

Data Link Layer

Compiled by: Hiranya Prasad Bastakoti

Contents:

- Function of Data Link Layer
- Overview of Logical Link Control (LLC) and Media Access Control (MAC)
- Framing and Flow control Mechanism
- Error Detection and Correction techniques
- Channel Allocation techniques
- Ethernet standards
- Wireless LAN
- Overview Virtual Circuit Switching, Frame Relay & ATM
- DLL Protocol

Function of Data Link Layer

- The data-link layer is responsible for transferring a datagram across an individual link.
- A link is the communication channels that connect two adjacent hosts or routers.
- Examples of link-layer protocols include Ethernet, token ring, FDDI, and PPP.
- In order to move a datagram from source host to destination host, the datagram must be moved over each of the individual links in the path.
- The data-link layer is responsible for transferring a datagram that comes from the network layer across an individual link.

Functions

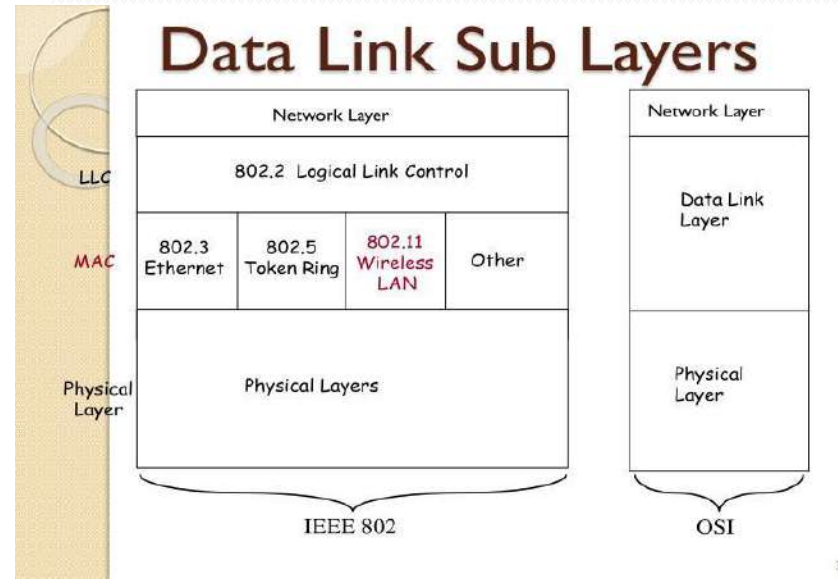
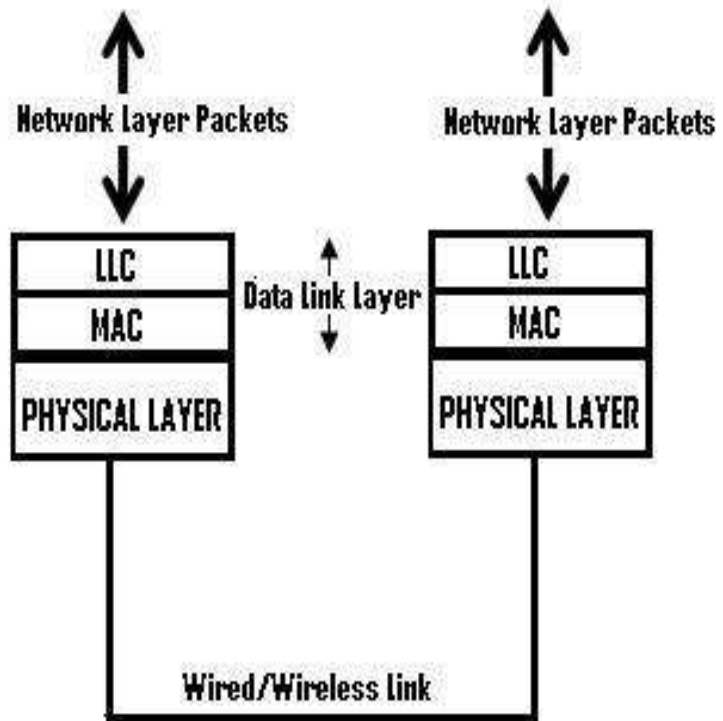
- Framing and link access: Almost all link-layer protocols encapsulate each network-layer datagram within a network-layer datagram is inserted, and a number of header fields. A data-link protocol specifies the structure of the frame, as well as a channel access protocol that specifies the rules by which a frame is transmitted onto the link.
- Reliable delivery: When a link-layer protocol provides reliable-delivery service, it guarantees to move each network-layer datagram across the link without error. This is achieved with acknowledgments and retransmissions.
- Flow control: A link-layer protocol can provide flow control in order to prevent the sending node on one side of a link from overwhelming the receiving node on the other side of the link.

- **Error detection:** Many link-layer protocols provide a mechanism to detect the presence of one or more errors. This is done by having the transmitting node set error-detection bits in the frame, and having the receiving node perform an error check. Error detection is a very common service among link-layer protocols.
- **Error correction:** Error correction is similar to error detection, except that a receiver cannot only detect whether errors have been introduced in the frame but can also determine exactly where in the frame the errors have occurred (and hence correct these errors).
- **Half-duplex and full-duplex:** With full-duplex transmission, the nodes at both ends of a link may transmit packets at the same time. With half-duplex transmission, a node cannot both transmit and receive at the same time.

Overview of Logical Link Control (LLC) and Media Access Control (MAC)

The data link layer is made up of two sublayers:

- LLC (Logical Link Control) Layer
- MAC(Media Access Control)Layer
- Both of these two sublayers are responsible for different functions for the data link layer.
- LLC interacts with the network layer above and the lower sub-layer, termed as MAC, that interacts with the physical layer below, as shown in the diagram given below:



LLC (Logical Link Control) Layer

- LLC is responsible for handling multiple Layer3 protocols (multiplexing/de-multiplexing) and link services like reliability and flow control, The functional overview of LLC are:
- This sublayer multiplexes protocols running a top the data link layer, and optionally provides flow control, acknowledgment, and error recovery.
- The LLC provides addressing and control of the data link. It specifies which mechanisms are to be used for addressing stations over the transmission medium and for controlling the data exchanged between the originator and recipient machines.

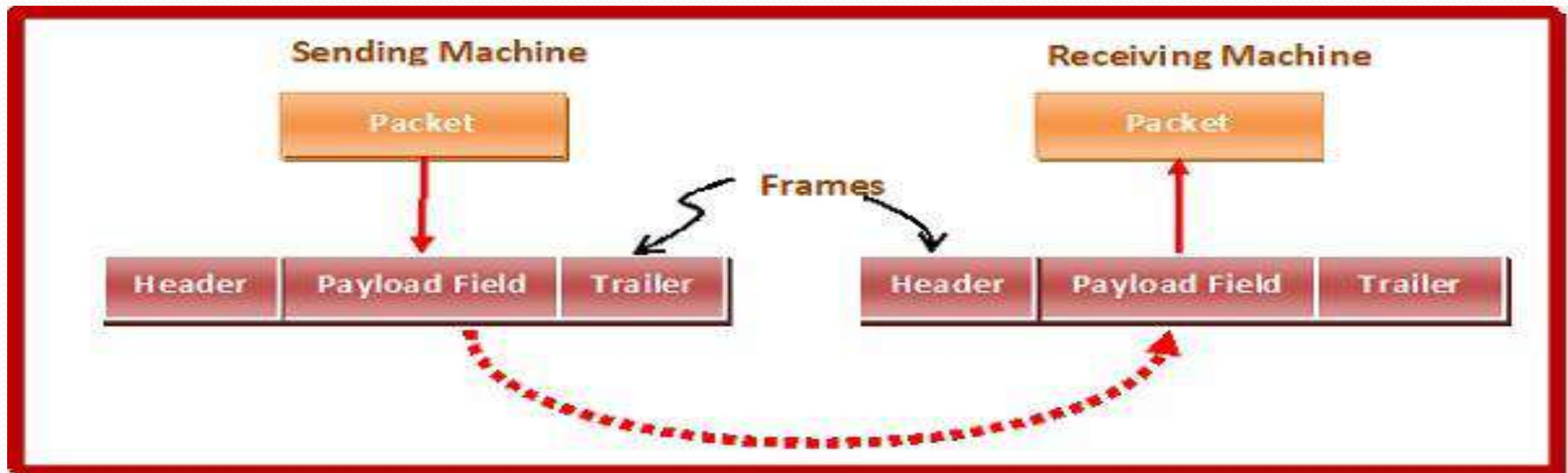
MAC Layer

- Media Access Control (MAC) sublayer provides control for accessing the transmission medium.
- It is responsible for moving data packets from one network interface card (NIC) to another, across a shared transmission medium.
- Physical addressing is handled at the MAC sublayer. MAC is also handled at this layer. This refers to the method used to allocate network access to computers and prevent them from transmitting at the same time, causing data collisions.
- Common MAC methods include Carrier Sense Multiple Access/Collision Detection (CSMA/CD), used by Ethernet networks, Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA), used by AppleTalk networks, and token passing, used by Token Ring and Fiber Distributed Data Interface (FDDI) networks.

Framing and Flow control Mechanism

Framing:

- In the physical layer, data transmission involves synchronized transmission of bits from the source to the destination. The data link layer packs these bits into frames.
- Data-link layer takes the packets from the Network Layer and encapsulates them into frames. If the frame size becomes too large, then the packet may be divided into small sized frames. Smaller sized frames makes flow control and error control more efficient.
- Then, it sends each frame bit-by-bit on the hardware. At receiver's end, data link layer picks up signals from hardware and assembles them into frames.



Parts of a Frame

- Frame Header – It contains the source and the destination addresses of the frame.
- Payload field – It contains the message to be delivered.
- Trailer – It contains the error detection and error correction bits.
- Flag – It marks the beginning and end of the frame.



Types of Framing

Fixed-sized Framing

- Here the size of the frame is fixed and so the frame length acts as delimiter of the frame. Consequently, it does not require additional boundary bits to identify the start and end of the frame.
- Example – ATM cells.

Variable – Sized Framing

- Here, the size of each frame to be transmitted may be different. So additional mechanisms are kept to mark the end of one frame and the beginning of the next frame.
- It is used in local area networks.

Flow Control

- Flow control is an important issue in data link layer that control data between sender and receiver
- When a data frame (Layer-2 data) is sent from one host to another over a single medium, it is required that the sender and receiver should work at the same speed. That is, sender sends at a speed on which the receiver can process and accept the data.
- What if the speed (hardware/software) of the sender or receiver differs? If sender is sending too fast the receiver may be overloaded, (swamped) and data may be lost.
- Flow Control coordinates that amount of data that can be sent before receiving acknowledgement.
- It makes the sender wait for some sort of an ACK before continuing to send more data.
- Flow control tells the sender how much data to be sent.

Flow control Techniques

```
graph TD; A[Flow control Techniques] --> B[Stop and Wait]; A --> C[Sliding Window];
```

Stop and Wait

Sliding Window

Stop and Wait

- Sends one frame at the time.
- The sender waits for acknowledgement of every frame that it sends.
- The receiver indicates its willingness to accept another frame by sending acknowledgement of the frame that it receives.
- Only when acknowledgement has been received next frame is sent.

Acknowledgement

```
graph TD; A[Acknowledgement] --> B[Positive ack (transmits the next frame)]; A --> C[Negative ack (retransmits the same frame)];
```

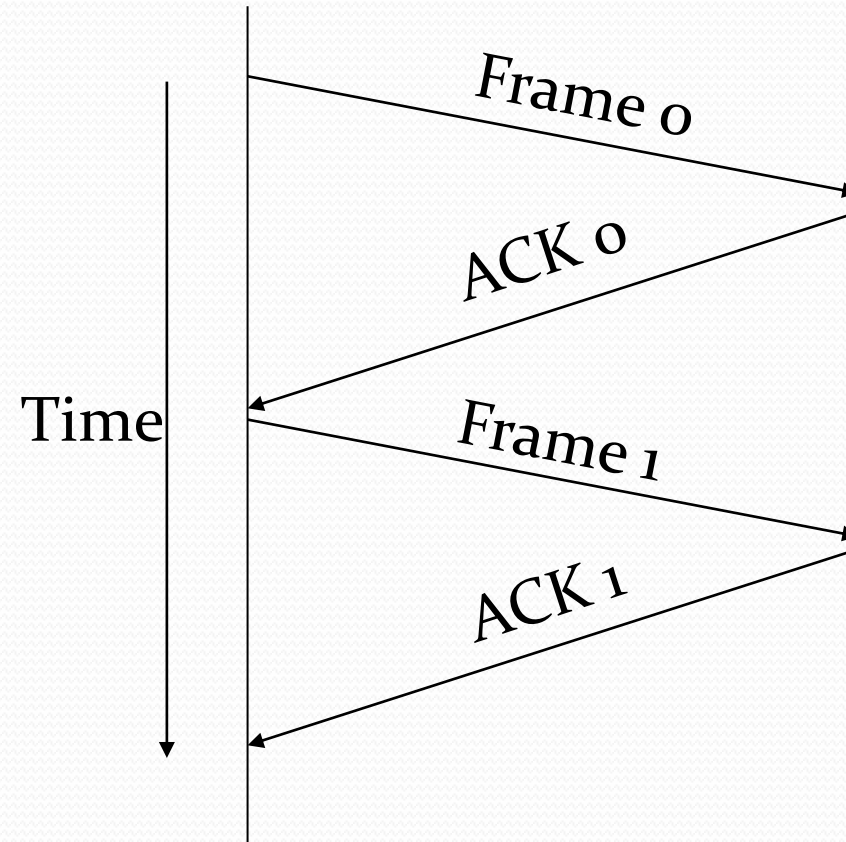
Positive ack (transmits the next frame)

Negative ack (retransmits the same frame)

- The receiver can thus stop flow of data by just withholding the acknowledgement.

Sender

Receiver



Advantages

- Each frame is transmitted only after first frame is acknowledged.
- Data frame is not lost.

Disadvantages

- Inefficient, only one frame can be in transmission at a time.
- The time spent for waiting acknowledgment between each frame add significant amount to total transmission time.

Sliding Window

- Sends multiple packets or frames without waiting for acknowledgment.
- Frames can be sent one right after another and its capacity can be used effectively.
- The receiver acknowledges only some of the frames using single ACK to confirm receipt of multiple data frames.
- Sender and receiver have a window which can hold frames.
- The sender can send as many frames that would fit into a window.
- For each window of size n , frames get numbered from 0 to $n-1$.

- If $n=8$ the frames are numbered 0,1,2,3,4,5,6,7. (the size of the window is n)
- When the receiver sends ACK it includes the number of the next frame it expects to receive.
- When the sender sees an ACK with the number 5, it knows that all frames up through number 4 have been received.

