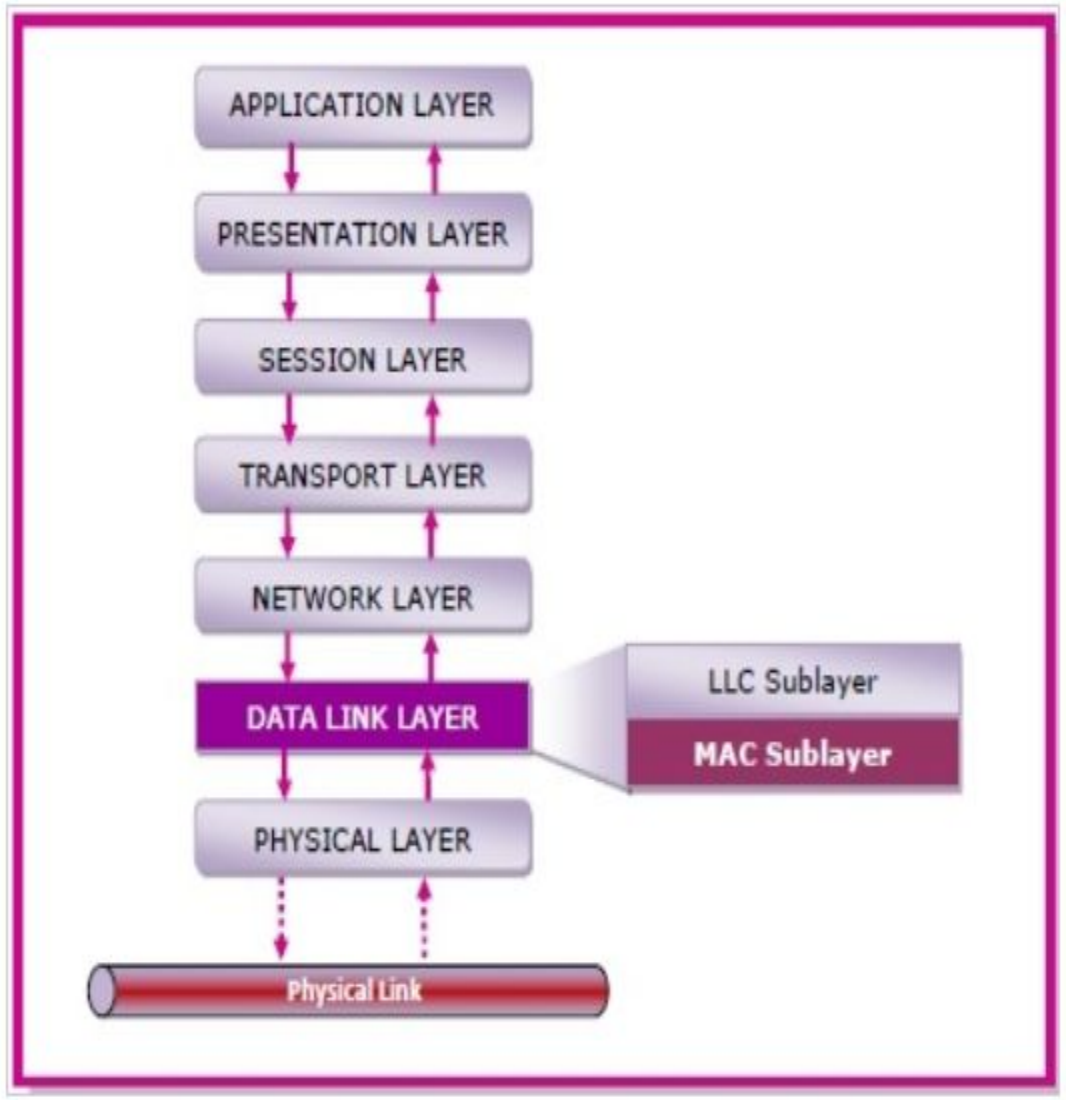
Unit-2

Medium Access Sub-Layer

Medium Access Sub-Layer:

- The medium access control (MAC) is a sublayer of the data link layer of the open system interconnections (OSI) reference model for data transmission.
- It is responsible for flow control and multiplexing for transmission medium. It sends data over the network interface card(NIC).
- The data link layer is the second lowest layer. It is divided into two sublayers −
  - The logical link control (LLC) sublayer
  - The medium access control (MAC) sublayer

MAC Sub-layer:

