Tutorial
ELEC3506/9506
Communication Networks

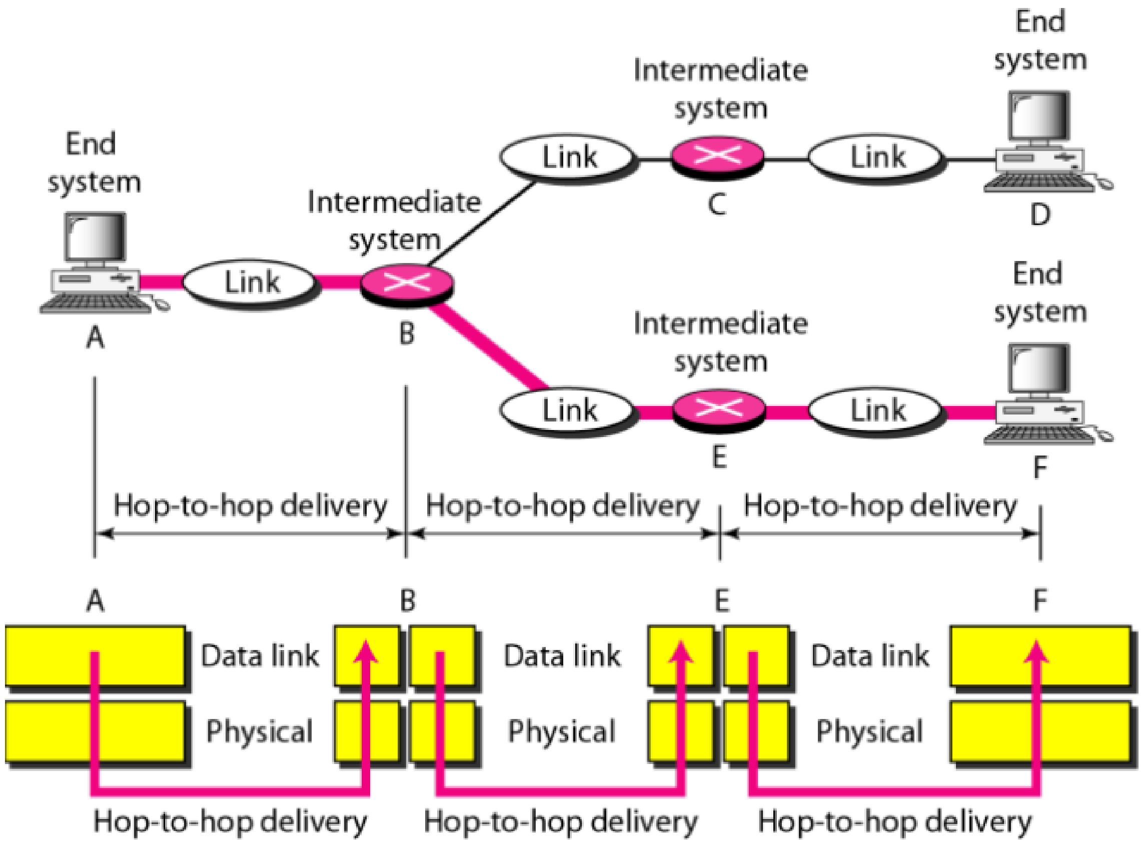
School of Electrical and Information Engineering
The University of Sydney

Dr. Shuvashis Saha
shuvashis.saha@sydney.edu.au

Tutorial 03 – Week 04

Q1. Briefly describe the services provided by the data link layer.

- **Framing Data Bits**: Divides the stream of bits received from the network layer into manageable frames.
- **Moving Frames**: Transfers frames from one hop (node) to the next in the network.
- **Physical Addressing**: Provides physical addresses (MAC addresses) for identifying the sender and receiver.
- **Flow Control**: Prevents the sender from overwhelming the receiver with too much data too quickly.
- **Error Control**: Adds reliability by detecting and correcting errors in the data transmitted over the physical layer.
- **Access Control**: Manages which device has control over the network link at any given time to avoid conflicts.



Q2. Define framing and the reason for its need.

❑ Framing

A process in data link layer to divide the stream of bits received from the network layer into frames.

❑ Reasons for framing:

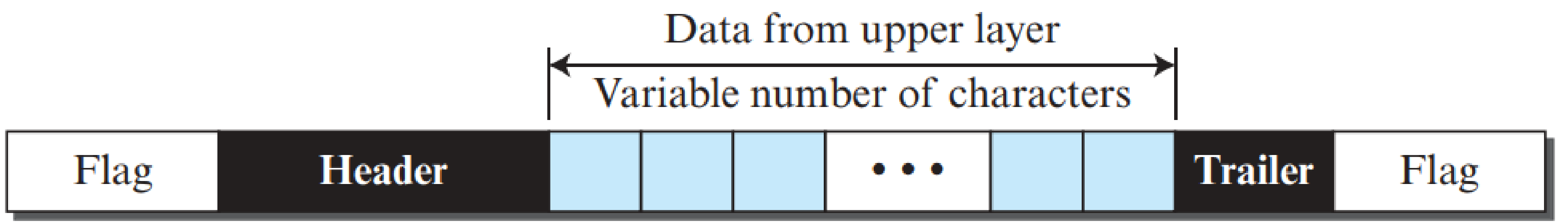
- Framing adds the physical sender and destination addresses. The destination address specifies where the frame should go; the sender address is used to send an acknowledgement (ACK) back to the sender.
- Framing in data link layer divides the message into appropriate-sized frames such that the flow control and error control become efficient. Smaller-sized frames make flow control and error control more efficient.

A frame has the following parts:

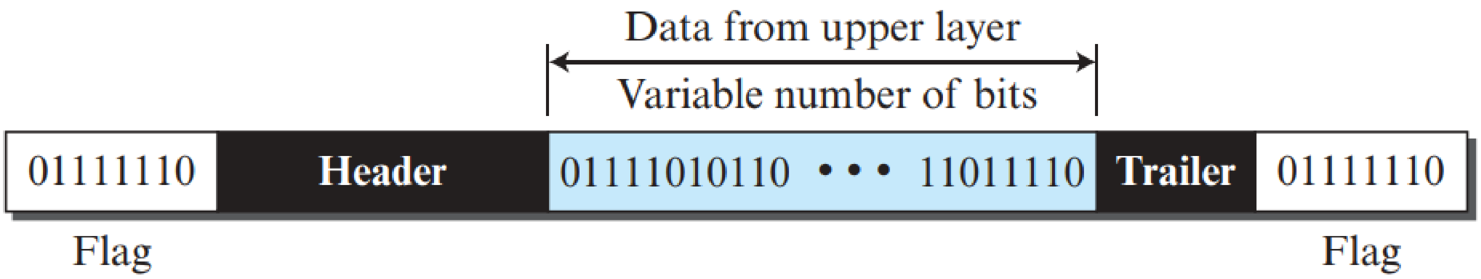
- ❑ **Frame header**: Contains the source and destination address
- ❑ **Payload field**: Contains the message to be delivered.
- ❑ **Trailer**: Contains error detection & correction bits.
- ❑ **Flag**: Marks the beginning and end of the frame.

Q3. Compare and contrast byte-oriented and bit-oriented protocols. Which category has been popular in the past? Which category is popular now?

- **Byte-oriented (Character-oriented) protocol**
  - Data to be carried are 8-bit characters from a coding system, e.g., ASCII code
  - Character-oriented protocols were popular when only text was exchanged by the data link layers



- **Bit-oriented protocol:**
  - Data is transmitted as a stream of bits.
  - More popular today, because we need to send text, graphic, audio, and video, which can be better represented by a bit pattern rather than by using a sequence of characters.