Sender



Data 0

ACK 0

Data 1

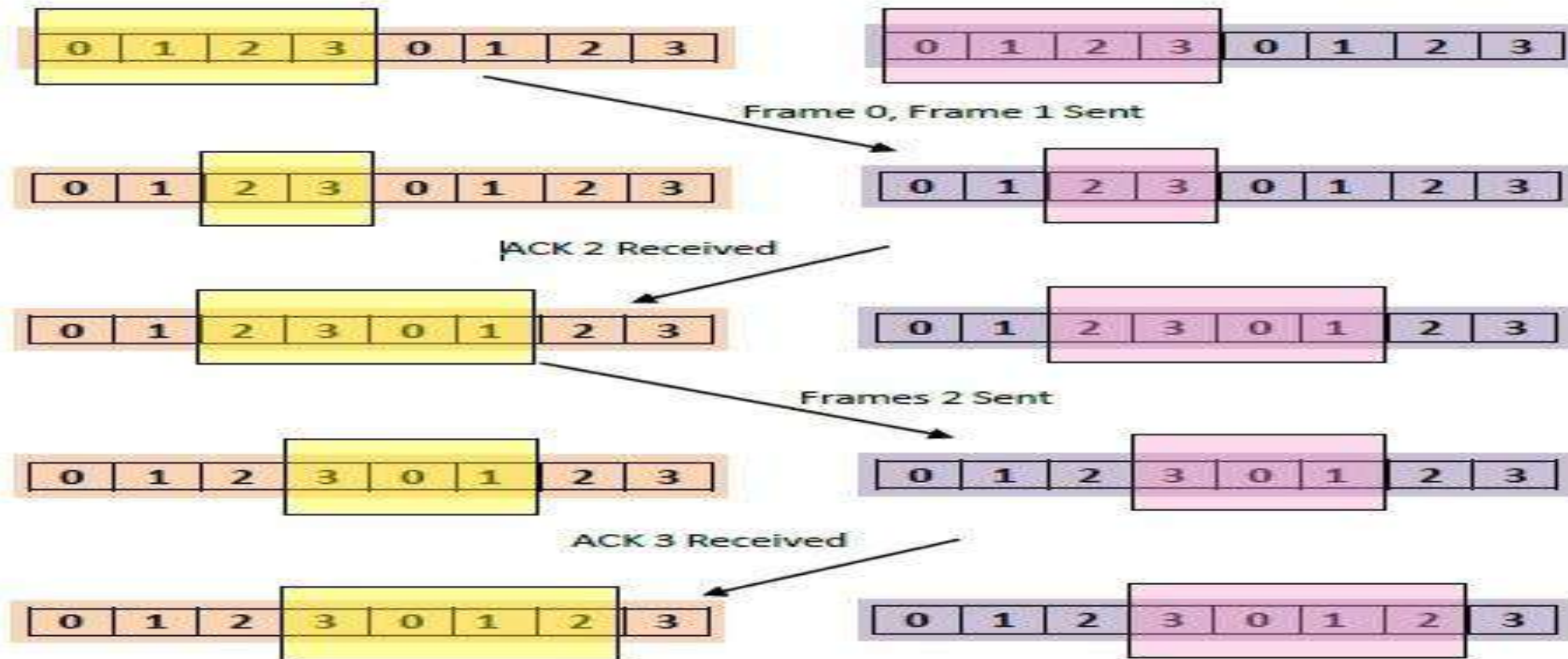
ACK 1

Receiver



Sending Window

Receiving Window



Error Control

- Error control includes both error detection and error correction.
- It allows the receiver to inform the sender if a frame is lost or damaged during transmission and coordinates the retransmission of those frames by the sender.
- Error control in the data link layer is based on automatic repeat request (ARQ). Whenever an error is detected, specified frames are retransmitted

Requirements for error control mechanism:

- **Error detection** - The sender and receiver, either both or any, must certain that there is some error in the transit.
- **Positive ACK** - When the receiver receives a correct frame, it should acknowledge it.
- **Negative ACK** - When the receiver receives a damaged frame or a duplicate frame, it sends a NACK back to the sender and the sender must retransmit the correct frame.
- **Retransmission:** The sender maintains a clock and sets a timeout period. If an acknowledgement of a data-frame previously transmitted does not arrive before the timeout the sender retransmits the frame, thinking that the frame or it's acknowledgement is lost in transit.

Error Control Techniques

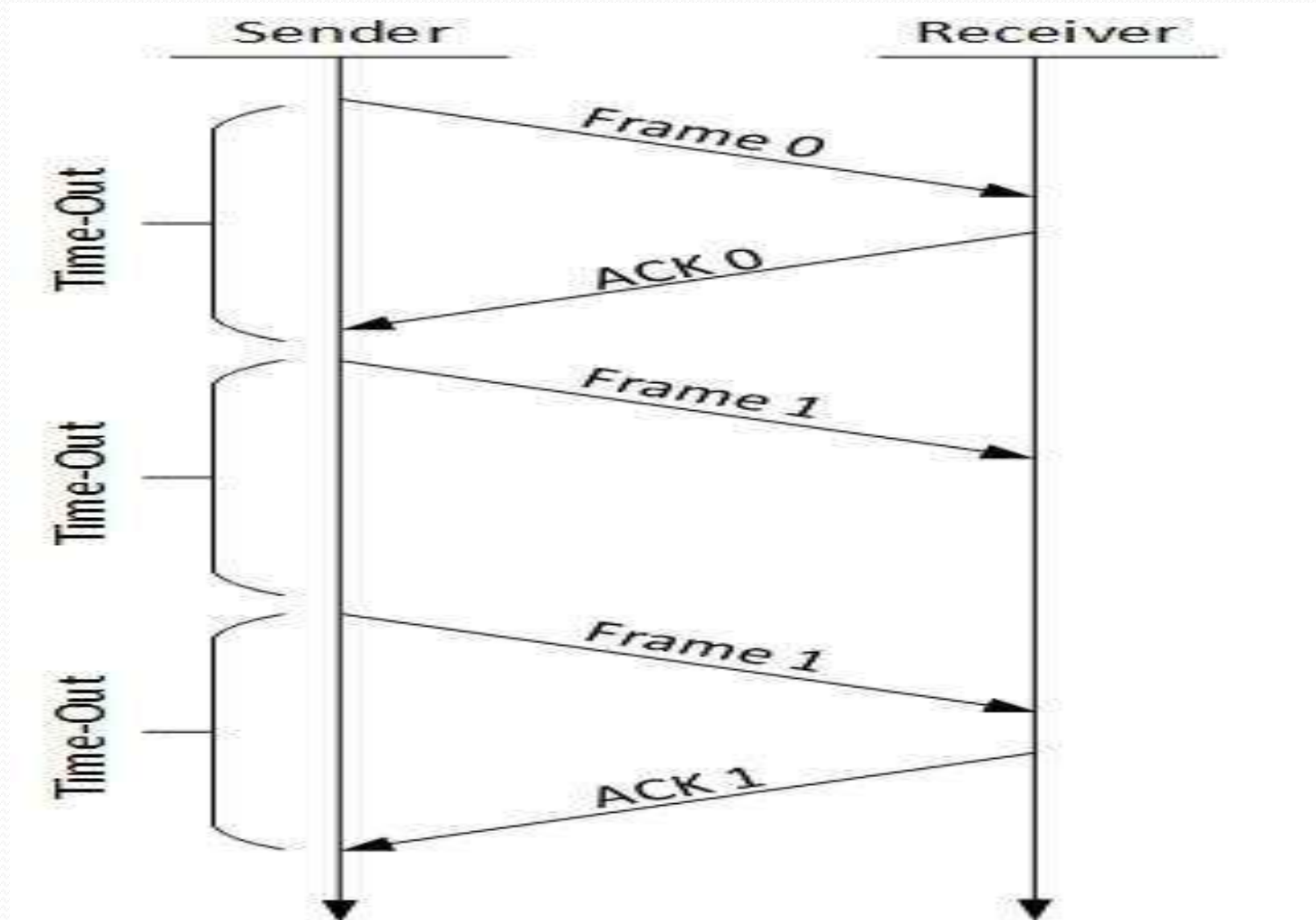
- Stop-and-Wait ARQ
- Go-Back-N ARQ
- Selective-Repeat ARQ
- Piggybacking

ARQ(Automatic Repeat reQuest) protocols offers services of :

- packet ordering (packets are delivered in the same ordered they are sent);
- loss-free: packets are delivered without losses
- error free: packets are guaranteed to be delivered without errors.

ARQ protocols are based on retransmission. For example, when you listen to someone else, you either let him know you got the message with a positive acknowledgments (e.g. "OK") or that you lost the message and you want him to repeat it with a negative acknowledgments (e.g. "Please repeat that.").

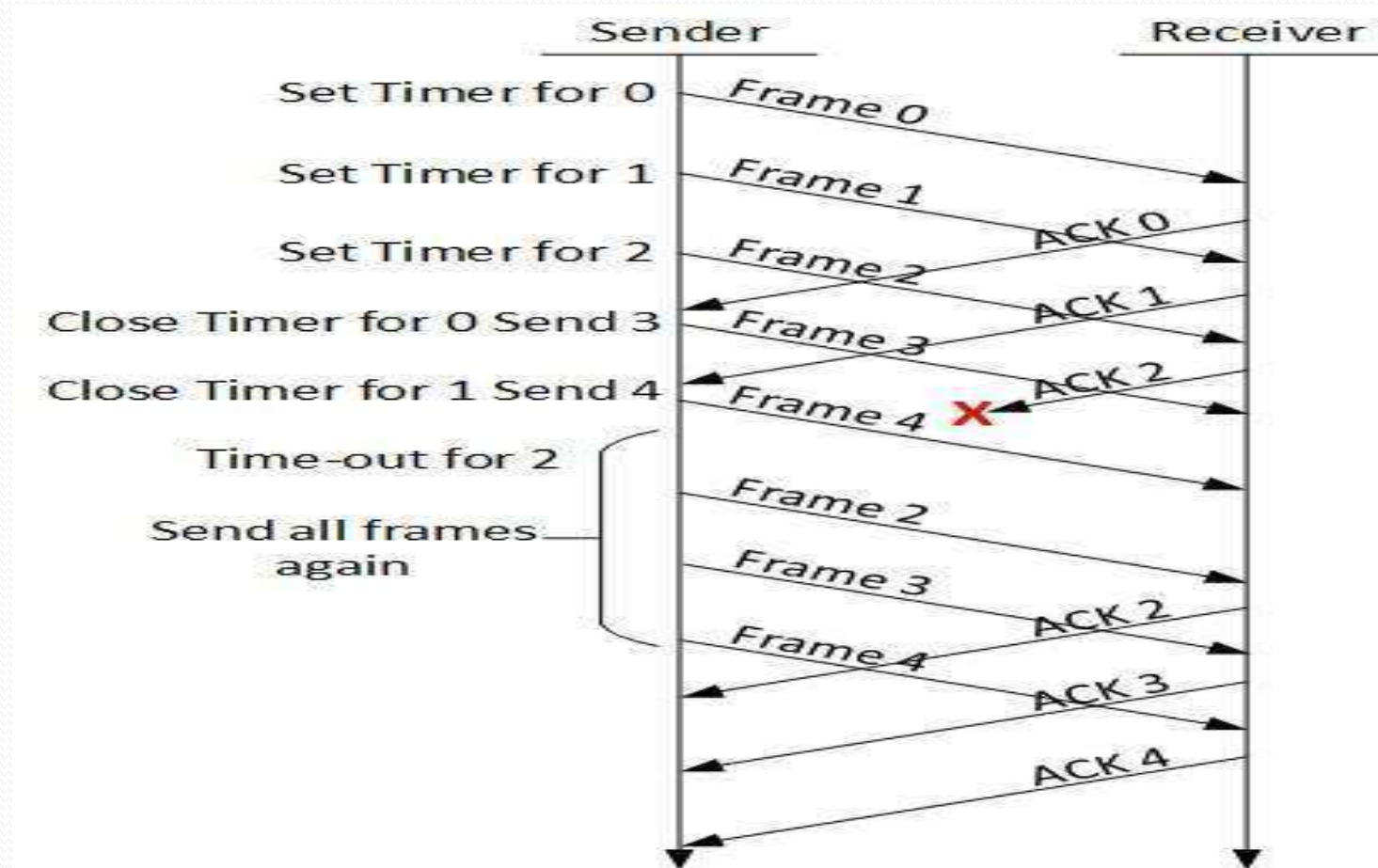
Stop-and-Wait ARQ



The following transition may occur in Stop-and-Wait ARQ:

- The sender maintains a timeout counter.
- When a frame is sent, the sender starts the timeout counter.
- If acknowledgement of frame comes in time, the sender transmits the next frame in queue.
- If acknowledgement does not come in time, the sender assumes that either the frame or its acknowledgement is lost in transit. Sender retransmits the frame and starts the timeout counter.
- If a negative acknowledgement is received, the sender retransmits the frame.

Go Back- N ARQ

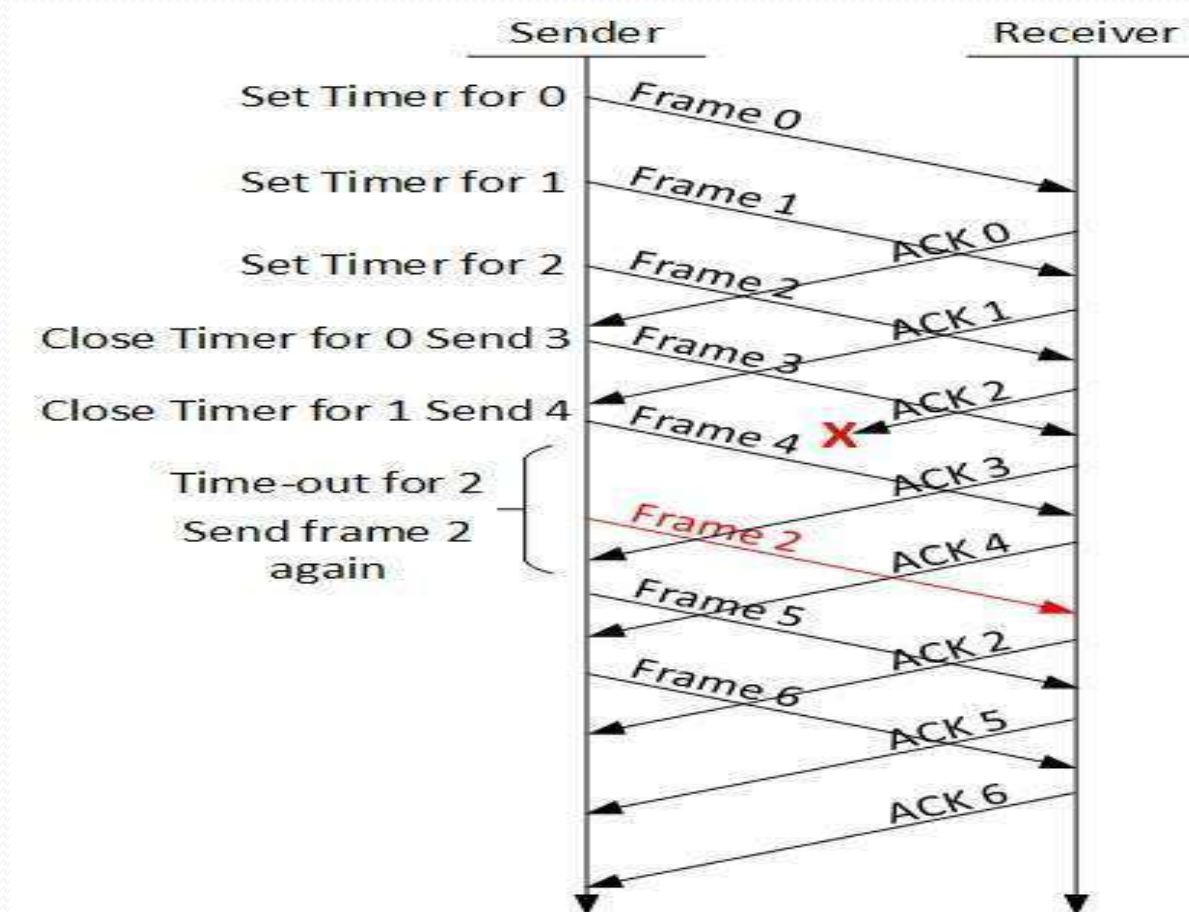


Go-Back-N ARQ

- Stop and wait ARQ mechanism does not utilize the resources at their best. When the acknowledgement is received, the sender sits idle and does nothing.
- In Go-Back-N ARQ method, both sender and receiver maintain a window.
- The sending-window size enables the sender to send multiple frames without receiving the acknowledgement of the previous ones. The receiving-window enables the receiver to receive multiple frames and acknowledge them. The receiver keeps track of incoming frame's sequence number.

- When the sender sends all the frames in window, it checks up to what sequence number it has received positive acknowledgement.
- If all frames are positively acknowledged, the sender sends next set of frames. If sender finds that it has received NACK or has not receive any ACK for a particular frame, it retransmits all the frames after which it does not receive any positive ACK.

