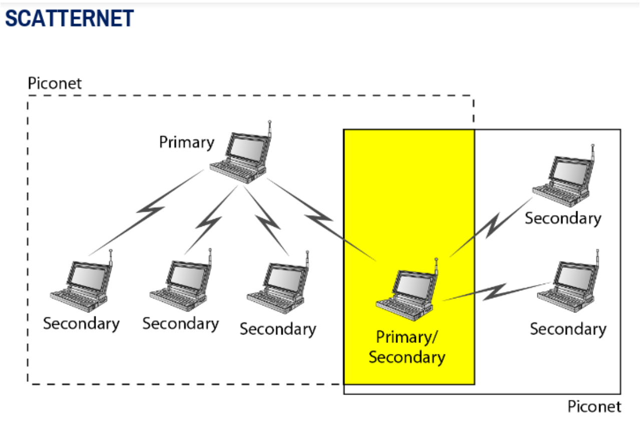
Bluetooth:

Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop), cameras, printers, coffee makers, and so on. A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously; the devices, sometimes called gadgets, find each other and make a network called a piconet. A Bluetooth LAN can even be connected to the Internet if one of the gadgets has this capability. A Bluetooth LAN, by nature, cannot be large. If there are many gadgets that try to connect, there is chaos.

- **Bluetooth Architecture:**
  Bluetooth defines two types of networks: piconet and scatternet.
  - **Piconet:** A Bluetooth network is called a piconet, or a small net. 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.
  - **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. A station can be a member of two piconets.

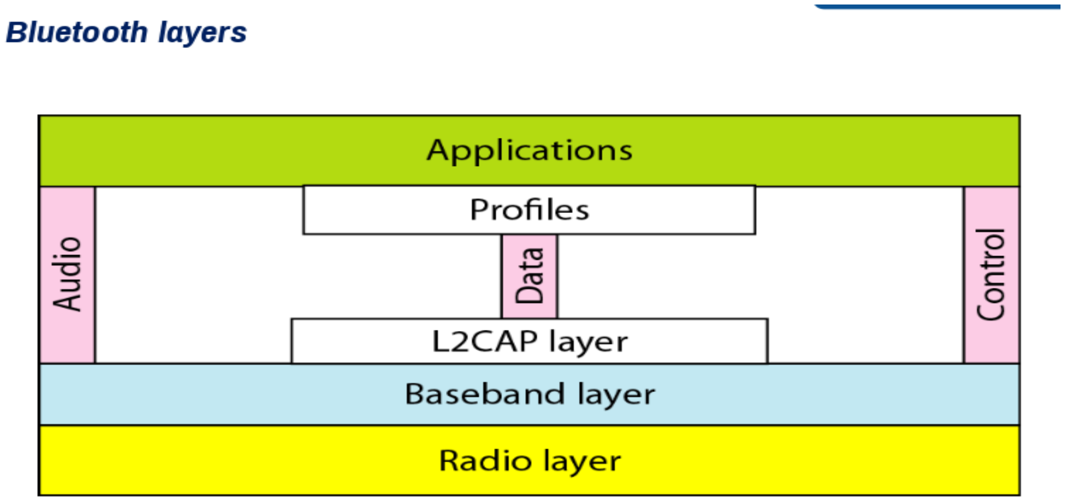


Bluetooth :Two types of networks



SCATTERNET

- **Bluetooth Layers:**



- **Radio Layer:** The radio layer is roughly equivalent to the physical layer of the Internet model. Bluetooth devices are low-power and have a range of 10m.
- **Baseband layer:** The baseband layer is roughly equivalent to the MAC sublayer in LANs. The access method is TDMA (see Chapter 12). The primary and secondary communicate with each other using time slots. The length of a time slot is exactly the same as the dwell time, 625 Ils. This means that during the time that one frequency is used, a sender sends a frame to a secondary, or a secondary sends a frame to the primary. Note that the communication is only between the primary and a secondary; secondaries cannot communicate directly with one another.
- **LWCAP layer:** The Logical Link Control and Adaptation Protocol, or L2CAP (L2 here means LL), is roughly equivalent to the LLC sublayer in LANs

Chapter – 15: Connecting Devices – no info on any slides, notes are from geeksforgeeks

Introduction: LANs do not normally operate in isolation. They are connected to one another or to the Internet. To connect LANs, or segments ofLANs, we use connecting devices. Connecting devices can operate in different layers of the Internet model. In this chapter, we discuss only those that operate in the physical and data link layers

1.) **Repeater –** operates at the physical layer. Job is to regenerate the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network. They do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

2.) **Hub –** 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. Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.

- **Active Hub -** hubs which have their own power supply and can clean, boost and relay the signal along with the network. It serves both as a repeater as well as wiring centre. These are used to extend the maximum distance between nodes.

- **Passive Hub** - These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.

3.) **Bridge –** operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.
   - **Transparent bridges -** These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.
   - **Source routing bridges -** In these bridges, routing operation is performed by source station and the frame specifies which route to follow.

4.) **Switch** – is a data link layer device. A switch is a multiport bridge with a buffer and a design that can boost its efficiency (a large number of ports imply less traffic) and performance. The switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only. In other words, switch divides collision domain of hosts, but broadcast domain remains same.

5.) **Router** – mainly a network layer device. It is a device like a switch that routes data packets based on their IP addresses. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.

6.) **Gateway** - A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.