Q4. Compare and contrast the three most common error detection methods

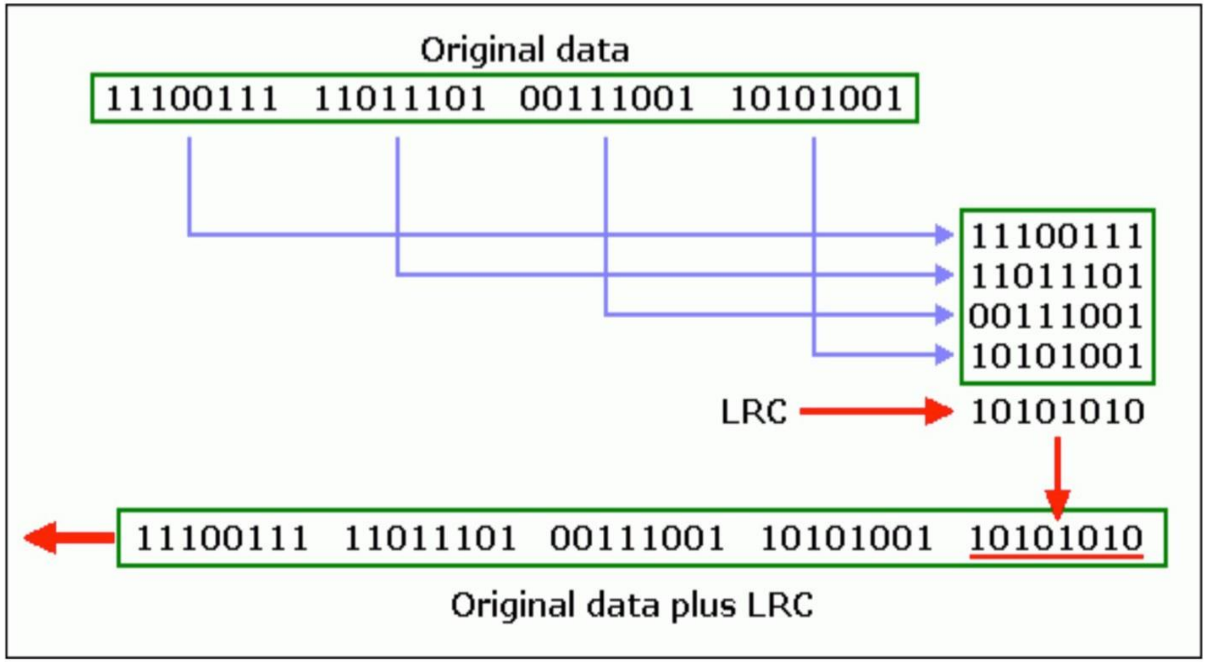
- **Parity Checking (Vertical Redundancy Checking - VRC)**
  - One of the oldest and simplest methods
  - Adds 1 additional bit to each byte in the message.
  - Even parity causes the sum of all bits to be even.
  - Odd parity causes the sum of bits to be odd
- **Simple but only has about a 50% reliability rate.**

Example: Even Parity

Message	Codeword
000	0000
001	0011
010	0101
011	0110
100	1001
101	1010
110	1100
111	1111

Q4. Compare and contrast the three most common error detection methods

- **Longitudinal Redundancy Checking (LRC)**
  - A block of bits is divided into rows and redundant row of bits is added to the whole block.



- At the receiver side, this redundant row is used to detect the error.
- The receiver calculates the LRC and compares it to the LRC appended to the transmitted data. If two LRCs match, no error is detected.
- Compared to VRC, LRC increases the likelihood of detecting burst errors.

THE UNIVERSITY OF SYDNEY

Q4. Compare and contrast the three most common error detection methods

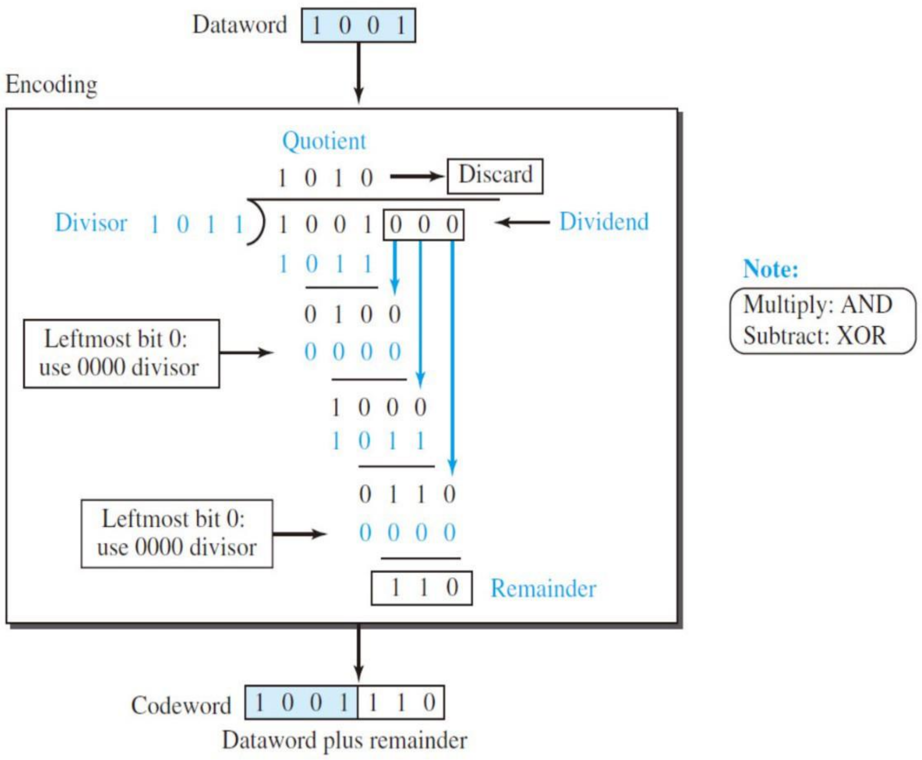
- **Cyclic Redundancy Check Codes (CRC)**
  - Message length k, codeword length n
  - **Encode**
    - Multiply $u(x)$ with x^{n-k}
    - Divided $u(x)x^{n-k}$ by $g(x)$ and obtain the remainder $b(x)$
    - Forming the codeword

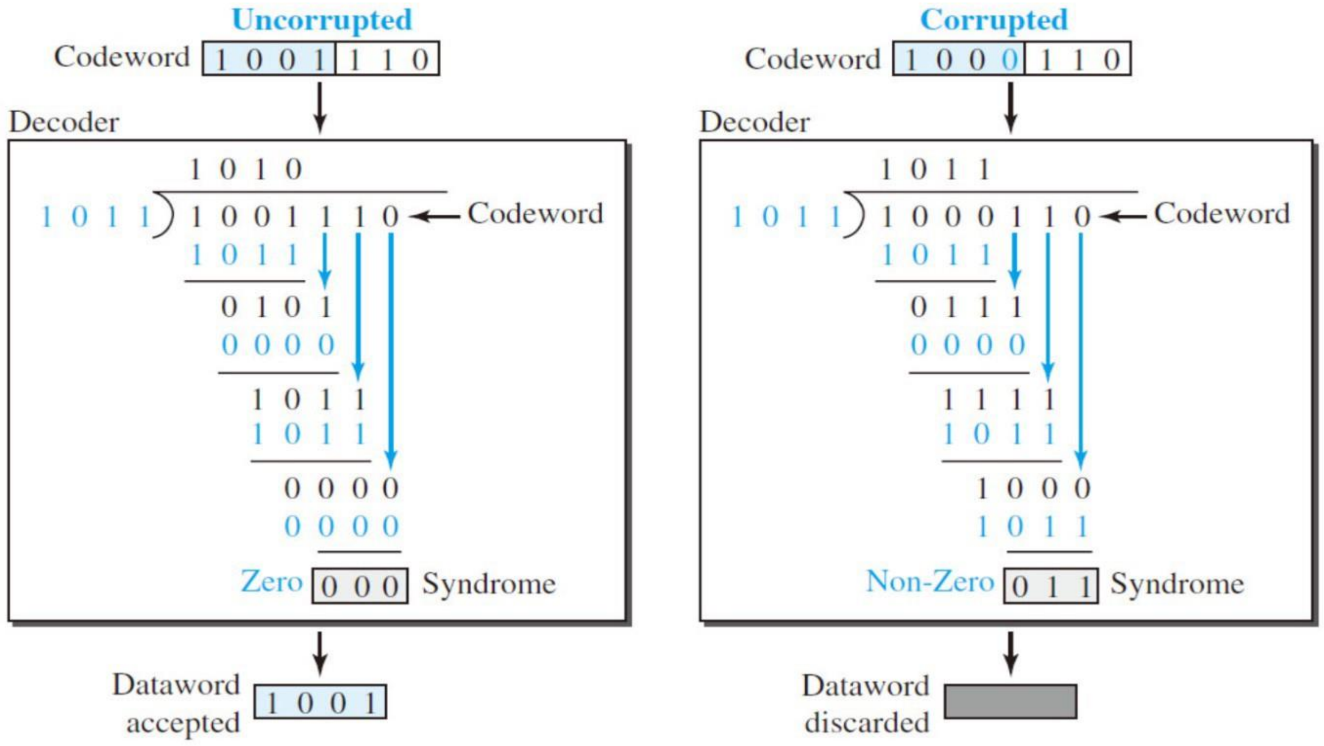
      $\boldsymbol{v(x) = b(x) + u(x)x^{n-k}}$