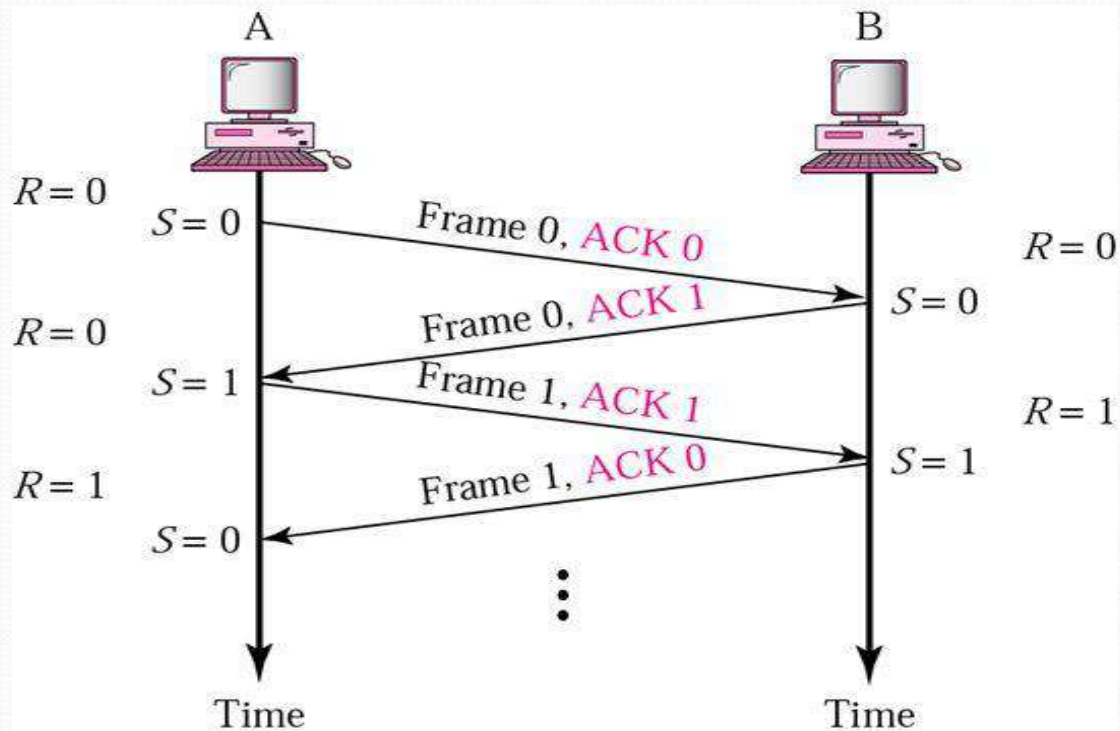
Selective Repeat ARQ



- In Go-back-N ARQ, it is assumed that the receiver does not have any buffer space for its window size and has to process each frame as it comes. This enforces the sender to retransmit all the frames which are not acknowledged.
- In Selective-Repeat ARQ, the receiver while keeping track of sequence numbers, buffers the frames in memory and sends NACK for only frame which is missing or damaged.
- The sender in this case, sends only packet for which NACK is received

Piggybacking

Piggybacking



- A method to combine a data frame with ACK.
- Station A and B both have data to send.
- Instead of sending separately, station A sends a data frame that includes an ACK.
- Station B does the same thing.
- Piggybacking saves bandwidth.

Piggybacking

- In two way communication, Whenever a data frame is received, the receiver waits and does not send the control frame (acknowledgement) back to the sender immediately.
- The receiver waits until its network layer passes in the next data packet. The delayed acknowledgement is then attached to this outgoing data frame.
- This technique of temporarily delaying the acknowledgement so that it can be hooked with next outgoing data frame is known as piggybacking.
- The major advantage of piggybacking is better use of available channel bandwidth.

The disadvantages of piggybacking are:

- Additional complexity.
- If the data link layer waits too long before transmitting the acknowledgement, then retransmission of frame would take place.

What is Error ??

- Network must be able to transfer data with accuracy
- But anytime data transmitted from one node to the next, they can become corrupted in passage
- Many factors can alter or wipe out one or more bits of a given data unit
- Condition where sender's info doesn't match receiver's info are **Errors**

What is Error Control ?

Technique of detecting and correcting blocks of data during communication

Checks reliability of characters both at bit and packet level

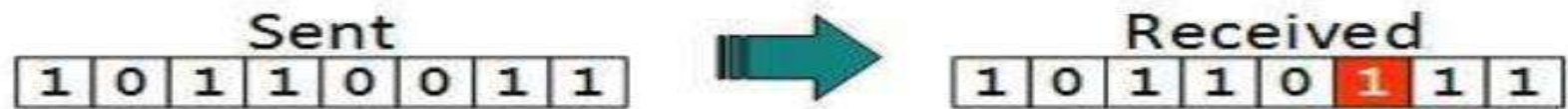
If proper Error Control is in place then data transfer will be accurate

Error Detection Techniques

- First step in error correction process
- Simpler than actual error correction
- Implemented either at Datalink layer or Transport layer of OSI model
- Error Detection Codes are additional data added to given digital message to help and detect if there is any error during transmission of message

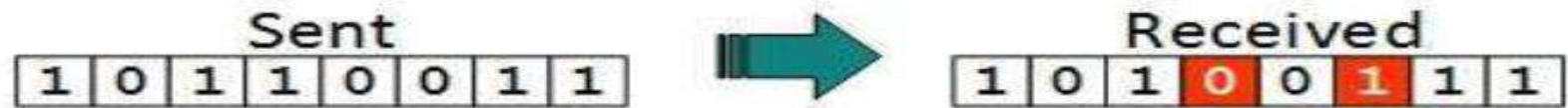
Types of Error

Single bit error



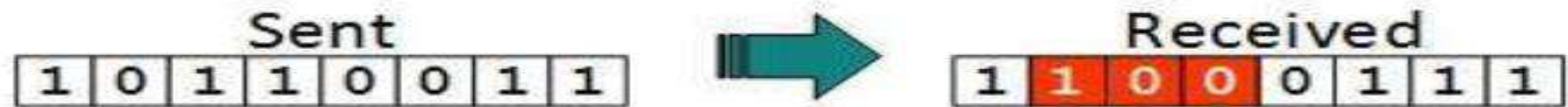
In a frame, there is only one bit, anywhere though, which is corrupt.

Multiple bits error



Frame is received with more than one bits in corrupted state.

Burst error



Frame contains more than 1 consecutive bits corrupted.

Some Error Detection Techniques

Parity Check

- Simple Parity Check
- Two Dimensional Parity Check

Checksum

Cyclic Redundancy Check (CRC)

Hamming Code

Some Error Detection Techniques

Parity Check

- Simple Parity Check
- Two Dimensional Parity Check

Checksum

Cyclic Redundancy Check (CRC)

Hamming Code

Simple Parity Check

- A redundant bit call **parity bit** is added to every data unit so that the total number of 1s in the unit (including the parity bit) becomes even (or odd)
 - 1 is added to the block if it contains odd number of 1's, and
 - 0 is added if it contains even number of 1's
- This scheme makes the total number of 1's even, that is why it is called also even parity checking

Simple Parity Check

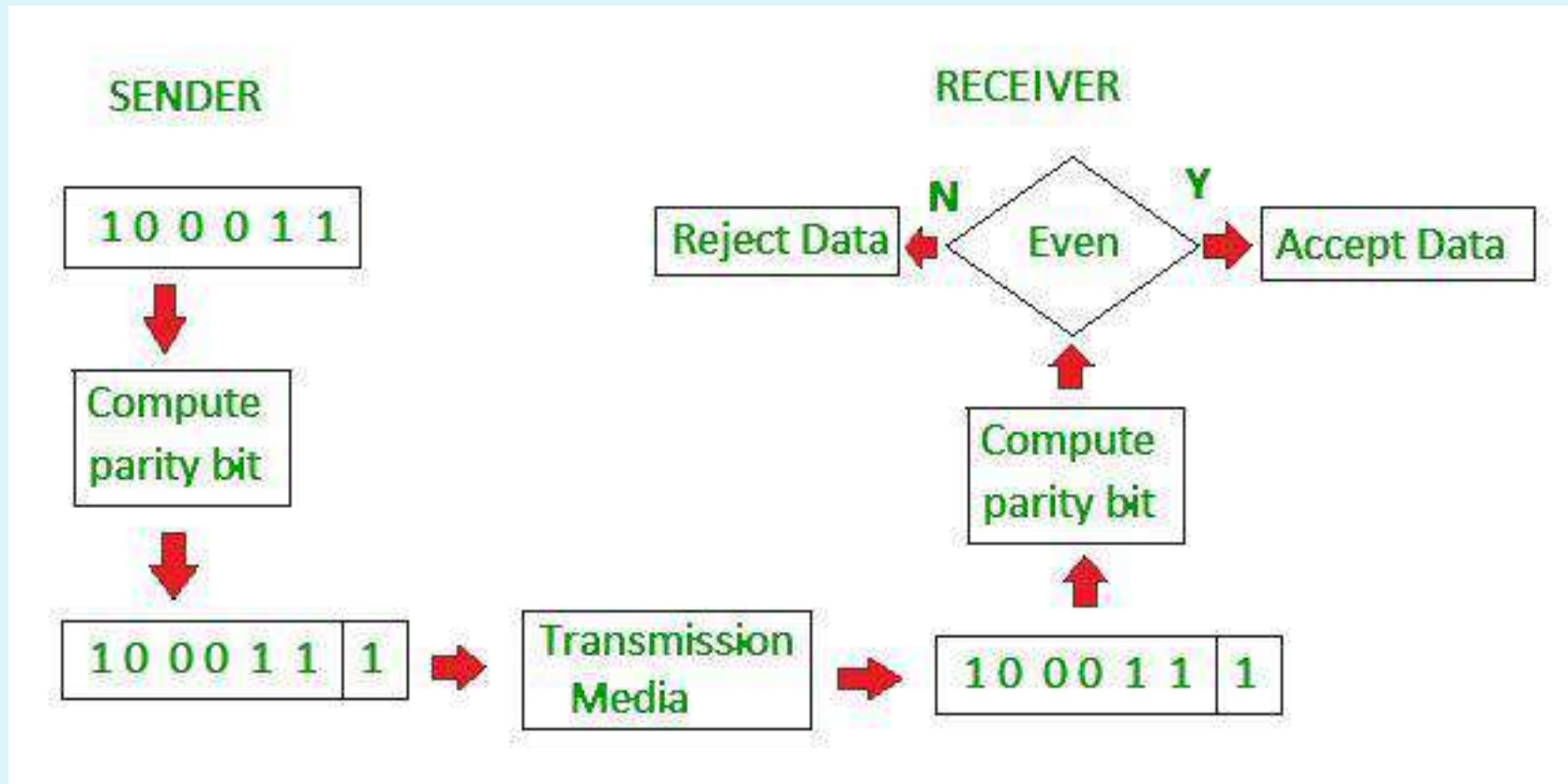


Fig : Simple parity check

Two-dimensional Parity Check

- Parity check bits are calculated for each row which is equivalent to a simple parity check bit
- Parity check bits are also calculated for all columns, then both are sent along with data
- At the receiving end these are compared with parity bits calculated on the received data

Two-dimensional Parity Check

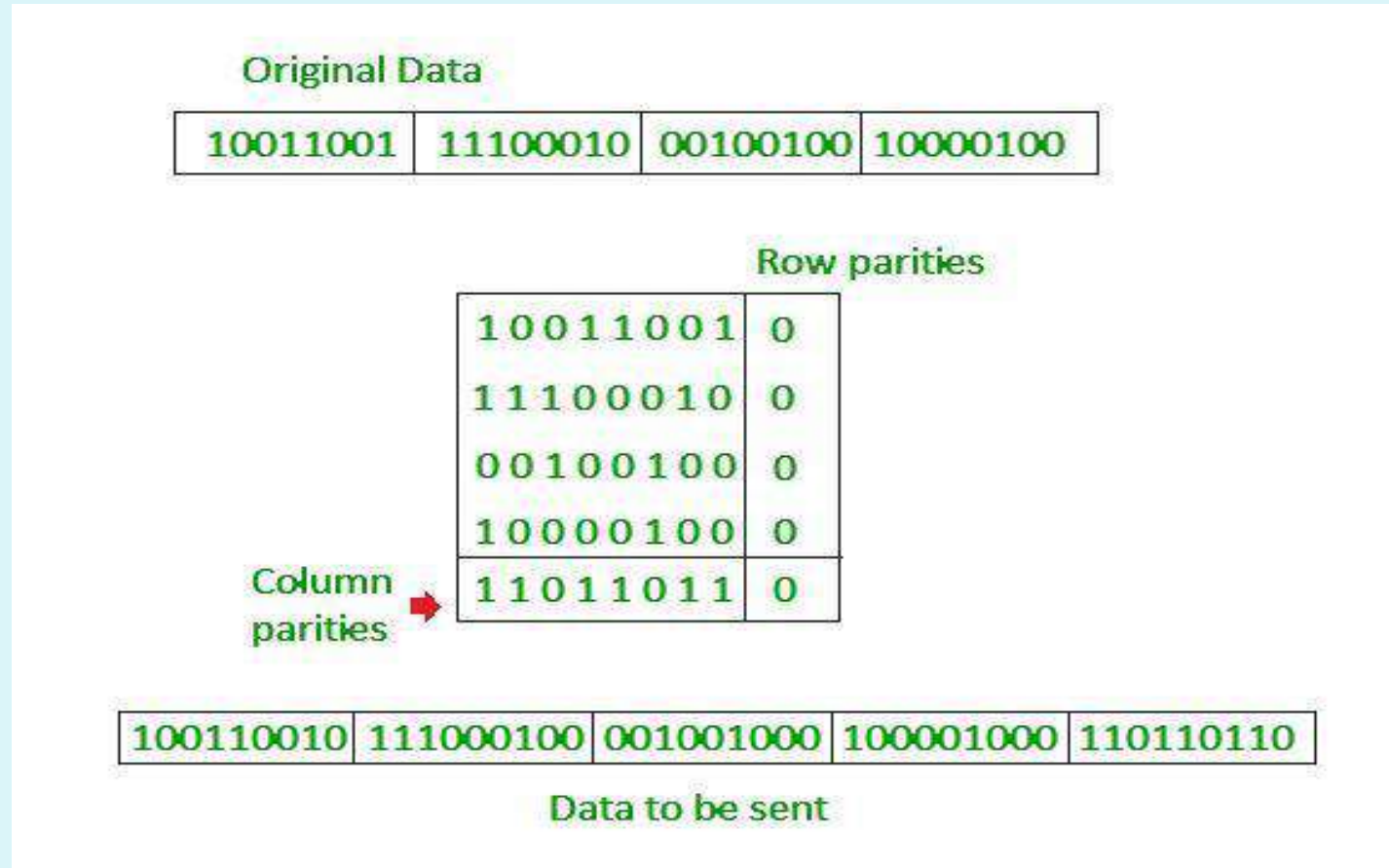


Fig : Two-dimensional parity check

Checksum

- Data is divided into k segments each of m bits
- In the sender's end the segments are added using 1's complement arithmetic to get the sum. Sum is complimented to get the checksum
- The checksum segment is sent along with the data segments
- At the receiver's end, all the received segments are added using 1's complement arithmetic to get the sum. Sum is complemented

Checksum

- If the result is 0, the received data is accepted; other it is discarded
- Like parity checks it is based on Redundancy