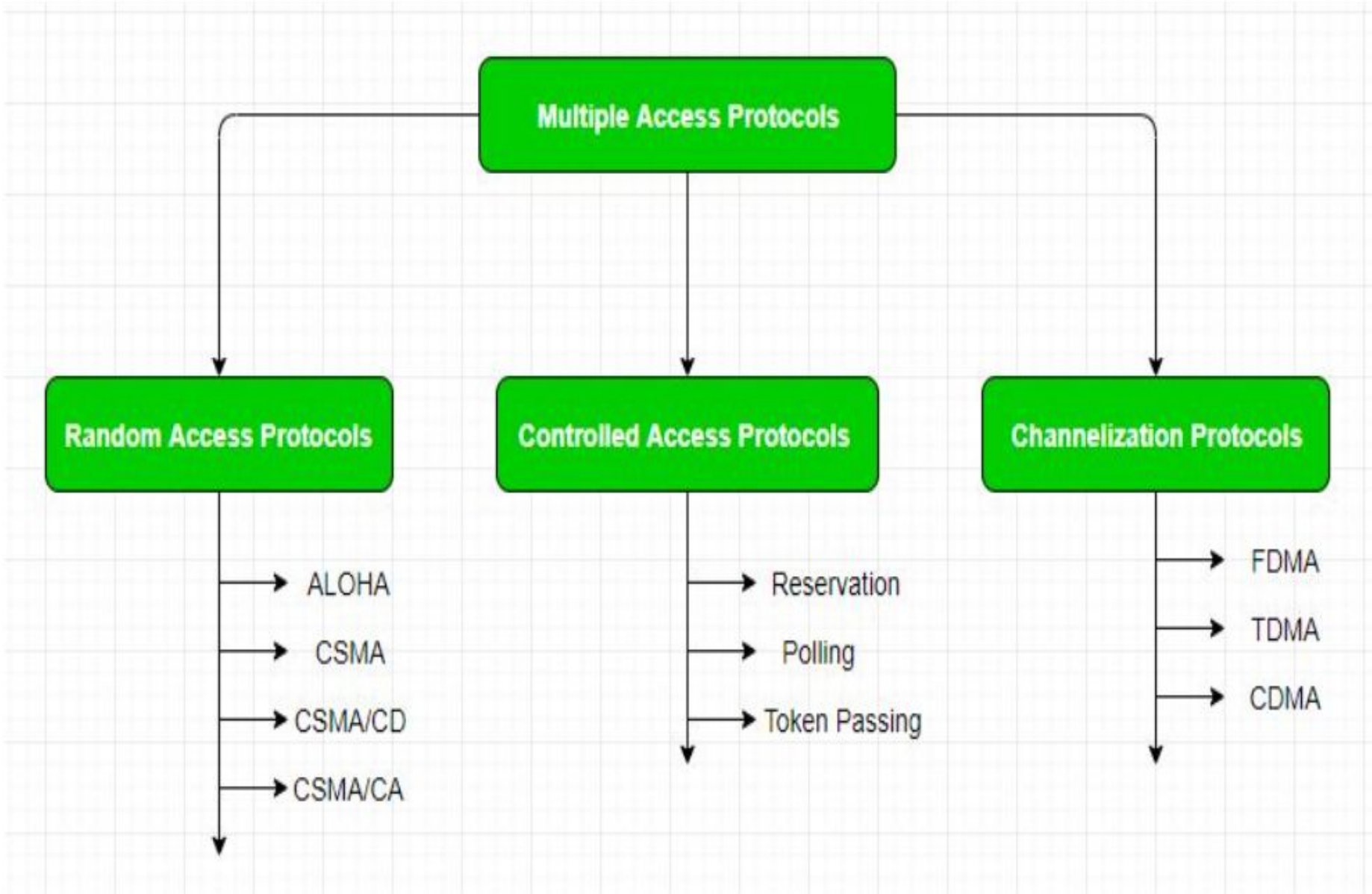


Functions of MAC Layer:

- Abstraction of the physical layer to the LLC and upper layers of the
- Responsible for encapsulating frames so that they are suitable for transmission via the physical medium.
- addressing of source station as well as the destination station
- Multiple access resolutions when more than one data frame is to be transmitted. It determines the channel access methods for transmission.
- collision resolution and initiating retransmission in case of collisions.
- generates the frame check sequences

MAC Address

- MAC address or media access control address is a unique identifier allotted to a network interface controller (**NIC**) of a device.
- It is used as a network address for data transmission within a network segment like **Ethernet, Wi-Fi, and Bluetooth**.
- MAC address is assigned to a network adapter at the time of manufacturing. It is hardwired or hard-coded in the network interface card (NIC). A MAC address comprises of six groups of two hexadecimal digits, separated by hyphens, colons, or no separators. An example of a MAC address is **00:0A:89:5B:F0:11.**


Multiple Access Protocols
Random Access Protocols
Controlled Access Protocols
Channelization Protocols
ALOHA
CSMA
CSMA/CD
CSMA/CA
Reservation
Polling
Token Passing
FDMA
TDMA
CDMA

Pure Aloha Protocol

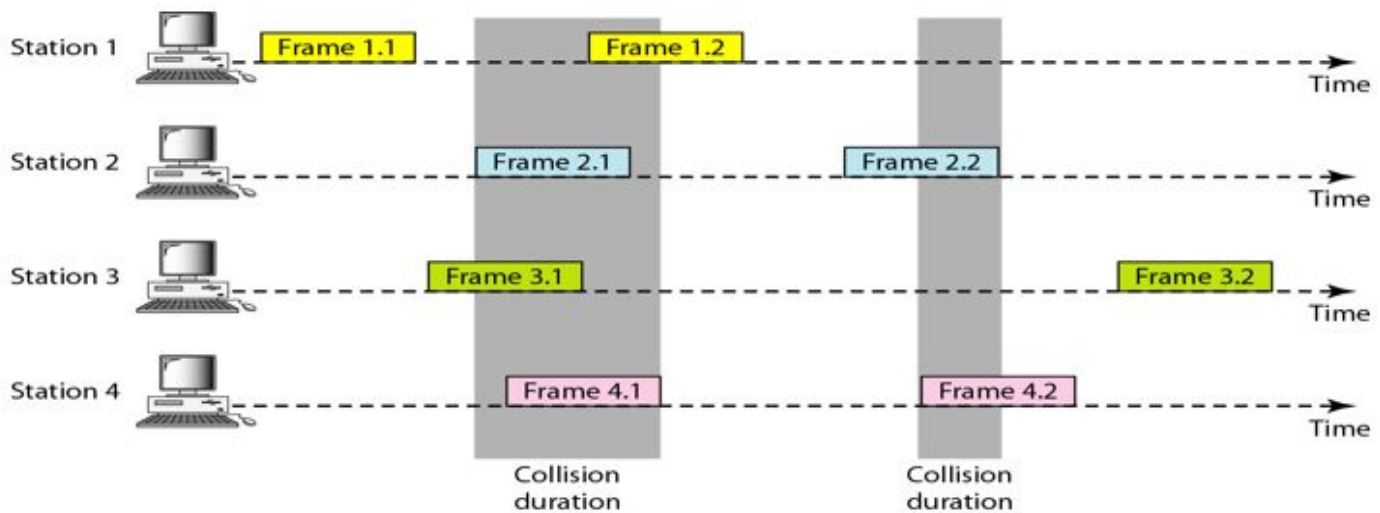
- It allows users to transmit whenever they have data to be sent.
- Senders wait to see if a collision occurred (after whole message has been sent).
- If collision occurs, each station involved waits a **random amount of time** then tries again.
- Systems in which multiple users share a common channel in a way that can lead to conflicts are widely known as **contention systems**.
- Whenever two frames try to occupy the channel at the same time, there will be a collision and both will be garbled.
- If the first bit of a new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be retransmitted later.