- Decode
  - Divide $v(x)$ by $g(x)$
  - If the remainder is zero, no error
  - Otherwise, error
  - CRC can detect more types of error than VRC and LRC.

Cyclic Redundancy Check Codes (CRC)

Encoder





Q5. Compare and contrast flow control and error control. How does error control complement flow control?

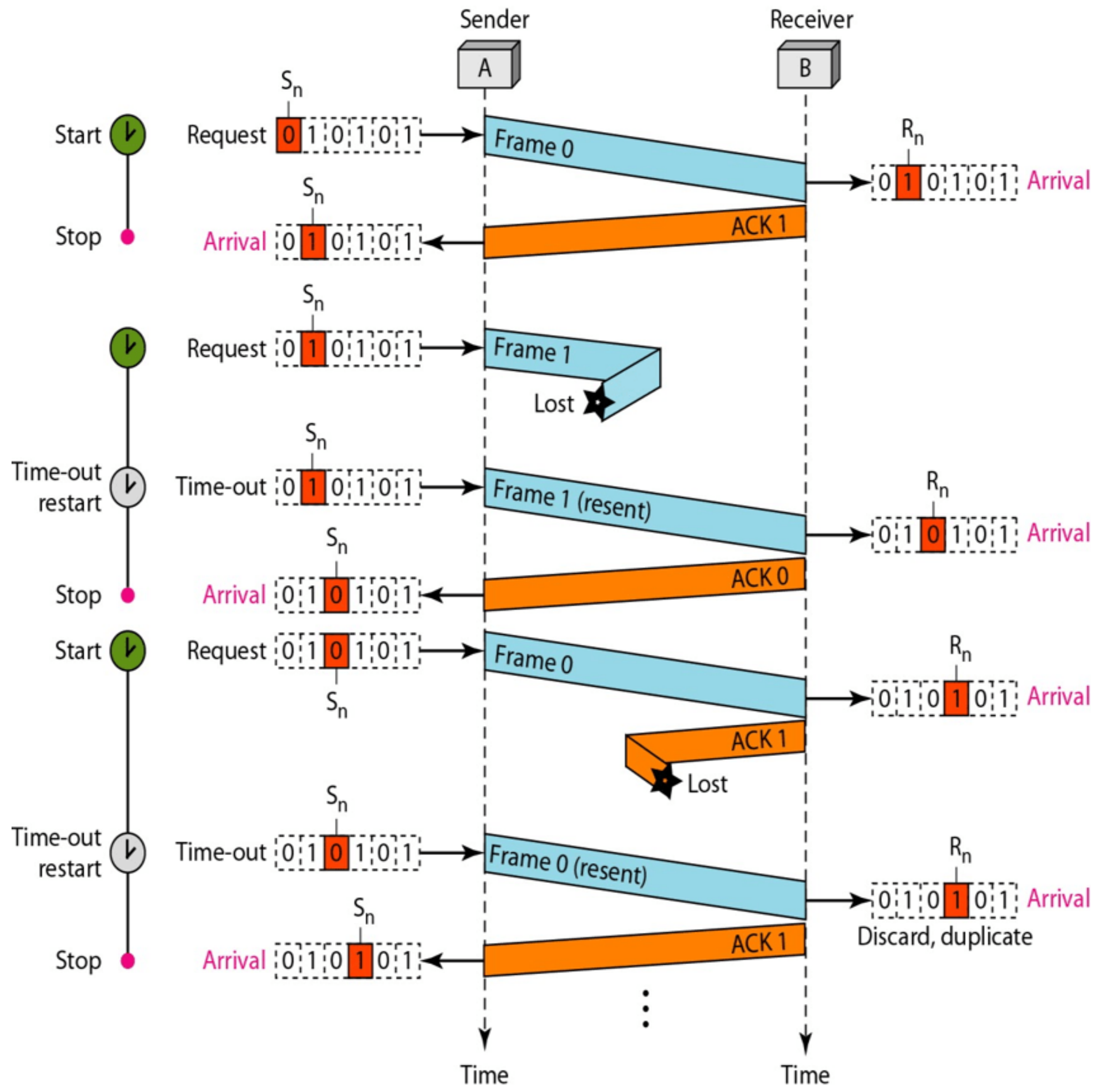
- **Flow Control** refers to a set of procedures used to restrict the amount of data that sender can send before waiting for acknowledgement.
  - Any receiving device has a limited speed for processing data.
  - The processing rate of the receiver is usually slower than the transmission rate.
  - Each receiving device has a buffer for storing the incoming data before they are processed.
  - When the buffer begins to fill up, the receiver must tell the sender to slow down the transmission.

- **Error control** refers to a set of procedures used to detect and correct errors.
  - Both flow control and error control help in proper delivering of data to the receiver.
  - Flow control ensures that frames are not discarded due to buffer overflow. Error control complements flow control by ensuring that the frames received at the received side are error-free.

Q6. State three error control protocols for noisy channels (as discussed in the lecture).

- ❑ Stop-and-wait Automatic Repeat reQuest (ARQ) (Send one frame at a time)
- ❑ Go-back-N ARQ (Send several frames at a time)
- ❑ Selective-Repeat ARQ (Send several frames at a time)

Q7. Why is stop-and-wait ARQ inefficient?



- Slow speed : The sender has to wait for a round trip time (RTT) before another frame can be sent.