Checksum

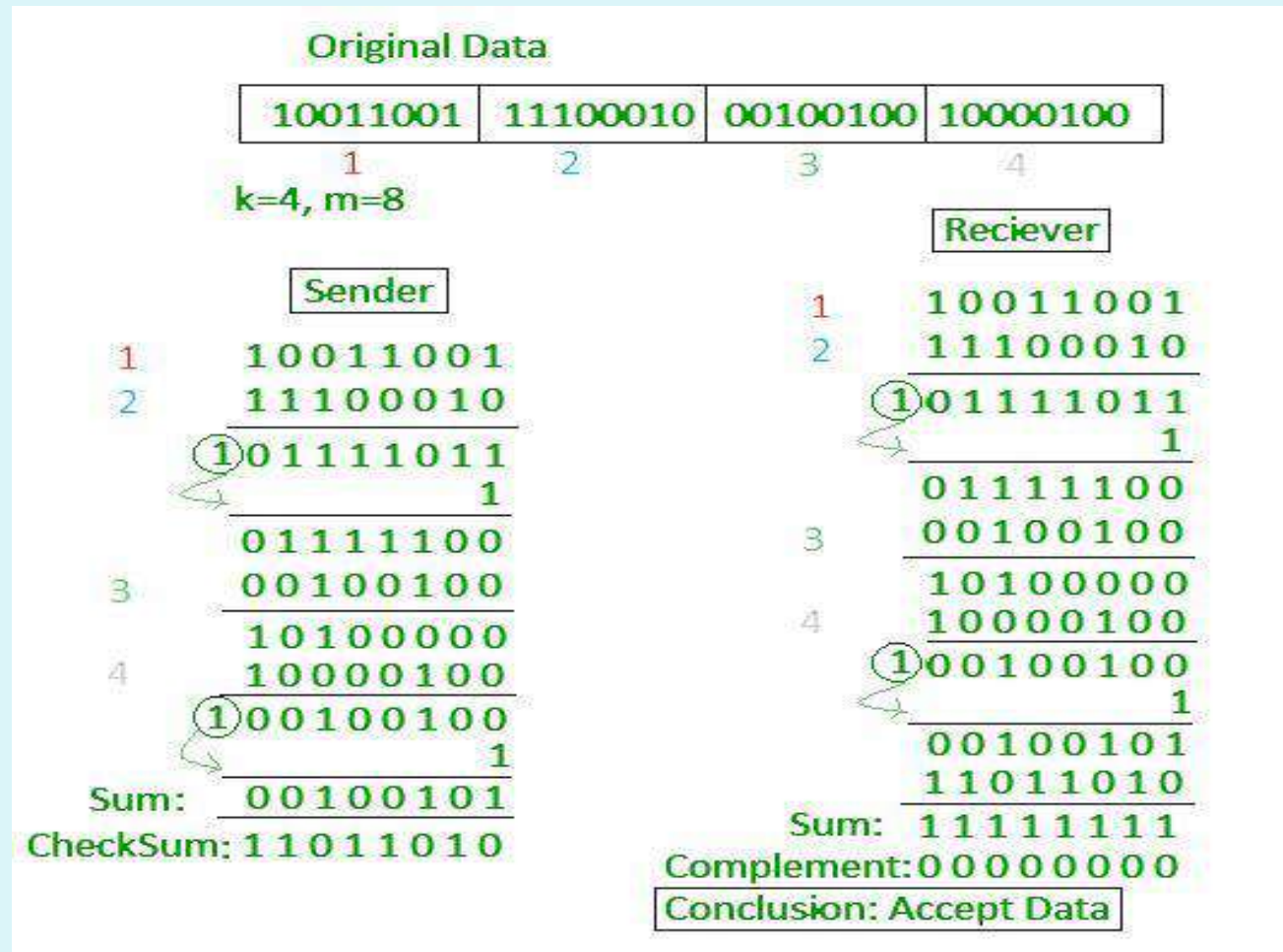


Fig : Checksum Example

Cyclic Redundancy Check (CRC)

- Unlike checksum scheme, which is based on addition, CRC is based on binary division
- In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number
- At the destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted.

Cyclic Redundancy Check (CRC)

- A remainder indicates that the data unit has been damaged in transit and therefore must be rejected
- Most powerful of redundancy checking techniques

Cyclic Redundancy Check (CRC)

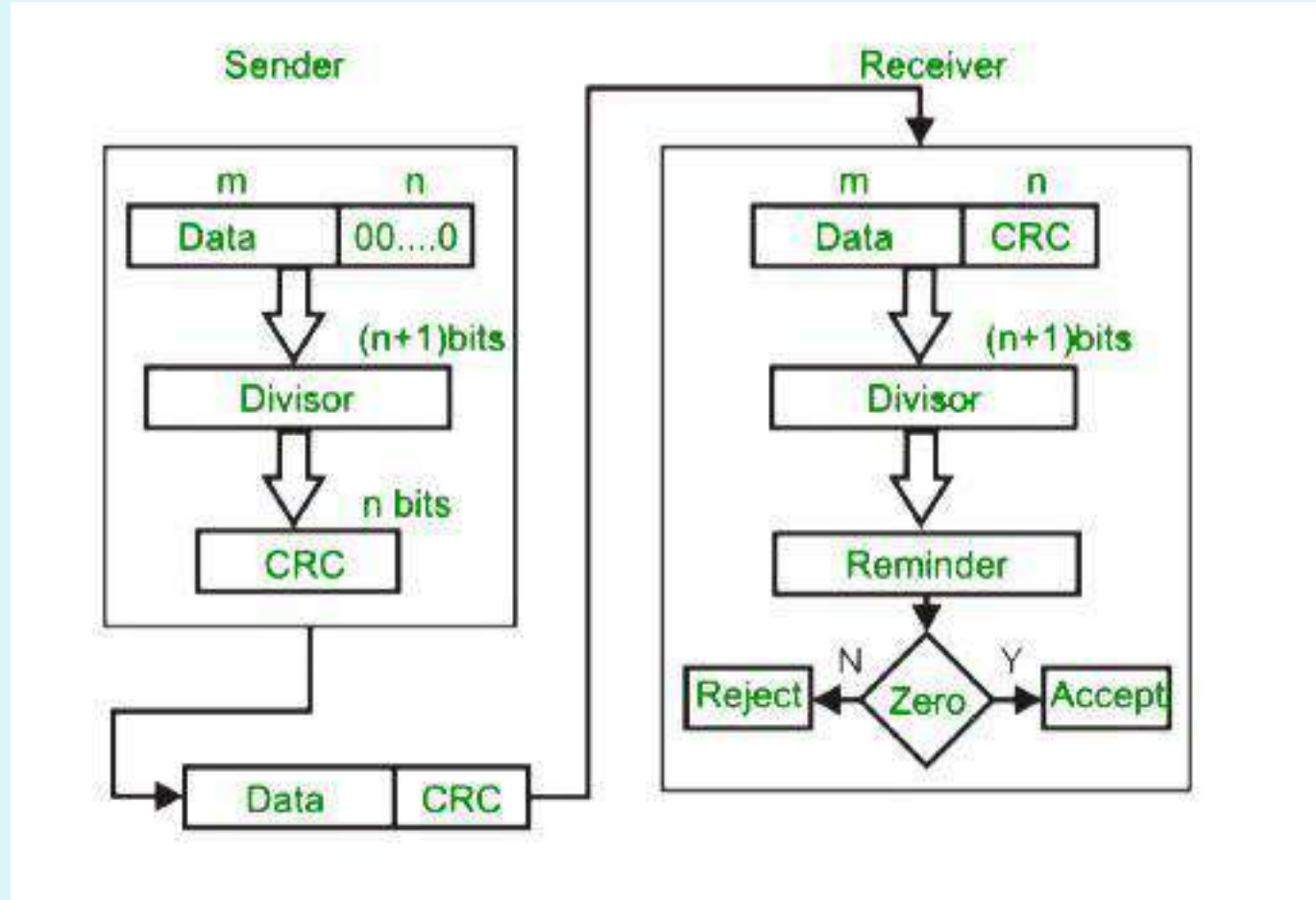


Fig : How CRC works

Cyclic Redundancy Check (CRC)

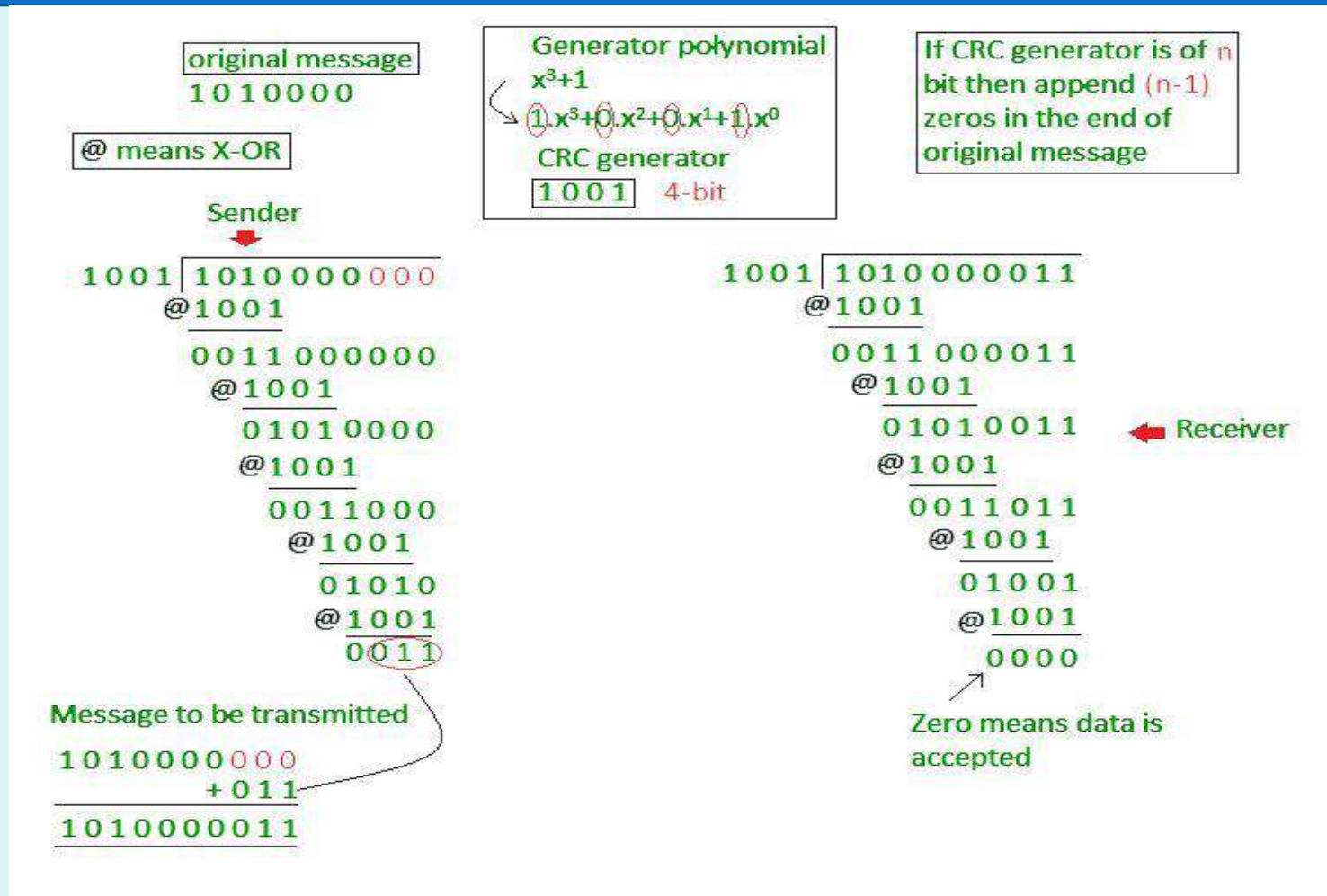


Fig : Example of CRC

Cyclic Redundancy Check

- Powerful error detection scheme
- Rather than addition, binary division is used → Finite Algebra Theory (Galois Fields)
- Can be easily implemented with small amount of hardware
 - Shift registers
 - XOR (for addition and subtraction)

Cyclic Redundancy Check

- Let us assume k message bits and n bits of redundancy $\underbrace{\text{xxxxxxxxxx}}_{k \text{ bits}} \underbrace{\text{yyyy}}_{n \text{ bits}} \}$ Block of length $k+n$

- Associate bits with coefficients of a polynomial

$$\begin{array}{ccccccc} 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1X^6 + 0X^5 + 1X^4 + 1X^3 + 0X^2 + 1X + 1 \\ = X^6 + X^4 + X^3 + X + 1 \end{array}$$

Cyclic Redundancy Check

- Let $M(x)$ be the **message polynomial**
- Let $P(x)$ be the **generator polynomial**
 - $P(x)$ is fixed for a given CRC scheme
 - $P(x)$ is known both by sender and receiver
- Create a block polynomial $F(x)$ based on $M(x)$ and $P(x)$ such that $F(x)$ is divisible by $P(x)$

$$\frac{F(x)}{P(x)} = Q(x) + \frac{0}{P(x)}$$

Cyclic Redundancy Check

- Sending
 1. Multiply $M(x)$ by x^n
 2. Divide $x^nM(x)$ by $P(x)$
 3. Ignore the quotient and keep the remainder $C(x)$
 4. Form and send $F(x) = x^nM(x) + C(x)$
- Receiving
 1. Receive $F'(x)$
 2. Divide $F'(x)$ by $P(x)$
 3. Accept if remainder is 0, reject otherwise

Example

• Send

- $M(x) = 110011 \rightarrow x^5 + x^4 + x + 1$ (6 bits)
- $P(x) = 11001 \rightarrow x^4 + x^3 + 1$ (5 bits, $n = 4$)
 \rightarrow 4 bits of redundancy
- Form $x^n M(x) \rightarrow 110011 \text{ 0000}$
 $\rightarrow x^9 + x^8 + x^5 + x^4$
- Divide $x^n M(x)$ by $P(x)$ to find $C(x)$

$$\begin{array}{r}
 100001 \\
 11001 \overline{) 1100110000} \\
 \underline{11001} \\
 10000 \\
 \underline{11001} \\
 1001 = C(x)
 \end{array}$$

Send the block 110011 1001

• Receive

$$\begin{array}{r}
 11001 \overline{) 1100111001} \\
 \underline{11001} \\
 11001 \\
 \underline{11001} \\
 00000 \\
 \downarrow \\
 \text{No remainder} \\
 \rightarrow \text{Accept}
 \end{array}$$

Hamming Code

- Hamming code is a set of error-correction codes that can be used to **detect and correct the errors** that can occur when the data is moved or stored from the sender to the receiver. It is **technique developed by R.W. Hamming for error correction**.
- **Redundant bits –**
- Redundant bits are extra binary bits that are generated and added to the information-carrying bits of data transfer to ensure that no bits were lost during the data transfer.
- Suppose the number of data bits is 7, then the number of redundant bits can be calculated using:
$$= 2^4 \geq 7 + 4 + 1$$

Thus, the number of redundant bits= 4

- **Determining the position of redundant bits –**

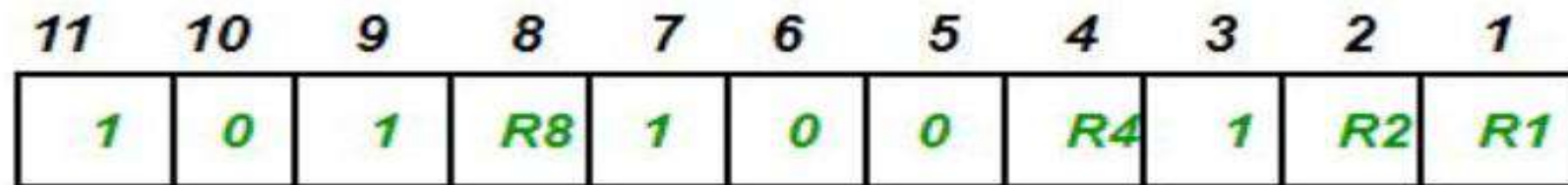
These redundancy bits are placed at the positions which correspond to the power of 2.