Pure ALOHA – Cont…

- Frames are transmitted at completely arbitrary times.
- The throughput of the Pure ALOHA is maximized when the frames are of uniform length.
- The formula to calculate the throughput of the Pure ALOHA is

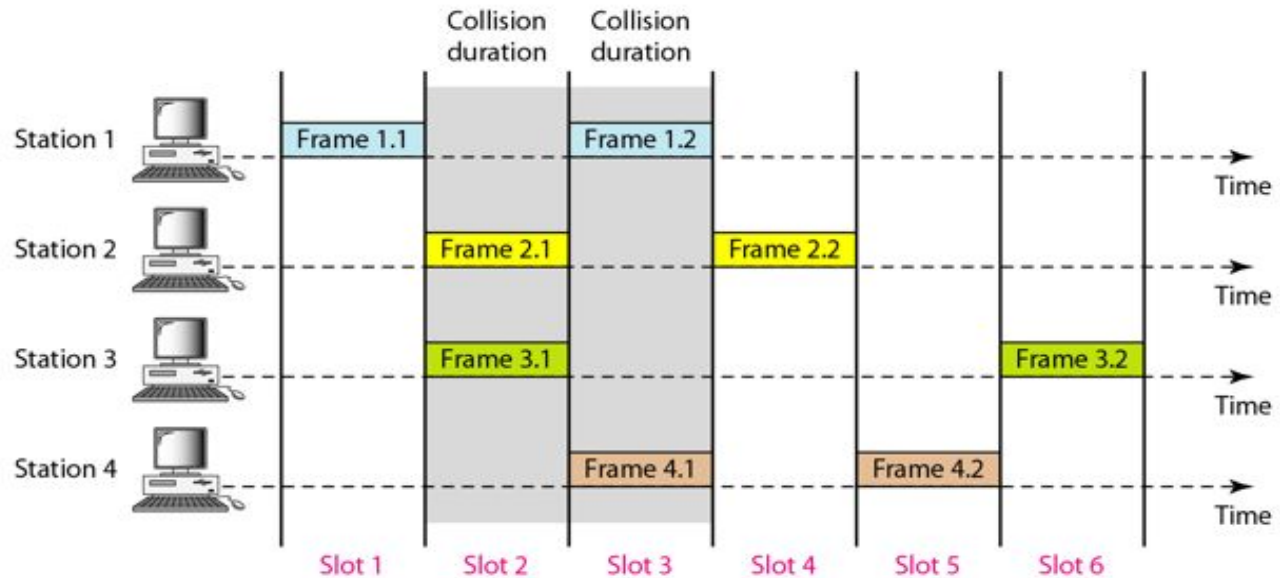
S-=G*e^-2G

- The throughput is maximum when G=1/2 which is 18% of the total transmitted data frames.

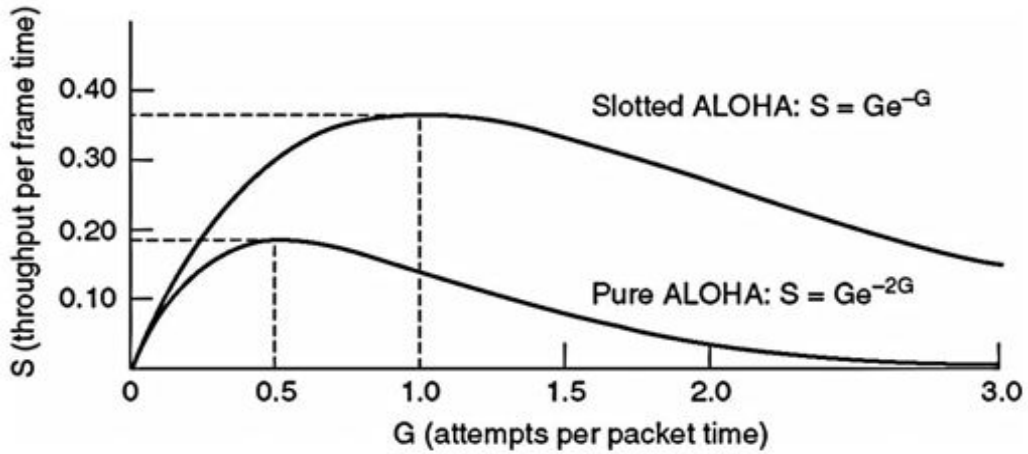


Slotted Aloha

- It was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high.
- The time of the shared channel is divided into discrete intervals called slots.
- The stations can send a frame only at the beginning of the slot and only one frame is sent in each slot.



Slotted Aloha – Cont…



- If any station is not able to place the frame onto the channel at the beginning of the slot then the station has to wait until the beginning of the next time slot.
- The formula to calculate the throughput of the Slotted ALOHA is

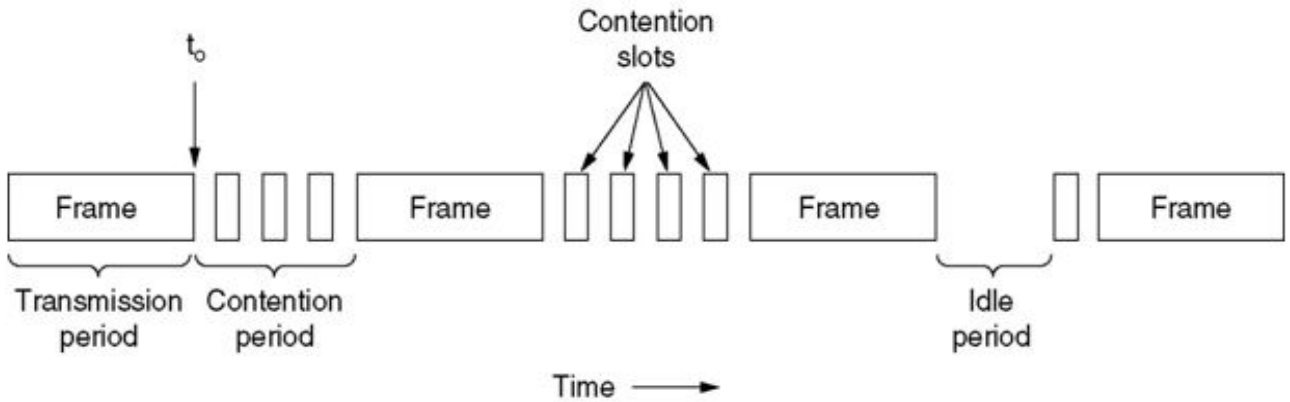
  S=G*e^-G

- The throughput is maximum when G=1 which is 37% of the total transmitted data frames.
- 37% of the time slot is empty, 37% successes and 26% collision.

CSMA/CD (CSMA with Collision Detection)

- If two stations sense the channel to be idle and begin transmitting simultaneously, they will both detect the collision almost immediately.
- Rather than finish transmitting, they should abruptly stop transmitting as soon as the collision is detected.
- Quickly terminating damaged frames saves time and bandwidth.
- This protocol, known as CSMA/CD (CSMA with Collision Detection) is widely used on LANs in the MAC sub layer.