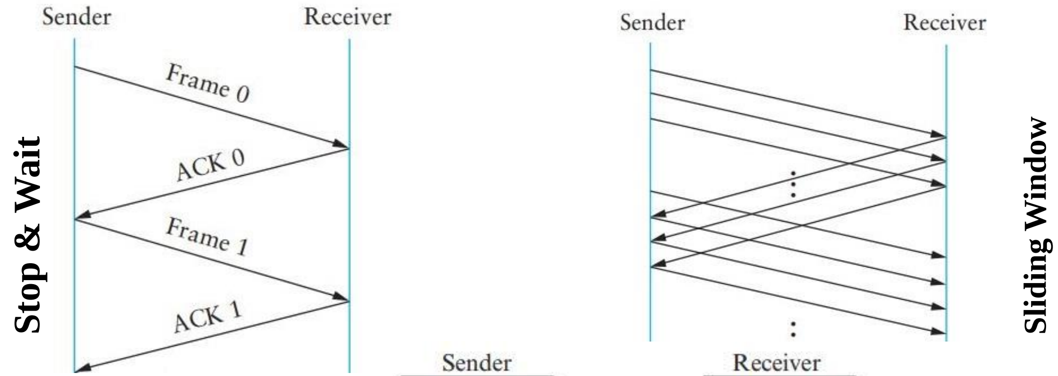
- Low bandwidth ulitization : Only one frame can be sent at a time

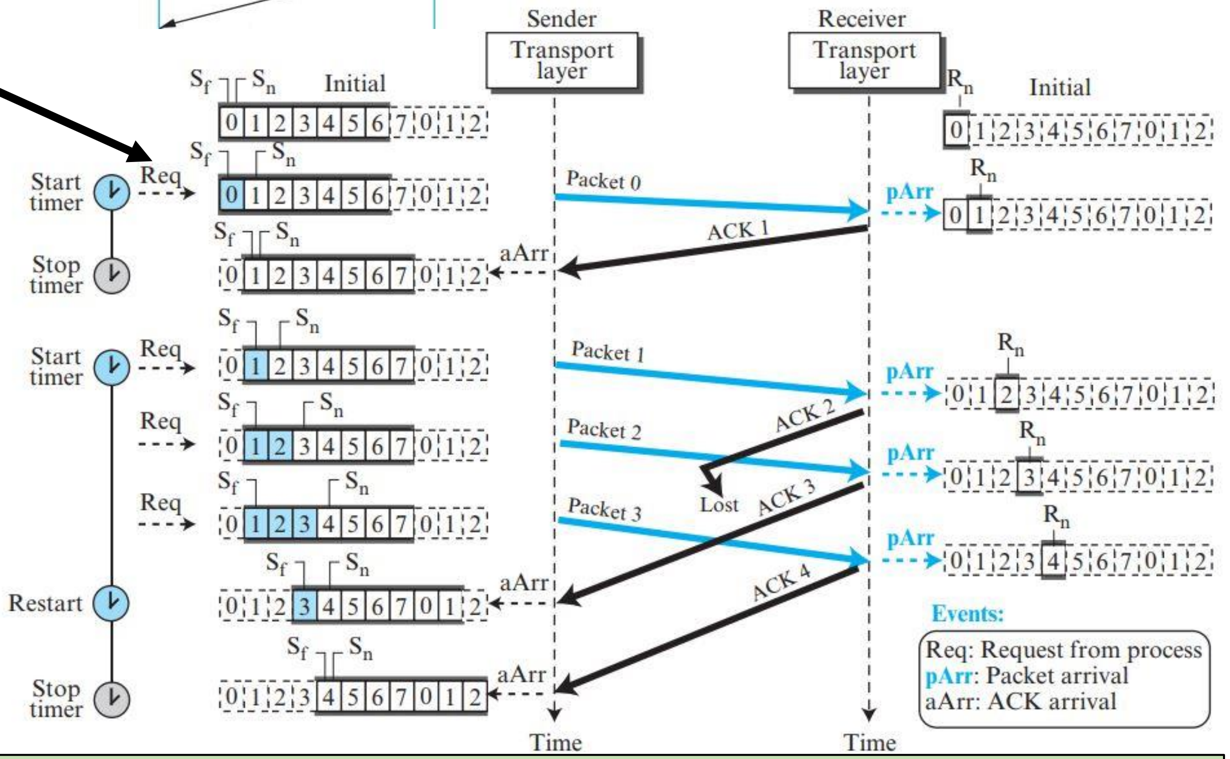
Q8. What are the advantages and disadvantages of Go-Back-N ARQ?

THE UNIVERSITY OF SYDNEY

Advantages

- **Multiple packet transmission**: the sender is allowed to transmit multiple packets (when available) without waiting for an acknowledgment.
- **Cumulative ACK**: Go-Back-N can acknowledge more than one frame with a single ACK, which reduces the time and bandwidth wasted for sending ACKs.
- **Complexity**: Less complicated than the Selective-Repeat ARQ. In case of Selective-Repeat ARQ, negative ACK (NACK) is required.
- **Buffering**: No buffering is needed at the receiver.
- **Sorting**: No packet sorting is needed at the receiver.



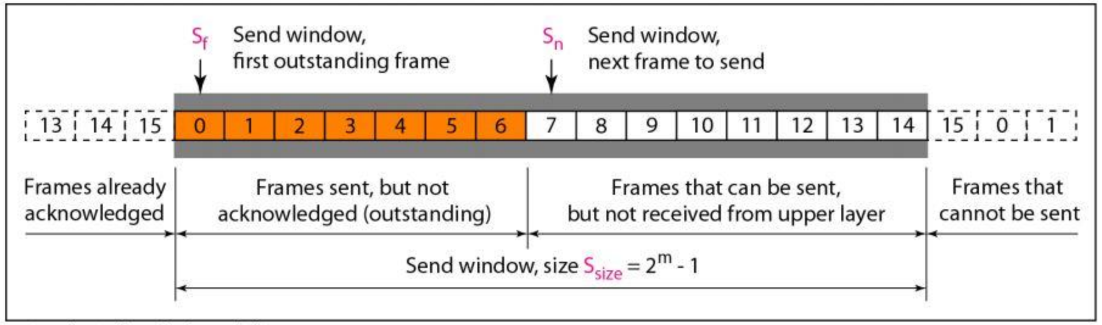


- ❖ Assume a sender sends 6 packets: packets 0, 1, 2, 3, 4, and 5. The sender receives an ACK with ackNo = 3. **That means?**
- ❖ If the system is using GBN, it means that packets 0, 1, and 2 have been received uncorrupted and the receiver is expecting packet 3.

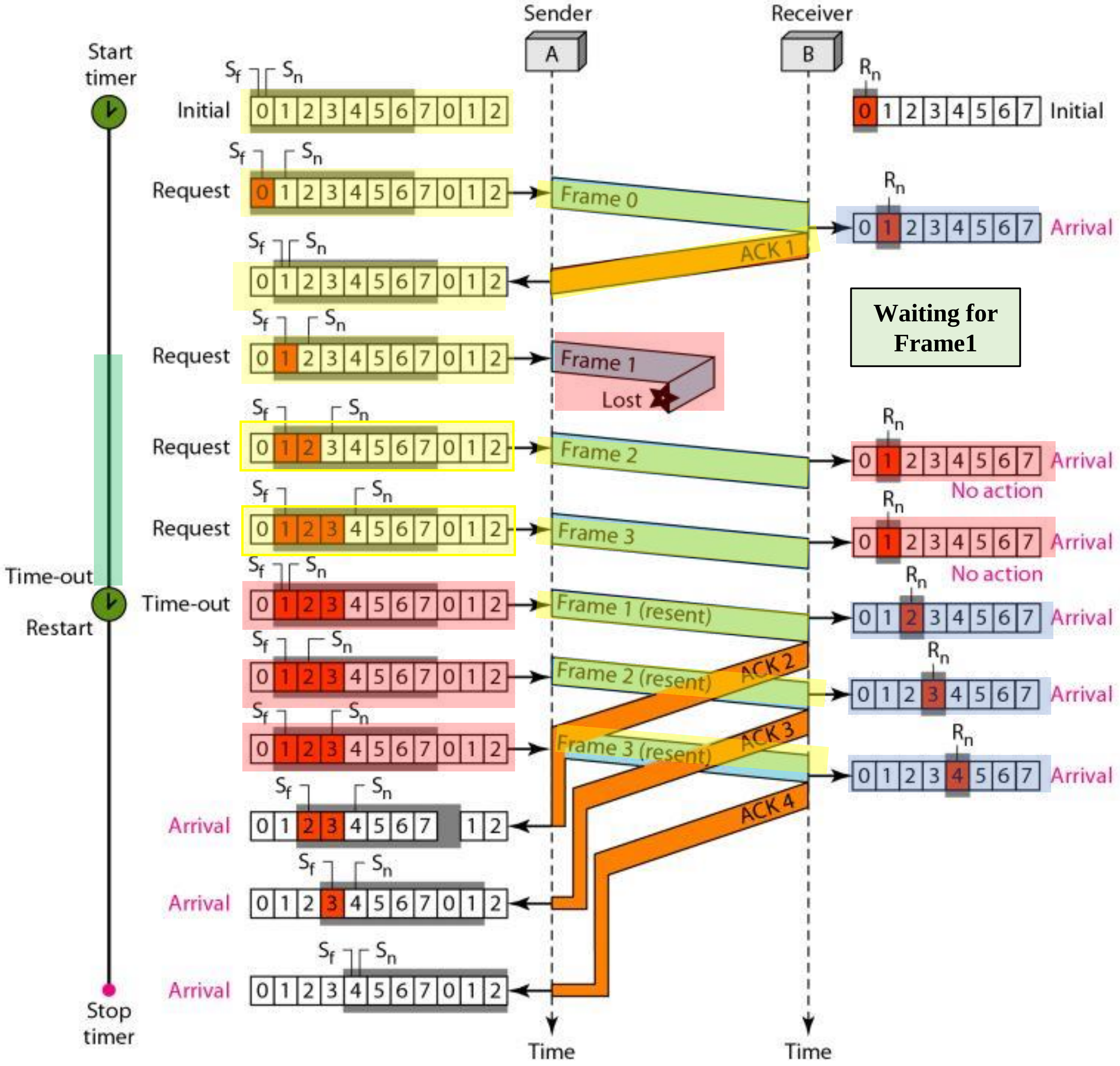
Q8. What are the advantages and disadvantages of Go-Back-N ARQ?