As in the above example:

- The number of data bits = 7
- The number of redundant bits = 4
- The total number of bits = 11
- The redundant bits are placed at positions corresponding to power of 2- 1, 2, 4, and 8



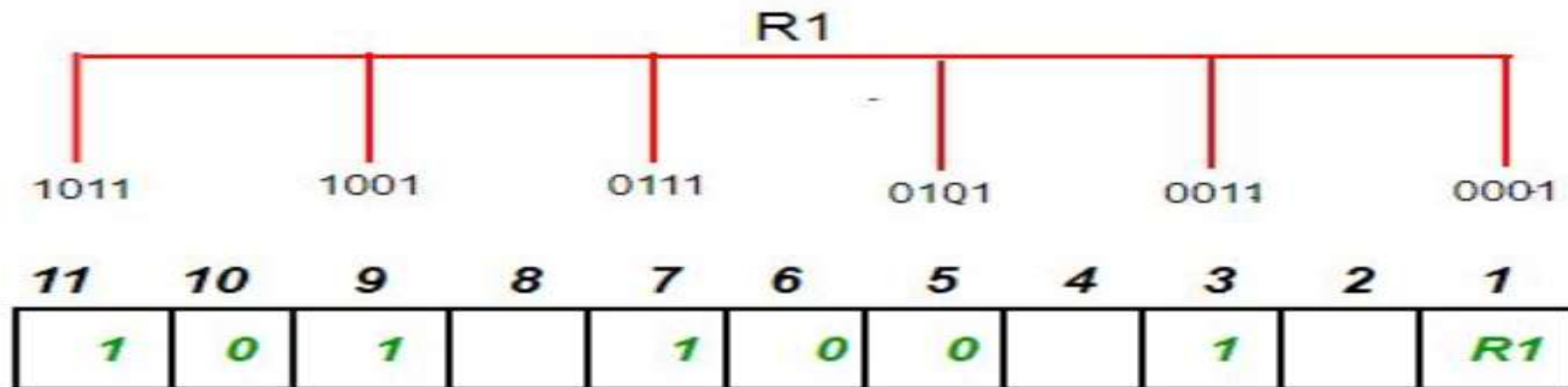
Suppose the data to be transmitted is 1011001, the bits will be placed as follows:



Determining the Parity bits –

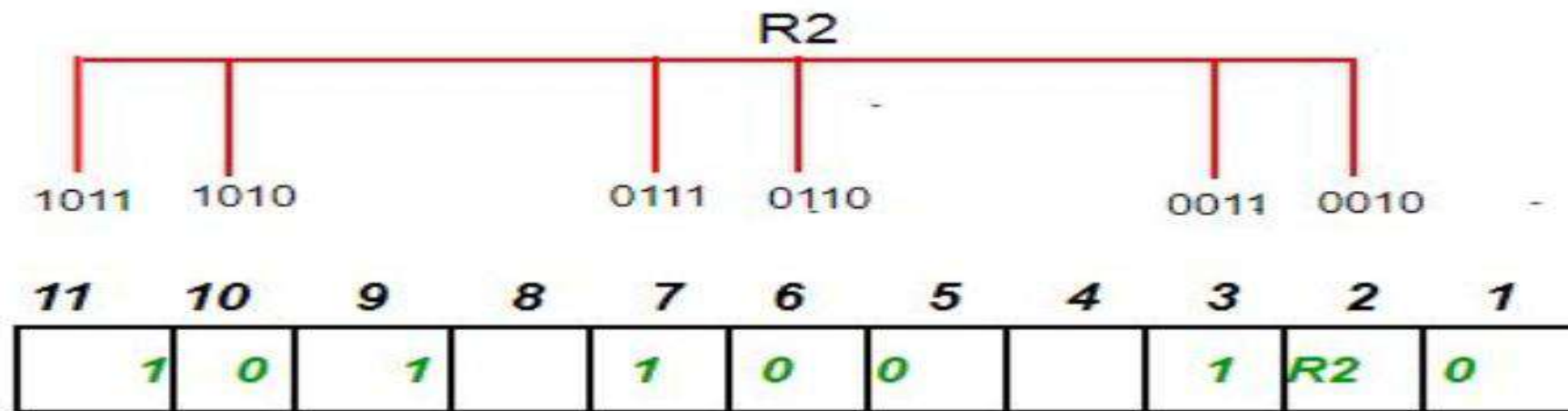
1. R1 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the least significant position.

R1: bits 1, 3, 5, 7, 9, 11



To find the redundant bit R1, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R1 is an even number the value of R1 (parity bit's value) = 0

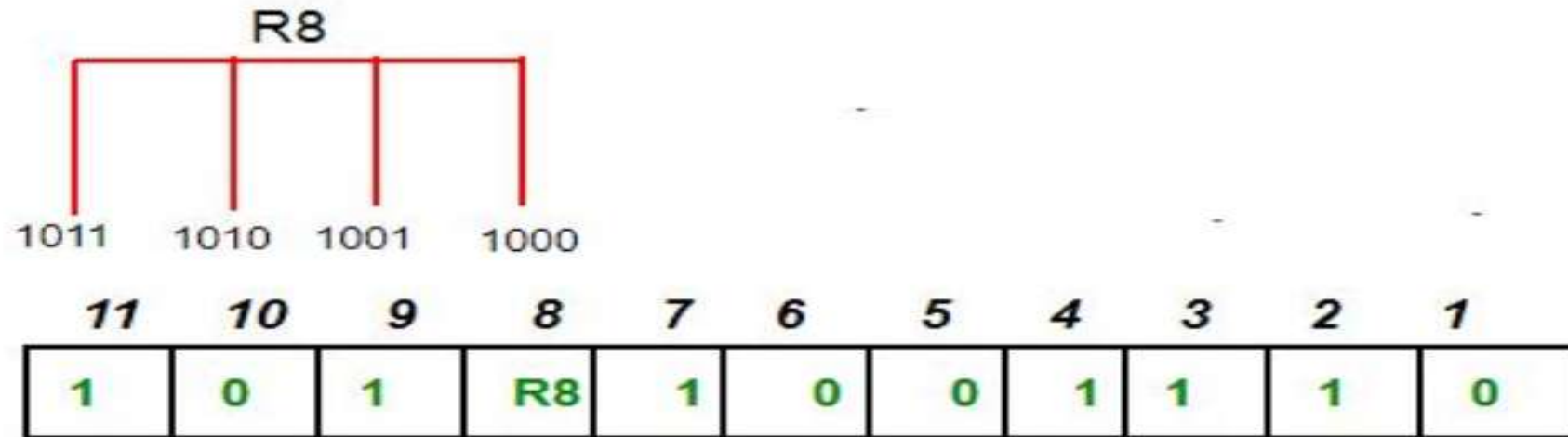
2. R2 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the second position from the least significant bit.
R2: bits 2,3,6,7,10,11



To find the redundant bit R2, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R2 is an odd number the value of R2 (parity bit's value) = 1

4. R8 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the fourth position from the least significant bit.

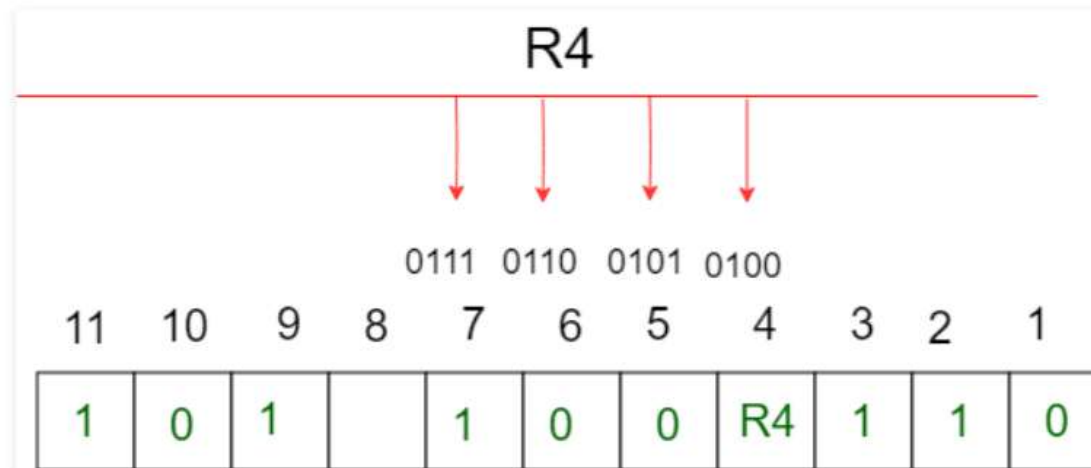
R8: bit 8,9,10,11



To find the redundant bit R8, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R8 is an even number the value of R8 (parity bit's value) = 0.

3. R4 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the third position from the least significant bit.

R4: bits 4, 5, 6, 7



To find the redundant bit R4, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R4 is an odd number the value of R4 (parity bit's value) = 1

Thus, the data transferred is:

11	10	9	8	7	6	5	4	3	2	1
1	0	1	0	1	0	0	1	1	1	0

Multiple Access Protocol

- Multiple access protocols regulate nodes transmission onto the shared broadcast channel. Moreover, also the communication due to the coordination of the transmission must use the channel itself.
- Multiple access protocol is based on distributed algorithm that determines how stations share channel, i.e., determine when station can transmit m communication about channel sharing must use channel itself!

what to look for in multiple access protocols:

- synchronous or asynchronous
- information needed about other stations
- robustness (e.g., to channel errors)
- performance

Ideal Multiple Access Protocol

Broadcast channel of rate R bps

1. When one node wants to transmit, it can send at rate R
2. When M nodes want to transmit, each can send at average rate R/M (no overhead)
3. Fully decentralized
 - No special node to coordinate transmissions
 - No synchronization of clocks, slots
4. Simple



Three broad classes:

- **Channel Partitioning**

- Divide channel into smaller “pieces” (time slots, frequency)
- Allocate piece to node for exclusive use

- **Random Access**

- Channel not divided, allow collisions
- “Recover” from collisions

- **Taking turns**

- Nodes take turns, but nodes with more to send can perhaps take longer turns

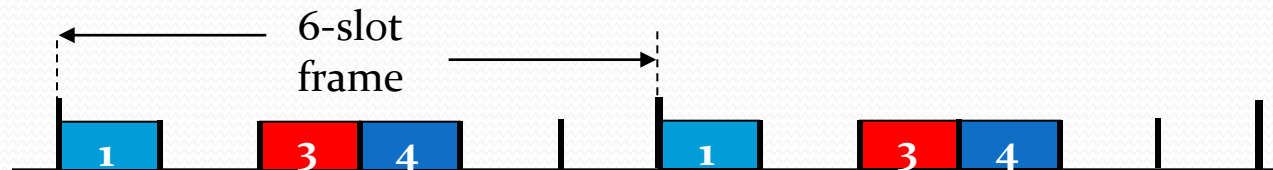
Multiple Access Links and Protocols

- Point-to-point link (single wire, e.g. PPP, SLIP):
- A point-to-point link consists of a single sender on one end of the link, and a single receiver at the other end of the link.
- Many link-layer protocols have been designed for point-to-point links; PPP and HDLC for example
- Broadcast link (shared wire or wireless medium; e.g, Ethernet, Wavelan, etc.):
- The second type of link, a broadcast link, can have multiple sending and receiving nodes all connected to the same, single, shared broadcast channel, where each node on the channel receives a copy of any sent frame, e.g. Ethernet

Channel Partitioning MAC protocols: TDMA

TDMA: time division multiple access

- Access to channel in "rounds"
- Each station gets fixed length slot (length = pkt trans time) in each round
- Unused slots go idle
- Example: 6-station LAN, 1,3,4 have pkt, slots 2,5,6 idle



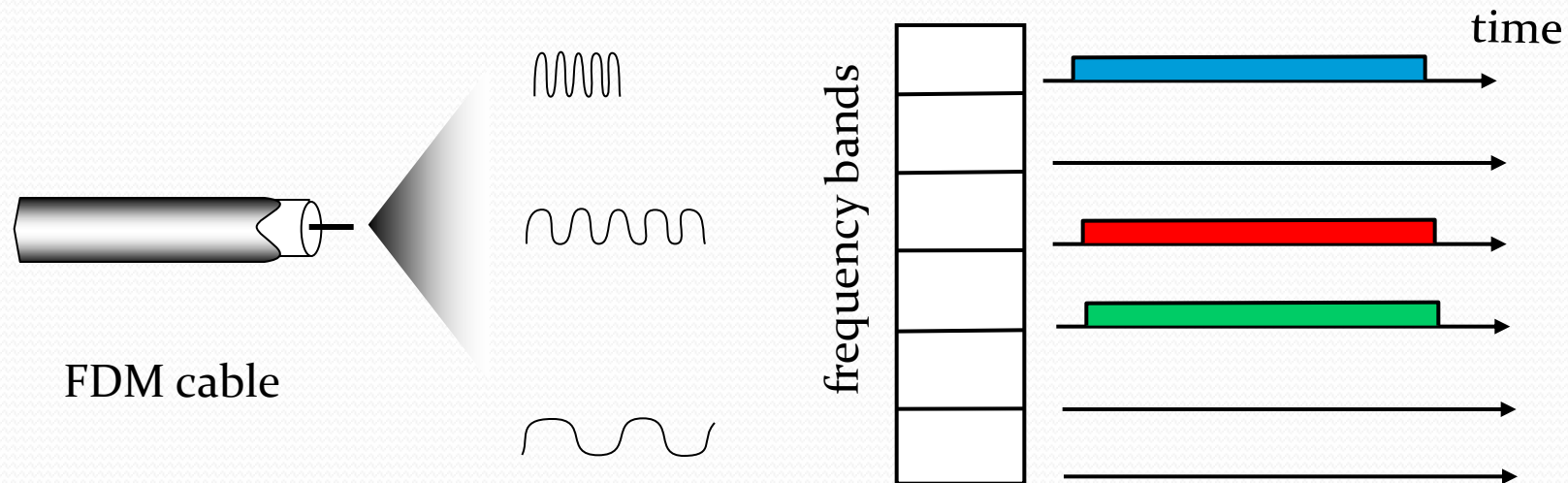
- For a TDM link, time is divided into time frames of fixed duration, and each frame is divided into a fixed number of time slots. When the network establishes a connection across a link, the network dedicates one time slot in every frame to the connection. These slots are dedicated for the sole use of that connection, with a time slot available for use (in every frame) to transmit the connection's data. Whenever a node has a frame to send, it transmits the frame's bits during its assigned time slot in the revolving TDM frame.

- Typically, frame sizes are chosen so that a single frame can be transmitting during a slot time. The figure shows a simple six-node TDM example where 3 nodes have some traffic to transmit (stations 1,3,4) and use their slots, while the others (stations 2,5,6) have no traffic and their slots remain unused. Once everyone has had its chance to talk, the pattern repeats. TDM is appealing as it eliminates collisions and is perfectly fair: each node gets a dedicated transmission rate of R/N bps during each frame time. However, it has two major drawbacks. First, a node is limited to an average rate of R/N bps even when it is the only node with frames to send. A second drawback is that a node must always wait for its turn in the transmission sequence--again, even when it is the only node with a frame to send.

Channel Partitioning MAC protocols: FDMA

FDMA: frequency division multiple access

- Channel spectrum divided into frequency bands
- Each station assigned fixed frequency band
- Unused transmission time in frequency bands go idle
- Example: 6-station LAN, 1,3,4 have pkt, frequency bands 2,5,6 idle



- FDM divides the R bps channel into different frequencies (each with a bandwidth of R/N) and assigns each frequency to one of the N nodes. FDM thus creates N smaller channels of R/N bps out of the single, larger R bps channel. FDM shares both the advantages and drawbacks of TDM. It avoids collisions and divides the bandwidth fairly among the N nodes. The figure shows the same six-node example where 3 nodes have some traffic to transmit (stations 1,3,4) and use their frequency, while the others (stations 2,5,6) have no traffic and their frequency remain unused. However, even with FDM a node is limited to a bandwidth of R/N , even when it is the only node with frames to send.

CDMA (Code Division Multiple Access)

- unique “code” assigned to each user; ie, code set partitioning
- used mostly in wireless broadcast channels (cellular, satellite, etc)
- all users share same frequency, but each user has own “chipping” sequence (ie, code) to encode data
- *encoded signal* = (original data) X (chipping sequence)
- *decoding*: inner-product of encoded signal and chipping sequence
- allows multiple users to “coexist” and transmit simultaneously with minimal interference (if codes are almost “orthogonal”)

CDMA

- Code division multiple access (CDMA) assigns a different code to each node. Each node then uses its unique code to encode the data bits it sends.
- CDMA allows different nodes to transmit simultaneously and yet have their respective receivers correctly receive a sender's encoded data bits (assuming the receiver knows the sender's code) in spite of interfering transmissions by other nodes. In a CDMA protocol, each bit being sent by the sender is encoded by multiplying the bit by a signal (the code) that changes at a much faster rate (known as the chipping rate) than the original sequence of data bits. CDMA works under the assumption that the interfering transmitted bit signals are additive, i.e. coded with orthogonal code. Therefore, each receiver can recover the data sent by a given sender out of the aggregate signal simply by using the sender's code.