CSMA/CD – Cont...



- At the point marked t_0, a station has finished transmitting its frame. Any other station having a frame to send may now attempt to do so.
- After a station detects a collision, it aborts transmission, waits a random period of time, and then tries again, assuming that no other station has started transmitting in the meantime.
- Therefore, CSMA/CD will consist of alternating contention and transmission periods, with idle periods occurring when all stations are quiet.

Algorithms

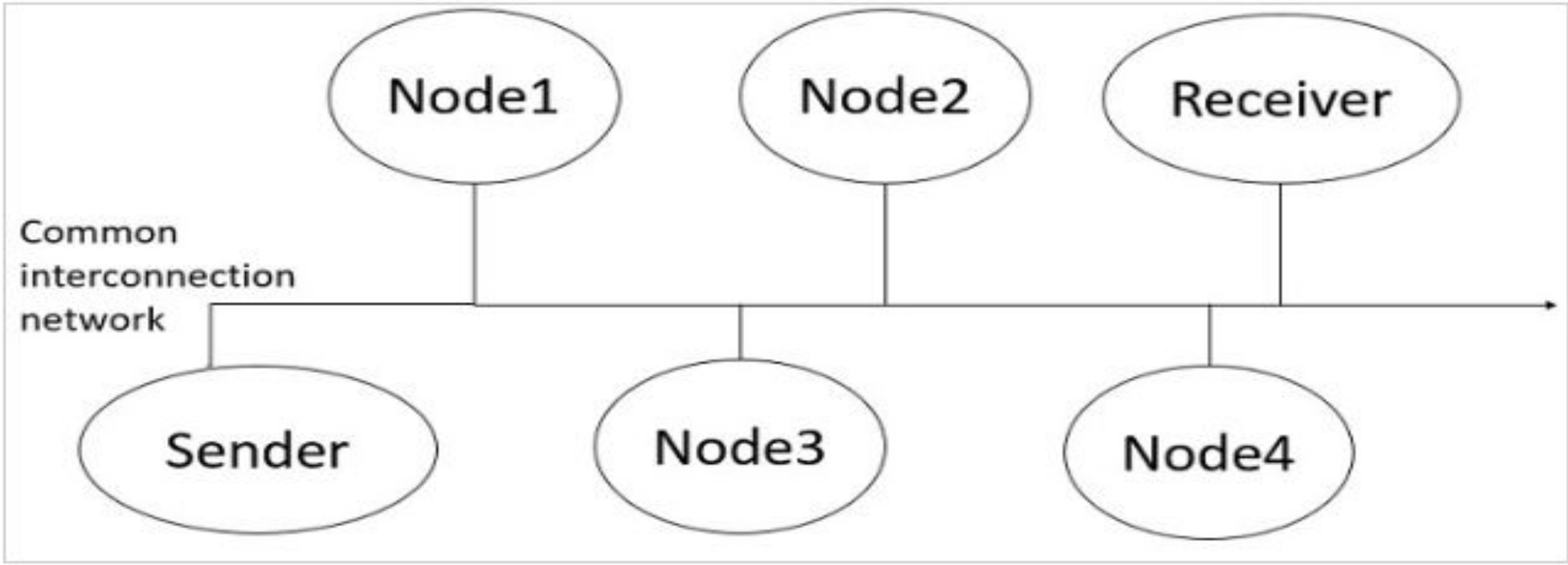
The algorithm of CSMA/CD is:

- When a frame is ready, the transmitting station checks whether the channel is idle or busy.
- If the channel is busy, the station waits until the channel becomes idle.
- If the channel is idle, the station starts transmitting and continually monitors the channel to detect collision.
- If a collision is detected, the station starts the collision resolution algorithm.
- The station resets the retransmission counters and completes frame transmission.

The algorithm of Collision Resolution is:

- The station continues transmission of the current frame for a specified time along with a jam signal, to ensure that all the other stations detect collision.
- The station increments the retransmission counter.
- If the maximum number of retransmission attempts is reached, then the station aborts transmission.
- Otherwise, the station waits for a backoff period which is generally a function of the number of collisions and restart main algorithm.

The Carrier Sense Multiple Access (CSMA) Protocol is diagrammatically represented as follows −



Key points to remember

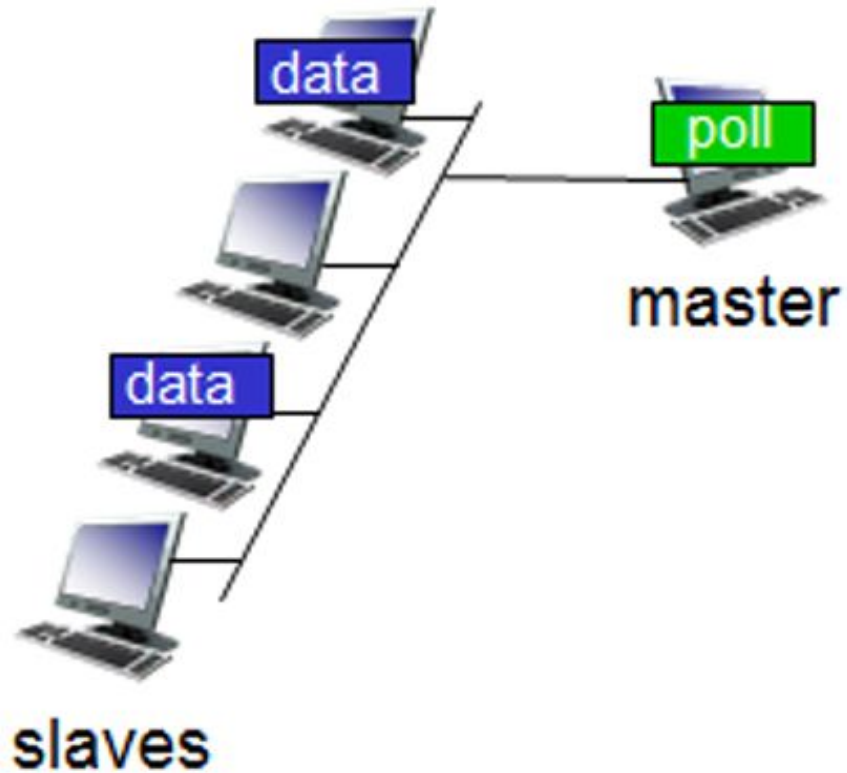
- CSMA/CD can handle network traffic effectively
- High network traffic can be reduced by increasing the waiting time between transmissions
- This reduces overall network traffic and improves efficiency
- Large packets are not preferable as they take longer to transmit and increase collision chances
- Smaller packets are favorable for high-speed bandwidth and network efficiency

Polling

- It requires one of the nodes to be designated as a master node.
- The master node polls each of the nodes in a round-robin fashion.
- The master node first sends a message to node 1, saying that it (node 1) can transmit up to some maximum number of frames.
- After node 1 transmits some frames, the master node tells node 2 it (node 2) can transmit up to the maximum number of frames.
- The master node can determine when a node has finished sending its frames by observing the lack of a signal on the channel.