Disadvantages

- **Retransmission**: This protocol is very inefficient for a noisy link. Unnecessary resending uses up the bandwidth and slows down the transmission.
- **Transmitter Buffer**: Buffer requirement at the transmitter. Transmitter needs to store N packets.



a. Send window before sliding



- **High bandwidth requirement**

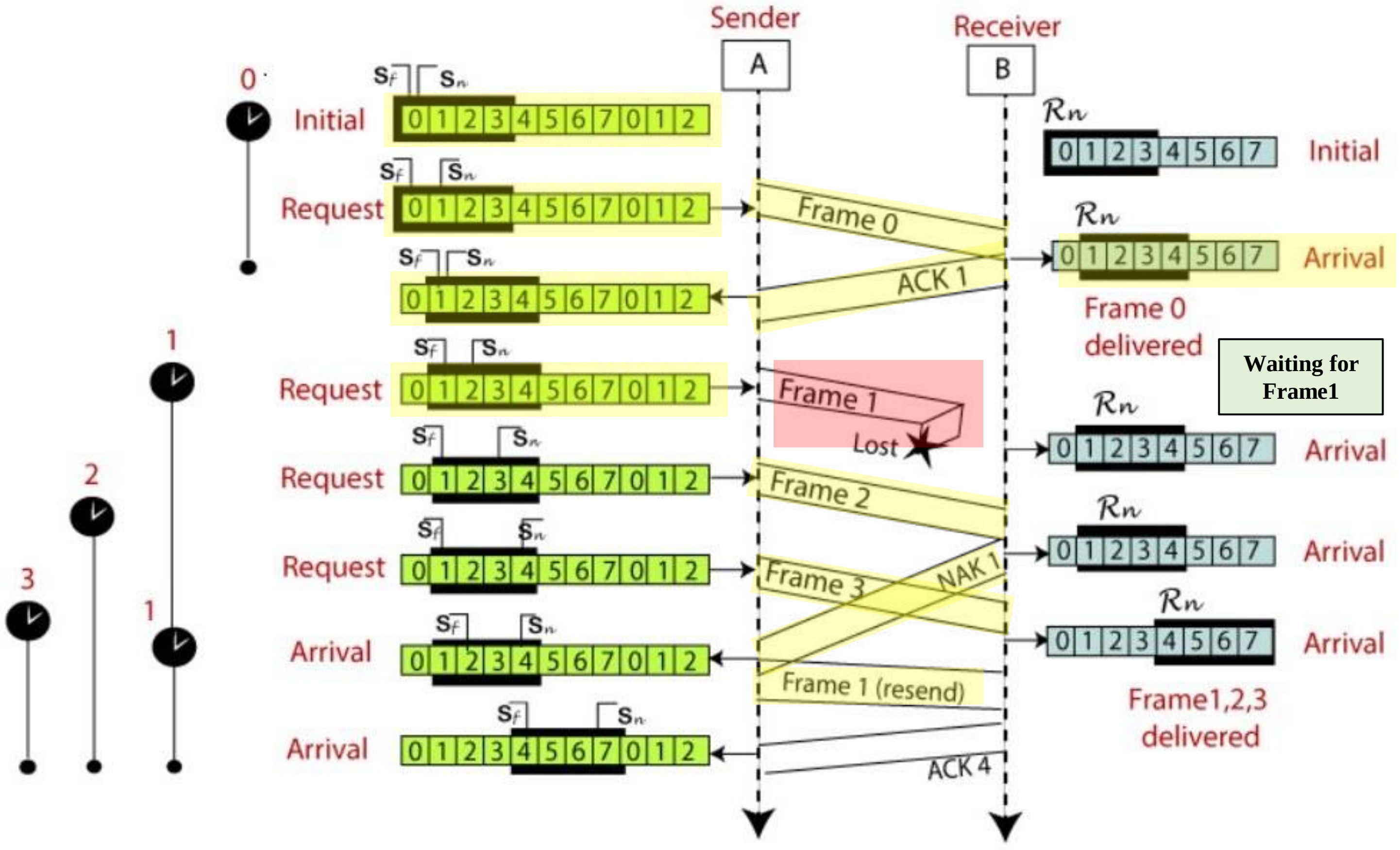
Q9. How does Selective Repeat ARQ address the deficiencies of Go-Back-N ARQ? (Cont…)

- Unnecessary retransmission of the successfully received packets is one of the major problems in Go back N protocol.

- In **Selective-Repeat ARQ**, unnecessary transmission is avoided by sending only the frames that are corrupted or missing.

- **Negative Acknowledgement**: Selective-Repeat ARQ uses negative acknowledgement (NAK) which can speed up the retransmission of frames.

- Before the sender's timer expires for a lost frame, the receiver can send a NAK to let the sender know that a frame was lost or received incorrectly.



Q10. Standard Ethernet defines several Physical layer implementations. Discuss the most common implementation categories?

- Standard Ethernet has defined several physical layer implementations, out of which the following four are commonly used.

Name	Media	Max Length	Line Encoding
10Base5	Thick coaxial cable	500 m	Manchester
10Base2	Thin coaxial cable	185 m	Manchester
10Base-T	2 UTP	100 m	Manchester
10Base-F	2 Fiber	2000 m	Manchester

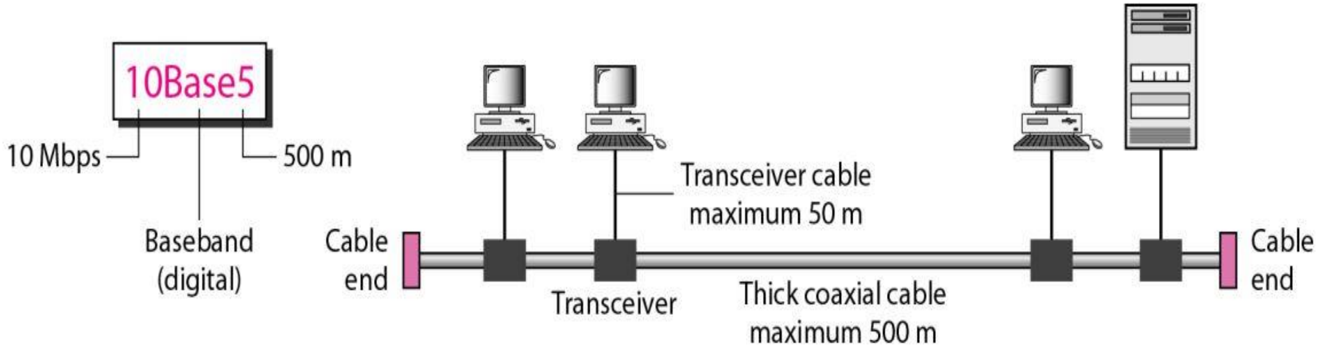
Q10. Standard Ethernet defines several Physical layer implementations. Discuss the most common implementation categories?