Random Access Protocol

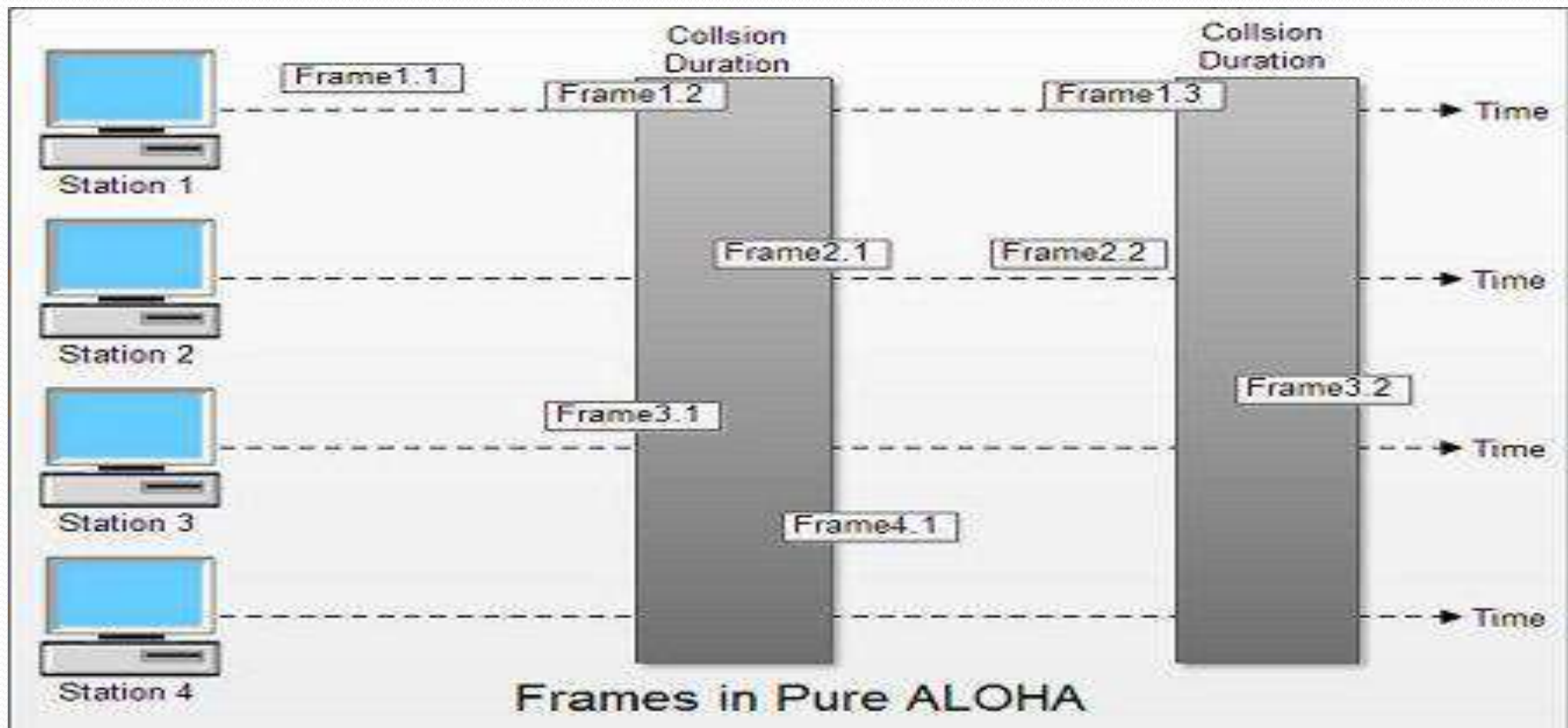
- In a random access protocol, a transmitting node always transmits at the full rate of the channel, namely, R bps. When there is a collision, each node involved in the collision repeatedly retransmits its frame until the frame gets through without a collision. But when a node experiences a collision, it doesn't necessarily retransmit the frame right away. Instead it waits a random delay before retransmitting the frame.
- Each node involved in a collision chooses independent random delays. Because after a collision the random delays are independently chosen, it is possible that one of the nodes will pick a delay that is sufficiently less than the delays of the other colliding nodes and will therefore be able to sneak its frame into the channel without a collision.

ALOHA

- It was developed at the University of Hawaii in the early 1970s to connect computers situated on different Hawaiian islands. The computers of the ALOHA network transmit on the same radio channel whenever they have a packet to transmit. From time-to-time packet transmission will collide, but these can be treated as transmission errors, and recovery can take place by retransmission. When traffic is very light, the probability of collision is very small, and so retransmissions need to be carried out infrequently.
- ALOHA scheme requires stations to use a random retransmission time. (This randomization is intended to spread out the retransmission and reduces the likelihood of additional collisions between stations.)
- ALOHA is the father of multiple access protocols.
- Types: Pure ALOHA and Slotted ALOHA

Pure Aloha

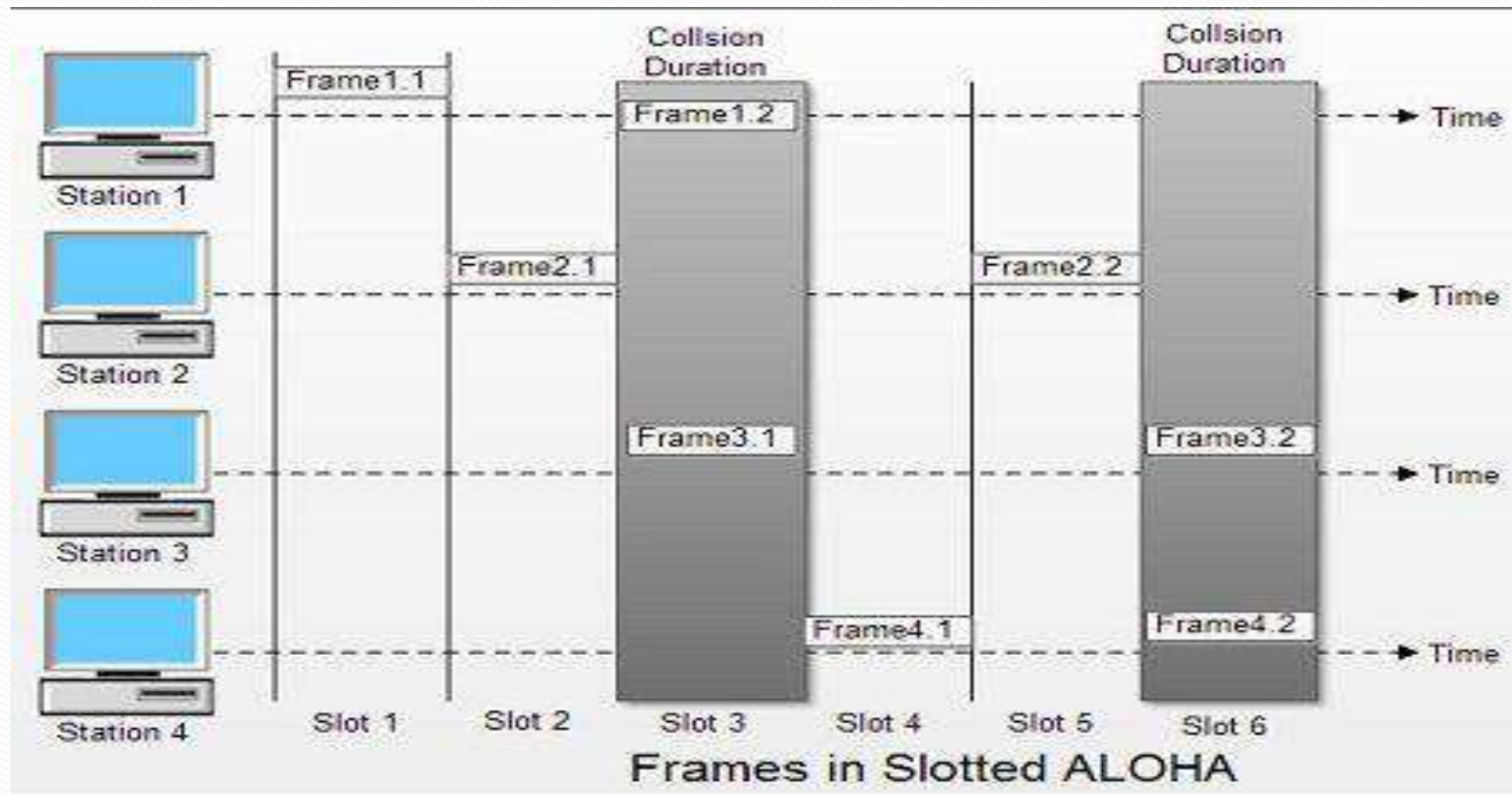
- In pure ALOHA, the stations transmit frames whenever they have data to send.
- When two or more stations transmit simultaneously, there is collision and the frames are destroyed.
- In pure ALOHA, whenever any station transmits a frame, it expects the acknowledgement from the receiver.
- If acknowledgement is not received within specified time, the station assumes that the frame (or acknowledgement) has been destroyed.
- If the frame is destroyed because of collision the 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.
- Therefore pure ALOHA dictates that when time-out period passes, each station must wait for a random amount of time before resending its frame. This randomness will help avoid more collisions.



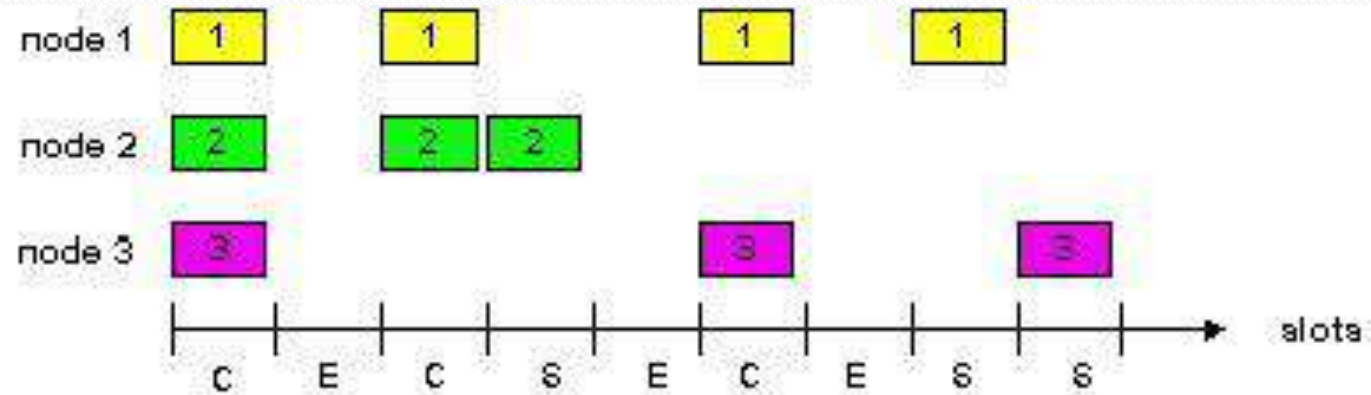
- In fig there are four stations that .contended with one another for access to shared channel. All these stations are transmitting frames. Some of these frames collide because multiple frames are in contention for the shared channel. Only two frames, frame 1.1 and frame 2.2 survive. All other frames are destroyed.
- • Whenever two frames try to occupy the channel at the same time, there will be a collision and both will be damaged. If 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.

Slotted ALOHA

- Slotted ALOHA was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high.
- In slotted ALOHA, 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.
- In slotted ALOHA, if any station is not able to place the frame onto the channel at the beginning of the slot *i.e.* it misses the time slot then the station has to wait until the beginning of the next time slot.
- In slotted ALOHA, there is still a possibility of collision if two stations try to send at the beginning of the same time slot as shown in fig.
- Slotted ALOHA still has an edge over pure ALOHA as chances of collision are reduced to one-half.



Slotted ALOHA



Pros

- single active node can continuously transmit at full rate of channel
- highly decentralized: only slots in nodes need to be in sync
- simple

Cons

- collisions, wasting slots
- idle slots
- nodes may be able to detect collision in less than time to transmit packet
- clock synchronization

BASIS FOR COMPARISON	PURE ALOHA	SLOTTED ALOHA
Introduced	Introduced by Norman Abramson and his associates at the University of Hawaii in 1970.	Introduced by Roberts in 1972.
Frame Transmission	The user can transmit the data frame whenever the station has the data to be transmitted.	The user has to wait till the next time slot start, to transmit the data frame.
Time	In Pure ALOHA the time is continuous.	In Slotted ALOHA the time is discrete.
Successful Transmission	The probability of successful transmission of the data frame is: $S = G * e^{-2G}$	The probability of successful transmission of the data frame is: $S = G * e^{-G}$
Synchronization	The time is not globally synchronized.	The time here is globally synchronized.
Throughput	The maximum throughput	The maximum throughput

CSMA: Carrier Sense Multiple Access)

CSMA: listen before transmit:

- If channel sensed idle: transmit entire pkt
- If channel sensed busy, defer transmission
 - **Persistent CSMA**: retry immediately with probability p when channel becomes idle (may cause instability)
 - **Non-persistent CSMA**: retry after random interval
- human analogy: don't interrupt others!

- CSMA improves on Aloha by requiring that stations listen before transmitting (compare to CB radio).
- Some collisions can be avoided, but not completely. This is because of propagation delays.
- Two or more stations may sense that the medium (= the channel) is free and start transmitting at time instants that are close enough for a collision to occur. Assume propagation time between A and B is 2 ms and that all stations are silent until time 0. At time 0, station A starts transmitting for 10 ms, at time 1 ms, station B has not received any signal from A yet, so it can start transmitting. At time 2ms, station B senses the collision but it is too late according to the protocol.

CSMA collisions

collisions can occur:

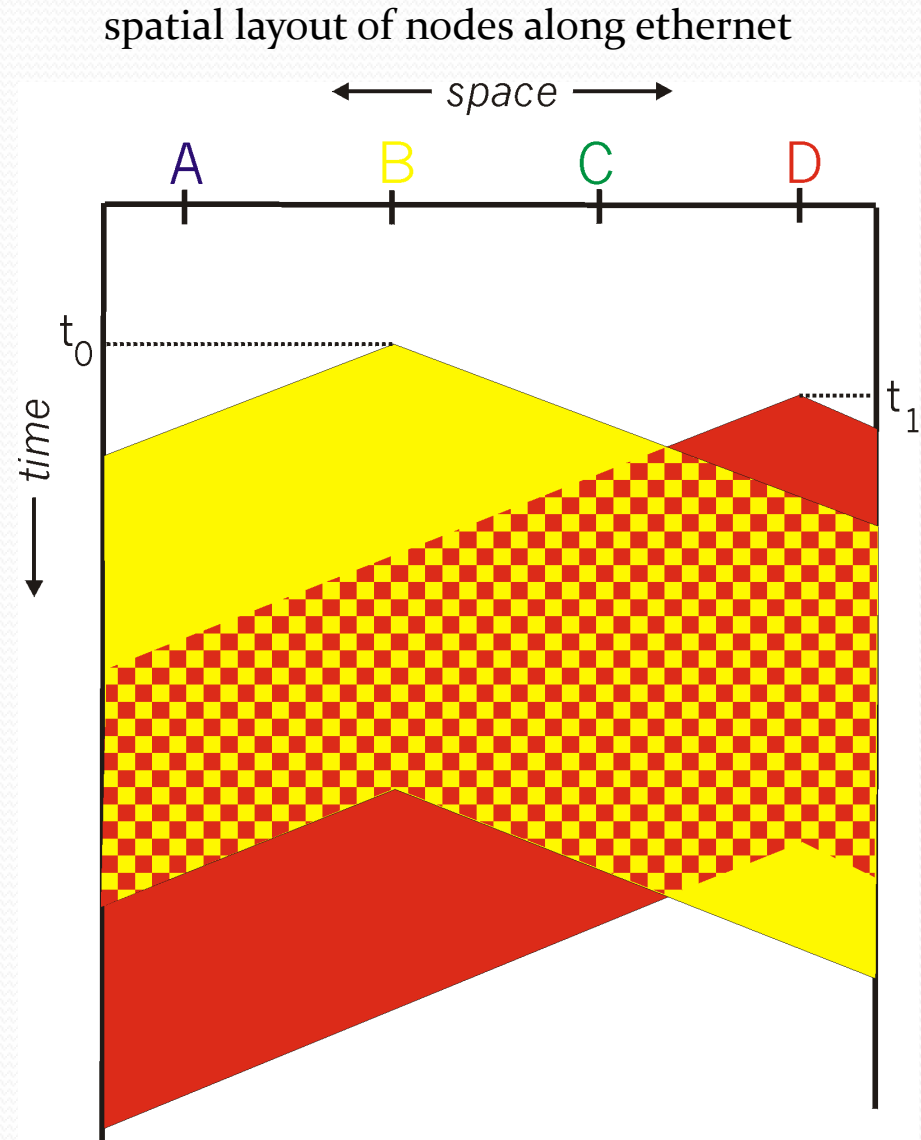
propagation delay means
two nodes may not yet
hear each other's
transmission

collision:

entire packet transmission
time wasted

note:

role of distance and
propagation delay in
determining collision prob.