Polling – Cont…

- The procedure continues in this manner, with the master node polling each of the nodes in a cyclic manner.
- The polling protocol eliminates the collisions and empty slots that plague random access protocols.



Advantages of Polling:

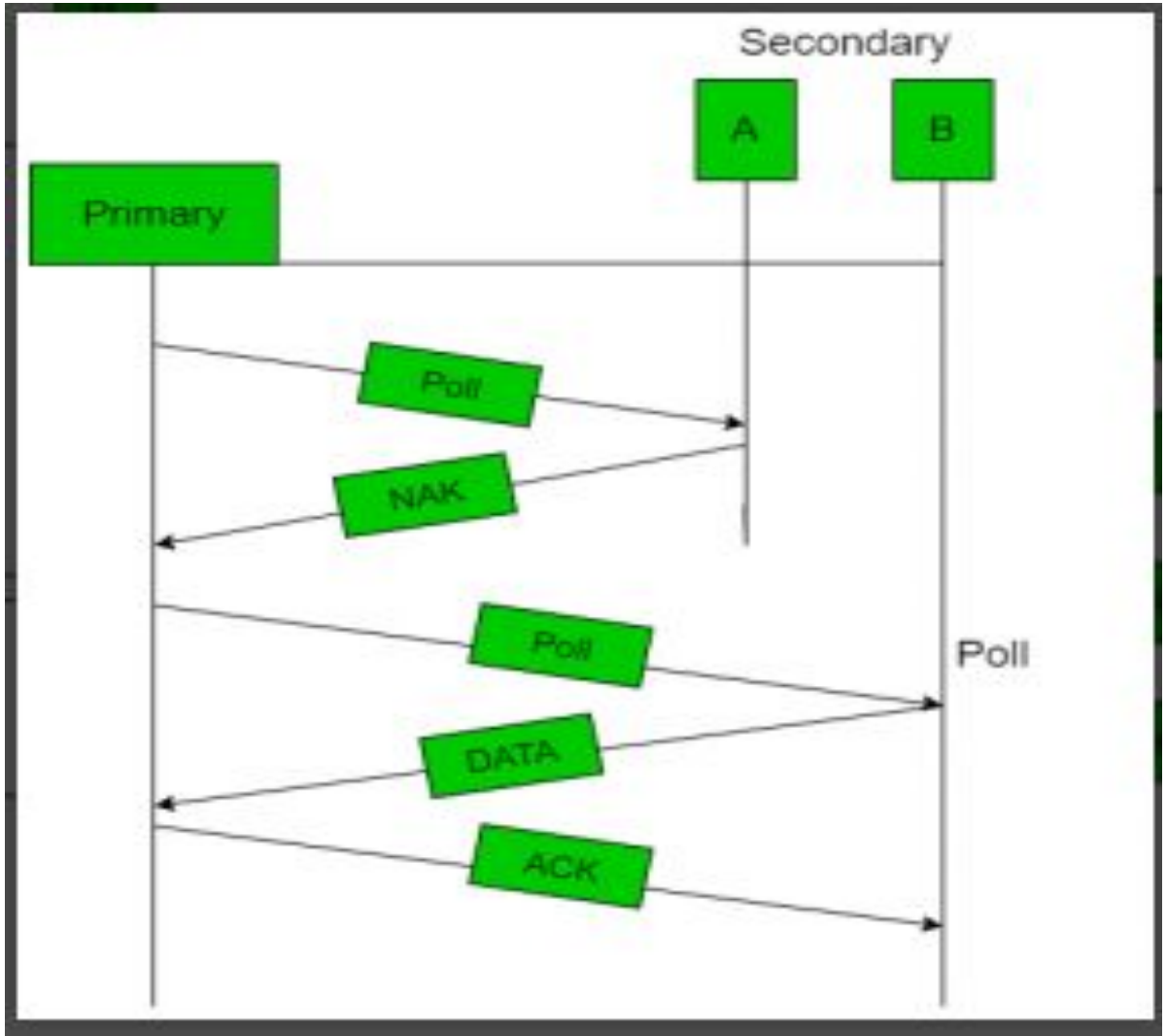
- The maximum and minimum access time and data rates on the channel are fixed predictable.
- It has maximum *efficiency.*
- It has maximum *bandwidth.*
- No slot is wasted in polling.
- There is assignment of priority to ensure faster access from some secondary.

Disadvantages of Polling:

- It consume *more time.*
- Since every station has an equal chance of winning in every round, link sharing is *biased.*
- Only some station might run out of data to send.
- An increase in the turnaround time leads to a drop in the data rates of the channel under low loads.

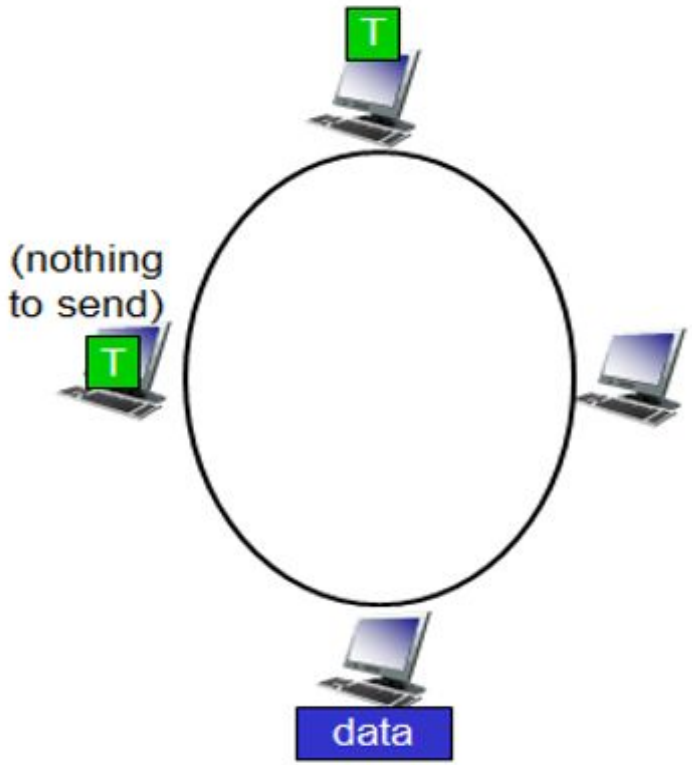
Efficiency Let Tpoll be the time for polling and Tt be the time required for transmission of data. Then,

```
Efficiency = Tt/(Tt + Tpoll)
```