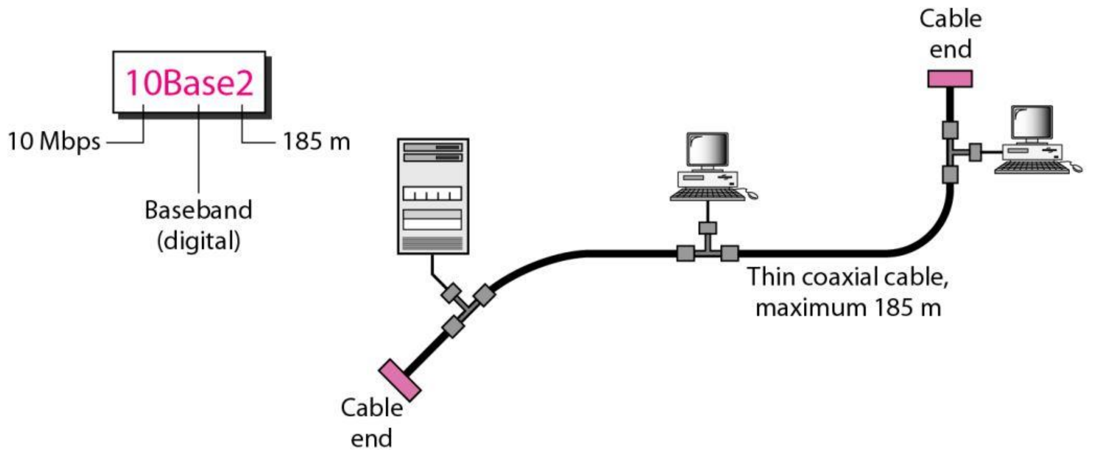
10Base5 (Thick Ethernet)

- 10Base5 is implemented in bus topology with an external transceiver connected to coaxial cable.
- The transceiver deals with transmitting, receiving and detecting collisions in the network.
- The 10Base5 Ethernet is also referred to by other names including thick **Ethernet** or **Thicknet**.
- The maximum length of the cable should not be more than 500 m.

10Base2 (Thin Ethernet)

- 10Base2 is also implemented in the bus topology but with a thinner and flexible coaxial cable.
- The cable can be bent to pass very close to the stations.
- The transceiver is normally part of the NIC card, which is installed inside the station.
- The 10Base2 Ethernet is also referred to as **Thin Ethernet** or **Cheapernet**.
- The maximum length of the cable should not be more than 185 m





THE UNIVERSITY OF SYDNEY

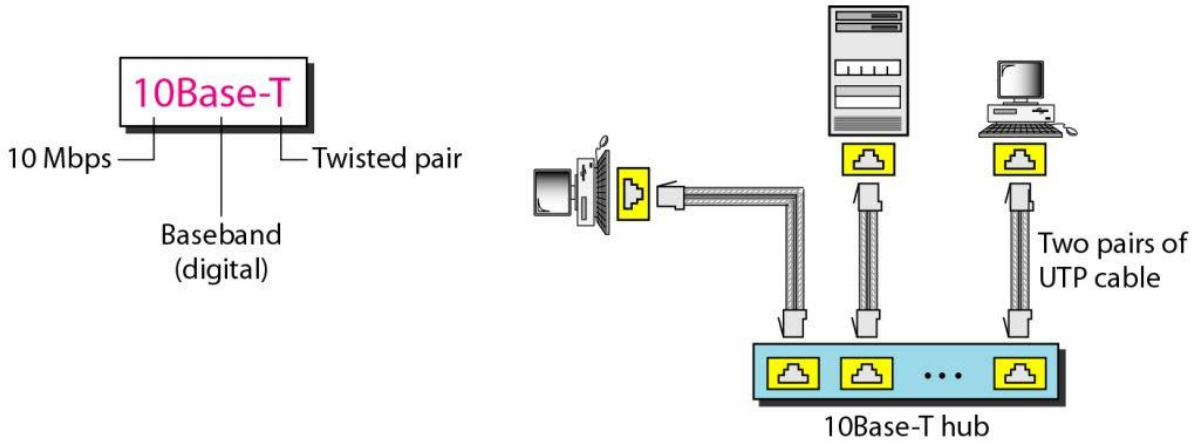
Q10. Standard Ethernet defines several Physical layer implementations. Discuss the most common implementation categories?

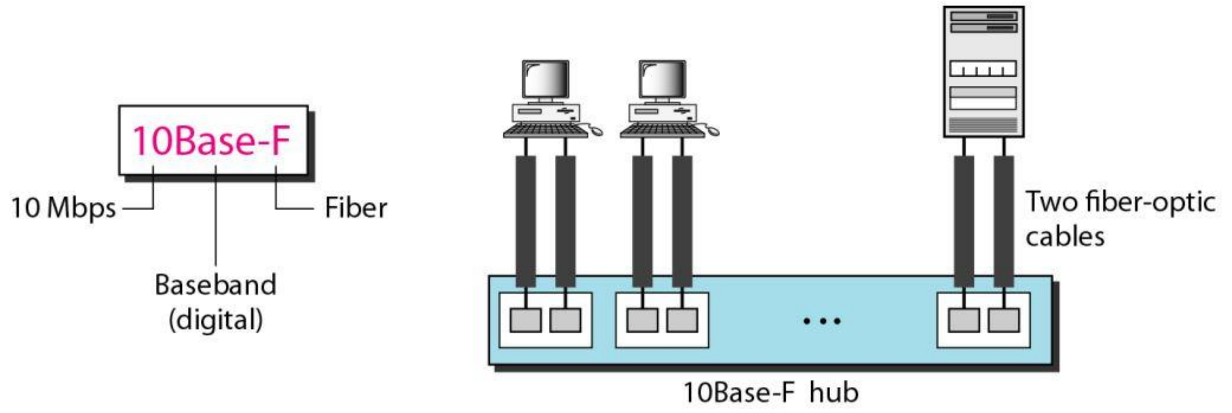
10Base-T (Twisted-Pair Ethernet)

- The third implementation is called l0Base-T or twisted-pair Ethernet.
- 10Base-T uses two pairs of twisted cable and is implemented in star topology.
- All nodes are connected to the hub via two pairs of cable and thus, creating a separate path for sending and receiving the data.
- The maximum length of the cable should not be more than 100 m.