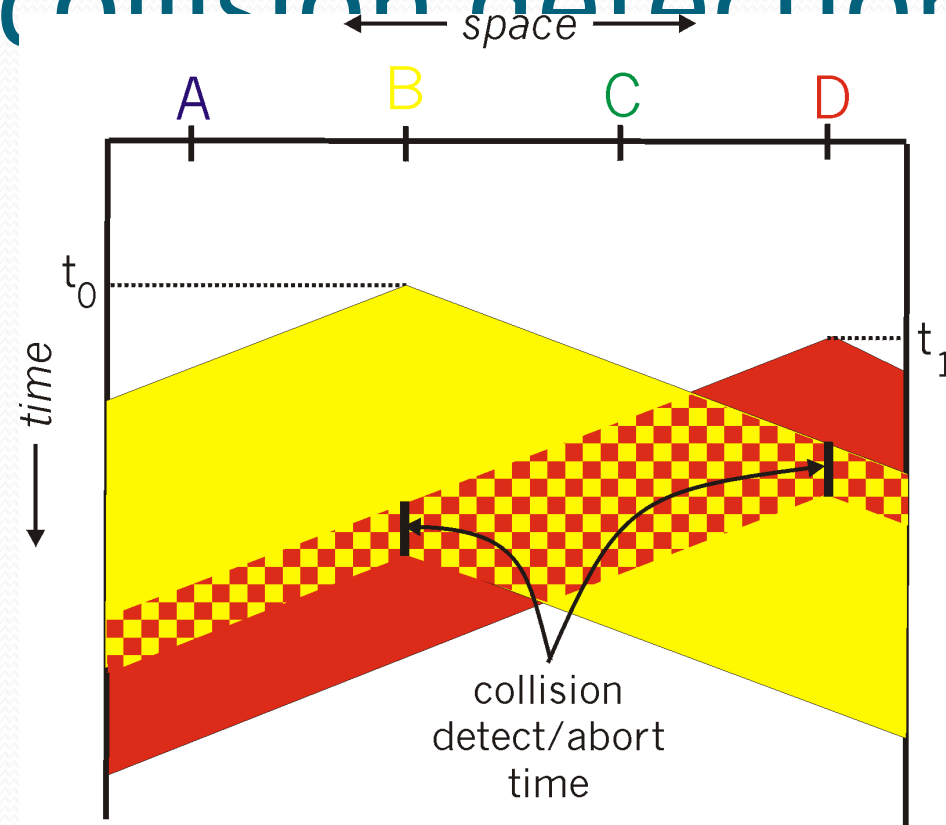



CSMA/CD (Collision Detection)

CSMA/CD: carrier sensing, deferral as in CSMA

- collisions *detected* within short time
- colliding transmissions aborted, reducing channel wastage
- persistent or non-persistent retransmission
- collision detection:
 - easy in wired LANs: measure signal strengths, compare transmitted, received signals
 - difficult in wireless LANs: receiver shut off while transmitting
- human analogy: the polite conversationalist

CSMA/CD collision detection





CSMA/CD is the protocol used by Ethernet. In addition to CSMA, it requires that a sending station monitors the channel and detects a collision.

The benefit is that a collision is detected within a propagation round trip time. These mechanisms give CSMA/CD much better performance than slotted ALOHA in a LAN environment.

In fact, if the maximum propagation delay between stations is very small, the efficiency of CSMA/CD can approach 100%. Collisions may still occur

CSMA/CA

- CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) is a protocol for carrier transmission in 802.11 networks.
- Unlike CSMA/CD (Carrier Sense Multiple Access/Collision Detect) which deals with transmissions after a collision has occurred, CSMA/CA acts to prevent collisions before they happen.
- In CSMA/CA, as soon as a node receives a packet that is to be sent, it checks to be sure the channel is clear (no other node is transmitting at the time). If the channel is clear, then the packet is sent.
- If the channel is not clear, the node waits for a randomly chosen period of time, and then checks again to see if the channel is clear. This period of time is called the backoff factor, and is counted down by a backoff counter. If the channel is clear when the backoff counter reaches zero, the node transmits the packet. If the channel is not clear when the backoff counter reaches zero, the backoff factor is set again, and the process is repeated.

Taking Turns MAC protocols

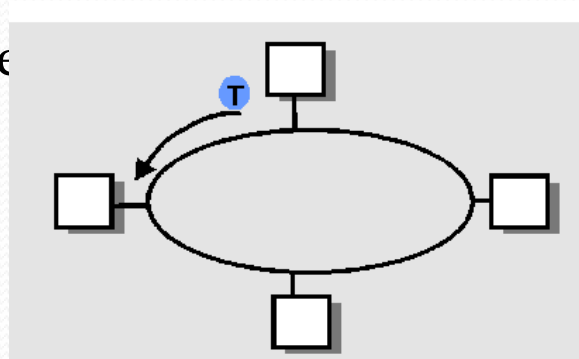
Polling:

- master node invites slave nodes to transmit in turn
- Request to Send, Clear to Send msgs
- concerns:
 - polling overhead
 - latency
 - single point of failure (master)

Animation

Token passing:

- ❑ **control token** passed from one node to next sequentially.
- ❑ token message
- ❑ concerns:
 - token overhead
 - latency
 - single point of failure (token)



e.g. FDDI, IEEE 802.5

Polling

- The polling protocol 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 (i.e. with an alternate fair scheme).
- In particular, the master node first sends a message to node 1, saying that it can transmit up to some maximum number of frames. After node 1 transmits some frames, the master node tells node 2 it 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.)
- 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 the empty slots that plague the random access protocols.
- This allows it to have a much higher efficiency. But it also has a few drawbacks:
 - (1) the protocol introduces a polling delay--the amount of time required to notify a node that it can transmit. (If, for example, only one node is active, then the node will transmit at a rate less than R bps, as the master node must poll each of the inactive nodes in turn, each time the active node has sent its maximum number of frames.)
 - (2) is that if the master node fails, the entire channel becomes inoperative

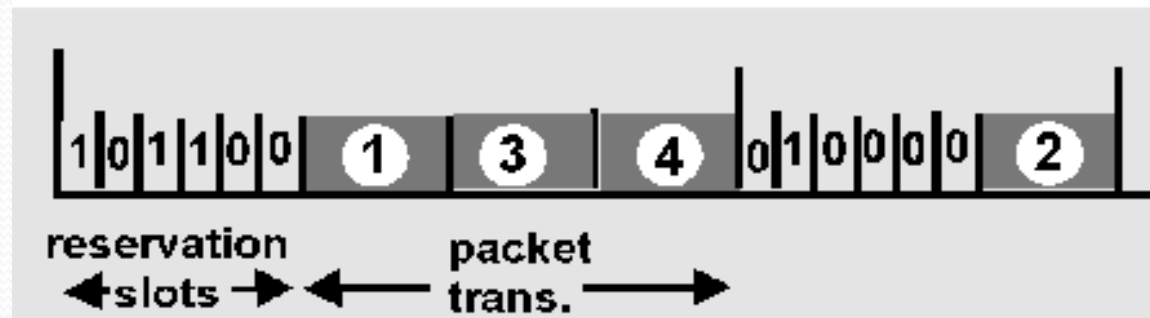
Token Passing

- In token-passing protocol 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, 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 a node does have frames to transmit when it receives the token, it sends up to a maximum number of frames and then forwards the token to the next node. Token passing is decentralized and has a high efficiency.
- But it has its problems as well. For example, the failure of one node can crash the entire channel. Or if a node accidentally neglects to release the token, then some recovery procedure must be invoked to get the token back in circulation.
- Examples of token passing technologies are fiber distributed data interface (FDDI) and Token-Ring (IEEE 802.5).

Reservation-based protocols

Distributed Polling:

- time divided into slots
- begins with N short **reservation slots**
 - reservation slot time equal to channel end-end propagation delay
 - station with message to send posts reservation
 - reservation seen by all stations
- after slot reservation, message transmissions are ordered by known priority
- Nodes can transmit only up to a max number of frames



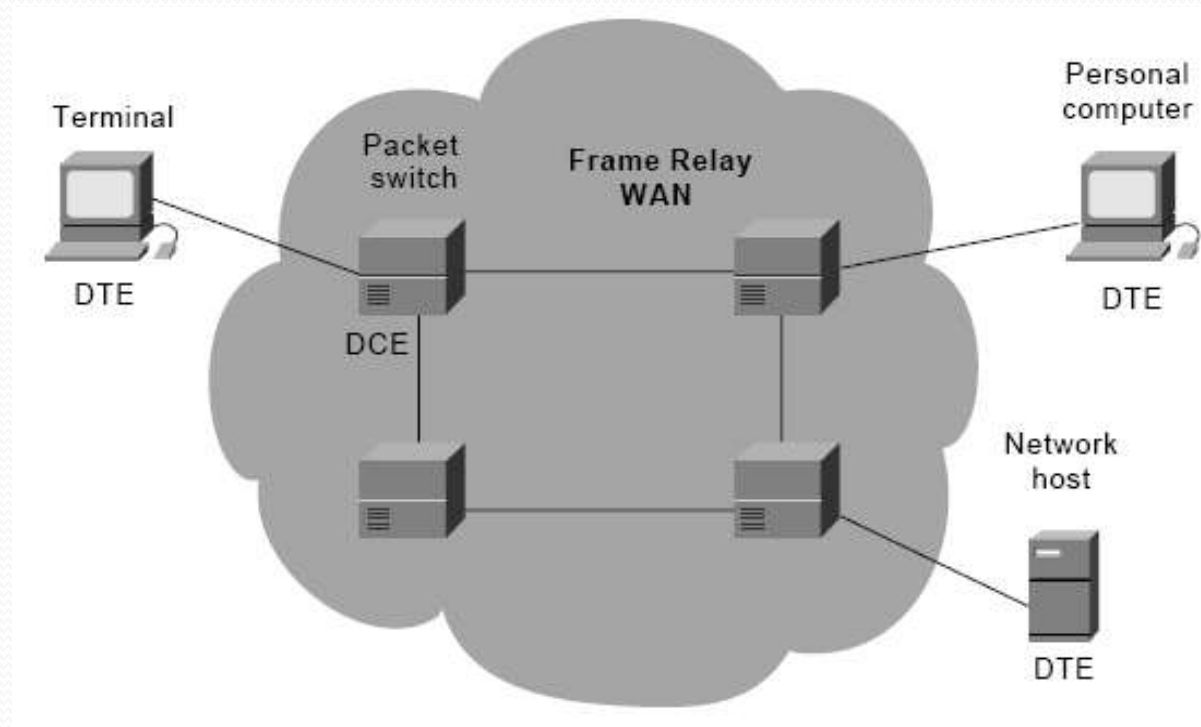
Frame Relay

- Frame Relay (FR) is a high-performance WAN protocol that operates at the **physical** and **data link** layers of the OSI reference model.
- FR originally was designed for use across **Integrated Service Digital Network** (ISDN) interfaces.
- Today, it is used over a variety of other network **interfaces** as well.
- FR is an example of a **packet-switched** technology.
- Packet-switched networks enable end stations to dynamically share the network medium and the available bandwidth.

Frame Relay Devices

- Devices attached to a Frame Relay WAN fall into the following two general categories:
 - **Data terminal equipment (DTE)**
 - DTEs generally are considered to be terminating equipment for a specific network and typically are located on the premises of a customer.
 - Example of DTE devices are terminals, personal computers, routers, and bridges.
 - **Data circuit-terminating equipment (DCE)**
 - DCEs are carrier-owned internetworking devices.
 - The purpose of DCE equipments is to provide clocking and switching services in a network, which are the devices that actually transmit data through the WAN.

Frame Relay Devices (cont.)



Advantages of the Frame Relay

- Efficient communication process.
- It performs fewer functions at the user-network interface.
- Delay is also lowered.
- Produces higher throughput.
- It is cost effective.
- It is faster than its predecessor X.25.

Disadvantages of the Frame Relay

- Unreliable service.
- The order of the arriving packets may not be maintained.
- The erroneous packets are directly dropped.
- The frame relay does not offer any flow control.
- There is no provision of the acknowledgement of the received packets and retransmission control for the frames

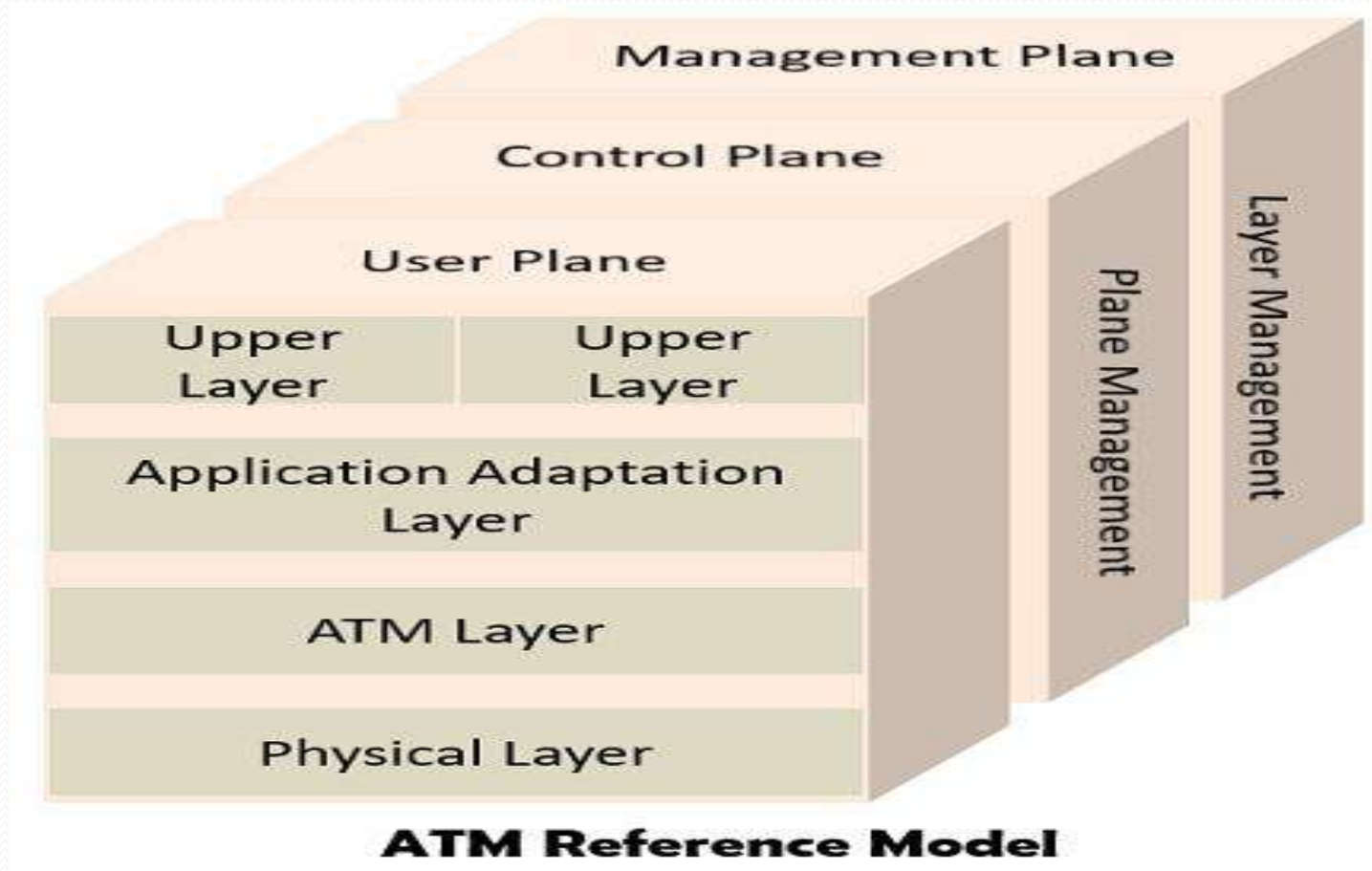
ATM

- **ATM** stands for **Asynchronous Transmission Mode**;
- it is a switching technique developed by integrating the features of the telecommunication and computer networks.
- ATM make use of cells in order to transfer information of many service forms such as voice, data and video.
- These cells are encoded by using asynchronous time division multiplexing. It also enables the communication between the devices works at the variable speed by combining the multiplexing and switching, and it is appropriate for the bursty traffic.
- These cells are nothing but the collection of fixed size packets.