Token Passing

- There is no master node.
- A small, special-purpose frame known as a token is exchanged among the nodes in some fixed order.
- For example, node 1 might always send the token to node 2, node 2 might always send the token to node 3, and node N might always send the token to node 1.
- When a node receives a token, it holds onto the token only if it has some frames to transmit; otherwise, it immediately forwards the token to the next node.
- If failure of one node can crash the entire channel. Or if a node accidentally neglects to release the token.



Performance of token ring can be concluded by 2 parameters:-

1. **Delay**, is a measure of time between when a packet is ready and when it is delivered. So, the average time (delay) required to send a token to the next station = a/N.
2. **Throughput**, which is a measure of successful traffic.

Throughput, $S = 1/(1 + a/N)$ for $a<1$

and

$S = 1/\{a(1 + 1/N)\}$ for $a>1$.

where N = number of stations

$a = Tp/Tt$

(Tp = propagation delay and Tt = transmission delay)

Advantages of Token passing:

- It may now be applied with routers cabling and includes built-in debugging features like *protective relay and auto reconfiguration.*
- It provides *good throughput* when conditions of high load.

Disadvantages of Token passing:

- Its cost is *expensive.*
- Topology components are more expensive than those of other, more widely used standard.
- The hardware element of the token rings are designed to be tricky. This implies that you should choose on manufacture and use them exclusively.

IEEE 802.3 frame format

Basic frame format which is required for all MAC implementation is defined in **IEEE 802.3 standard**. Though several optional formats are being used to extend the protocol's basic capability.

IEEE 802.3 ETHERNET Frame Format

1. **PREAMBLE –** Ethernet frame starts with a 7-Bytes Preamble. This is a pattern of alternative 0's and 1's which indicates starting of the frame and allow sender and receiver to establish bit synchronization. Initially, PRE (Preamble) was introduced to allow for the loss of a few bits due to signal delays.
2. **Start of frame delimiter (SFD) –** This is a 1-Byte field that is always set to 10101011. SFD indicates that upcoming bits are starting the frame, which is the destination address. Sometimes SFD is considered part of PRE, this is the reason Preamble is described as 8 Bytes in many places. The SFD warns station or stations that this is the last chance for synchronization.
3. **Destination Address –** This is a 6-Byte field that contains the MAC address of the machine for which data is destined.
4. **Source Address –** This is a 6-Byte field that contains the MAC address of the source machine. As Source Address is always an individual address (Unicast), the least significant bit of the first byte is always 0.

5.Length – Length is a 2-Byte field, which indicates the length of the entire Ethernet frame. This 16-bit field can hold a length value between 0 to 65534, but length cannot be larger than 1500 Bytes because of some own limitations of Ethernet.

6.Data – This is the place where actual data is inserted, also known as **Payload**. Both IP header and data will be inserted here if Internet Protocol is used over Ethernet. The maximum data present may be as long as 1500 Bytes. In case data length is less than minimum length i.e. 46 bytes, then padding 0's is added to meet the minimum possible length.

7.Cyclic Redundancy Check (CRC) – CRC is 4 Byte field. This field contains a 32-bits hash code of data, which is generated over the Destination Address, Source Address, Length, and Data field. If the checksum computed by destination is not the same as sent checksum value, data received is corrupted.

8.VLAN Tagging – The Ethernet frame can also include a VLAN (Virtual Local Area Network) tag, which is a 4-byte field inserted after the source address and before the EtherType field. This tag allows network administrators to logically separate a physical network into multiple virtual networks, each with its own VLAN ID.

9.Jumbo Frames – In addition to the standard Ethernet frame size of 1518 bytes, some network devices support Jumbo Frames, which are frames with a payload larger than 1500 bytes. Jumbo Frames can increase network throughput by reducing the overhead associated with transmitting a large number of small frames.

Disadvantages:

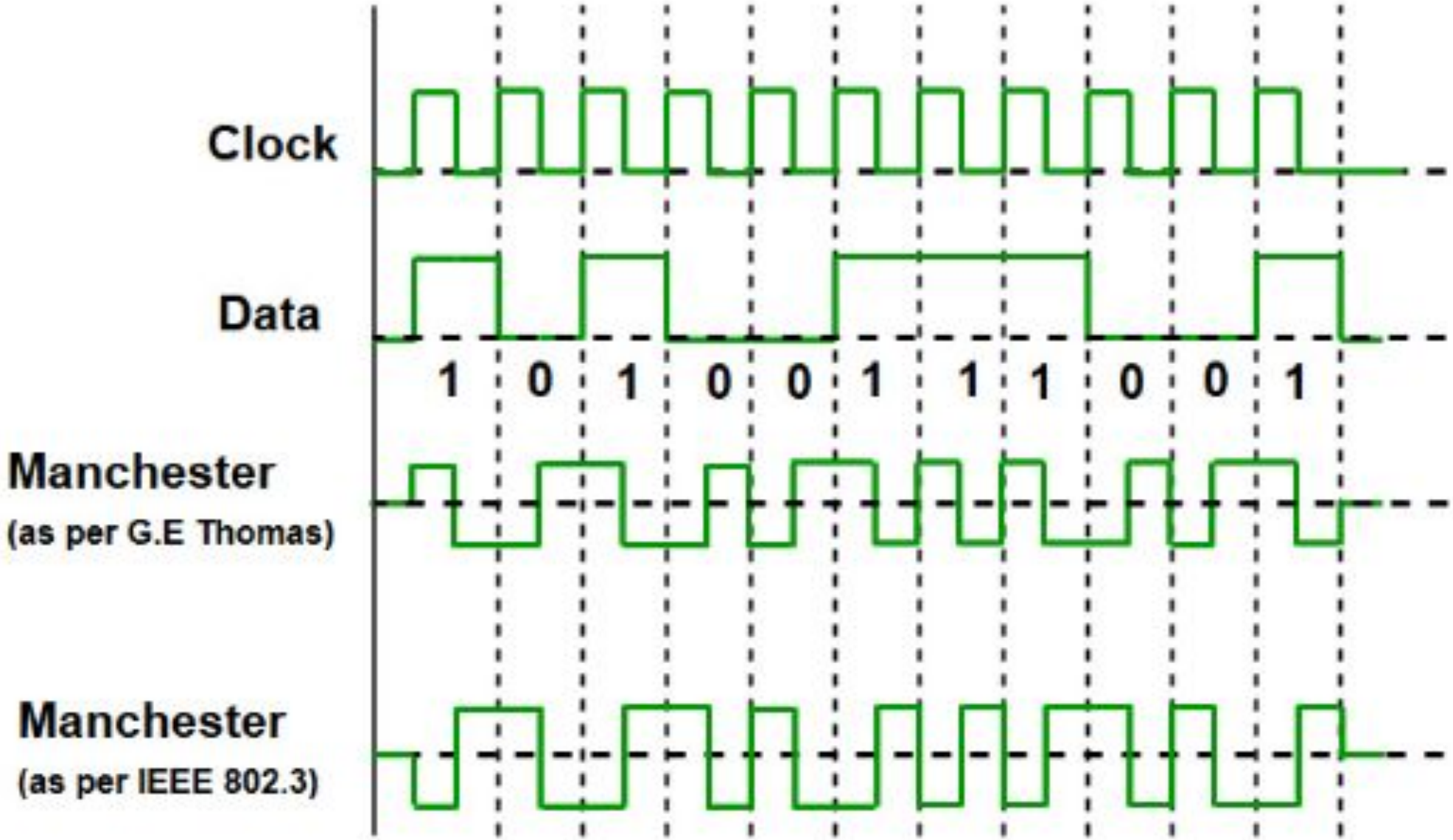
- Limited frame size
- Broadcast storms
- Security vulnerabilities
- Limited speed
- Limited distance

Advantages:

- Simple format
- Flexibility
- Widely adopted
- Error detection
- Support for VLANs

Manchester encoding

- Manchester encoding is a synchronous clock encoding technique used by the physical layer of the Open System Interconnection [OSI] to encode the clock and data of a synchronous bit stream.
- In manchester duration of a bit is divided into two halves.
- The voltage remains the same at one level during the first half & moves to the other level
- The transition at the middle of the bit provides synchronization.
- There is always a transition at the middle of the bit, but the bit values are determined at the beginning of the bit. if next bit is zero there is transition if next bit is 1 there is none.


Clock
Data
1 0 1 0 0 1 1 1 0 0 1
Manchester
(as per G.E Thomas)
Manchester
(as per IEEE 802.3)

Non-return-to-zero [NRZ] –

NRZ code's voltage level is constant during a bit interval. When there is a long sequence of 0s and 1s, there is a problem at the receiving end. The problem is that the synchronization is lost due to a lack of transmissions.

It is of 2 types:

1. **NRZ-level encoding –**

   The polarity of signals changes when the incoming signal changes from '1' to '0' or from '0' to '1'. It considers the first bit of data as polarity change.

1. **NRZ-Inverted/ Differential encoding –**

   In this, the transitions at the beginning of the bit interval are equal to 1 and if there is no transition at the beginning of the bit interval is equal to 0.

Characteristics of Manchester Encoding –

- A logic 0 is indicated by a 0 to 1 transition at the center of the bit and logic 1 by 1 to 0 transition.
- signal transitions do not always occur at the ‘bit boundary’ but there is always a transition at the center of each bit
- The **Differential Physical Layer Transmission** does not employ an inverting line driver to convert the binary digits into an electrical signal.
- When a high to low transition happens, a ‘1’ is recorded; when a low to high transition occurs, a ‘0’ is recorded.
- Manchester encoding can also be used for multi-level signaling, where multiple voltage levels are used to represent different data states.
- It is a self-clocking protocol, meaning that the receiver can determine the clock frequency from the incoming data.

Advantages of Manchester Encoding:

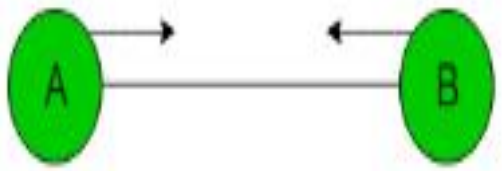
- Self-clocking
- Reduced DC component
- Error detection
- Simplicity

Disadvantages of Manchester Encoding:

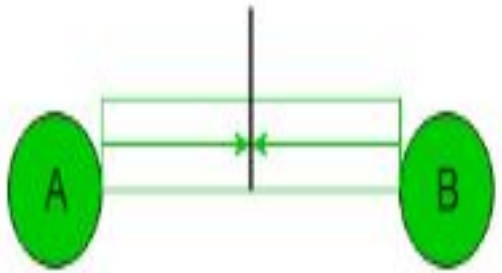
- Lower data rate
- Higher bandwidth requirement
- Clock synchronization
- Reduced transmission distance

Binary exponential back off algorithm

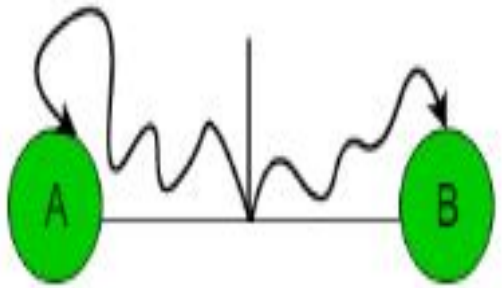
- Back-off algorithm is a **collision resolution** mechanism which is used in random access MAC protocols (CSMA/CD).
- This algorithm is generally used in Ethernet to schedule re-transmissions after collisions.
- If a collision takes place between 2 stations, they may restart transmission as soon as they can after the collision.
- This will always lead to another collision and form an infinite loop of collisions leading to a deadlock.