10Base-F (Fiber Ethernet)

- It is the most common 10-Mbps Ethernet that is implemented in star topology.
- It uses a pair of fiber optic cables to connect the nodes to the central hub.
- The transceiver is normally part of the NIC card, which is installed inside the station.
- The 10Base-F Ethernet is also referred to as **Fiber Ethernet**.
- The maximum length of the cable should not be more than 2000 m

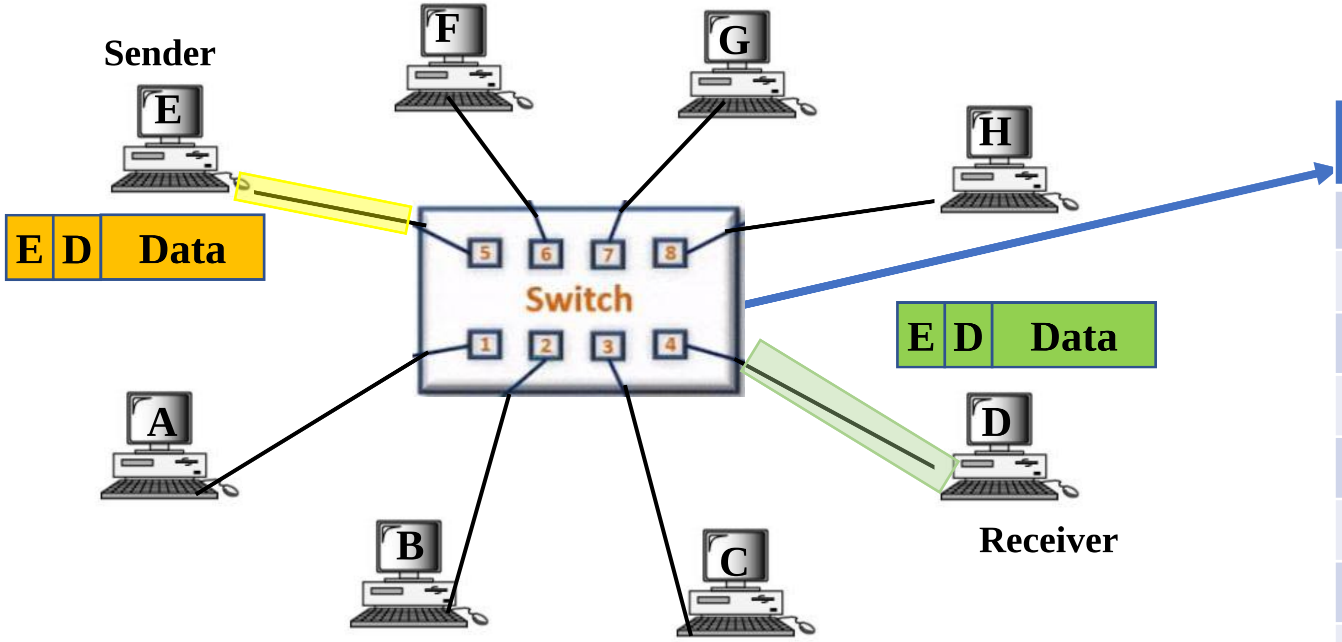




Q11. What is switched Ethernet?

- **Switch Ethernet** : It connects all the devices on same network, so that they can communicate with one another.

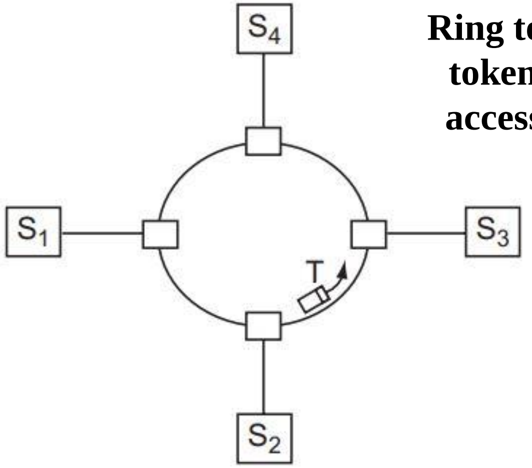
- When a port of the switch receives a frame, it checks the destination address in the frame and then sends the frame to the corresponding port for outgoing data.
- In switch Ethernet, MAC address Table (Forwarding Table) are used to forward the data.
- Bandwidth is shared only between the station and the switch.



MAC Address	Port
A	1
B	2
C	3
D	4
E	5
F	6
G	7
H	8

Q12. What are the advantages of token passing?

- **Token Passing**: A token is regularly passed from one node to another. And if a node has some information to pass on the network, the node releases the information.
- If the node does not have any data to release on the network, then it transfers the token to the next node.



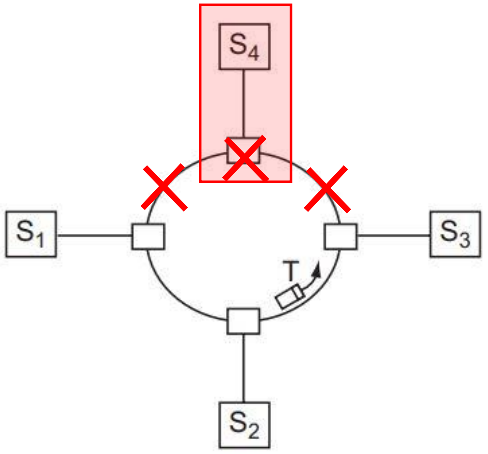
Ring topology in token-passing access method

Advantages of Token Passing

- Reduced chances of data collision as each node release a data packet after receiving the token.
- Token passing makes ring topology perform better than bus topology under heavy traffic.
- No need of server to control connectivity among the nodes.
- The channel bandwidth can be fully utilized when demand is heavy

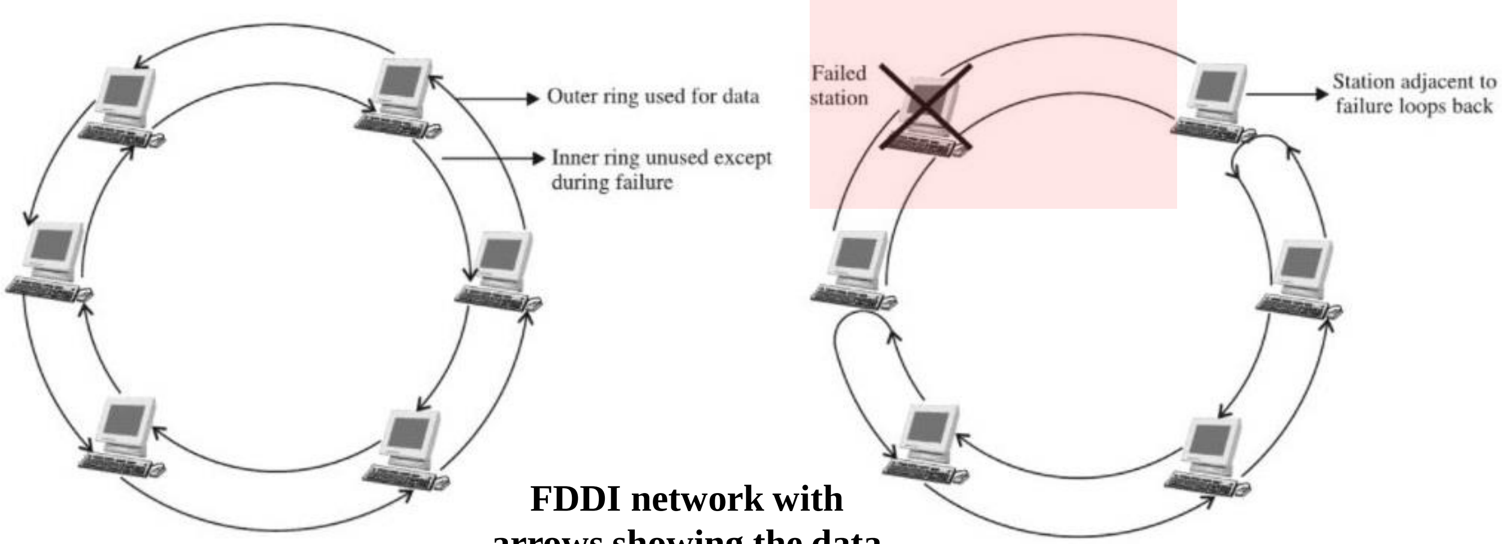
Q13. In the event of failure, how does the FDDI network automatically reconfigure?

- ❑ The problem with the **Token Ring** topology is that if one of the links-the medium between two adjacent stations fails, the whole system fails.
- ❑ To solve this problem, dual ring topology is used.



- ❑ **One of the dual ring token topology is Fiber Distributed Data Interface (FDDI).**
- ❑ **FDDI networks called counter rotating as direction of data flows between two rings are opposite.**

- ❑ The primary ring carries data, while the secondary ring is usually reserved as a backup in case a fault occurs on the primary ring.
- ❑ In the event of a failure on the primary ring, FDDI automatically reconfigures itself to use the secondary ring.
- ❑ This process of reconfiguring is called self-healing and FDDI is known as a self-healing network.