Architecture of ATM

- The ATM reference model consists of layers and planes as shown in the diagram. There are three basic layers in the ATM- physical, ATM and ATM AAL layer.
- **Physical Layer:** This layer of the ATM handles the medium dependent transmissions.
- **ATM Layer:** The ATM layer is similar to data link layer which enables the sharing of virtual circuits between the different users and transmission of the cells over the virtual circuit.
- **Application Adaptation Layer (AAL):** The AAL is responsible for hiding the ATM implementation details from the higher layers. It also transforms the data into 48 bit cell payloads.

- The different planes included in the ATM reference model are control, user and management.
- **Control:** The main function of this plane is to produce and manage the signalling request.
- **User:** This plane handles the transfer of the data.
- **Management:** Layer related functions such as failure detection, problems regarding protocols are governed by this plane. It also involves the functions related to the complete system.



Advantages of the ATM

- It can easily interface with the existing network such as PSTN, ISDN. It can be used over SONET/SDH.
- Seamless integration with the different types of networks (LAN, MAN and WAN).
- Effective utilization of the network resources.
- It is less susceptible to the noise degradation.
- Provides large bandwidth.

Disadvantages of the ATM

- Cost of switching devices is higher.
- Overhead generated by the cell header is more.
- ATM QoS mechanism is quite complex.

Key Differences Between Frame Relay and ATM

- The packet size in the frame relay varies while ATM uses a fixed size packet known as a cell.
- ATM produces fewer overheads as compared to the frame relay technology.
- Frame relay is less expensive respective to the ATM.
- ATM is faster than the frame relay.
- ATM provides error and flow control mechanism, whereas the frame relay does not provide it.
- Frame relay is less reliable than the ATM.
- Throughput generated by frame relay is medium. In contrast, ATM has a higher throughput.
- The delay in the frame relay is more. As against, it is less in case of ATM.

Wireless LAN

- A wireless LAN is a wireless computer network that links two or more devices using wireless communication to form a local area network within a limited area such as a home, school, computer laboratory, campus, office building etc.
- The IEEE 802.11 group of standards specify the technologies for wireless LANs.
- 802.11 standards use the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance) for path sharing and include an encryption method, the Wired Equivalent Privacy algorithm

Wireless LAN



Spread Spectrum

- Spread spectrum is a technique used for transmitting radio or telecommunications signals.
- The term refers to the practice of spreading the transmitted signal to occupy the frequency spectrum available for transmission.
- Although spread spectrum techniques were originally designed for military uses, they are now being used widely for commercial purpose
- This is a technique in which a telecommunication signal is transmitted on a bandwidth considerably larger than the frequency content of the original information.
- Frequency hopping is a basic modulation technique used in spread spectrum signal transmission.
- Spread-spectrum telecommunications is a signal structuring technique that employs direct sequence, frequency hopping, or a hybrid of these, which can be used for multiple access and/or multiple functions.
- This technique decreases the potential interference to other receivers while achieving privacy. Spread spectrum generally makes use of a sequential noise-like signal structure to spread the normally narrowband information signal over a relatively wideband (radio) band of frequencies.
- **Frequency-hopping** spread spectrum (FHSS) is a method of transmitting radio signals by rapidly switching a carrier among many **frequency** channels, using a pseudorandom sequence known to both transmitter and receiver.

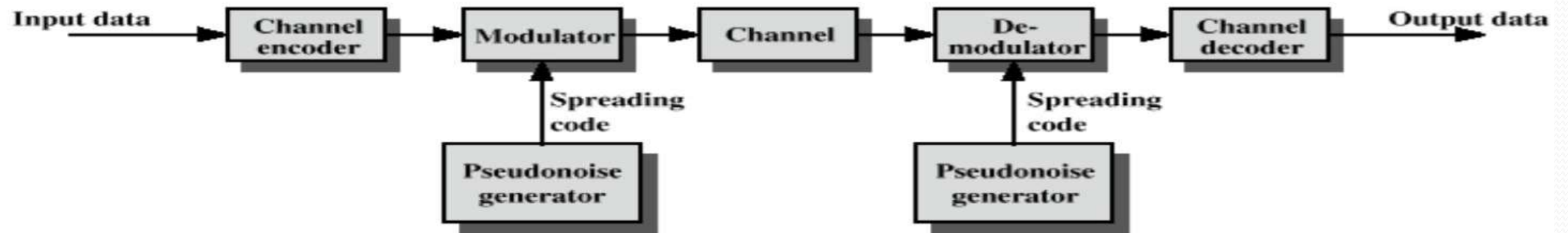


Figure 7.1 General Model of Spread Spectrum Digital Communication System

A coded sequence of 1s and 0s with certain auto-correlation properties, called as **Pseudo-Noise coding sequence** is used in spread spectrum techniques. It is a maximum-length sequence, which is a type of cyclic code

Advantages:

- Cross-talk elimination
- Better output with data integrity
- Reduced effect of multipath fading
- Better security
- Reduction in noise
- Co-existence with other systems
- Longer operative distances
- Hard to detect
- Not easy to demodulate/decode
- Difficult to jam the signals

Application:

- It is used in mobile communications.
- It is used in distance measurement.
- It is used in selective calling.
- It is used in CDMA communication

Bluetooth

- Bluetooth is a wireless technology standard for exchanging data between fixed and mobile devices over short distances using short-wavelength UHF radio waves in the industrial, scientific and medical radio bands, from 2.400 to 2.485 GHz, and building personal area networks.
- A variety of digital devices use Bluetooth, including MP3 players, mobile and peripheral devices and personal computers.

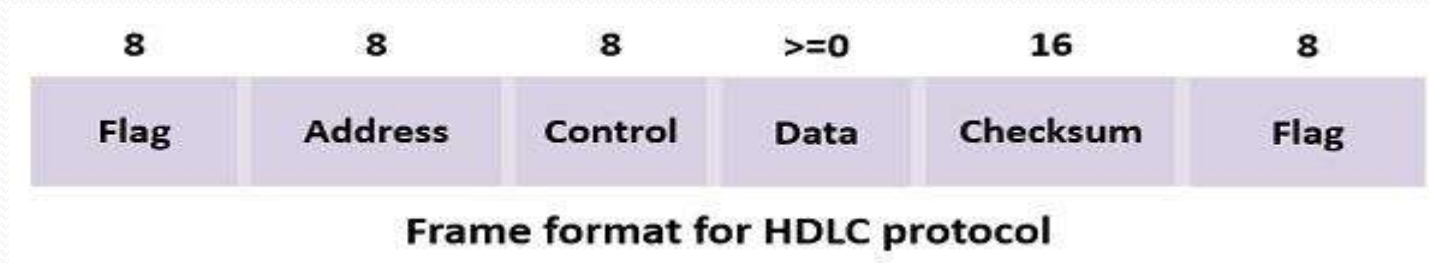
key features of Bluetooth technology:

- Less complication
- Less power consumption
- Available at cheaper rates
- Robustness

HDLC

- **HDLC (High-level Data Link Control)** is a WAN protocol intended to perform the encapsulation of the data in the data link layer. The encapsulation of the data means to change the format of the data.
- The HDLC protocol follows the bit-oriented concept and uses bit stuffing for achieving data transparency. Here bit oriented approach signifies that the single bit is used to present the control information. The frame structure of HDLC contains the address, control, data, checksum and flag fields.
- The default encapsulation protocol in the Cisco devices is the HDLC. The Cisco proprietary HDLC only works when the devices in both of the ends of the link are of cisco. Standard HDLC can have different devices in the ends

Frame format for the bit-oriented protocols



- Address field – It is used to describe the terminal.
- Control field – The bits in the control field is intended for the sequence number and acknowledgements.
- **Data field** – This field is used to hold the information.
- **Checksum field** -In this field, the bits are reserved for the performing the cyclic redundancy code.

HDLC Commands and Requests

- The HDLC uses a group of commands and responses for its working. There are three types of frames information, supervisory and unnumbered.
- **Information transfer format (I-Frame)** – It transports the numbered frames in a sequential manner, which contain the information field.
- **Supervisory format (S-Frame)** – The supervisory frames conduct the managerial functions such as acknowledgement, information transfer status, polling and error recovery. The commands and requests included in this are RECEIVE READY, RECEIVE NOT READY, REJECT, etcetera.
- **Unnumbered format (U-Frame)** – It basically extends the data link control functions. There several commands and requests fall under this category such as RESET, TEST, FRAME REJECT, REQUEST DISCONNECT, etc

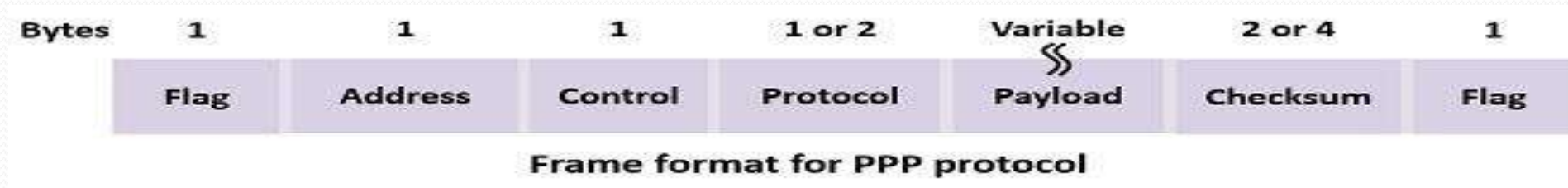
PPP

- **PPP (Point-to-Point Protocol)** is also a WAN protocol, but there are several enhancements made in the PPP protocol after HDLC.
- Priorly, the PPP protocol is not proprietary, which means that it can be used with two different type of devices without committing changes over the format of the data. All of the links collaboratively treated as single, independent IP network which is having its own frame format, hardware addressing method, and data link protocol.
- A point-to-point connection is obtained without assigning multiple IP addresses to the tangible wires, and it just needs the IP network number.

Features of PPP

- To clearly identify the start and end of the frame, the framing method is used on the asynchronous data. It is also beneficial in the detection of the errors.
- A **link control protocol** is used for enabling the network lines, testing them, terminate them when no longer used. This link control protocol is basically helpful in handling the synchronous and asynchronous circuits, and byte and bit-oriented encodings.
- It can select the **NCP (Network Control Protocol)** for each supported network layer.

Frame format of PPP



- The PPP frame contains two flag fields, a **protocol** field to determine the type of packet residing in the **payload**, and a payload field which can vary. However, the rest of the fields are the same as the HDLC protocol.
- Address field – It is used to describe the terminal.
- Control field – The bits in the control field are intended for the sequence number and acknowledgements.
- **Data field** – This field is used to hold the information.
- **Checksum field** - In this field, the bits are reserved for performing the cyclic redundancy code.

Key Differences Between HDLC and PPP

- The HDLC is a bit-oriented protocol while PPP is byte-oriented as well as bit oriented because it can be sent over the dial-up modem lines and also true bit-oriented HDLC.
- Only synchronous media can be used in HDLC. In contrast, PPP can work with synchronous and asynchronous media.
- No link authentication is provided in HDLC, whereas it is provided in PPP.
- PPP can dynamically assign and frees up the IP address according to the use. As against, this not the case in HDLC.
- Interoperability between the non-cisco devices in HDLC is not achievable. However, this limitation of HDLC is eliminated from the PPP protocol.

Ethernet -802.3

- 802.3 is the standard which Ethernet operates by. It is the standard for CSMA/CD (Carrier Sense Multiple Access with Collision Detection). This standard encompasses both the MAC and Physical Layer standards.

CSMA/CD is what Ethernet uses to control access to the network medium (network cable). If there is no data, any node may attempt to transmit, if the nodes detect a collision, both stop transmitting and wait a random amount of time before retransmitting the data.

The original 802.3 standard is 10 Mbps (Megabits per second). 802.3u defined the 100 Mbps (Fast Ethernet) standard, 802.3z/802.3ab defined 1000 Mbps Gigabit Ethernet, and 802.3ae define 10 Gigabit Ethernet.

Commonly, Ethernet networks transmit data in packets, or small bits of information. A packet can be a minimum size of 72 bytes or a maximum of 1518 bytes.

The most common topology for Ethernet is the star topology.

802.5 Token Ring

- The token is a special frame which is designed to travel from node to node around the ring. When it does not have any data attached to it, a node on the network can modify the frame, attach its data and transmit. Each node on the network checks the token as it passes to see if the data is intended for that node, if it is; it accepts the data and transmits a new token. If it is not intended for that node, it retransmits the token on to the next node.

The token ring network is designed in such a way that each node on the network is guaranteed access to the token at some point. This equalizes the data transfer on the network. This is different from an Ethernet network where each workstation has equal access to grab the available bandwidth, with the possible of a node using more bandwidth than other nodes.

Originally, token ring operated at a speed of about 4 Mbps and 16 Mbps. 802.5t allows for 100 Mbps speeds and 802.5v provides for 1 Gbps over fiber.

Token ring can be run over a star topology as well as the ring topology.

There are three major cable types for token ring: Unshielded twisted pair (UTP), Shielded twisted pair (STP), and fiber.

Token ring utilizes a Multi-station Access Unit (MAU) as a central wiring hub. This is also sometimes called a MSAU when referring to token ring networks.

802.4 Token Bus

- The token bus Computer network station must have possession of a token before it can transmit on the computer network.
- The IEEE 802.4 Committee has defined **token bus** standards as broadband computer networks, as opposed to Ethernet's baseband transmission technique. Physically, the token bus is a linear or tree-shape cable to which the stations are attached.
- **The topology of the computer network can include groups of workstations connected by long trunk cables.**
- Logically, the stations are organized into a ring. These workstations branch from hubs in a star configuration, so the network has both a bus and star topology. Token bus topology is well suited to groups of users that are separated by some distance.
- **IEEE 802.4 token bus networks are constructed with 75-ohm coaxial cable using a bus topology.** The broadband characteristics of the 802.4 standard support transmission over several different channels simultaneously.

802.11 Standards

- **IEEE 802.11a:** In terms of speed, the 802.11a standard was far ahead of the original 802.11 standards. 802.11a specified speeds of up to 54Mbps in the 5GHz band, but most commonly, communication takes place at 6Mbps, 12Mbps, or 24Mbps. 802.11a is incompatible with the 802.11b and 802.11g wireless standards.
- **IEEE 802.11b:** The 802.11b standard provides for a maximum transmission speed of 11Mbps. However, devices are designed to be backward-compatible with previous 802.11 standards that provided for speeds of 1, 2, and 5.5Mbps. 802.11b uses a 2.4GHz RF range and is compatible with 802.11g.
- **IEEE 802.11g:** 802.11g is a popular wireless standard today. 802.11g offers wireless transmission over distances of 150 feet and speeds up to 54Mbps compared with the 11Mbps of the 802.11b standard. Like 802.11b, 802.11g operates in the 2.4GHz range and therefore is compatible with it.
- **IEEE 802.11n:** The newest of the wireless standards listed in the Network+ objectives is 802.11n. The goal of the 802.11n standard is to significantly increase throughput in both the 2.4GHz and the 5GHz frequency range. The baseline goal of the standard was to reach speeds of 100Mbps, but given the right conditions, it is estimated that the 802.11n speeds might reach a staggering 600Mbps. In practical operation, 802.11n speeds will be much slower.

IEEE Standard	Frequency/Medium	Speed	Topology	Transmission Range	Access Method
802.11	2.4GHz RF	1 to 2Mbps	Ad hoc/infrastructure	20 feet indoors.	CSMA/CA
802.11a	5GHz	Up to 54Mbps	Ad hoc/infrastructure	25 to 75 feet indoors; range can be affected by building materials.	CSMA/CA
802.11b	2.4GHz	Up to 11Mbps	Ad hoc/infrastructure	Up to 150 feet indoors; range can be affected by building materials.	CSMA/CA
802.11g	2.4GHz	Up to 54Mbps	Ad hoc/infrastructure	Up to 150 feet indoors; range can be affected by building materials.	CSMA/CA
802.11n	2.4GHz/5GHz	Up to 600Mbps	Ad hoc/infrastructure	175+ feet indoors; range can be affected by building materials.	CSMA/CA