At t = 0 , both A and B start transmission



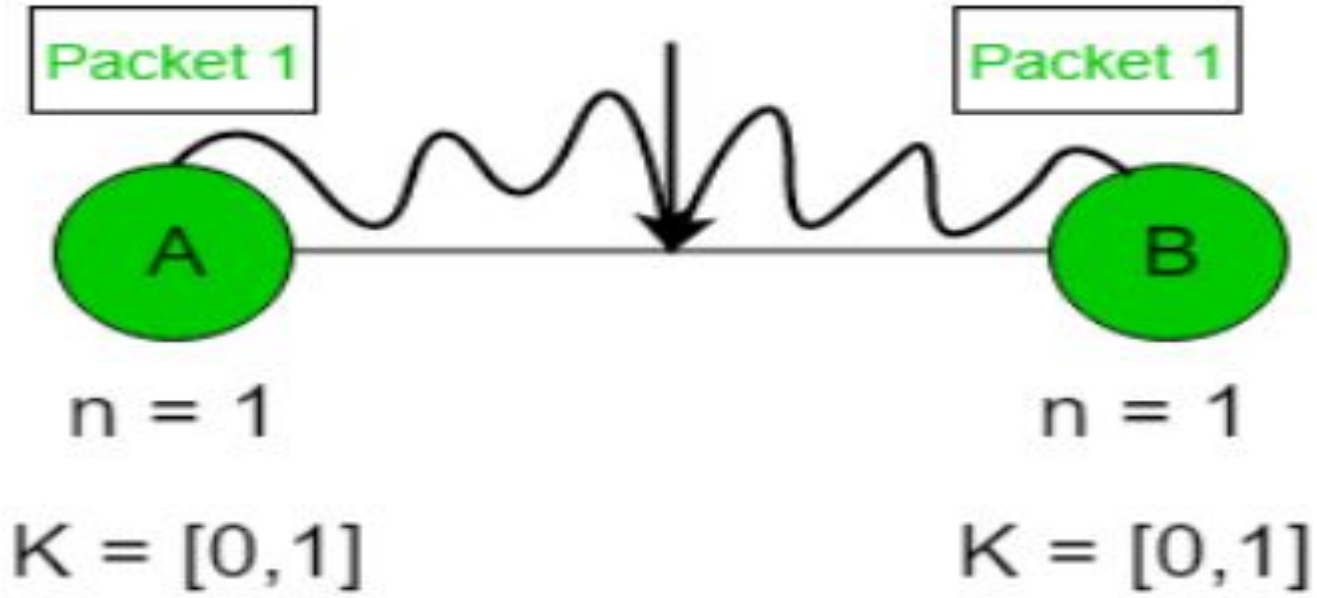
Packets of both A and B collide



Both stations A and B detect collision

Waiting time = back-off time
Let n = collision number or re-transmission serial number.
Then,
Waiting time = K * T_{slot}
where K = [0, $2^n - 1$]

Example – Case-1 : Suppose 2 stations A and B start transmitting data (Packet 1) at the same time then, collision occurs. So, the collision number n for both their data (Packet 1) = 1. Now, both the station randomly pick an integer from the set K i.e. {0, 1}.



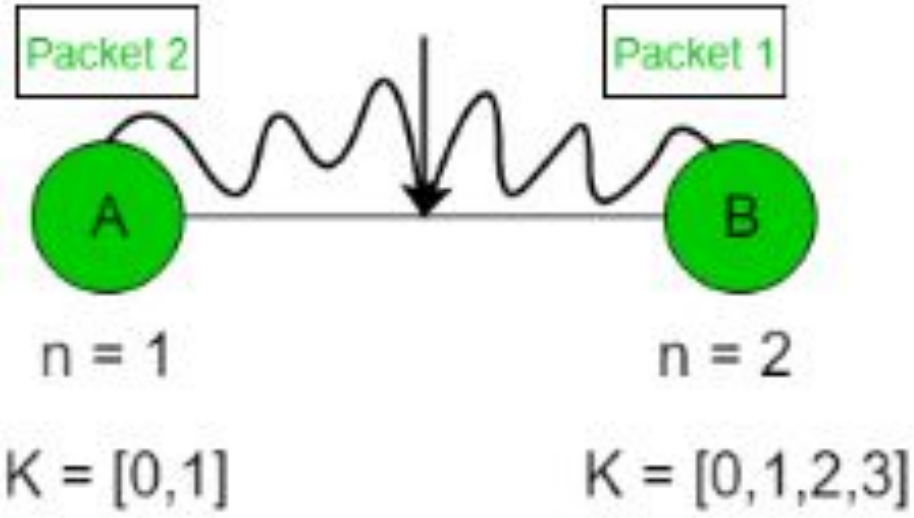
Value of K

A	B
0	0
0	1
1	0
1	1

- **When both A and B choose K = 0** –> Waiting time for A = 0 * T_{slot} = 0 Waiting time for B = 0 * T_{slot} = 0 Therefore, both stations will transmit at the same time and hence collision occurs.
- **When A chooses K = 0 and B chooses K = 1** –> Waiting time for A = 0 * T_{slot} = 0 Waiting time for B = 1 * T_{slot} = T_{slot} Therefore, A transmits the packet and B waits for time T_{slot} for transmitting and hence A wins.
- **When A chooses K = 1 and B chooses K = 0** –> Waiting time for A = 1 * T_{slot} = T_{slot} Waiting time for B = 0 * T_{slot} = 0 Therefore, B transmits the packet and A waits for time T_{slot} for transmitting and hence B wins.
- **When both A and B choose K = 1** –> Waiting time for A = 1 * T_{slot} = T_{slot} Waiting time for B = 1 * T_{slot} = T_{slot} Therefore, both will wait for the same time T_{slot} and then transmit. Hence, a collision occurs.

```
Probability that A wins = 1/4
Probability that B wins = 1/4
Probability of collision  = 2/4
```

Case-2: Assume that A wins in Case 1 and transmitted its data(Packet 1). Now, as soon as B transmits its packet 1, A transmits its packet 2. Hence, collision occurs. Now collision no. n becomes 1 for packet 2 of A and becomes 2 for packet 1 of B. For packet 2 of A, K = {0, 1} For packet 1 of B, K = {0, 1, 2, 3}



Value of K

A	B
0	0
0	1
0	2
0	3
1	0
1	1
1	2
1	3

```
Probability that A wins = 5/8
Probability that B wins = 1/8
Probability of collision  = 2/8
```

So, the probability of collision decreases as compared to Case 1.

Advantage

- Improves network performance
- Increases channel utilization
- Reduces delays
- Fairness
- Adaptability
- Scalability
- Energy Efficiency
- Robustness

Disadvantages –

- Capture effect
- Increased overhead