FDDI network with arrows showing the data flowing directions

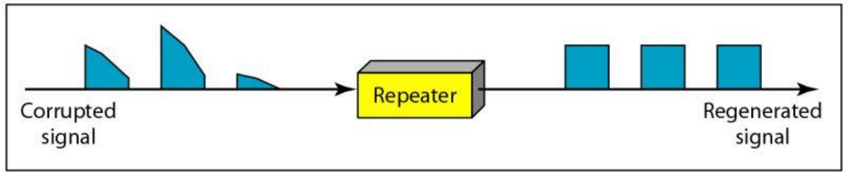
Q14. Compare and contrast between a hub (repeater) and a bridge.

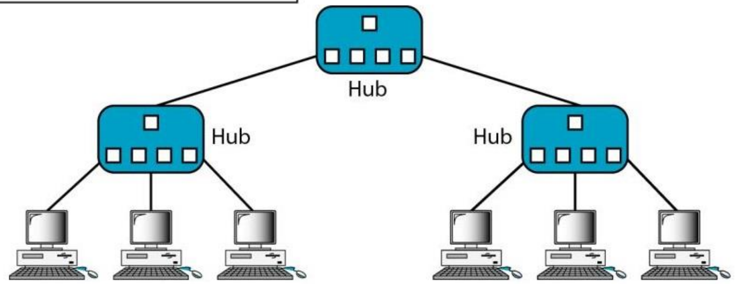
Repeater

- Hub or Repeater operates at the physical layer of OSI model.
- Receives a signal and before it becomes too weak or corrupted, regenerates the original bit pattern.
- It is used to extend the physical length of a network.
- Repeater do not understand complete frame.
- Repeater cannot perform packet filtering.

Hub

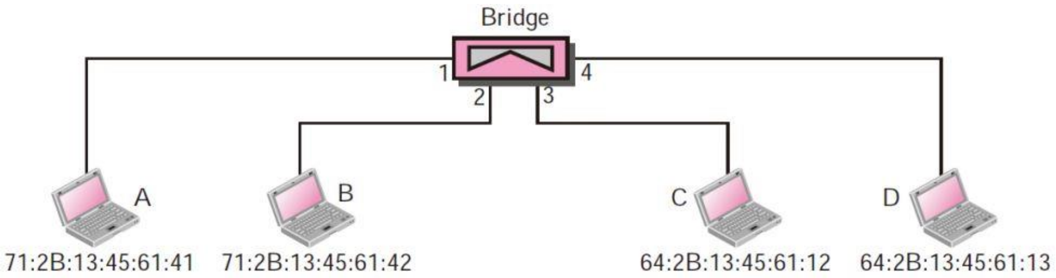
- A Hub is actually a multiport repeater.
- Broadcasts the message sent by one station to all other stations.
- It is most commonly used to connect multiple machines to the same LAN.





Bridge

- Bridge operates at the data link layer of OSI model.
- It can check the destination address of a frame and decide if the frame should be forwarded or discarded.
- It is mostly used in LANs.
- The complete frames is understood by bridge.
- Filtering of the packets in network is achieved by the bridge.

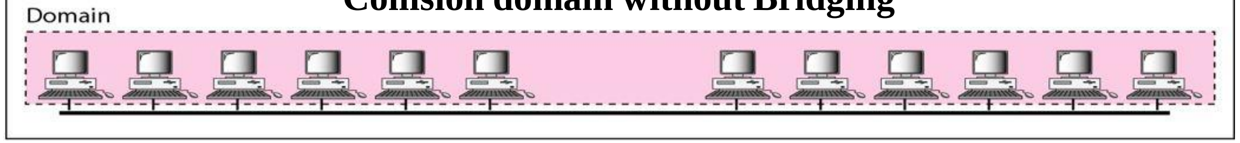


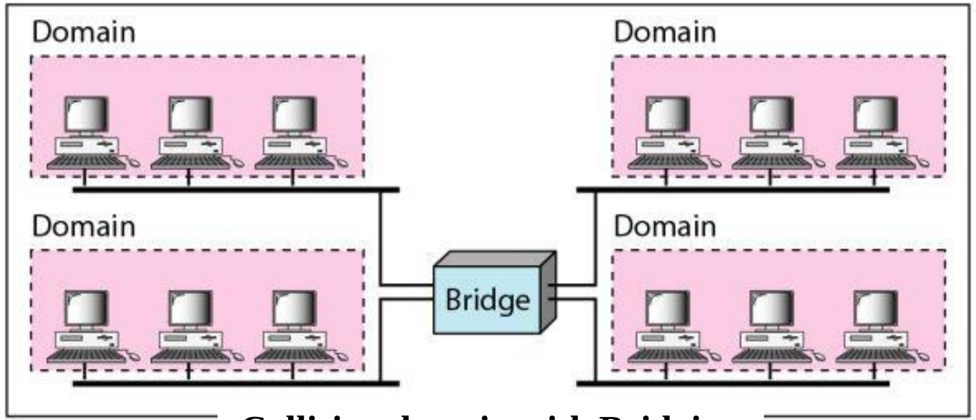
Q15. Compare and contrast between a bridge and a switch (Layer 2).

Bridge

- ❑ Bridge operated in the same LAN and performs relatively slow.
- ❑ Bridge has limited number of ports.
- ❑ Method of switching of a Bridge is store and forward.
- ❑ The collision domain becomes smaller

Collision domain without Bridging



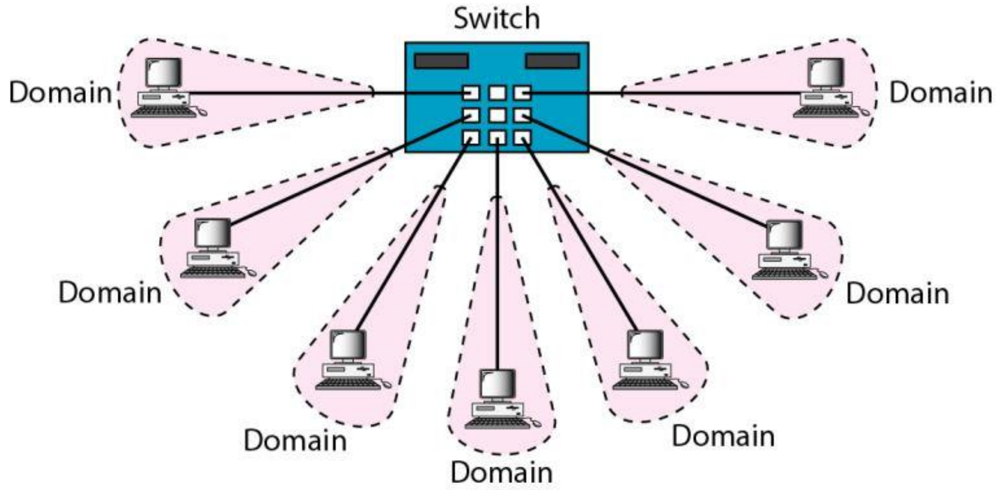


Collision domain with Bridging

Switch (Layer 2)

- ❑ A layer 2 switch is an N-port bridge with additional sophistication that allows faster handling of the packets.
- ❑ Switch can have many ports.
- ❑ Method of switching of a Switch can be store and forward, cut-through, or fragment-free.
- ❑ The probability of collision is reduced tremendously

Collision domain with Switch



Q15. Compare and contrast between a bridge and a switch (Layer 2).

Bridge & Switch (Layer 2)

- ❑ In general, a switch is a multi-port bridge.
- ❑ Both operate in physical and data link layers .
- ❑ Both make filtering decisions based on the physical address of the frame they receive.
- ❑ Both Bridge and Switch have forwarding table of MAC address and port number.